



**UNIVERSIDAD POLITÉCNICA SALESIANA**

**SEDE GUAYAQUIL**

**CARRERA: INGENIERÍA DE SISTEMAS**

**Tesis previa a la obtención del título de:  
INGENIERO DE SISTEMA**

**TEMA:**

**INFORME DE EVALUACIÓN DE SEGURIDAD EN LA INFORMACIÓN  
BASADA EN LA NORMA ISO 27001 EN EL DEPARTAMENTO DE TI DE UNA  
EMPRESA DE LÁCTEOS**

**AUTORES:**

**JORGE LUIS VALDIVIEZO TROYA  
ROBERTO JOSUE RODRÍGUEZ POVEDA**

**DIRECTOR:**

**MSIG. NELSON MORA**

**Guayaquil, marzo 2015**

## **DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO**

Nosotros, Jorge Valdiviezo Troya y Roberto Rodríguez Poveda autorizamos a la Universidad Politécnica Salesiana la publicación total o parcial de este trabajo de grado y su reproducción sin fines de lucro.

Además declaramos que los conceptos y análisis desarrollados y las conclusiones del presente trabajo son de exclusiva responsabilidad de los autores.

Guayaquil, Marzo del 2015

---

**Jorge Valdiviezo Troya**

C.I 0930823448

---

**Roberto Rodríguez Poveda**

C.I 0925438541

## **DEDICATORIA**

A mi familia, por brindarme su apoyo incondicional en todas las decisiones que he tomado y por inculcarme valores que me han ayudado a ser una persona de bien.

Por enseñarme a luchar día a día por mis objetivos, superando cada obstáculo que se presenta.

**Jorge Valdiviezo Troya**

El presente proyecto de tesis va dedicado a la memoria de mi Abuelo Eduardo Poveda González, que yo sé que desde el cielo estará feliz de que su nieto alcance uno de sus sueños.

El mismo también va dedicado a mi madre Teresa Poveda Terranova y a mi padre Xavier Bustamante Torres, los cuales fueron forjadores de mi dedicación, coraje y esfuerzo en cada uno de mis años de estudio.

**Roberto Rodríguez Poveda**

## **AGRADECIMIENTO**

Agradezco a Dios por permitirme estar con vida y darme las fuerzas necesarias para poder cumplir con esta meta importante para mí.

A mis padres Galo Valdiviezo y Elba Troya, quienes me han brindado su apoyo constante e incondicional a lo largo de esta carrera y por enseñarme a ser una persona de bien en la vida.

A mi novia Angely por brindarme las palabras de ánimo necesarias para poder salir adelante y no darme por vencido en el camino al cumplimiento de esta meta.

A todos los docentes que fueron parte fundamental para poder alcanzar este objetivo, ya que con sus enseñanzas me permitieron crecer en mi vida profesional.

A mi docente tutor Nelson Mora por ser la guía a lo largo de este proceso y darnos las recomendaciones necesarias para el correcto desarrollo de este trabajo

**Jorge Valdiviezo Troya**

## **AGRADECIMIENTO**

Primero agradecer a Dios por darme salud, vida y sabiduría en todos estos años de mi etapa universitaria.

Agradecer infinitamente a toda mi familia ya que es un pilar fundamental en mi vida, a mis padres, hermanos, tíos, abuelos, primos decirles gracias ya que con su ayuda, buenos ánimos, aliento constante este sueño de ser ingeniero se cumplirá.

No olvidarme de todos mis amigos de colegio, universidad o trabajo y agradecerle a mi compañera fiel Gabriela Alvear Richards por siempre estar en los buenos y malos momentos.

Agradecer a mis profesores, ya que con sus enseñanzas he logrado salir adelante en el campo laboral y desenvolverme en este trabajo de tesis, y un agradecimiento especial a nuestro tutor Msig. Nelson Mora.

**Roberto Rodríguez Poveda**

## RESUMEN

Este trabajo está basado en la elaboración de un informe de evaluación que permite detectar los errores o falencias que existen en la empresa con respecto a la seguridad de la información. Este informe fue basado en un análisis de riesgo que permite detectar las amenazas y vulnerabilidades de los activos más críticos del departamento de TI. En el mismo se proponen controles adecuados tomando como referencia la norma ISO 27001, para que la empresa pueda minimizar dichos riesgos. Además se facilita una serie de recomendaciones para poder implementar los controles propuestos y con esto disminuir dichas falencias a las que se encuentra expuesto el centro de cómputo y los servicios informáticos de la organización.

Para el caso de estudio propuesto, se usó la metodología de investigación de riesgos “MAGERIT”, la cual brinda las herramientas necesarias para poder realizar una matriz de evaluación en la cual se identificaron los activos, amenazas, vulnerabilidades, y a través de niveles de valoración para cada elemento, permitió hallar el riesgo de cada activo del departamento.

Para realizar un análisis de tráfico en la red, se utilizó la aplicación llamada Wireshark. Este es un programa que permite analizar los protocolos de red, a través de una interfaz gráfica, permitiendo detectar los paquetes no autorizados que transitan por la red de la organización.

La norma ISO 27001 también propone un Sistema de Gestión de Seguridad de la Información (SGSI), la cual sirve para definir políticas que regularizan la seguridad de la información dentro de la organización.

Este sistema será analizado y posteriormente implementado (quedando a decisión de la gerencia) luego de establecer los controles que permitan minimizar los riesgos detectados que afectan a los activos que manejan información de la organización.

## **ABSTRACT**

This work is based in the realization of an assessment report that allows us identify the mistakes and shortcomings that exist in the company. This report was based on a risk assessment that allows us to identify threats and vulnerabilities of the most critical assets in the IT department. In the same report are proposed appropriate controls according to the standard ISO 27001, in order that the company can minimize these risks. In addition it is provided a series of recommendations to implement the proposed controls to reduce the threats and vulnerabilities that are exposed the data center and computer services of the TI department on the organization.

For the proposed study case, research methodology risk "MAGERIT" was used, which gave us the necessary tools to perform an evaluation matrix in which the assets, threats, vulnerabilities were identified, and across levels valuation level for each element, allowed us to find the risk of each asset of the department.

To perform a network traffic analysis, the application called Wireshark was used. This is a program for analyzing network protocols, through a graphical interface, allowing detecting unauthorized packets transiting the network of the organization.

The ISO 27001 standard also proposes a Safety Management System (SMS), which is used to define policies that regularize information security within the organization. This system will be analyzed and subsequently implemented (being a management decision) after establishing controls that minimize identified risks that are affecting the assets that manage organizational information.

## ÍNDICE INICIAL

DECLARATORIA DE RESPONSABILIDAD Y AUTORIZACIÓN DE USO DEL TRABAJO DE GRADO .....	II
DEDICATORIA .....	III
AGRADECIMIENTO .....	IV
RESUMEN.....	VI
ABSTRACT .....	VII

## ÍNDICE DE CONTENIDO

CAPÍTULO 1 .....	1
PLANTEAMIENTO DEL PROBLEMA.....	1
1.1 Formulación del problema .....	1
1.2 Objetivos.....	2
1.3 Justificación .....	3
CAPÍTULO 2 .....	4
MARCO TEÓRICO.....	4
2.1 Antecedentes investigativos.....	4
2.2 Marco conceptual .....	12
2.3 Formulación de la hipótesis y variables .....	15
2.4 Señalamiento de variables e indicadores .....	16
2.5 Matriz causa y efecto.....	17
CAPÍTULO 3 .....	19
MARCO METODOLÓGICO .....	19



3.1 Métodos de investigación .....	19
3.2 Tipos de investigación.....	19
3.3 Población y muestra .....	20
3.4 Recolección de información .....	21
3.5 Procesamiento de información.....	22
CAPÍTULO 4 .....	23
ANÁLISIS DEL PROYECTO .....	23
4.1 Situación actual de la empresa .....	23
4.2 Metodología de evaluación de riesgos.....	37
4.3 Identificación de los activos.....	39
4.4 Dimensiones de valoración de seguridad .....	51
4.5 Criterios de valoración.....	51
4.6 Identificación de amenazas y vulnerabilidades.....	55
4.7 Exposición del riesgo .....	63
4.8 Selección de opciones para el tratamiento del riesgo.....	63
4.9 Selección de controles para reducir los riesgos a un nivel aceptable.....	65
4.10 Valoración de riesgos .....	65
4.11 Software empleado en identificación de amenaza .....	69
4.12 Análisis de los resultados e interpretación de datos.....	73
4.13 Verificación de la hipótesis.....	79
4.14 Resumen de riesgos detectados en la empresa y sus controles seleccionados.....	79
CAPÍTULO 5 .....	96
CONCLUSIONES Y RECOMENDACIONES .....	96
5.1 Conclusiones .....	96
5.2 Recomendaciones.....	96

CAPÍTULO 6 .....	97
PROPUESTA .....	97
6.1 Datos informativos .....	97
6.2 Antecedentes de la propuesta.....	97
6.3 Justificación .....	98
6.4 Objetivos.....	99
6.5 Análisis de factibilidad .....	100
6.6 Fundamentación .....	100
6.7 Metodología, modelo operativo .....	101
6.8 Administración.....	145
BIBLIOGRAFÍA .....	146
ANEXOS.....	148
A.1 Imágenes de plantillas, encuestas y checklist realizadas.....	148
A.1.1 Plantilla de Levantamiento de Activos - APLICACIONES - SOFTWARE ACTUALIZACIONES SISTEMA OPERATIVO .....	148
A.1.2 Plantilla de Levantamiento de Activos - SERVICIOS - TRANSACCIÓN DE PAGO A PROVEEDORES.....	149
A.1.3 Plantilla de Levantamiento de Activos - EQUIPOS INFORMÁTICOS - ESTACIONES DE TRABAJO – COMPUTADORA .....	150
A.1.4 Plantilla de Levantamiento de Activos – REDES DE COMUNICACIÓN - CABLEADO ESTRUCTURADO.....	151
A.1.5 Plantilla de Levantamiento de Activos - INSTALACIONES - DATA CENTER PLANTA .....	152
A.1.6 Plantilla de Levantamiento de Activos - PERSONAS - USUARIOS DE LA ORGANIZACIÓN .....	153
A.1.7 CheckList – Routers .....	154

A.1.8 CheckList – Switchs .....	155
A.1.9 CheckList – PC.....	156
A.1.10 CheckList – Servidores .....	157
A.1.11 CheckList – Cableado y Redes.....	158
A.2 Imágenes data center .....	159
A.2.1 Servidor en rack de comunicaciones .....	159
A.3 Imágenes de servidores (software).....	161
A.3.1 Servidor de Carpetas Compartidas – Folder Redirection .....	161
A.3.2 Servidor de Directorio Activo .....	161
A.3.3 Servidor de Exchange Server .....	162
A.3.4 Servidor de Forefront (Firewall-proxy) .....	163
A.3.5 Servidor de ORACLE.....	163
A.3.6 Servidor de Actualizaciones.....	164
A.4 Imágenes de las instalaciones .....	165
A.4.1 Imágenes de las instalaciones – Amenaza Daño por Agua.....	165
A.4.2 Imágenes de las instalaciones – Amenaza Condiciones inadecuadas de temperatura y humedad .....	165
A.4.3 Imágenes de las instalaciones – Amenaza Robo .....	168
A.4.4 Imágenes de las instalaciones – Defecto de infraestructura.....	169
A.5 Identificación de activos.....	170
A.6 Identificación de amenazas .....	180
A.7 Criterios de valoración .....	181
A.7.1 Criterios de valoración de activos .....	181
A.7.2 Criterios de valoración de amenazas .....	182

A.7.3 Criterios de valoración de vulnerabilidades .....	182
A.8 Valoración de activos .....	182
A.9 Valoración de amenazas .....	185
A.10 Riesgos vs activos afectados.....	201
A.11 Análisis de riesgo .....	204
A.12 Dominios, objetivos de control y controles de la ISO/IEC 27001:2005.....	230

## ÍNDICE DE TABLAS

Tabla 1 - tabla planear-hacer-chequear-actuar .....	7
Tabla 2 - matriz causa efecto.....	17
Tabla 3 - plantilla de identificación de activos.....	39
Tabla 4 - tabla de valoración de disponibilidad.....	52
Tabla 5 - tabla de valoración de integridad .....	52
Tabla 6 - tabla de valoración de confidencialidad .....	53
Tabla 7 - tabla de valoración de amenaza .....	54
Tabla 8 - tabla de valoración de probabilidad de ocurrencia .....	54
Tabla 9 - tabla de valoración de vulnerabilidad .....	55
Tabla 10 - tabla de amenazas de origen natural .....	55
Tabla 11 - tabla de amenazas de origen industrial.....	56
Tabla 12 - tabla de amenazas de origen no intencional .....	56
Tabla 13 - tabla de amenazas de origen intencional .....	57
Tabla 14 - tabla de amenazas y vulnerabilidad - equipos .....	58

Tabla 15 - tabla de amenazas y vulnerabilidad – aplicaciones.....	59
Tabla 16 - tabla de amenazas y vulnerabilidad – activo servicios.....	60
Tabla 17 - tabla de amenazas y vulnerabilidad - redes .....	61
Tabla 18 - tabla de amenazas y vulnerabilidad - instalaciones .....	62
Tabla 19 - tabla de amenazas y vulnerabilidad - personas.....	62
Tabla 20 - tabla ejemplo de valoración de activos .....	66
Tabla 21 - tabla ejemplo de valoración de amenazas .....	66
Tabla 22 - tabla ejemplo de valoración de vulnerabilidad .....	66
Tabla 23 - tabla ejemplo de valoración del riesgo.....	68
Tabla 24 - tabla total de activos afectados .....	73
Tabla 25 - tabla de activos afectados y no afectados.....	73
Tabla 26 - tabla porcentaje de afectación de activos .....	74
Tabla 27 - detalle de activos afectados .....	76
Tabla 28 - acciones y controles – riesgo: condiciones inadecuadas de temperatura.....	80
Tabla 29 - acciones y controles – riesgo: daños por agua.....	81
Tabla 30 - acciones y controles – riesgo: fuego .....	82
Tabla 31 - acciones y controles – riesgo. Corte de suministro eléctrico.....	83
Tabla 32 - acciones y controles – riesgo: caída del sistema por agotamiento de recursos ..	84
Tabla 33 - acciones y controles – riesgo: errores de usuario .....	85
Tabla 34 - acciones y controles – riesgo: errores de mantenimiento y actualización de programas .....	86
Tabla 35 - acciones y controles – riesgo: suplantación de identidad.....	88
Tabla 36 - acciones y controles – riesgo: uso no previsto de recursos .....	90
Tabla 37 - acciones y controles – riesgo: difusión de software dañino .....	90

Tabla 38 - acciones y controles – riesgo: vulnerabilidad de los programas.....	91
Tabla 39 - acciones y controles – riesgo: desastres industriales (fugas de amoniaco) .....	92
Tabla 40 - acciones y controles – riesgo: indisponibilidad del personal .....	93
Tabla 41 - acciones y controles – riesgo: manipulación de equipos.....	93
Tabla 42 - acciones y controles – riesgo: manipulación de programas .....	94
Tabla 43 - acciones y controles – riesgo: restauración fallida de los respaldos.....	95

### **ÍNDICE DE ILUSTRACIONES**

Ilustración 1 - tabla planear-hacer-chequear-actuar.....	6
Ilustración 2 - salvapantalla de programa belarc advisor 1.....	47
Ilustración 3 - salvapantalla de programa belarc advisor 2.....	48
Ilustración 4 - salvapantalla de programa belarc advisor 3.....	49
Ilustración 5 - salvapantalla de programa belarc advisor 4.....	50
Ilustración 6 - salvapantalla de programa wireshark 1 .....	71
Ilustración 7 - salvapantalla de programa wireshark 2 .....	72
Ilustración 8 - numero de activos afectados por amenazas .....	75

# CAPÍTULO 1

## PLANTEAMIENTO DEL PROBLEMA

Luego de realizar un análisis en el departamento de TI de la empresa de Lácteos a la cual llamaremos “LacteoSA”, se pudo determinar que la organización cuenta, de manera formal, solo con políticas pero no con procedimientos, esto hace que no se garantice la disponibilidad, integridad y confidencialidad de la información, ya que no están establecidas bajo un estándar definido y en consecuencia no existe una identificación clara de los riesgos existentes.

Se considera necesario que se desarrollen políticas y procedimientos basados en la norma ISO 27001, ya que esta permite regular, gestionar y mitigar los riesgos a los que está expuesta la organización. De esta forma se pretende evitar incidentes que causen pérdida de información, indisponibilidad de servicios, violación de seguridades entre otros.

### 1.1 Formulación del problema

#### 1.1.1 Pregunta General:

¿Cómo puede contar la organización con políticas y procedimientos basada en una metodología que asegure un correcto análisis de los riesgos y prevención de los mismos para mantener segura la información?

#### 1.1.2 Preguntas Específicas:

¿Cómo mejorar la seguridad de la información en la empresa?

¿Cómo evitar la pérdida de información en la organización?

¿Cómo conocer los procesos que necesitan mayor prioridad dentro de la organización?

¿Cómo evitar que usuarios no autorizados accedan a la información que es confidencial?

¿Cómo actuar si un fallo eléctrico produce la quema de uno de los servidores que contiene información crítica para la empresa?

## **1.2 Objetivos**

### **1.2.1 Objetivos generales**

Evaluar mediante análisis y dar recomendaciones a la empresa para definir políticas y procedimientos basados en metodologías apegadas a la norma ISO 27001, para salvaguardar la información y permitir alcanzar un nivel de madurez óptimo para la organización.

### **1.2.2 Objetivos específicos**

- Analizar políticas de seguridad actuales en la empresa para verificar su efectividad.
- Proponer controles adecuados para prevenir riesgos detectados.
- Identificar los activos que manejan información crítica de la empresa.
- Brindar recomendaciones para controlar la información que es manejada por el recurso humano de la organización.
- Definir potenciales amenazas que puedan causar pérdida de la información en la empresa.



### **1.3 Justificación**

En Ecuador, pocas empresas se encuentran certificadas en la Norma ISO 27001, esto hace notar la poca concienciación que existe sobre los riesgos que pueden presentarse. Actualmente los procesos de las organizaciones dependen mucho de los sistemas de información y estos están expuestos a diferentes tipos de amenazas que podrían detectar cualquier vulnerabilidad presente y poner en riesgo los activos críticos que poseen información.

Al momento de asegurar la información de la empresa, se deben considerar todos los posibles riesgos que puedan afectar la misma. El hacking y los virus informáticos suelen ser las amenazas más conocidas, pero también pueden ocurrir incidentes causados voluntaria o involuntariamente por el personal de la organización o desastres naturales que ponen en riesgo la seguridad de la información.

En las empresas, la información es considerada un activo muy importante, por esta razón, es necesario asegurar la confidencialidad, integridad y disponibilidad de la misma. Estas características pueden ser factores esenciales para mantener los niveles de competencia y lograr los objetivos propuestos por la organización.

Con políticas basadas en el estándar de la norma ISO 27001, la organización podría determinar los posibles riesgos a la que está expuesta y elaborar procedimientos a seguir en el caso de que se presente un siniestro natural o provocado, robo o pérdida de información, etc.

Por las razones antes mencionadas, este trabajo ayudará a mejorar las políticas existentes y definir procedimientos alineados a una metodología establecida por el estándar ISO 27001.

## **CAPÍTULO 2**

### **MARCO TEÓRICO**

#### **2.1 Antecedentes investigativos**

##### **2.1.1 ISO/IEC 27001.**

El estándar para la seguridad de la información ISO/IEC 27001, fue probado y publicado como estándar internacional en octubre del 2005 por la International Organization for Standardization (ISO) y por la comisión International Electrotechnical Commission (IEC).

La ISO 27001 es un estándar internacional el cual se ha preparado para brindar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI).

El manejo de un SGSI en una empresa da como resultado orden y control aparte de una decisión estratégica por parte de la organización.

La implementación de un SGSI en la organización está estrechamente relacionada por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización.

##### **2.1.1.1 Antecedentes del estándar ISO/IEC 27001**

Hace varios años no existía una certificación o proceso en el cual se permitiera certificar las buenas prácticas de seguridad informática y las diferentes alternativas, en esos momentos se certificaba en normas inglesas (BS) o españolas (UNE).

Hasta el año 2005 el estándar más conocido en este entorno de seguridad era el ISO 17799, pero al ser un código de prácticas limitaba bastante, en el momento que se publica su última revisión, se anunció el desarrollo de una serie de estándares ISO 27000, dedicada a la exclusividad de la seguridad informática.

Con esta serie de estándares se le daría un nuevo alcance a la seguridad, porque no sólo es llevar un código de mejores prácticas sino establecer un estándar certificable de forma similar al ISO 9000 (el primero de esa serie en publicarse fue el ISO 27001). (Logisman, 2011).

#### **2.1.1.2 Funcionamiento ISO 27001**

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan.

Las medidas de seguridad (o controles) que se van a implementar se presentan, por lo general, bajo la forma de políticas, procedimientos e implementación técnica. (Alan Calder, 2012).

#### **2.1.1.3 Enfoque de la ISO 27001**

La ISO 27001 se enfoca en el proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización.

La organización debe identificar y controlar varias actividades para poder llevar de manera efectiva su desarrollo.

Toda actividad que use recursos y tiene algún control para que se dé la transformación de insumos en outputs, se puede considerar un proceso. El output normalmente se convierte en el insumo del proceso siguiente.

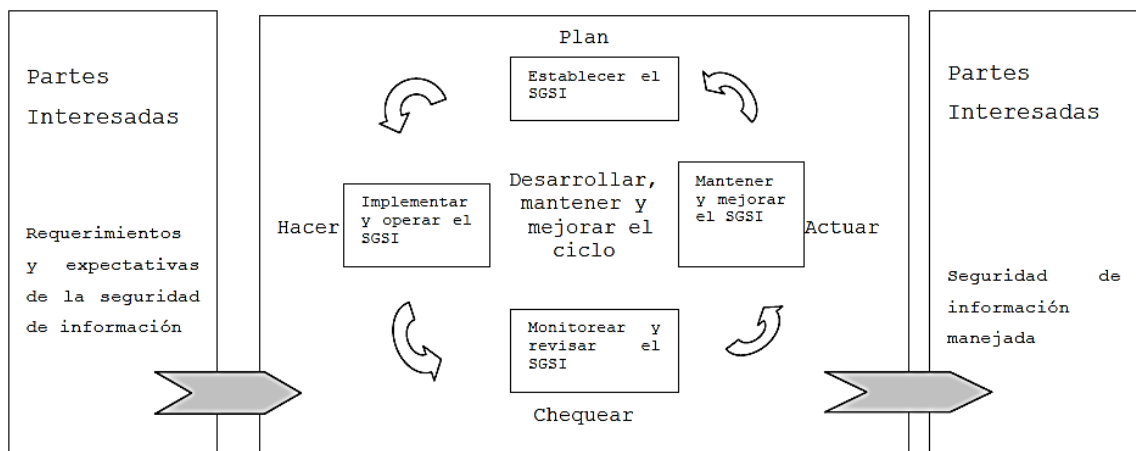
La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos, y su gestión, puede considerarse un ‘enfoque del proceso’.

El enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar fomenta que los usuarios enfatizen gran importancia de:

Conocer requerimientos de seguridad de la información en la organización y la prioridad para establecer políticas y objetivos para la correcta seguridad de la información.

- Implementar y operar controles para manejar los riesgos de la seguridad de la información.
- Controlar y revisar el desempeño y la eficacia del SGSI.
- Mejoramiento continuo en base a la medición del objetivo.

**Ilustración 1 - Tabla Planear-Hacer-Chequear-Actuar**



Fuente: ISO/IEC 27001:2005

**Tabla 1 - Tabla Planear-Hacer-Chequear-Actuar**

<b>PLANEAR</b> <b>(ESTABLECER EL SGSI)</b>	Establecer política, objetivos, procesos y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales de la organización.
<b>HACER</b> <b>(IMPLEMENTAR Y OPERAR EL SGSI)</b>	Implementar y operar la política, controles, procesos y procedimientos SGSI.
<b>CHEQUEAR</b> <b>(MONITOREAR Y REVISAR EL SGSI)</b>	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias prácticas SGSI y reportar los resultados a la gerencia para su revisión.
<b>ACTUAR</b> <b>(MANTENER Y MEJORAR EL SGSI)</b>	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

**Elaborado por:** Los Autores

#### **2.1.1.4 Dominios de la ISO/IEC 27001**

##### **1. Dominio Política de Seguridad**

Su objetivo es garantizar a la organización el soporte y gestión necesarios para la seguridad de la información según los requisitos institucionales y normativos. Además establece la política conforme a los objetivos de las organizaciones manifestando el compromiso con la Seguridad de la Información.

2. **Dominio Organización de la Seguridad de la Información**

Su finalidad es instaurar un marco de referencia para definir el camino para la implementación y control de la seguridad de la información dentro de la organización. La dirección de la organización es la responsable de determinar la política de seguridad, asimismo debe establecer los roles de los comités y nombrar al encargado a través de una resolución. El encargado coordinará y revisará el proceso.

3. **Dominio Gestión de Activos**

Este dominio tiene como objetivo realizar una protección adecuada de los activos de la organización. En todo momento los activos estarán inventariados y estarán controlados por un responsable que también se encargará de manipularlos correctamente.

4. **Dominio Seguridad de los Recursos Humanos**

Su objetivo es fijar las medidas necesarias para controlar la seguridad de la información, que sea manejada por los recursos humanos de la organización.

5. **Dominio: Seguridad física y del ambiente**

Con este dominio se consigue proteger a las instalaciones de la organización y a toda la información que maneja. Para ello entre otros, se establecen barreras de seguridad y controles de acceso.

6. **Dominio: Gestión de las comunicaciones y operaciones**

El objetivo es determinar los procedimientos y responsabilidades de las operaciones que realiza la organización, asegurándose que todos los procesos que estén relacionados con la información se ejecuten adecuadamente.

7. **Dominio Control de Acceso**

Con él se asegura el acceso autorizado a los sistemas de información de la organización. Por ello, es necesario realizar diversas acciones como controles para evitar el acceso de usuarios no autorizados, controles de entrada.

8. **Dominio Adquisición, desarrollo y mantenimiento de los sistemas de información**

Este dominio está dirigido a aquellas organizaciones que desarrollen software internamente o que tengan un contrato con otra organización que sea la encargada de desarrollarlo. Se tiene que establecer los requisitos en la etapa de implementación o desarrollo del software para que sea seguro.

9. **Dominio: Gestión de incidentes en la seguridad de la información**

Con este dominio se aplica un proceso de mejora continua en la gestión de percances de seguridad de la información.

10. **Dominio: Gestión de la Continuidad del Negocio**

El objetivo es asegurar la continuidad operativa de la organización. Se requiere aplicar controles que eviten o reduzcan los incidentes de las actividades desarrolladas por la organización que puedan generar un impacto.

11. **Dominio: Cumplimiento**

Su finalidad es asegurar que los requisitos legales de seguridad referidos al diseño, operación, uso y gestión de los sistemas de información se cumplan.

### **2.1.1.5 ¿Para quién es significativo?**

ISO 27001 es una norma adecuada para cualquier organización, grande o pequeña, de cualquier sector o parte del mundo. La norma es particularmente interesante si la protección de la información es crítica, como en finanzas, sanidad sector público y tecnología de la información (TI). ISO 27001 también es muy eficaz para organizaciones que gestionan la información por encargo de otros, por ejemplo, empresas de subcontratación de TI. Puede utilizarse para garantizar a los clientes que su información está protegida.

(Alan Calder, 2012)

### **2.1.1.6 ¿Qué versión de la ISO 27001 está actualmente vigente en el Ecuador?**

La versión que está actualmente vigente en el Ecuador es la ISO/IEC 27001 versión 2005, ya que la actual versión del 2013 aún no está contemplada por la INEN.

## **2.1.2 Sistema de gestión de seguridad de información**

Un SGSI es el diseño, implantación, mantenimiento de un conjunto de procesos para gestionar eficientemente la accesibilidad de la información, buscando asegurar la confidencialidad, integridad y disponibilidad de los activos de información minimizando a la vez los riesgos de seguridad de la información.

(Carlos, 2008)

### **2.1.2.1 Confidencialidad en un SGSI**

Propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

(AENOR, 2014)



### **2.1.2.2 Integridad en un SGSI**

Propiedad que busca mantener los datos libres de modificaciones no autorizadas. Es decir, la integridad es el mantener con exactitud la información tal cual fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

(AENOR, 2014)

### **2.1.2.3 Disponibilidad en un SGSI**

Es la característica de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. A Groso modo, la disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

(AENOR, 2014)

### **2.1.2.4 Beneficios de un SGSI**

- Cumplir con los requerimientos legales.- Cada vez hay más y más leyes, normativas y requerimientos contractuales relacionados con la seguridad de la información. La buena noticia es que la mayoría de ellos se pueden resolver implementando ISO 27001 ya que esta norma le proporciona una metodología para cumplir con todos ellos.
- Obtener una ventaja comercial.- Si su empresa obtiene la certificación y sus competidores no, es posible que usted obtenga una ventaja sobre ellos ante los ojos de los clientes a los que les interesa mantener en forma segura su información.
- Menores costos.- La filosofía principal de ISO 27001 es evitar que se produzcan incidentes de seguridad, y cada incidente, ya sea grande o pequeño, cuesta dinero; por lo tanto, evitándolos su empresa va a ahorrar mucho dinero. Y lo

mejor de todo es que la inversión en ISO 27001 es mucho menor que el ahorro que obtendrá.

- Una mejor organización – en general, las empresas de rápido crecimiento no tienen tiempo para hacer una pausa y definir sus procesos y procedimientos; como consecuencia, muchas veces los empleados no saben qué hay que hacer, cuándo y quién debe hacerlo.
- La implementación de ISO 27001 ayuda a resolver este tipo de situaciones ya que alienta a las empresas a escribir sus principales procesos (incluso los que no están relacionados con la seguridad), lo que les permite reducir el tiempo perdido de sus empleados. (Carlos, 2008)

## **2.2 Marco conceptual**

**Ordenador.-** Máquina capaz de aceptar unos datos de entrada, efectuar con ellos operaciones lógicas y aritméticas, y proporcionar los datos resultantes a través de un medio de salida; todo ello sin la intervención de un operador humano y bajo el control de un programa de instrucciones previamente almacenado en el ordenador  
(Alberto Prieto, 2002)

**Hardware.-** La máquina en sí; es decir, el conjunto de circuitos electrónicos, cables, dispositivos electromecánicos y otros elementos físicos que forman los ordenadores.  
(Alberto Prieto, 2002)

**Software.-** Conjunto de programas ejecutables por el ordenador  
(Alberto Prieto, 2002)

**Datos.-** Es una información breve y concreta, proporcionada en un formato específico y que puede ser procesada por un ordenador  
(Arribas, 2006)

**Información.-** Es un conjunto de datos interrelacionados y ordenados según una estructura específica, esta información puede almacenarse, procesarse y transmitirse electrónicamente, además de transformar su formato para su introducción y comprensión por un ser humano (mediante un teclado, pantalla, listado de impresora, etc.)

(Arribas, 2006)

**Internet.-** Internet es una gran red internacional de ordenadores. (Es, mejor dicho, una red de redes, como veremos más adelante). Permite, como todas las redes, compartir recursos. Es decir: mediante el ordenador, establecer una comunicación inmediata con cualquier parte del mundo para obtener información sobre un tema, ver los fondos de la Biblioteca del Congreso de los Estados Unidos, o conseguir un programa o un juego determinado para el ordenador. En definitiva: establecer vínculos comunicativos con millones de personas de todo el mundo, bien sea para fines académicos o de investigación, o personales.

(Cuadernos de Documentación Multimedia Vol. 5., 1996)

**DNS.-** Domain Name System. Sistema de Nombres por Dominios. Cada usuario tiene un nombre, una dirección única e irrepetible en la red. Al igual que cada teléfono tiene un número y no hay dos iguales, Internet asigna un nombre a cada ordenador. Este nombre no es aleatorio: corresponde a unas determinadas siglas más o menos relacionadas con la institución o red a la que está conectado.

(Cuadernos de Documentación Multimedia Vol. 5., 1996)

**Red.-** Una red de comunicaciones es un conjunto de medios de transmisión y conmutación para el envío de información entre puntos separados geográficamente. Esta definición resulta extremadamente general y en la actualidad existen un gran número de implementaciones diferentes que responden a necesidades específicas, tales como redes de acceso de datos, troncales, inalámbricas, redes de voz, etc.

(Hesselbach, 2002)

**Red de área local (LAN).**- Recibe este nombre debido a que la zona donde se encuentran todas las maquinas conectadas a la red está claramente definida dentro de una habitación, un edificio e incluso varios edificios dentro de una localidad. Otra característica es que la comunicación entre todos los elementos que la forman (a la red LAN), se puede llevar a cabo por medio de un cableado que transmita las señales de cada computadora a otras.

(Pérez, 2003)

**Topología.**- La topología (de red) es la disposición lógica de los elementos (enlaces, nodos) de una red. Así pueden definirse diversos modelos de topologías básicas:

- MALLA
- ESTRELLA
- ARBOL
- BUS
- ANILLO

(Hesselbach, 2002)

**Proxy.**- Un proxy se utiliza para filtrar las peticiones de páginas provenientes de los usuarios que se encuentran en su red local y con destino web situados en el exterior es decir internet.

(ROYER, 2004)

**Firewall.**- Tiene como misión controlar los datos que entran y salen de la red, existen firewall por software y hardware.

(ROYER, 2004)

**Virus.**- Un virus informático es un programa de computadora que tiene la capacidad de causar daño y su característica más relevante es que puede replicarse a sí mismo y propagarse a otras computadoras. Infecta “entidades ejecutables”: cualquier archivo o sector de las unidades de almacenamiento que contenga códigos de instrucción que el

procesador valla a ejecutar. Se programa en lenguaje ensamblador y por lo tanto, requiere algunos conocimientos del funcionamiento interno de la computadora.

(ANGELICA MOSQUERA QUINTO, 2011)

**Antivirus-**Un antivirus es un programa cuya finalidad es prevenir y evitar la infección de virus, impidiendo también su propagación. Tiene capacidad para detectar y eliminar los virus y restaurar los archivos afectados por su infección (en principio).

(ANGELICA MOSQUERA QUINTO, 2011)

**Hacker.-** Es alguien con profundos conocimientos sobre la tecnología, Esta puede ser la informática, la electrónica o las comunicaciones, El hacker normalmente conoce todos los terrenos en los que reposa la actual tecnología. Así pues, el verdadero hacker es alguien que tiene ansias por saberlo todo, le gusta la investigación y sobre todo lo que resulta más difícil de descifrar.

(Michelena, 2003)

## **2.3 Formulación de la hipótesis y variables**

### **2.3.1 Hipótesis general**

Las políticas definidas actualmente en la organización permiten identificar y prevenir riesgos en la seguridad de la información.

### **2.3.2 Hipótesis específica**

- Disminuir las posibles fugas de información o pérdida de la misma.
- Mitigar los riesgos de perdida de información dentro de la organización.
- Conocer los procesos más críticos o de mayor prioridad dentro de la organización.
- Garantizar el correcto acceso del personal de la organización a la información pertinente.

- Establecer procedimientos de contingencia para cualquier problema, fallo o catástrofe que ocurra.

## **2.4 Señalamiento de variables e indicadores**

### **2.4.1 Variables independientes**

- Horario Laboral del Empleado
- Respaldo de Información

### **2.4.2 Variables dependientes**

- Horario de uso de las PC's de la empresa
- Restauración de información en caso de alguna pérdida
- Personas que tienen accesos para crear reportes

### **2.4.3 Indicadores**

- Horas Laborables por día
- Número de respaldos por mes
- Número de personas dentro de la LAN
- Número de Personas dentro del sistema
- Número de personas con acceso a recursos informáticos

## 2.5 Matriz causa y efecto

**Tabla 2 - Matriz Causa Efecto**

<b>Problema General</b>	<b>Objetivo General</b>	<b>Hipótesis General</b>
¿Cómo puede contar la organización con políticas y procedimientos basada en una metodología que asegure un correcto análisis de los riesgos y prevención de los mismos para mantener segura la información?	Evaluar mediante análisis y dar recomendaciones a la empresa para definir políticas y procedimientos basados en metodologías apegadas a la norma ISO 27001, para salvaguardar la información y permitir alcanzar un nivel de madurez óptimo para la organización.	Las políticas definidas actualmente en la organización permiten identificar y prevenir riesgos en la seguridad de la información.
<b>Problemas Específicos</b>	<b>Objetivos Específicos</b>	<b>Hipótesis Específicas</b>
¿Cómo mejorar la seguridad de la información en la empresa?	Analizar políticas de seguridad actuales en la empresa para verificar su efectividad.	Disminuir las posibles fugas de información o pérdida de la misma.
¿Cómo evitar la pérdida de información en la organización?	Proponer controles adecuados para prevenir riesgos detectados.	Mitigar los riesgos de pérdida de información dentro de la organización.
¿Cómo conocer los procesos que necesitan mayor prioridad dentro de la organización?	Identificar los activos que manejan información crítica de la empresa.	Conocer los procesos más críticos o de mayor prioridad dentro de la organización.
¿Cómo evitar que	Brindar recomendaciones para	Garantizar el correcto

<p>usuarios no autorizados accedan a la información que es confidencial?</p>	<p>controlar la información que es manejada por el recurso humano de la organización.</p>	<p>acceso del personal de la organización a la información pertinente.</p>
<p>¿Cómo actuar si un fallo eléctrico produce la quema de uno de los servidores que contiene información crítica para la empresa?</p>	<p>Definir potenciales amenazas que puedan causar pérdida de la información en la empresa.</p>	<p>Establecer procedimientos de contingencia para cualquier problema, fallo o catástrofe que ocurra.</p>

**Elaborado por:** Los Autores



## CAPÍTULO 3

### MARCO METODOLÓGICO

#### 3.1 Métodos de investigación

- **El método hipotético**

Para el desarrollo del trabajo se utilizará el método hipotético deductivo, ya que planteamos hipótesis que son sujetas a la verificación a través de la investigación.

- **El método empírico**

También se utilizará el método empírico de observación científica que permitirá extraer información para su posterior análisis.

#### 3.2 Tipos de investigación

- **Investigación descriptiva**

Es descriptiva porque detallamos la actual situación de la empresa en cuanto a la seguridad de la información.

- **Investigación explicativa**

Es explicativa porque por medio de la investigación determinamos los posibles riesgos que pueden ocasionar pérdida de información y se evaluará si los controles que existen son óptimos.

- **Investigación de campo**

Es de campo porque se basa en la observación de la ejecución de las políticas establecidas dentro de la empresa.

### 3.3 Población y muestra

La población del estudio será de 50 personas que se dividen en todos los departamentos de la empresa que tienen acceso a la información que es responsabilidad del departamento de TI. Para calcular la muestra, tomaremos como base la fórmula:

$$n = \frac{N * Z^2 * p * q}{(N-1) * d^2 + Z^2 * p * q}$$

Dónde:

- $n$  = el tamaño de la muestra.
- $N$  = Total de la población.
- $Z$  = Valor obtenido mediante niveles de confianza.
- $p$  = Proporción esperada.
- $q = 1 - p$
- $d$  = Precisión
- Reemplazando valores:
- $N = 50$
- $Z = 1.96$  (si la seguridad es del 95%)
- $p = 5\% = 0.05$
- $q = 0.95$
- $d = 5\% = 0.05$
- $n = 50 * (1.96)^2 * (0.05) * (0.95) / ((50-1) * (0.05)^2 + ((1.96)^2 * 0.05 * 0.95))$

Tenemos como resultado que la muestra será de 30 personas escogidas de forma aleatoria.

### 3.4 Recolección de información

#### 3.4.1 Fuentes

- **Fuentes Primarias.-** Se obtiene información por contacto directo con el sujeto de estudio; por medio de observación, cuestionarios, entrevista, etc. Es aquella que el investigador recoge directamente a través de un contacto inmediato con su objeto de análisis. (Gutierrez Cervantes)
- **Fuentes Secundarios.-** Es aquella que el investigador recoge a partir de investigaciones ya hechas por otros investigadores con propósitos diferentes. La información secundaria existe antes de que el investigador plantee su hipótesis, y por lo general, nunca se entra en contacto directo con el objeto de estudio. Información obtenida desde documentos; libros, expedientes, estadísticas, datos, censo, base de datos. (Gutierrez Cervantes)

#### 3.4.2 Técnicas

- **Listas de chequeos**  
Listas de chequeos realizadas por medio de la observación del cumplimiento de requisitos para una correcta seguridad de la información.
- **Encuestas**  
Encuestas descriptivas realizadas a los empleados que tengan acceso a la información de la empresa. Estas encuestas se realizarán a través de correo electrónico y servirá para conocer la situación actual de la empresa en cuanto a la seguridad de la información.
- **Entrevistas**  
Entrevistas estandarizadas que se realizará a los directores de las diferentes áreas que tengan acceso a la información sensible de la empresa.

### **3.5 Procesamiento de información**

Para el procesamiento de los datos usaremos el aplicativo utilitario Microsoft Excel en el cual elaboraremos una tabla para poder tabular las encuestas y entrevistas realizadas al personal de la organización.

Para el procesamiento de datos de las entrevistas aplicaremos los siguientes pasos:

1. Obtener la Información.
2. Transcribir y ordenar la información para su análisis.
3. Codificar la información mediante la agrupación de categorías de ideas.
4. Integrar la información relacionando las categorías obtenidas en el punto 3.

Para el análisis de los datos se basará en el tipo de hipótesis formulada para el proyecto.

## CAPÍTULO 4

### ANÁLISIS DEL PROYECTO

#### 4.1 Situación actual de la empresa

En primera instancia, se realizó una visita a las instalaciones de la organización, encontrando en ella que el departamento de TI cuenta con infraestructura, servicios, aplicaciones y políticas creadas para el control interno del personal y de los procesos. Cabe mencionar que en la empresa no se encontraron procedimientos definidos de manera formal (documentados).

##### 4.1.1 Infraestructura

La empresa cuenta con infraestructura informática la cual el departamento de TI es el responsable de la misma. A continuación se detalla dicha infraestructura.

##### 4.1.1.1 Data Center

La organización cuenta con un Data Center en el cual se encuentran los servidores de la empresa. Estos equipos se encuentran ordenados en soportes metálicos (RACKS) que ayudan a la protección de los mismos y brindan una mejor organización dentro del área. Este espacio físico dispone de un aire acondicionado automático que mantiene el ambiente a 20 grados centígrados. Esta área está restringida por lo que permanece bajo llave y solo tiene acceso el personal autorizado de TI. (**Ver Anexo A.2**)

##### 4.1.1.2 Servidores

Los servidores son equipos que almacenan información y permiten la ejecución de ciertas aplicaciones fundamentales para el desarrollo de las actividades de la organización.

Entre los servidores que dispone la compañía son:

- **Servidor de carpetas compartidas file users.-** Mantiene los archivos y las carpetas compartidas de los usuarios de la organización. Este servidor también cumple con la función de respaldar los archivos del escritorio y mis documentos mediante una política implementada en el DA; a esta función se le llama Folder Redirection.

(Ver Anexo A.3.1)

- **Servidor de directorio activo.-** Permite crear, administrar y eliminar los usuarios, grupos de usuarios y políticas que se utilizaran en la red dentro de la organización. Estas configuraciones se realizan después de haber definido un dominio y permite administrar el control de inicios de sesión de los usuarios en los equipos conectados a la empresa. (Ver Anexo A.3.2)

- **Servidor de correo electrónico.-** Permite administrar las cuentas de correo de los usuarios que trabajan en la empresa. El protocolo utilizado para el envío de correos es el SMTP, mientras que el protocolo que se utiliza para la recepción de los correos es el POP3 en el caso de las estaciones de trabajo, y el IMAP para el caso de los dispositivos móviles. (Ver Anexo A.3.3)

- **Servidor de internet Proxy – Firewall.-** Permite administrar las reglas de acceso a internet para usuarios, grupos de usuarios o equipos conectados a la red de la empresa. También cumple con la misión de restringir el acceso de usuarios no autorizados que desde la Internet intenten acceder a la red interna de la organización. (Ver Anexo A.3.4)

- **Servidores de aplicación y de Base de Datos.-** La empresa cuenta con 2 servidores de aplicación: uno para la aplicación que maneja la parte administrativa financiera y el otro para la aplicación de Recurso Humanos. Cada servidor cuenta con su base de datos independiente manteniendo así toda la información centralizada en los mismos. (Ver Anexo A.3.5)

- **Servidor de actualizaciones y antivirus.-** Provee a las máquinas conectadas a la organización las actualizaciones necesarias del Sistema Operativo para su correcto funcionamiento. También provee a los equipos antivirus que ayudan con la detección y eliminación de virus que se presenten en los equipos de la empresa. **(Ver Anexo A.3.6)**
- **Servidor de Respaldo.-** Cumple con la función de guardar respaldos diarios de las configuraciones y archivos de los servidores de carpetas compartidas, correos y los de aplicaciones. Estos respaldos se hacen en horarios establecidos todos los días de manera automática.
- **Servidor de cámaras IP.-** Administra las cámaras IP instaladas dentro de la empresa a través de un software. Este servidor también guarda las grabaciones de tipo video realizadas por dichas cámaras.

#### **4.1.1.3 Cableado estructurado**

También conocido como Red interna de la organización. Es la que mantiene interconectados los departamentos de la empresa, esta permite trabajar con aplicaciones que necesitan acceso a Bases de datos, compartir archivos, multimedia, etc.

La red interna está conformada por cable UTP (cable de cobre) Categoría 6A y por enlaces de fibra Óptica que interconectan los diferentes bloques de la planta con el departamento de TI. Todo el cableado de la organización se encuentra recubierto por tubos de acero inoxidable con la finalidad de proteger y prevenir posibles daños.

#### **4.1.1.4 Dispositivos de Respaldo**

La organización cuenta con dispositivos de almacenamiento de información como son Discos Duros externos.

#### **4.1.1.5 Estaciones de trabajo**

Las estaciones de trabajo son equipos informáticos ubicados en los diferentes departamentos de la organización y son usados por los usuarios finales. Estos equipos son entregados a una persona la cual se hace responsable del buen uso y cuidado del mismo. Los departamentos que cuentan con estaciones de trabajo son:

- Contabilidad
- Talento Humano
- Producción
- Sistemas
- Logística
- Ventas y cobranzas
- Compras

#### **4.1.2 Servicios**

A continuación se describen los diferentes servicios usados por los usuarios de la organización. Cabe mencionar que el responsable de los servicios mencionados es el departamento de TI.

##### **4.1.2.1 Internet**

Este servicio es el que permite la navegación de los usuarios a los sitios web autorizados por parte de la organización. Para el control de accesos a los sitios web, utilizan un servicio Proxy -firewall donde se configura para autorizar o denegar accesos a páginas publicadas en internet.

Para gestionar los accesos a los sitios web, cada usuario pertenece a un grupo de usuarios. Estos grupos fueron creados por el departamento de TI el cual es el responsable de autorizar y denegar la navegación de cada grupo. Los grupos de usuarios se detallan a continuación:



- **Navegación Total** (Dirigentes, coordinadores de cada área de la empresa)
- **Navegación Intermedia** (Personal administrativo de la empresa)
- **Navegación Básica** (Todo el personal de la empresa que no se encuentre en los grupos anteriores)

#### **4.1.2.2 Correo Electrónico**

Este servicio permite a los usuarios de la organización tener su propia cuenta de correo electrónico. Con esta cuenta cada usuario puede enviar y recibir mensajes ya sea internos (originados dentro de la empresa) o externos (originados fuera de la empresa).

#### **4.1.2.3 Telefonía Fija**

La organización cuenta con una central telefónica la cual permite la comunicación entre los departamentos (por medio de extensiones telefónicas) y fuera de la empresa.

#### **4.1.2.4 Soporte Técnico**

Este servicio consiste en brindar asistencia al usuario de la organización en el caso de que tenga algún problema con un equipo (hardware) o aplicación (software) que no le permita realizar sus actividades diarias.

#### **4.1.2.5 Base de Datos**

También conocido como servicio de banco de datos. Este servicio es el que permite acceder a un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para usarlos en un futuro. Existen programas denominados sistemas gestores de Bases de datos (DBMS) que permiten acceder a los datos que se encuentran en la Base de datos de manera rápida y estructurada.

#### **4.1.2.6 Direccionamiento de Carpeta**

Este servicio consiste en que los archivos y carpetas de los usuarios sean compartidos y respaldados de manera automática y transparente. Existen políticas que permiten o niegan el acceso de usuarios a estos archivos.

#### **4.1.3 Aplicaciones**

Las aplicaciones son programas informáticos diseñados para realizar uno o varios trabajos específicos. Estas aplicaciones por lo general son usadas por los usuarios finales y el departamento de sistemas es el responsable de dar soporte en el caso de que se necesite.

##### **4.1.3.1 Aplicación Administrativa**

Esta aplicación es usada por los departamentos de Contabilidad, Logística, Producción, compras y ventas. Es la que permite realizar todos los procesos administrativos como por ejemplo: asientos contables, ingreso de artículos a bodega, Cotizaciones e ingreso de facturas de compras, facturas de ventas, pago a proveedores, etc. Para acceder a esta aplicación, cada usuario debe de estar creado en el sistema y tener configurado los roles respectivos; esta configuración la realiza el departamento de TI.

##### **4.1.3.2 Aplicación de Recursos Humanos**

Esta aplicación es usada por el departamento de Talento Humano. Es la que permite llevar un control de todo el personal de la empresa. También esta aplicación es la que permite generar roles, descuentos, horas extras de cada empleado de la organización.

El acceso a esta aplicación lo tiene solo el personal de Talento Humano. Los usuarios deben de estar creados en el sistema para poder trabajar en el mismo. Esta configuración la realiza el departamento de TI.

#### **4.1.3.3 Antivirus**

Esta aplicación es la encargada de brindar protección a las estaciones de trabajo de cada usuario de manera automática. Un antivirus sirve para detectar, advertir y eliminar posibles virus que intenten acceder a los equipos y causar daño en la información que contiene el mismo. El antivirus es actualizado a cada estación de trabajo de manera automática, realiza escaneos del equipo periódicamente y ayuda a la detección y eliminación de archivos maliciosos que puedan poner en riesgo los datos que contiene el equipo.

#### **4.1.3.4 Aplicación de Cámaras IP**

Esta aplicación permite gestionar las grabaciones de las cámaras instaladas dentro de la organización. Esta aplicación es solo utilizada por el coordinador de sistemas y revisada por la gerencia de la empresa.

#### **4.1.4 Políticas**

El departamento de sistemas cuenta con políticas establecidas para el control de los procesos y equipos de los cuales son responsables. A continuación se detallan las políticas con las que cuentan.

##### **4.1.4.1 Política de Instalación y configuración de estaciones de trabajo**

El objetivo de esta política consiste en realizar las instalaciones y configuraciones apropiadas de las estaciones de trabajo al servicio de los usuarios de la organización. Se aplica a los productos de hardware, software y redes que el usuario final utiliza en su jornada laboral. En esta política se detallan los siguientes puntos:

- El equipo puede provenir de una compra (equipo nuevo) o bien de un requerimiento de reinstalación de software (equipos existentes).
- Se debe identificar claramente cuáles son las herramientas de software que determinado usuario necesita tener instalado en su computador. Estos son:

Sistemas operativos, hojas de cálculo, procesador de texto, presentación de diapositivas, software empresarial, compresión de archivos, etc.

- Es imperativo que todo software instalado en la empresa esté alineado a su licencia de uso. Es decir que si se instala un software comercial, se debe primero comprar su licencia y respetar su acuerdo de uso; si se trata de un software libre, se debe de seguir las condiciones de uso descritas en su acuerdo de licencia.
- Luego de la entrega del equipo instalado y configurado correctamente, se debe recibir por parte del usuario un correo electrónico o un documento por escrito que indique la aceptación del producto recibido.
- El personal de sistemas debe de llevar un inventario de los equipos instalados en la empresa.
- El usuario final es quien custodia el producto recibido y se hace responsable de la integridad y buen uso del equipo en cuestión.

#### **4.1.4.2 Política de seguridad física de las estaciones de trabajo**

Esta política establece a través de procedimientos los pasos a seguir para la seguridad física de las estaciones de trabajo. Esta política detalla los siguientes puntos:

- El personal del departamento de sistemas tiene la responsabilidad de ubicar las estaciones de trabajo en un lugar con un punto eléctrico adecuado, con protecciones de voltaje y cortes de luz, y en un ambiente con temperatura y humedad adecuadas.
- El personal de sistemas realiza de forma periódica (cada 3 meses) mantenimiento preventivo a las estaciones de trabajo. Esto se realiza con un proveedor externo.
- Por motivos de seguridad, el departamento de sistemas puede realizar inspecciones en cualquier momento del hardware o software de los equipos de cómputo de la empresa.

- El departamento de sistemas es el responsable de realizar las actualizaciones tanto de los parches como de los antivirus instalados en las estaciones de trabajo.
- El empleado a cargo de una estación de trabajo tiene la responsabilidad de velar por la integridad de la misma; por lo cual se realiza un ACTA DE ENTREGA – RECEPCION de los equipos entregados a su custodia.
- Los usuarios serán responsables de cualquier daño del equipo producido por derrame de líquidos, golpes o cualquier otra causa provocada por el descuido del usuario.
- Los usuarios que tengan equipos móviles tales como computadoras portátiles, no deberán utilizarlo en lugares públicos ni conectarlos a redes ajenas a la organización.

#### **4.1.4.3 Política de uso de las estaciones de trabajo**

Esta política consiste en establecer la metodología para la instalación y configuración de las estaciones de trabajo.

Esta política detalla los siguientes puntos:

Instalación y configuración de software

- Solamente se podrá utilizar software aprobado por el departamento de sistemas y la gerencia.
- El personal de sistemas es el único autorizado para instalar, modificar o eliminar aplicaciones o software en general.

Instalación y configuración del hardware

- Las estaciones de trabajo solamente podrán utilizar hardware aprobado por el departamento de sistemas, según lo amerite el perfil del usuario.

- El personal de sistemas es el único autorizado para instalar, modificar o eliminar componentes de hardware según sea el requerimiento.

En esta política también se determina como uso inaceptable:

- Instalación o distribución de software pirata o que no cuente con su respectiva licencia de uso.
- Uso, instalación de programas maliciosos.
- Revelar contraseñas o compartir el uso de cuentas de usuario.
- Cambiar configuraciones realizadas por la organización, tales como: dirección IP, nombre del equipo, software antivirus, sistema operativo, opciones de navegación de los exploradores de internet, etc.
- Uso del equipo para actividades de uso personal.
- Usar equipos ajenos, esto incluye usar la estación de trabajo de otros compañeros que pertenezcan a la organización.
- Usuarios que cambien el equipo del lugar al que han sido asignados, esta actividad debe ser realizada por el departamento de sistemas.

#### **4.1.4.4 Política para la gestión de cuentas de usuario**

Esta política consiste en establecer la metodología para la creación, modificación, inactivación o eliminación de cuentas de usuarios y la asignación de autorizaciones de acceso a los sistemas.

Esta política menciona los siguientes puntos:

- Toda petición para creación, bloqueo o eliminación de usuarios, y para dar permisos de accesos a los diferentes aplicativos del sistema solo podrán ser

generadas tanto por el coordinador de talento humano o por el coordinador del departamento al que pertenece el colaborador

- Solo el personal encargado del departamento de sistemas podrán crear, bloquear o eliminar a los usuarios indicados por el coordinador solicitante, previo envío de un correo electrónico; de igual forma con los diferentes accesos a los diferentes aplicativos y servicios que tiene la empresa.
- En caso de requerirse, un representante del departamento de sistemas, se acercará al departamento del nuevo usuario y le dará la inducción básica para que pueda comenzar con sus actividades en la estación de trabajo.

#### **4.1.4.5 Política para la gestión de contraseñas de usuarios**

El objetivo de esta política es dar a conocer el correcto uso de las cuentas de usuario y contraseñas de acceso a los sistemas de la empresa.

Esta política detalla los siguientes puntos:

- El uso de la cuenta de usuario es responsabilidad exclusiva de la persona a la que está asignada.
- La cuenta de usuario será protegida mediante una contraseña. La contraseña es personal e intransferible, no debe compartir la cuenta de usuario con otra persona.
- Toda contraseña es sensible a mayúsculas y minúsculas.
- Si se detecta o sospecha que las actividades de una cuenta de usuario puede comprometer la integridad o seguridad de la información, el acceso a dicha cuenta será suspendido temporalmente y será reactivada solo después de haber tomado las medidas pertinentes con dicha cuenta.

- Se definen los tipos de cuentas de usuario:
  - **Cuentas de usuario administrador.-** Son las cuentas de usuario que permiten al administrador del sistema gestionar todas las demás cuentas y acceder con altos privilegios a los sistemas de la empresa.
  - **Cuentas de usuario estándar.-** Son todas las cuentas al servicio del usuario final, que están reguladas por autorizaciones definidas por el administrador del sistema.
- Las contraseñas del usuario administrador deberán ser cambiadas como mínimo cada 2 meses.
- Todas las contraseñas de usuario estándar deberán ser cambiadas al menos cada 90 días.
- Se evitará mencionar y en la medida de lo posible, teclear contraseñas en frente de otros usuarios.

#### **4.1.4.6 Política de manejo de unidades compartidas**

Esta política consiste en establecer la metodología para el uso y administración de las unidades compartidas, esta política describe los siguientes puntos:

- Dentro de las unidades compartidas existirá una carpeta con el nombre del departamento de la empresa, esta carpeta es privada y solo podrá ser vista por el personal perteneciente al departamento.
- Adicionalmente, existe una carpeta que se llama pública, a la cual tendrá acceso todo el personal de la empresa para poder leer, crear, modificar o eliminar directorios o archivos.
- El departamento de sistemas tiene la responsabilidad de hacer el respaldo de esta información diariamente una vez al día en horas no laborables y de forma automática.



- El personal de sistemas son los únicos autorizados para quitar, otorgar o limitar el acceso a un recurso compartido.
- Para efectos de la seguridad de la información, los archivos ubicados en “Mis Documentos” y en “Escritorio” de cada equipo por sesión de usuario serán respaldados en servidores del centro de cómputo.

#### **4.1.4.7 Política de respaldo de información**

Esta política tiene como objetivo respaldar la información de las bases de datos, programas ejecutables y carpetas compartidas en la red (incluyendo los archivos de los usuarios en la red).

Esta política detalla los siguientes puntos:

- El respaldo de las bases de datos y su replicación se realiza diariamente, cuatro veces al día y de manera automática. La ubicación de los archivos de respaldo están en un servidor ubicado en el edificio principal.
- El respaldo de las carpetas compartidas en la red se realizan diariamente, una vez al día, de manera automática y usando otro servidor como destino.
- Los archivos de respaldo de las bases de datos también se respaldan en un servidor remoto.
- No se respalda archivos de las estaciones de trabajo que estén fuera de “Mis Documentos” o “Escritorio”. Tampoco se respaldan archivos multimedia que no sean pertinente a lo laboral.

#### **4.1.4.8 Política de atención de requerimientos de usuarios**

Esta política consiste en establecer la metodología para la atención de requerimientos de usuarios de la organización.

Esta política menciona los siguientes puntos:

- Todo requerimiento de soporte a usuario debe ser solicitado por el correo electrónico y dirigido al personal de soporte del respectivo producto informático, con copia al coordinador del departamento y al coordinador de sistemas.
- Si el requerimiento debe ser atendido por personal externo, el departamento de sistemas se encargará de coordinar con el proveedor la venida del técnico que ejecutará el trabajo. Si el trabajo del proveedor externo requiere acceso remoto, el departamento de sistemas se encargará de gestionar el acceso.
- Todo requerimiento nuevo debe ser documentado y registrado en una base de conocimiento con la finalidad de que esté accesible a otros colaboradores que a futuro puedan ser responsables de dar soporte en el producto en cuestión.
- Si se trata de un requerimiento frecuente, se procederá a documentar solo los cambios que se presenten a lo largo del tiempo a partir de la creación del documento inicial.

#### **4.1.4.9 Política de elaboración y gestión de documentación técnica**

Esta política consiste en establecer la metodología para la elaboración de la documentación técnica del departamento de sistemas, esta política detalla los siguientes puntos:

- Los documentos deberán ubicarse en una carpeta compartida en la red. A esta carpeta deben tener acceso solo el personal de sistemas y solo podrán leerla mas no modificarla. Sólo el responsable del documento puede modificarlo a menos que designe a alguien para hacerlo.
- La documentación debe de estar agrupada por sub-departamentos: hardware, software, redes o cualquier otro sub-departamento que se cree a futuro.
- Cada documento debe de tener un prefijo que indique al sub-departamento y un secuencial por sub-departamento que los distinga del resto.

- El archivo puede ser una hoja de cálculo, un documento, una imagen o cualquier otro medio que sea útil para explicar un tema técnico.

## **4.2 Metodología de evaluación de riesgos**

En esta tesis se empleará la metodología de investigación de riesgos denominado Magerit, la misma que indicará los caminos correctos para el mejor control de los activos.

La metodología evalúa y determina si los activos de la empresa u organización tienen vulnerabilidades por medio de la medición de la protección que tuviesen dichos activos, esto a su vez, permite establecer varios controles que ayudan en gran medida a mejorar y disminuir posibles riesgos.

Magerit identifica el riesgo luego determina la vulnerabilidad a la que está expuesto el activo y recomienda el control para reducir el daño.

Está compuesta de cuatro etapas las cuales aclara la forma de trabajar de la metodología y son las siguientes:

- Planificar, se considera como el inicio del proyecto y es aquí en donde se dan los lineamientos a los que se piensa llegar.
- Análisis, en esta etapa se identifican y cuantifican todos los activos que se encuentran en la organización y a su vez se obtiene una estimación que se desea y se pueda controlar.
- Gestión de Riesgos, en esta etapa se identifica las funciones y controles.
- Selección, en esta etapa se seleccionan las salvaguardas o mejor conocidos como controles.

#### **4.2.1 Objetivos de la Metodología Magerit**

Los objetivos directos e indirectos de Magerit son los siguientes:

##### **Directos:**

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.

##### **Indirectos:**

1. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

#### **4.2.2 Beneficios del uso de la metodología Magerit para la organización**

- **Beneficios a nivel interno**

La organización se beneficia en lo que respecta a seguridad informática, ya que al implementar los controles necesarios, se mitigará los posibles riesgos que tuviesen los activos informáticos, además, que al momento de una evaluación, auditoría, certificación o acreditación, la empresa ya estará preparada.

- **Beneficios a nivel externo**

Al tener una seguridad eficiente de la información, la empresa tendrá una ventaja competitiva sobre sus competidores, ya que se asegura a los clientes habituales o potenciales que su información tiene los controles y seguridades necesarias para realizar un trabajo eficiente.

### 4.3 Identificación de los activos

Para la correcta identificación de los activos se realizaron entrevistas con jefes de área, listas de checks y encuestas a los usuarios, una vez realizado esto los activos se clasificaron de la siguiente manera:

- **Aplicaciones informáticas** (software) tales como Base de datos y aplicaciones administrativas.
- **Equipos informáticos** (hardware) tales como servidores, computadoras, dispositivos de almacenamiento de datos.
- **Redes de comunicaciones** que permiten el intercambio de datos dentro y fuera de la organización.
- **Instalaciones** que acogen equipos informáticos, de comunicaciones y personas.
- **Servicios** de computación y de comunicación, otros servicios que se necesiten para poder organizar el sistema.
- **Personas** que utiliza todos los elementos mencionados anteriormente.

#### 4.3.1 Plantilla de identificación de activos

A continuación se muestra la plantilla que se utilizó para la identificación de activos.

(Ver Anexo A.5)

**Tabla 3** - Plantilla de identificación de Activos

<b>CODIGO</b>	<b>NOMBRE</b>	<b>DESCRIPCION</b>	<b>CANTIDAD</b>	<b>CLASIFICACIÓN</b>	<b>DEPARTAMENTO</b>
Código de identificación del activo	Nombre del activo	Descripción del activo (uso en la empresa)	Cantidad de elementos	Tipo de clasificación de activo	Nombre del Departamento donde se encuentra el activo

**Elaborado por:** Los Autores

#### 4.3.2 Plantilla de Levantamiento de Activos - APLICACIONES

A continuación se muestra la plantilla que se utilizó para el levantamiento de activos – Aplicaciones. (Ver Anexo A.1.1)

#### LEVANTAMIENTO DE ACTIVOS – APLICACIONES

Nombre: \_\_\_\_\_

Departamento: \_\_\_\_\_

APLICACIONES	
CODIGO:	NOMBRE:
DESCRIPCION:	
RESPONSABLE:	
TIPO:	

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD		
INTEGRIDAD		
CONFIDENCIALIDAD		

DEPENDENCIA DE ACTIVOS INFERIORES	
activo:	grado:
¿Por qué?:	

FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

Elaborado por: Los Autores

### 4.3.3 Plantilla de Levantamiento de Activos - SERVICIOS

A continuación se muestra la plantilla que se utilizó para el levantamiento de activos – Servicios. (Ver Anexo A.1.2)

#### LEVANTAMIENTO DE ACTIVOS – SERVICIOS

Nombre: \_\_\_\_\_

Departamento: \_\_\_\_\_

SERVICIOS	
CODIGO:	NOMBRE:
DESCRIPCION:	
RESPONSABLE:	
TIPO:	

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD		
INTEGRIDAD		
CONFIDENCIALIDAD		

DEPENDENCIA DE ACTIVOS INFERIORES	
activo:	grado:
¿Por qué?:	

FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

Elaborado por: Los Autores

#### 4.3.4 Plantilla de Levantamiento de Activos - EQUIPOS INFORMÁTICOS

A continuación se muestra la plantilla que se utilizó para el levantamiento de activos – Equipos Informáticos. (Ver Anexo A.1.3)

#### LEVANTAMIENTO DE ACTIVOS – EQUIPOS INFORMATICOS

Nombre: \_\_\_\_\_

Departamento: \_\_\_\_\_

EQUIPOS INFORMATICOS	
CODIGO:	NOMBRE:
DESCRIPCION:	
RESPONSABLE:	
UBICACIÓN:	
NUMERO:	
TIPO:	

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD		
INTEGRIDAD		
CONFIDENCIALIDAD		

DEPENDENCIA DE ACTIVOS INFERIORES	
activo:	grado:
¿Por qué?:	

#### FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

Elaborado por: Los Autores



#### 4.3.5 Plantilla de Levantamiento de Activos – REDES DE COMUNICACIÓN

A continuación se muestra la plantilla que se utilizó para el levantamiento de activos – Redes de Comunicación. (Ver Anexo A.1.4)

#### LEVANTAMIENTO DE ACTIVOS – REDES DE COMUNICACION

Nombre: \_\_\_\_\_

Departamento: \_\_\_\_\_

REDES DE COMUNICACIÓN	
CODIGO:	NOMBRE:
DESCRIPCION:	
RESPONSABLE:	
UBICACIÓN:	
NUMERO:	
TIPO:	

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD		
INTEGRIDAD		
CONFIDENCIALIDAD		

DEPENDENCIA DE ACTIVOS INFERIORES	
activo:	grado:
¿Por qué?:	

#### FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, <b><u>ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS</u></b> , ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA
---

Elaborado por: Los Autores

#### 4.3.6 Plantilla de Levantamiento de Activos - INSTALACIONES

A continuación se muestra la plantilla que se utilizó para el levantamiento de activos – Instalaciones. (Ver Anexo A.1.5)

#### LEVANTAMIENTO DE ACTIVOS – INSTALACIONES

Nombre: \_\_\_\_\_

Departamento: \_\_\_\_\_

INSTALACIONES	
CODIGO:	NOMBRE:
DESCRIPCION:	
RESPONSABLE:	
UBICACIÓN:	
NUMERO:	
TIPO:	

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD		
INTEGRIDAD		
CONFIDENCIALIDAD		

DEPENDENCIA DE ACTIVOS INFERIORES	
activo:	grado:
¿Por qué?:	

FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

Elaborado por: Los Autores

#### 4.3.7 Plantilla de Levantamiento de Activos - PERSONAS

A continuación se muestra la plantilla que se utilizó para el levantamiento de activos – Personas. (Ver Anexo A.1.6)

#### LEVANTAMIENTO DE ACTIVOS – PERSONAS

Nombre: \_\_\_\_\_

Departamento: \_\_\_\_\_

PERSONAS	
CODIGO:	NOMBRE:
DESCRIPCION:	
NUMERO:	
TIPO:	

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD		
INTEGRIDAD		
CONFIDENCIALIDAD		

\_\_\_\_\_  
FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

Elaborado por: Los Autores

#### 4.3.8 Software empleado en identificación de activos

**Belarc Advisor** construye un perfil detallado del software y hardware instalados en la PC, incluyendo los hotfixes de Microsoft y muestra el resultado en el explorador Web. Toda la información del perfil se mantiene privada en la PC y no se envía a ningún servidor Web.



Los productos comerciales de Belarc son utilizados para la administración de licencias de software, planeación de actualizaciones de hardware, estatus de seguridad cibernética, cumplimiento en auditorías informáticas, administración de activos de TI, administración de configuraciones, etc.


##### **Requisitos del producto:**

- **Sistemas Operativos:** Windows 8, 7, Vista, XP, Me, 98, 95, 2012, 2008 R2, 2008, 2003, 2000, NT 4.
- **Navegador:** IE, Firebird, Safari, y Opera.
- **Tamaño del archivo:** 3597 KB.
- **Licencia:** La licencia asociada a este producto es gratuita sólo para uso personal. En redes corporativas, públicas, instancias de gobierno, o de cualquier otro tipo, se encuentra prohibida su instalación y uso.

El software Belarc Advisor servirá para ayudar al inventario de activos de la compañía, verificación de ip para su posterior ordenamiento, programas instalados, y características de tipo hardware y software de la pc donde se ejecute.

### 4.3.8.1 Capturas del Belarc Advisor

Ilustración 2 - Salvapantalla de Programa Belarc Advisor 1



The license associated with the Belarc Advisor product allows for **free personal use only**. Use on computers in a corporate, educational, military or government installation is prohibited. See the [license agreement](#) for details. The information on this page was created locally on your computer by the Belarc Advisor. Your computer profile was not sent to a web server. [Click here for more info.](#)

**System Security Status**

Security Benchmark Score  
*Available only for Windows 7, Vista, and XP Pro*

?

Virus Protection

Up-to-date

✔

Security Updates

49 missing

✘

**Computer Profile Summary**

Computer Name: sist13-indu (in INDLAC)  
 Profile Date: domingo, 08 de febrero de 2015 9:24:44  
 Advisor Version: 8.4  
 Windows Logon: jvaldiviezo  
 Active Directory OU: SISTEMAS PC  
 DNS Suffix: indulac.ec

**Operating System**

Windows 8.1 Professional (x64) (build 9600)  
 Install Language: Español (España, internacional)  
 System Locale: Español (Ecuador)  
 Installed: 28/02/2014 4:05:02  
 Boot Mode: Legacy BIOS in UEFI (Secure Boot not supported)

**Processor <sup>a</sup>**

3.00 gigahertz Intel Core i7-4770  
 256 kilobyte primary memory cache  
 1024 kilobyte secondary memory cache  
 8192 kilobyte tertiary memory cache  
 64-bit ready  
 Multi-core (4 total)

**System Model**

Enclosure Type: Desktop

**Main Circuit Board <sup>b</sup>**

Board: Intel Corporation DH87L AAG74240-403  
 Serial Number: BQRL336000P4  
 Bus Clock: 100 megahertz  
 UEFI: Intel Corp. RLH8710H.86A.0320.2013.0606.1802.06/06/2013

**In page Links:**

- [Software Licenses](#)
- [Software Versions & Usage](#)
- new** [Missing Updates](#)
- [USB Storage Use](#)
- [Hosted Virtual Machines](#)
- [Network Map](#)

**System Security Status**

Security Benchmark Score  
*Available only for Windows 7, Vista, and XP Pro*

?

Virus Protection

Up-to-date

✔

Security Updates

49 missing

✘

**Computer Profile Summary**

Computer Name: sist13-indu (in INDLAC)  
 Profile Date: domingo, 08 de febrero de 2015 9:24:44  
 Advisor Version: 8.4  
 Windows Logon: jvaldiviezo  
 Active Directory OU: SISTEMAS PC  
 DNS Suffix: indulac.ec

**Operating System**

Windows 8.1 Professional (x64) (build 9600)  
 Install Language: Español (España, internacional)  
 System Locale: Español (Ecuador)  
 Installed: 28/02/2014 4:05:02  
 Boot Mode: Legacy BIOS in UEFI (Secure Boot not supported)

**Processor <sup>a</sup>**

3.00 gigahertz Intel Core i7-4770  
 256 kilobyte primary memory cache  
 1024 kilobyte secondary memory cache  
 8192 kilobyte tertiary memory cache  
 64-bit ready  
 Multi-core (4 total)

**System Model**

Enclosure Type: Desktop

**Main Circuit Board <sup>b</sup>**

Board: Intel Corporation DH87L AAG74240-403  
 Serial Number: BQRL336000P4  
 Bus Clock: 100 megahertz  
 UEFI: Intel Corp. RLH8710H.86A.0320.2013.0606.1802.06/06/2013

**In page Links:**

- [Software Licenses](#)
- [Software Versions & Usage](#)
- new** [Missing Updates](#)
- [USB Storage Use](#)
- [Hosted Virtual Machines](#)
- [Network Map](#)

Fuente: Programa Belarc Advisor versión 8.4

Ilustración 3 - Salvapantalla de Programa Belarc Advisor 2

Installed Hotfixes	Drives	Memory Modules c,d										
	<p>3000.23 Gigabytes Usable Hard Drive Capacity 2350.77 Gigabytes Hard Drive Free Space</p> <p>HL-DT-ST DVD-RAM GH24NS95 [Optical drive] ST2000DM001-1CH164 [Hard drive] (2000.40 GB) -- drive 1, s/n W340DF0N, rev CC29, <a href="#">SMART</a> Status: Healthy WDC WD10EZEX-00BNS-A0 [Hard drive] (1000.20 GB) -- drive 0, s/n WD-WCC3F1424754, rev 01.01A01, <a href="#">SMART</a> Status: Healthy</p>	<p>32428 Megabytes Usable Installed Memory</p> <p>Slot 'DIMM 3' has 8192 MB (serial number 11487144) Slot 'DIMM 1' has 8192 MB (serial number 12481244) Slot 'DIMM 4' has 8192 MB (serial number 11482243) Slot 'DIMM 2' has 8192 MB (serial number 11481244)</p> <p><b>Local Drive Volumes</b></p> <p>c: (NTFS on drive 0) * 502.95 GB 376.57 GB free d: (NTFS on drive 0) 496.89 GB 337.43 GB free f: (NTFS on drive 1) 2000.40 GB 1636.78 GB free</p>										
		<p>* Operating System is installed on c:</p> <p><b>Network Drives</b></p> <p>mounted by jvaldiviezo at 08/02/2015 9:19:47</p> <p>g: \\srvind03\openseidreproduccion 4.29 GB 88.88 GB free h: \\srvind03\openseidreproduccion 2.15 GB 88.88 GB free j: \\srvind03\fileuser 536.87 GB 88.88 GB free q: \\srvind03\openseidreac 8.59 GB 88.88 GB free w: \\srvind02\evolucion 53.69 GB 279.32 GB free</p>										
	<p><b>Users (mouse over user name for details)</b></p> <table border="1"> <thead> <tr> <th>local user accounts</th> <th>last logon</th> </tr> </thead> <tbody> <tr> <td>Administrador</td> <td>28/02/2014 4:07:14 (admin)</td> </tr> <tr> <td>✘ User</td> <td>28/02/2014 4:05:04</td> </tr> </tbody> </table> <p><b>local system accounts</b></p> <p>✘ Invitado never</p> <p><b>INDULAC domain logons</b></p> <table border="1"> <thead> <tr> <th>asoto</th> <th>jvaldiviezo</th> </tr> </thead> <tbody> <tr> <td>26/01/2015 14:43:21</td> <td>04/02/2015 11:11:58 (admin)</td> </tr> </tbody> </table> <p>✘ Marks a disabled account;  Marks a locked account</p>	local user accounts	last logon	Administrador	28/02/2014 4:07:14 (admin)	✘ User	28/02/2014 4:05:04	asoto	jvaldiviezo	26/01/2015 14:43:21	04/02/2015 11:11:58 (admin)	<p><b>Printers</b></p> <p>EPSON TX420W Series on USB001 HP LaserJet M1522 MFP Series PCL 6 on HPLaserJetM1522nrMFP HP LaserJet Professional P1606dn on IP_192.168.0.175 hpfax1 on HPFax1 Microsoft Shared Fax Driver on SHRFAX: Microsoft XPS Document Writer v4 on PORTPROMPT: PrimoPDF on PrimoPort: Send to Microsoft OneNote 15 Driver on nul:</p>
local user accounts	last logon											
Administrador	28/02/2014 4:07:14 (admin)											
✘ User	28/02/2014 4:05:04											
asoto	jvaldiviezo											
26/01/2015 14:43:21	04/02/2015 11:11:58 (admin)											
	<p><b>Controllers</b></p> <p>Controladora SATA AHCI estándar [Controller]</p>	<p><b>Display</b></p> <p>Adaptador de pantalla básico de Microsoft [Display adapter] Monitor genérico.cmu.no.es.PnP</p>										

Fuente: Programa Belarc Advisor versión 8.4

Ilustración 4 - Salvapantalla de Programa Belarc Advisor 3

Windows Defender	Communications	Other Devices
Adaptador de extensión de conmutador virtual para Hyper-V		Altavoces (Realtek High Definition Audio)
Adaptador de extensión de conmutador virtual para Hyper-V #2		Microfono (Realtek High Definition Audio)
Adaptador de extensión de conmutador virtual para Hyper-V #3		Realtek Digital Output (Realtek High Definition Audio)
Adaptador de red de depuración de kernel de Microsoft		Realtek Digital Output(Optical) (Realtek High Definition Audio)
Adaptador ISATAP de Microsoft		Dispositivo de control del consumidor compatible con HID
Adaptador virtual de Ethernet para Hyper-V #2		Dispositivo de entrada USB (3x)
primary Auto IP Address: 192.168.0.74 / 24		HP LJ M1522mf Scan
Gateway: 192.168.0.4		Dispositivo de teclado HID [Keyboard]
Dhcp Server: 192.168.0.2		Mouse compatible con HID
Physical Address: 00:22:4D:AB:06:5F		Cola de impresión raiz
Connection Speed: 1 Gbps		Enviar a OneNote 2013
Adaptador virtual de Ethernet para Hyper-V #3		Fax
IP Address: 192.168.10.10 / 24		HP LaserJet M1522 MFP Series Fax
Physical Address: 00:15:5D:00:4A:00		HP LaserJet M1522 MFP Series PCL 6
Connection Speed: 10 Gbps		HP LaserJet Professional P1606dn
Conexión Ethernet Intel(R) I217-V		Microsoft XPS Document Writer
VirtualBox Host-Only Ethernet Adapter		PrimoPDF
Networking Dns Servers: 192.168.0.2		Servicio de localización de Windows
192.168.0.1		Controlador de filtro de tarjeta inteligente (6x)
		Aladdin iFD Handler (2x)
		Aladdin VR Handler
		Rainbow iKey Enumerator
		Rainbow iKey Virtual Reader (2x)
		AKS ifdh 0
		AKS ifdh 1
		AKS VR 0
		Bus adaptador de transición IPv4 IPv6 de Microsoft
		Lightweight Sensors Root Enumerator
		Microsoft Device Association Root Enumerator
		Rainbow Technologies iKeyVirtualReader 0
		Rainbow Technologies iKeyVirtualReader 1
		Smart Card Device Enumeration Bus
		Concentrador raiz USB (2x)
		Concentrador raiz USB (AHCI)
		Dispositivo compuesto USB
		Generic USB Hub (2x)
		Instantánea de volumen genérico
		<b>Hosted Virtual Machines (mouse over name for details)</b>
	<b>USB Storage Use in past 30 Days (mouse over last used for details)</b>	

Fuente: Programa Belarc Advisor versión 8.4

**Ilustración 5-** Salvapantalla de Programa Belarc Advisor 4

[See your entire network map...](#)  
[click for Belarc's System Management products](#)

Network Map (mouse over IP address for physical address) [[Back to Top](#)]

IP	Device Type	Device Details	Device Roles
192.168.0.1	Windows 2008 Server	srv-master.indulac.ec, HP Compaq	Domain Name Server, IIS <a href="#">Web Server</a> , Domain Controller, Time Source
192.168.0.2	Windows 2008 Server	Srv-mail (in INDULAC), srv-mail.indulac.ec, HP Compaq	DHCP Server, Domain Name Server, IIS <a href="#">Web Server</a> , Domain Controller, Time Source
192.168.0.3	Windows 2008 Server	Srv-safe (in INDULAC), MS Hyper-V	IIS <a href="#">Web Server</a> , SQL Server
192.168.0.4	Windows 2008 Server	Srv-proxy (in INDULAC), srv-proxy.indulac.ec, HP Compaq	Gateway, <a href="#">Web Server</a> , SQL Server
192.168.0.5	System	Srv-desa, srv-desa.indulac.ec, HP Compaq	
192.168.0.8	Windows 2012 Server	Srv-dyn-db (in INDULAC), MS Hyper-V	SQL Server
192.168.0.9	Windows 2008 Server	Srv-dyn-apli (in INDULAC), MS Hyper-V	IIS <a href="#">Web Server</a>
192.168.0.21	System	Srvind07, srvind07.indulac.ec, HP Compaq	
192.168.0.25	Windows 7 Workstation	Prueba-pc (in INDULAC), MS Hyper-V	
192.168.0.35	Windows Workstation	Powersist-pc (in WORKGROUP), MS Hyper-V	Samba Server
192.168.0.37	Windows 2008 Server	Srvind14 (in INDULAC), MS Hyper-V	SQL Server
192.168.0.39	Windows 2008 Server	Srvind24 (in INDULAC), MS Hyper-V	<a href="#">Web Server</a>
192.168.0.42	Windows 2008 Server	Gantia01-indu (in INDULAC), gantia01-indu.indulac.ec	IIS <a href="#">Web Server</a>
192.168.0.49	Windows 7 Workstation	Hp v1910 switch, HP Compaq	<a href="#">Web Server</a>
192.168.0.50	System	Labo00-indu (in INDULAC), labo00-indu.indulac.ec	Print Server, Browse Master
192.168.0.56	Windows 7 Workstation	Srvind17 (in INDULAC), MS Hyper-V	IIS <a href="#">Web Server</a> , SQL Server
192.168.0.57	Windows 2008 Server	Hp v1910 switch, HP Compaq	<a href="#">Web Server</a>
192.168.0.63	System	Sist15-indu (in INDULAC), sist15-indu.indulac.ec	Print Server, SQL Server
192.168.0.72	Windows 8 Workstation	Sist12-indu (in INDULAC), sist12-indu.indulac.ec	
192.168.0.73	Windows 8 Workstation	Sist13-indu (in INDULAC), sist13-indu.indulac.ec	<a href="#">Web Server</a> , Print Server, Browse Master
192.168.0.74	Windows 8 Workstation	Sist13-indu (in INDULAC), sist13-indu.indulac.ec	
192.168.0.160	Windows 7	Sist02-indu (in INDULAC),	

Fuente: Programa Belarc Advisor versión 8.4



## **4.4 Dimensiones de valoración de seguridad**

Las dimensiones son las características de los activos, independiente de otra, estas se utilizan para valorar las consecuencias de la amenaza y estas son:

- **Disponibilidad:**

La disponibilidad de los servicios o activos se refiere a la cualidad de ser usados cuando se los necesite. La falta de esta dimensión se asume como una interrupción del servicio. Esta dimensión afecta directamente a la producción de la organización.

- **Integridad:**

La integridad se refiere a la completitud y corrección de los datos. Si llegase a faltar esta dimensión indica que la información podría ser manipulada, corrupta o no estar completa.

- **Confidencialidad:**

La confidencialidad se refiere a que la información solo esté disponible a las personas autorizadas, la falta de esta dimensión ocasionaría la fuga de información, manipulación, eliminación o edición de la misma, así como accesos no autorizados.

## **4.5 Criterios de valoración**

### **4.5.1 Criterios de valoración de activos**

Para poder asignar un valor a los activos de la organización se han realizado las siguientes escalas de 3 valores, con el fin de que ofrezcan los siguientes aspectos:

- Una escala igual para todas las dimensiones, con el fin de comparar los riesgos.
- Escalas de diferenciación de valores.

**(Ver Anexo A.7.1)**

**Tabla 4 -** Tabla de Valoración de Disponibilidad

	<b>Valor</b>	<b>Clase</b>	<b>Descripción</b>
<b>Disponibilidad</b>	1	Bajo	Los procesos de la empresa no se ven afectados si esta información no se encuentra disponible.
	2	Mediano	Si la información no se encuentra disponible puede que afecte a los procesos que la utilizan. Sin embargo, existen métodos de contingencia para el desarrollo de las operaciones o el proceso podría esperar hasta que se encuentre disponible la información.
	3	Alto	Los procesos de la organización pueden llegar a tener un fatal efecto si esta información no se encuentra disponible en el momento que se la necesita.

**Elaborado por:** Los Autores

**Tabla 5 -** Tabla de Valoración de Integridad

	<b>Valor</b>	<b>Clase</b>	<b>Descripción</b>
<b>Integridad</b>	1	No requerida	Esta información es utilizada para consultas
	2	Requerida	Se requiere integridad en la información pero si el contenido de esta llega a ser falsificado, las operaciones no se verían afectadas gravemente.
	3	Obligatoria	Puede causar un efecto fatal en las operaciones de la empresa si la integridad de esta información se perdiera

**Elaborado por:** Los Autores

**Tabla 6 -** Tabla de Valoración de Confidencialidad

	<b>Valor</b>	<b>Clase</b>	<b>Descripción</b>
<b>Confidencialidad</b>	1	Acceso Publica	Información que puede ser revelada a terceras partes.
	2	Acceso Privado	Información que solo puede ser revelada al personal de la empresa. Si el contenido fuera revelado a terceras partes, no hubiera mucho efecto en las operaciones de la empresa.
	3	Restringido	Información que solo es revelada a partes específicas y departamentos de la organización. Si el contenido es revelado a personal no autorizado, puede haber un gran efecto en las operaciones de la empresa.

**Elaborado por:** Los Autores

#### **4.5.2 Criterios de valoración de amenazas**

Para poder evaluar las amenazas se tendrán dos parámetros los cuales serán:

- Degradación de Activo
- Probabilidad de Ocurrencia

**(Ver Anexo A.7.2)**

Las amenazas serán valoradas en tres categorías:

- Baja
- Media
- Alta

**Tabla 7** - Tabla de Valoración de Amenaza

<b>Dimensión</b>	<b>Valor</b>	<b>Clase</b>	<b>Descripción</b>
<b>Degradación del activo</b>	1	Bajo	Si ocurre la amenaza, el activo no se vería degradado gravemente.
	2	Medio	Si la amenaza ocurre, el activo se vería degradado de manera regular.
	3	Alto	Si la amenaza ocurre, el activo se vería degradado gravemente.

**Elaborado por:** Los Autores

**Tabla 8** - Tabla de Valoración de Probabilidad de Ocurrencia

<b>Dimensión</b>	<b>Valor</b>	<b>Clase</b>	<b>Descripción</b>
<b>Probabilidad de ocurrencia</b>	1	Bajo	Existe una baja probabilidad. La frecuencia de ocurrencia es una vez al año o menos.
	2	Medio	Existe una probabilidad moderada. La frecuencia de ocurrencia es una vez cada 6 meses o menos.
	3	Alto	Existe una alta probabilidad. La frecuencia de ocurrencia es una vez al mes o más.

**Elaborado por:** Los Autores

### **4.5.3 Criterios de valoración de vulnerabilidad**

Para poder evaluar las vulnerabilidades se debe tener en cuenta el control de seguridad establecido. (Ver Anexo A.7.3)

Las vulnerabilidades serán valoradas en tres categorías:

- Baja
- Media
- Alta

**Tabla 9 -** Tabla de Valoración de Vulnerabilidad

<b>Dimensión</b>	<b>Valor</b>	<b>Clase</b>	<b>Descripción</b>
<b>Control de seguridad</b>	1	Alto	Controles establecidos y adecuados para combatir la amenaza.
	2	Medio	Control medio de seguridad.
	3	Bajo	Escasos o inexistentes controles de seguridad.

**Elaborado por:** Los Autores

## **4.6 Identificación de amenazas y vulnerabilidades**

### **4.6.1 Identificación de amenazas**

El fin de este punto es la identificación de las posibles amenazas dentro de la organización y vulnerabilidad que puedan ser explotadas por dichas amenazas. A continuación detallaremos las principales amenazas. (**Ver Anexo A.6**)

#### **4.6.1.1 Amenazas de origen Natural**

**Tabla 10 -** Tabla de Amenazas de Origen Natural

<b>ORIGEN NATURAL</b>	
<b>Sucesos que pueden ocurrir sin intervención de los seres humanos como causa directa o indirecta.</b>	
<b>AMENAZA</b>	<b>ACTIVOS</b>
Fuego	Equipos informáticos - Información - Instalaciones - Energía – Documentos
Daños por agua	Equipos informáticos - Información - Energía – Documentos
Desastre Natural	Equipos informáticos - Información - Instalaciones - Energía - Documentos
<b>AFECTA A:</b>	
<b>Disponibilidad del servicio</b>	

**Elaborado por:** Los Autores

#### 4.6.1.2 Amenazas de origen Industrial

Tabla 11 - Tabla de Amenazas de Origen Industrial

<b>ORIGEN INDUSTRIAL</b>	
Sucesos que pueden ocurrir de forma accidental, derivados de la actividad humana de tipo industrial. Estas amenazas pueden darse de forma accidental o deliberada.	
<b>Amenaza</b>	<b>Activos</b>
Desastres industriales	Equipos informáticos - Información - Instalaciones - Energía – Documentos
Corte del suministro eléctrico	Equipos informáticos – Información
Condiciones inadecuadas de temperatura o humedad	Equipos informáticos – Información
<b>AFECTA A:</b>	
Disponibilidad del servicio, Confidencialidad de la información, Integridad de los Datos	
Elaborado por: Los Autores	

#### 4.6.1.3 Amenazas de origen no intencional

Tabla 12 - Tabla de Amenazas de Origen No Intencional

<b>ORIGEN NO INTENCIONADO</b>	
Fallos no intencionales causados por las personas.	
<b>Amenaza</b>	<b>Activos</b>
Errores de los usuarios	Datos - Claves - Servicios - Aplicaciones – Información
Difusión de software dañino	Aplicaciones
Fugas de información	Datos - Claves - Servicios - Aplicaciones - Comunicaciones - Información - Instalaciones – Personal

Vulnerabilidades de los programas (software)	Aplicaciones
Errores de mantenimiento actualización programas	Aplicaciones
Errores de mantenimiento actualización de equipos (hardware)	Equipo informático
Caída del sistema por agotamiento de recursos	Equipo informático - Servicios – Redes
Restauración fallida de respaldos	Aplicaciones – Información
Indisponibilidad del personal	Personal
<b>AFECTA A:</b>	
Disponibilidad del servicio, Confidencialidad de la información, Integridad de los Datos	
<b>Elaborado por:</b> Los Autores	

#### 4.6.1.4 Amenazas de origen intencional

Tabla 13 - Tabla de Amenazas de Origen Intencional

<b>ORIGEN INTENCIONADO</b>	
Fallos deliberados causados por las personas.	
<b>Amenaza</b>	<b>Activos</b>
Suplantación de la identidad del usuario	Datos - Claves - Servicios - Aplicaciones – Redes

Uso no previsto	Servicios - Aplicaciones - Equipos informáticos - Redes - Información – Instalaciones
Modificación deliberada de la información	Datos - Claves - Servicios - Aplicaciones - Comunicaciones - Información – Instalaciones
Divulgación de información	Datos - Claves - Servicios - Aplicaciones -Comunicaciones - Información - Instalaciones
Manipulación de programas	Software
Manipulación de los equipos	Equipos informáticos – Información
Robo	Equipos informáticos
Ingeniería social	Personal
<b>AFECTA A:</b>	
Disponibilidad del servicio, Confidencialidad de la información, Integridad de los Datos	

**Elaborado por:** Los Autores

#### 4.6.2 Identificación de vulnerabilidades

En las siguientes tablas se identifican las vulnerabilidades que se presentan en cada uno de los activos, y las amenazas que pueden explotar dichas vulnerabilidades.

##### 4.6.2.1 Amenazas y vulnerabilidades - Tipo de activo “Equipos”

**Tabla 14** - Tabla de Amenazas y Vulnerabilidad - Equipos

ACTIVOS	AMENAZA	VULNERABILIDAD
EQUIPOS	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección estructural contra agua
	Desastres naturales (Terremotos)	Problemas de origen estructural en el edificio



	donde se encuentre el activo
Errores de mantenimiento actualización de equipos	Controles bajos o nulos de actualización de equipos
Uso no previsto de los recursos	Falta de políticas sobre usos de los recursos y controles de acceso
Corte de suministro eléctrico	Funcionamiento inadecuado de los UPS
Condiciones inadecuadas de temperatura y humedad	Mal funcionamiento de climatización en la empresa
Robo	Falta de controles de entrada y salida de recursos a la organización

Elaborado por: Los Autores

#### 4.6.2.2 Amenazas y vulnerabilidades - Tipo de activo “Aplicaciones”

Tabla 15 - Tabla de Amenazas y Vulnerabilidad – Aplicaciones

ACTIVOS	AMENAZAS	VULNERABILIDAD
APLICACIONES	Errores de usuario	Falta de capacitación
	Difusión de software dañino	Falta o fallo en antivirus
	Fugas de información	Inexistentes controles de aseguramiento de información
	Vulnerabilidades de los programas	Problemas con actualización o software no depurado

Errores de mantenimiento y actualización de programas	Controles bajos o nulos de actualización de software
Uso no previsto de recursos	Falta de políticas sobre usos de los recursos y controles de acceso
Suplantación de identidad	Falta de controles de acceso del personal
Modificación deliberada de la información	Falta de procedimientos y control de cambios en la información

**Elaborado por:** Los Autores

#### 4.6.2.3 Amenazas y vulnerabilidades - Tipo de activo “Servicios”

**Tabla 16** - Tabla de Amenazas y Vulnerabilidad – Activo Servicios

ACTIVOS	AMENAZAS	VULNERABILIDAD
SERVICIOS	Errores de mantenimiento y actualización de programas	Controles bajos o nulos de actualización de software
	Difusión de software dañino	Falta o fallo en antivirus
	Restauración fallida de respaldos	Falta de procedimientos para generar respaldos y restaurar los mismos
	Caída del sistema por agotamiento de recursos	Equipos con características mínimas para el trabajo
	Alteración no autorizada	Falta de control de acceso.

autorizada de la configuración.	
Manipulación en la configuración.	Falta de políticas de seguridad.
Manipulación de programas	Falta de controles de modificación de programas
Modificación deliberada de la información	Falta de procedimientos y control de cambios en la información

**Elaborado por:** Los Autores

#### 4.6.2.4 Amenazas y vulnerabilidades - Tipo de activo “Redes”

**Tabla 17** - Tabla de Amenazas y Vulnerabilidad - Redes

<b>ACTIVOS</b>	<b>AMENAZAS</b>	<b>VULNERABILIDAD</b>
REDES	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección estructural contra agua
	Desastres naturales (terremotos)	Problemas de origen estructural en el edificio donde se encuentre el activo
	Desastres industriales (fuga de amoniaco)	Falta de controles ante posible fuga
	Corte de suministro eléctrico	Funcionamiento inadecuado de los ups
	Condiciones inadecuadas de temperatura y humedad	Mal funcionamiento de climatización en la empresa
	Caída del sistema por agotamiento de recursos	Equipos con características mínimas para el trabajo

Errores de mantenimiento	Controles bajos o nulos de actualización de equipos
--------------------------	---

**Elaborado por:** Los Autores

#### 4.6.2.5 Amenazas y vulnerabilidades - Tipo de activo “Instalaciones”

**Tabla 18** - Tabla de Amenazas y Vulnerabilidad - Instalaciones

ACTIVOS	AMENAZAS	VULNERABILIDAD
INSTALACIONES	Fuego	Falta de protección contra fuego
	Daños por agua	Falta de protección estructural contra agua
	Desastres naturales (terremotos)	Problemas de origen estructural en el edificio donde se encuentre el activo
	Desastres industriales (fuga de amoníaco)	Falta de controles ante posible fuga
	Corte de suministro eléctrico	Funcionamiento inadecuado de los ups
	Condiciones inadecuadas de temperatura y humedad	Mal funcionamiento de climatización en la empresa
	Suplantación de identidad	Falta de controles de acceso del personal

**Elaborado por:** Los Autores

#### 4.6.2.6 Amenazas y vulnerabilidades - Tipo de activo “Personas”

**Tabla 19** - Tabla de Amenazas y Vulnerabilidad - Personas

ACTIVOS	AMENAZAS	VULNERABILIDAD
PERSONAS	Fugas de información	Inexistentes controles de aseguramiento de información
	Desastres industriales	Falta de controles ante posible

(fuga de amoniaco)	fuga
Indisponibilidad del personal	Bajos o nulos controles de control de personal
Ingeniería social	Falta de procedimientos para el acceso a la información

**Elaborado por:** Los Autores

#### 4.7 Exposición del riesgo

Se buscara la probabilidad de que ocurra cada amenaza y el nivel de vulnerabilidad, teniendo como resultado el nivel de exposición de riesgo de cada activo de la empresa.

Valoración:

- **Amenaza**= probabilidad de ocurrencia de la amenaza, basados en registros de los últimos 2 años.
- **Vulnerabilidad** = probabilidad de ocurrencia

#### 4.8 Selección de opciones para el tratamiento del riesgo

Antes de considerar el tratamiento de un riesgo, la organización debe decidir el criterio para determinar si es que los riesgos son aceptados o no. Los riesgos pueden ser aceptados si, por ejemplo, se evalúa que el riesgo es menor o que el costo de tratarlo no es rentable para la organización. Estas decisiones deben ser grabadas.

Para cada uno de los riesgos identificados, siguiendo la evaluación del riesgo, se necesita realizar una decisión del tratamiento del riesgo. Posibles opciones para el tratamiento del riesgo incluye:

- a) Aplicar controles apropiados para reducir riesgos.
- b) Riesgos aceptados objetivamente y con conocimiento, satisfaciendo claramente el criterio para la aceptación del riesgo y la política de la organización.

- c) Transferir los riesgos asociados a terceros como son los proveedores y aseguradores.
- d) Evitar riesgos no permitiendo realizar acciones que puedan causar que estos riesgos ocurran.

### **Reducción del riesgo**

Para esta opción se deberá implementar las salvaguardas apropiados para disminuir a un nivel aceptable propuesto por la organización.

Al identificar y seleccionar los salvaguardas es necesario que concuerden las seguridades relacionadas con el riesgo, las vulnerabilidades, y las amenazas identificadas.

Las salvaguardas deben reducir la probabilidad de que la vulnerabilidad sea explotada por las amenazas y que si llegase a ocurrir la amenaza el impacto de esto no sea de mucho riesgo.

### **Aceptación del riesgo**

Se puede dar el caso en que la organización se les presente muchos problemas al implementar controles o no es viable económicamente ya que el control es más costoso que las consecuencias del riesgo. En este caso la mejor decisión sería la de aceptar dicho riesgo y aceptar las consecuencias si el riesgo ocurriese.

### **Transferencia del riesgo**

Esta opción para la organización se da cuando es muy complicada en el ámbito técnico como económico llevar este riesgo a aceptable, podría ser más factible la transferencia del riesgo a un ente aseguradora o a una empresa especializada en dicho riesgo.

## **Evitar el riesgo**

Esta opción se refiere a que la solución al riesgo es la modificación de las actividades del negocio o cadena de actividades para poder evitar la posible ocurrencia del riesgo.

Esta decisión debe ser analizada para que el cambio de alguna actividad para evitar el riesgo no afecte a la parte económica o comercial de la organización.

### **4.9 Selección de controles para reducir los riesgos a un nivel aceptable**

La selección de controles debe ser sustentada por los resultados de la evaluación del riesgo. Las vulnerabilidades con las amenazas asociadas indican donde la protección pudiera ser requerida y qué forma debe tener. Cuando se seleccionan controles para la implementación, un número de factores deben ser considerados:

- Uso de controles.
- Transparencia del usuario.
- Ayuda otorgada a los usuarios para desempeñar su función.
- Relativa fuerza de controles.
- Tipos de funciones desempeñadas.

### **4.10 Valoración de riesgos**

La valoración del riesgo se da una vez terminado el inventario de todos los activos de información, con su respectivo valor de confidencialidad, integridad y disponibilidad; la valoración de las amenazas, en este caso, se desglosó en degradación de activo y probabilidad de ocurrencia, la cual se hace un promedio para sacar el valor total de la amenaza y por último el valor de las vulnerabilidades.

## EJEMPLO

- **Valoración del Activo – A**

**Tabla 20** - Tabla Ejemplo de Valoración de activos

<b>Activo</b>	<b>Valor</b>
A.1 - Confidencialidad	1
A.2 - Integridad	2
A.3 - Disponibilidad	3

**Elaborado por:** Los Autores

- **Valoración de la Amenaza – B**

**Tabla 21** - Tabla Ejemplo de Valoración de Amenazas

<b>Amenaza</b>		<b>Valor</b>
<b>B.1.</b> Degradación de activo	<b>B.2.</b> Probabilidad de ocurrencia	<b>B=((B.1+B.2)/2)</b>
3	3	3

**Elaborado por:** Los Autores

- **Valoración de la Vulnerabilidad – C**

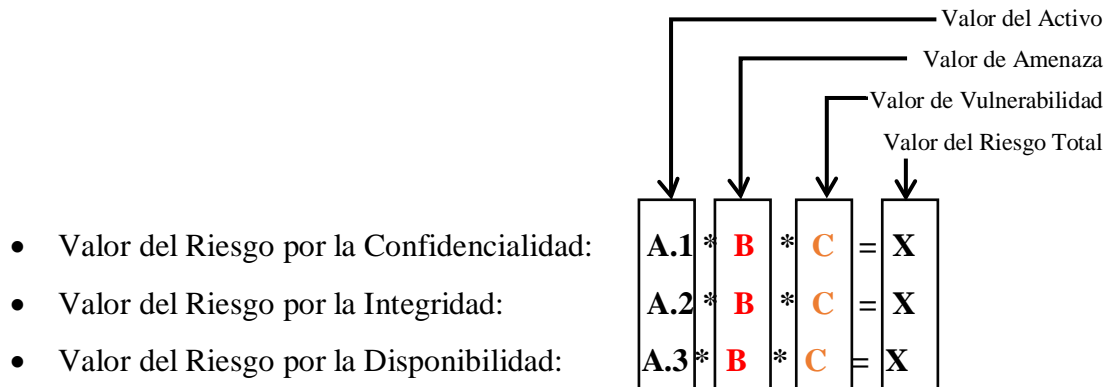
**Tabla 22** - Tabla Ejemplo de Valoración de Vulnerabilidad

<b>Vulnerabilidad</b>	<b>Valor</b>
C - Vulnerabilidad	1

**Elaborado por:** Los Autores



Una vez obtenido todos estos valores se procede a calcular los riesgos por confidencialidad, integridad y disponibilidad de la siguiente manera:



Una vez explicada la formula quedara de la siguiente manera reemplazando las variables por constantes:

- Valor del Riesgo por la Confidencialidad:  $1 * 3 * 1 = 3$
- Valor del Riesgo por la Integridad:  $2 * 3 * 1 = 6$
- Valor del Riesgo por la Disponibilidad:  $3 * 3 * 1 = 9$

En base a la información obtenida se puede realizar este cálculo y determinar el valor de riesgo de cada activo.

Una vez que tenemos la valoración de los riesgos por disponibilidad, integridad y confidencialidad procederemos a ver si el activo se somete a la reducción, aceptación, transferencia o evitar el riesgo.

Si el valor del riesgo supera la puntuación de 6 se procederá a reducir, transferencia o evitar, caso contrario a la aceptación del mismo. **(Ver Anexo A.11)**

**Tabla 23** - Tabla Ejemplo de Valoración del Riesgo

ACTIVO	VALOR DEL ACTIVO			AMENAZA			VULNERABILIDAD		VALORACION DEL RIESGO		
	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	DESCRIPCION	DEGRADACIÓN DE ACTIVO	PROBABILIDAD DE OCURENCIA	DESCRIPCION	CONTROL DE SEGURIDAD	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
TRANSACCION DE PAGO A PROVEEDORES	1	2	3	Errores de Usuario	2	2	Falta de capacitación	1	4,5	4,5	4,5
	3	3	3	Caída del sistema por agotamiento de recursos	1	1	Equipos con características mínimas para el trabajo	3	9	9	9

Elaborado por: Los Autores

## 4.11 Software empleado en identificación de amenaza

**Wireshark** es un analizador de protocolos de red, con interfaz gráfico, que permitirá capturar las tramas que entran y salen del ordenador para luego "diseccionarlas" y estudiar el contenido de las mismas. Wireshark, emplea la misma librería de captura de paquetes (libpcap) que otros sniffers conocidos, como tcpdump, aunque es capaz de leer muchos otros tipos de formato de captura, probablemente, lo más destacable sea su interfaz gráfica y la potente capacidad de filtrado que presenta.



Sirve para realizar análisis y solucionar problemas en redes de comunicaciones, para desarrollo de software y protocolos, y como una herramienta didáctica. Cuenta con todas las características estándar de un analizador de protocolos. Permite ver todo el tráfico que pasa a través de una red estableciendo la configuración en modo promiscuo.

Wireshark es software libre, y se ejecuta sobre la mayoría de sistemas operativos Unix y compatibles, incluyendo Linux, Solaris, FreeBSD, NetBSD, OpenBSD, Android, y Mac OS X, así como en Microsoft Windows.

### 4.11.1 Programa Sniffer

Un sniffer es una herramienta que se emplea para observar los mensajes que intercambian dos entidades en comunicación a través de una red. El sniffer (literalmente "olfateador") captura las tramas a nivel de enlace que se envían/reciben a través de los interfaces de red de las computadora.

Un dato importante es que un "sniffer" es un elemento pasivo: observa los mensajes que intercambian aplicaciones y protocolos, pero no genera información por sí mismo, ni es destinatario de ésta. Las tramas que captura son siempre una copia (exacta) de las que en realidad se envían/reciben en el ordenador.

Un analizador de protocolos es un sniffer al que se le ha dotado de funcionalidad suficiente como para entender y traducir los protocolos que se están hablando en la red. Es de utilidad para desarrollar y depurar protocolos y aplicaciones de red.

#### **4.11.2 Utilización de Wireshark**

- Resolver problemas en la red
- Examinar problemas de seguridad
- Depurar la implementación de los protocolos de red
- Aprender internamente cómo funciona una red
- Captura de paquetes en vivo desde una interfaz de red
- Muestra los paquetes con información detallada de los mismos
- Abre y guarda paquetes capturados
- Importar y exportar paquetes en diferentes formatos
- Filtrado de información de paquetes
- Resaltado de paquetes dependiendo el filtro
- Crear estadísticas

## 4.11.3 Capturas de Pantalla del WireShark

Ilustración 6 - Salvapantalla de Programa WireShark 1

The screenshot displays the Wireshark interface with the following details:

- Filter:** smtp
- Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
6310	39.826390000	192.168.0.2	59.6.151.224	TCP	54	smtp > 57094 [ACK] seq=217 Ack=306 win=233 Len=0
6311	39.857600000	192.168.0.2	202.103.241.169	TCP	54	smtp > 11-ffx [ACK] seq=217 Ack=289 win=253 Len=0
6312	39.871563000	61.164.145.61	192.168.0.2	SMTP	87	C: RCPT TO: <kevfr@gms2.hinet.net>
6313	39.873213000	192.168.0.2	88.247.164.136	SMTP	81	S: 550 5.7.1 unable to relay
6314	39.888821000	192.168.0.2	218.18.106.89	SMTP	84	C: RCPT TO: <pev@yahoo.com.tw>
6315	39.892819000	114.215.110.123	192.168.0.2	SMTP	81	S: 550 5.7.1 unable to relay
6316	39.904427000	192.168.0.2	194.40.210.2	SMTP	81	S: 550 5.7.1 unable to relay
6317	39.912593000	60.12.220.8	192.168.0.2	TCP	60	tr-fm-event > smtp [ACK] Seq=236 Ack=217 Win=252 Len=0
6318	39.914080000	212.83.186.216	192.168.0.2	SMTP	92	C: RCPT TO: <shantatffan@yahoo.com.tw>
6319	39.951178000	192.168.0.2	218.5.2.198	TCP	54	smtp > 65013 [ACK] seq=217 Ack=295 win=255 Len=0
6320	39.963590000	121.127.234.151	192.168.0.2	TCP	60	Fhpjip > smtp [ACK] Seq=257 Ack=217 Win=255 Len=0
6321	39.964448000	58.216.156.126	192.168.0.2	SMTP	88	C: RCPT TO: <11fd4@gms1.hinet.net>
6322	39.968993000	203.91.1119.146	192.168.0.2	SMTP	86	C: RCPT TO: <013876@yahoo.com.tw>
6323	40.008671000	88.85.228.70	192.168.0.2	SMTP	98	C: RCPT TO: <maria.yvd@yahoo.com.tw>
6324	40.049683000	222.198.128.76	192.168.0.2	SMTP	102	C: RCPT TO: <0602710ve0931406451ng@yahoo.com.tw>
6325	40.073601000	88.247.164.136	192.168.0.2	TCP	60	81436 > smtp [ACK] Seq=278 Ack=217 Win=231 Len=0
6326	40.073601000	192.168.0.2	91.164.153.61	SMTP	81	S: 550 5.7.1 unable to relay
6327	40.073601000	192.168.0.2	91.164.153.61	SMTP	81	S: 550 5.7.1 unable to relay
6328	40.080347000	159.282.166.100	192.168.0.2	SMTP	87	C: RCPT TO: <v3shantatffan@yahoo.com.tw>
6329	40.084597000	218.18.106.89	192.168.0.2	TCP	60	46251 > smtp [ACK] Seq=243 Ack=217 Win=255 Len=0
6330	40.105600000	194.40.210.2	192.168.0.2	TCP	60	53454 > smtp [ACK] Seq=233 Ack=298 Win=65280 Len=0
6331	40.107120000	192.168.0.2	114.215.110.123	TCP	54	smtp > 63789 [ACK] Seq=217 Ack=248 Win=256 Len=0
6332	40.122770000	192.168.0.2	212.83.186.216	TCP	54	smtp > 63789 [ACK] Seq=217 Ack=302 Win=233 Len=0
6333	40.123402000	192.168.0.2	60.164.184.50	SMTP	81	S: 550 5.7.1 unable to relay
6334	40.123525000	192.168.0.2	194.40.210.2	SMTP	81	S: 550 5.7.1 unable to relay
6335	40.141930000	192.168.0.73	192.168.0.2	TPKT	91	Continuation
6336	40.154090000	192.168.0.2	192.168.0.73	TPKT	491	Continuation
6337	40.169380000	192.168.0.2	88.216.136.126	TCP	54	smtp > 36682 [ACK] Seq=232 Ack=276 Win=231 Len=0
- Packet Details:**
  - Ethernet II, Src: Mikrotic, Dst: Hewlett-Packard (08:00:27:48:4b:07:4d) (Use: Hwaddr\_45:72:c2 (d4:85:64:45:72:c2))
  - Internet Protocol Version 4, Src: 192.168.0.73, Dst: 192.168.0.2 (192.168.0.2)
  - Transmission Control Protocol, Src Port: 60815 (60815), Dst Port: ms-wbt-server (3389), Seq: 1, Ack: 1, Len: 37
- Packet Bytes:** 0000 64 85 64 45 2a c2 00 22 4d 4b 07 4d 08 00 45 00 ..dE..M..M..E.  
0010 00 4d 4b 5d 40 00 80 06 2d b2 c0 48 00 49 c0 a8 .MKJb...I..  
0020 00 00 7f 8f 00 00 17 0d 09 30 07 64 47 23 63 .N...G.P..  
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 ..G.P..  
0040 94 23 97 91 00 80 36 83 af 3e f8 39 18 0e .#.....6...>H.C  
0050 5e 5b 03 7e 1c fe 02 0f 2a 7c fe  
0060 ..>H.C

Fuente: Programa WireShark 1.12.4

## Ilustración 7 - Salvapantalla de Programa WireShark 2

The screenshot displays the Wireshark interface with a list of captured packets and a detailed view of a selected packet.

**Packet List:**

No.	Time	Source	Destination	Protocol	Length	Info
6	0.031854000	192.168.0.2	211.149.226.138	SMTP	81	S: 530 5.7.1 Unable to relay
7	0.031854000	192.168.0.2	88.247.164.136	SMTP	81	S: 530 5.7.1 Unable to relay
17	0.123497000	192.168.0.2	162.222.169.38	SMTP	81	S: 530 5.7.1 Unable to relay
24	0.162229000	88.85.228.70	192.168.0.2	SMTP	91	C: RCPT TO: <v000792000@yahoo.com.tw>
29	0.219024000	192.168.0.2	162.222.169.38	SMTP	81	S: 530 5.7.1 Unable to relay
30	0.219068000	192.168.0.2	88.247.164.136	SMTP	81	S: 530 5.7.1 Unable to relay
33	0.234611000	192.168.0.2	59.6.151.247	SMTP	81	S: 530 5.7.1 Unable to relay
34	0.250197000	192.168.0.2	222.198.128.76	SMTP	81	S: 530 5.7.1 Unable to relay
35	0.250255000	192.168.0.2	64.185.111.10	SMTP	81	S: 530 5.7.1 Unable to relay
38	0.281387000	192.168.0.2	218.28.1.2	SMTP	81	S: 530 5.7.1 Unable to relay
39	0.281462000	192.168.0.2	201.91.64.109	SMTP	81	S: 530 5.7.1 Unable to relay
40	0.281520000	192.168.0.2	59.6.151.224	SMTP	81	S: 530 5.7.1 Unable to relay
41	0.313888000	162.222.169.38	192.168.0.2	SMTP	88	C: RCPT TO: <myshead2@yahoo.com.tw>
42	0.331020000	61.164.145.61	192.168.0.2	SMTP	91	C: RCPT TO: <pat03042002@yahoo.com.tw>
44	0.344402000	192.168.0.2	64.185.111.10	SMTP	81	S: 530 5.7.1 Unable to relay
50	0.378208000	192.168.0.2	203.91.119.146	SMTP	81	S: 530 5.7.1 Unable to relay
52	0.404697000	162.222.169.38	192.168.0.2	SMTP	92	C: RCPT TO: <andy@c631021@yahoo.com.tw>
53	0.421748000	192.168.0.2	162.222.169.38	SMTP	81	S: 530 5.7.1 Unable to relay
58	0.472578000	64.185.111.10	192.168.0.2	SMTP	92	C: RCPT TO: <charlypoter_v@hotmail.com>
64	0.539715000	119.252.166.100	192.168.0.2	SMTP	87	C: RCPT TO: <yaozsar@yahoo.com.tw>
67	0.568859000	64.185.111.10	192.168.0.2	SMTP	86	C: RCPT TO: <lamhdn0124@msn.com>
69	0.571525000	88.85.228.70	192.168.0.2	SMTP	91	C: RCPT TO: <ommoj00323@yahoo.com.tw>
70	0.592444000	192.168.0.2	218.52.2.98	SMTP	81	S: 530 5.7.1 Unable to relay
71	0.608416000	211.149.226.138	192.168.0.2	SMTP	84	C: RCPT TO: <myt2@yahoo.com.tw>
73	0.614302000	162.222.169.38	192.168.0.2	SMTP	60	C: RSET
74	0.640204000	192.168.0.2	119.252.166.100	SMTP	81	S: 530 5.7.1 Unable to relay
75	0.655793000	192.168.0.2	66.216.213.39	SMTP	81	S: 530 5.7.1 Unable to relay
76	0.660252000	59.6.151.247	192.168.0.2	SMTP	88	C: RCPT TO: <homesen@yahoo.com.tw>

**Packet 76 Details:**

- Frame 6: 81 bytes on wire (648 bits), 81 bytes captured (648 bits) on interface 0
- Ethernet II, Src: Hewlett-45:2a:c2 (d4:85:64:45:2a:c2), Dst: Hewlett-F7:d9:10 (00:22:64:f7:d9:10)
- Internet Protocol Version 4, Src: 192.168.0.2 (192.168.0.2), Dst: 211.149.226.138 (211.149.226.138)
- Transmission Control Protocol, Src Port: smtp (25), Dst Port: smtp (25), Seq: 21571, Len: 1, Ack: 1, Win: 27
- Simple Mail Transfer Protocol

**Packet 76 Hex:**

```

0000 00 22 64 f7 d9 10 d4 85 64 45 2a c2 08 00 45 00  .d....de....E.
0010 00 43 6a 88 40 00 06 00 00 c0 38 00 02 05 95  .CJ.0...0...
0020 00 0f 70 00 00 00 35 30 20 55 22 57 2e 31 20  ..*..c55 0'5'7.1.
0030 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..*..c55 0'5'7.1.
0040 55 6e 61 62 6c 65 20 74 6f 20 72 65 6c 61 79 0d  Unab...t o relay.

```

Fuente: Programa WireShark 1.12.4

## 4.12 Análisis de los resultados e interpretación de datos

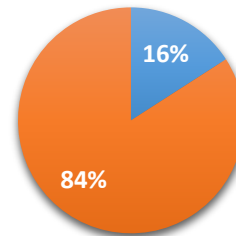
### 4.12.1 Total de Activos afectados

Tabla 24 - Tabla Total de Activos Afectados

<b>Total activos no afectados</b>	<b>7</b>
<b>Total activos afectados</b>	<b>37</b>
<b>TOTAL ACTIVOS</b>	<b>44</b>

Elaborado por: Los Autores

**% DE ACTIVOS QUE SON AFECTADOS AL MENOS POR UNA AMENAZA**  
**% DE ACTIVOS QUE SON AFECTADOS AL MENOS POR UNA AMENAZA**



■ Total activos no afectados  
 ■ Total activos afectados

Tabla 25 - Tabla de Activos Afectados y NO Afectados

ACTIVOS AFECTADOS	ACTIVOS NO AFECTADOS
ANTIVIRUS	DIRECTORIO ACTIVO
APLICACIONES ADMINISTRATIVAS Y RECURSOS HUMANOS	MANUALES
CABLEADO ESTRUCTURADO	MOTOR DE BASE DE DATOS
CORREO ELECTRONICO	NETWORKING
DATA CENTER PLANTA	NORMAS, POLITICAS Y PROCEDIMIENTOS DEL AREA
DISCOS DUROS USB DE RESPALDOS	SOPORTE EVOLUTION
ESTACIONES DE TRABAJO - COMPUTADORA - CONTABILIDAD	TRANSACCION DE COTIZACIONES Y COMPRAS
ESTACIONES DE TRABAJO - COMPUTADORA - TALENTO HUMANO	
ESTACIONES DE TRABAJO - COMPUTADORA - PRODUCCION	
ESTACIONES DE TRABAJO - COMPUTADORA - SISTEMAS	
ESTACIONES DE TRABAJO - COMPUTADORA - LOGISTICA	
ESTACIONES DE TRABAJO - COMPUTADORA - VENTAS	
ESTACIONES DE TRABAJO - COMPUTADORA - COMPRAS	
RESPALDO DE SERVIDORES	
ROUTER DE COMUNICACIONES	
SERVICIO DE INTERNET	
SERVICIO DE REDIRECCIONAMIENTO DE CARPETAS	
SERVIDOR DE ACTUALIZACIONES Y ANTIVIRUS	
SERVIDOR DE CARPETAS COMPARTIDAS	
SERVIDOR DE CORREO ELECTRÓNICO	
SERVIDOR DE DIRECTORIO ACTIVO	
SERVIDOR DE INTERNET PROXY – FIREWALL	
SERVIDOR DE RESPALDO	

SERVIDORES DE APLICACIÓN Y BASE DE DATOS
SERVIDORES PARA CÁMARAS IP
SOFTWARE ACTUALIZACIONES SISTEMA OPERATIVO
SOFTWARE CAMARAS IP
SOFTWARE PROXY - FIREWALL
SOPORTE OPENSIDE
SOPORTE TÉCNICO
SWITCH DE COMUNICACIONES
TELEFONÍA FIJA
TRANSACCION DE PAGO A PROVEEDORES
TRANSACCION DE PAGO DE NOMINAS
TRANSACCION DE REGISTRO DE FACTURA Y COBRANZA
TRANSACCION DE REGISTRO DE INVENTARIO A BODEGA
USUARIOS DE LA ORGANIZACIÓN

Elaborado por: Los Autores

#### 4.12.2 Amenazas que afectan a los activos

Tabla 26 - Tabla Porcentaje de afectación de activos

<b>AMENAZA</b>	<b>% DE AFECTACIÓN X TOTAL DE ACTIVOS</b>
<b>Caída del sistema por agotamiento de recursos</b>	<b>34,09%</b>
<b>Condiciones inadecuadas de temperatura y humedad</b>	<b>45,45%</b>
<b>Corte de suministro eléctrico</b>	<b>43,18%</b>
<b>Daños por agua</b>	<b>45,45%</b>
<b>Fuego</b>	<b>45,45%</b>
Desastres industriales (fuga de amoníaco)	2,27%
Difusión de software dañino	4,55%
Errores de mantenimiento actualización de programas	9,09%
Errores de usuario	11,36%
Indisponibilidad del personal	2,27%
Manipulación de equipos	15,91%
Manipulación de programas	2,27%
Restauración fallida de respaldos	2,27%



Suplantación de identidad	9,09%
Uso no previsto de recursos	6,82%
Vulnerabilidades de los programas	4,55%

Elaborado por: Los Autores

Ilustración 8 - Numero de Activos afectados por amenazas



Elaborado por: Los Autores

#### 4.12.3 Detalle de activos afectados clasificados por riesgos

Tabla 27 - Detalle de activos afectados

RIESGO	ACTIVOS QUE AFECTA
<b>CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD</b>	Cableado estructurado
	Data center planta
	Servidor de directorio activo
	Servidor de correo electrónico
	Servidor de internet proxy – firewall
	Servidor de carpetas compartidas
	Servidores de aplicación y base de datos
	Servidor de respaldo
	Servidor de actualizaciones y antivirus
	Servidores para cámaras ip
	Router de comunicaciones
	Switch de comunicaciones
	Estaciones de trabajo
	Discos duros USB de respaldos
<b>DAÑOS POR AGUA</b>	Cableado estructurado
	Data center planta
	Servidor de directorio activo
	Servidor de correo electrónico
	Servidor de internet proxy – firewall
	Servidor de carpetas compartidas
	Servidores de aplicación y base de datos
	Servidor de respaldo
	Servidor de actualizaciones y antivirus
	Servidores para cámaras ip
	Router de comunicaciones
	Switch de comunicaciones
	Estaciones de trabajo

	Discos duros USB de respaldos
	Cableado estructurado
	Data center planta
	Servidor de directorio activo
	Servidor de correo electrónico
	Servidor de internet proxy – firewall
	Servidor de carpetas compartidas
	Servidores de aplicación y base de datos
<b>FUEGO</b>	Servidor de respaldo
	Servidor de actualizaciones y antivirus
	Servidores para cámaras ip
	Router de comunicaciones
	Switch de comunicaciones
	Estaciones de trabajo
	Discos duros USB de respaldos
	Cableado estructurado
	Servidor de directorio activo
	Servidor de correo electrónico
	Servidor de internet proxy – firewall
	Servidor de carpetas compartidas
	Servidores de aplicación y base de datos
<b>CORTE DE SUMINISTRO ELECTRICO</b>	Servidor de respaldo
	Servidor de actualizaciones y antivirus
	Servidores para cámaras ip
	Router de comunicaciones
	Switch de comunicaciones
	Estaciones de trabajo
	Discos duros USB de respaldos
<b>CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS</b>	Transacción de pago a proveedores
	Transacción de pago de nominas

	Transacción de registro de inventario a bodega
	Transacción de registro de factura y cobranza
	Servicio de internet
	Servidor de correo electrónico
	Servidor de carpetas compartidas
	Estaciones de trabajo
	Discos duros USB de respaldos
<b>ERRORES DE USUARIO</b>	Soporte técnico
	Soporte openside
	Correo electrónico
	Aplicaciones administrativas y recursos humanos
	Software cámaras ip
<b>ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS</b>	Software actualizaciones sistema operativo
	Software proxy - firewall
	Aplicaciones administrativas y recursos humanos
	Respaldo de servidores
<b>SUPLANTACIÓN DE IDENTIDAD</b>	Transacción de pago a proveedores
	Transacción de registro de inventario a bodega
	Correo electrónico
	Aplicaciones administrativas y recursos humanos
<b>USO NO PREVISTO DE RECURSOS</b>	Telefonía fija
	Soporte técnico
	Servicio de redireccionamiento de carpetas
<b>DIFUSION DE SOFTWARE DAÑO</b>	Software proxy - firewall
	Antivirus
<b>VULNERABILIDADES DE LOS PROGRAMAS</b>	Aplicaciones administrativas y recursos humanos
	Software cámaras ip
<b>DESASTRES INDUSTRIALES (FUGA DE AMONIACO)</b>	Usuarios de la organización
<b>INDISPONIBILIDAD DEL PERSONAL</b>	Usuarios de la organización

<b>MANIPULACION DE EQUIPOS</b>	Estaciones de trabajo
<b>MANIPULACIÓN DE PROGRAMAS</b>	Software proxy - firewall
<b>RESTAURACIÓN FALLIDA DE RESPALDOS</b>	Respaldo de servidores

Elaborado por: Los Autores

#### **4.13 Verificación de la hipótesis**

La hipótesis planteada: “Las políticas definidas actualmente en la organización permiten identificar y prevenir riesgos en la seguridad de la información.” se verifica como falsa.

Con los resultados de las encuestas y entrevistas realizadas al personal de la organización, se pudo realizar el análisis de riesgo a cada activo del departamento. Con esto se pudo determinar que las políticas existentes en el departamento no permiten identificar las amenazas a las que se encuentran expuestos los activos; además se considera necesario controles que ayuden a disminuir el riesgo de pérdida de información y asegure la continuidad de los procesos de la empresa.

#### **4.14 Resumen de riesgos detectados en la empresa y sus controles seleccionados**

En esta sección se determinó los riesgos encontrados en la empresa y que estarían afectando a diferentes procesos. A cada riesgo se asignan diferentes controles basado en la norma ISO 27001.

En los siguientes cuadros se puede identificar el riesgo observado y determinado por medio de la matriz de amenazas, el proceso al que afecta y las acciones que permitirán que este riesgo disminuya lo máximo posible.

**4.14.1 Procesos críticos, resumen de riesgos detectados en la empresa y sus controles seleccionados**

**Tabla 28** - Acciones y Controles – Riesgo: Condiciones Inadecuadas de Temperatura

<b>RIESGO: CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD.</b>	
<b>Activo al que afecta:</b>	Redes, Instalaciones, Equipos informáticos, Aplicaciones informáticos, Servicios.
<b>ACCIONES – CONTROL</b>	
<b>A.9 SEGURIDAD FÍSICA Y AMBIENTAL</b>	
<b>A.9.1 Áreas seguras:</b>	Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.
A.9.1.1 Perímetro de seguridad física	Control: Deben de existir perímetros de seguridad (tales como paredes, tarjetas de control de entrada) para proteger áreas que contengan información de recursos y medios de procesamiento de información.
A.9.1.2 Controles de entrada físicos	Control: Las áreas de seguridad deben ser protegidas por controles de entrada adecuados que aseguren el acceso sólo al personal autorizado.
A.9.1.4 Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
<b>A.9.2 Seguridad del equipo</b>	Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización

A.9.2.1 Ubicación y protección del Equipo	Control: El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.4 Mantenimiento de equipo	Control: El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.

**Elaborado por:** Los Autores

**Tabla 29 - Acciones y Controles – Riesgo: Daños por Agua**

<b>RIESGO: DAÑOS POR AGUA</b>	
<b>Activo al que afecta:</b>	Redes, Instalaciones, Equipos informáticos, Aplicaciones informáticos, Servicios.
<b>ACCIONES – CONTROL</b>	
<b>A.9 SEGURIDAD FÍSICA Y AMBIENTAL</b>	
<b>A.9.1 Áreas seguras:</b>	Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.
A.9.1.1 Perímetro de seguridad física	Control: Deben de existir perímetros de seguridad (tales como paredes, tarjetas de control de entrada) para proteger áreas que contengan información de recursos y medios de procesamiento de información.
A.9.1.2 Controles de entrada físicos	Control: Las áreas de seguridad deben ser protegidas por controles de entrada adecuados que aseguren el acceso sólo al personal autorizado.
A.9.1.4 Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y

	otras formas de desastre natural o creado por el hombre.
<b>A.9.2 Seguridad del equipo</b>	Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
A.9.2.1 Ubicación y protección del Equipo	Control: El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.3 Seguridad en el cableado	Control: El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la interceptación o daño.
<b>Elaborado por:</b> Los Autores	

**Tabla 30** - Acciones y Controles – Riesgo: Fuego

<b>RIESGO: FUEGO</b>	
<b>Activo al que afecta:</b>	Redes, Instalaciones, Equipos informáticos, Aplicaciones informáticos, Servicios, Personas.
<b>ACCIONES – CONTROL</b>	
<b>A.9 SEGURIDAD FÍSICA Y AMBIENTAL</b>	
<b>A.9.1 Áreas seguras:</b>	Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.
A.9.1.1 Perímetro de seguridad física	Control: Deben de existir perímetros de seguridad (tales como paredes, tarjetas de control de entrada) para proteger áreas que contengan información de recursos y medios de procesamiento de información.



A.9.1.2 Controles de entrada físicos	Control: Las áreas de seguridad deben ser protegidas por controles de entrada adecuados que aseguren el acceso sólo al personal autorizado.
A.9.1.4 Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
<b>A.9.2 Seguridad del equipo</b>	Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
A.9.2.1 Ubicación y protección del equipo	Control: El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.3 Seguridad en el cableado	Control: El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la interceptación o daño.
<b>Elaborado por:</b> Los Autores	

**Tabla 31 - Acciones y Controles – Riesgo. Corte de suministro eléctrico**

<b>RIESGO: CORTE DE SUMINISTRO ELÉCTRICO</b>	
<b>Activo al que afecta:</b>	Redes, Equipos informáticos, Aplicaciones informáticas, Servicios.
<b>ACCIONES – CONTROL</b>	
<b>A.9 SEGURIDAD FÍSICA Y AMBIENTAL</b>	
<b>A.9.2 Seguridad del equipo</b>	Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción

	de las actividades de la organización
A.9.2.2 Servicios Públicos	Control: El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.

**Elaborado por:** Los Autores

**Tabla 32 - Acciones y Controles – Riesgo: Caída del sistema por agotamiento de recursos**

<b>RIESGO: CAÍDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS.</b>	
<b>Activo al que afecta:</b>	Redes, Equipos informáticos, Aplicaciones informáticas, Servicios.
<b>ACCIONES – CONTROL</b>	
<b>A.9 SEGURIDAD FÍSICA Y AMBIENTAL</b>	
<b>A.9.2 Seguridad del equipo</b>	Objetivo: Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización
A.9.2.4 Mantenimiento de equipos	Control: El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
<b>A.10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES</b>	
<b>A.10.3 Planeación y aceptación del sistema</b>	Objetivo: Minimizar el riesgo de fallas en los sistemas.
A.10.3.1 Gestión de capacidad	Control: Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.

**Elaborado por:** Los Autores

Tabla 33 - Acciones y Controles – Riesgo: Errores de usuario

<b>RIESGO: ERRORES DE USUARIO</b>	
<b>Activo al que afecta:</b>	Redes, Equipos informáticos, Aplicaciones informáticos, Servicios.
<b>ACCIONES – CONTROL</b>	
<b>A.8 SEGURIDAD DE LOS RECURSOS HUMANOS</b>	
<b>A.8.1 Antes del empleo</b>	Objetivo: Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.
A.8.1.1 Roles y responsabilidades	Control: Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
<b>A.8.2 Durante el empleo</b>	Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas e inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.
A.8.2.2 Capacitación y educación en seguridad de la información	Control: Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.

A.8.2.3 Proceso disciplinario	Control: Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
-------------------------------	--

## **A.10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES**

<b>A.10.1 Procedimientos y responsabilidades operacionales</b>	Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información
A.10.1.1 Procedimientos de operación documentados	Control: Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.

**Elaborado por:** Los Autores

**Tabla 34** - Acciones y Controles – Riesgo: Errores de mantenimiento y actualización de programas

### **RIESGO: ERRORES DE MANTENIMIENTO Y ACTUALIZACIÓN DE PROGRAMAS.**

**Activo al que afecta:** Aplicaciones informáticos, Servicios.

#### **ACCIONES – CONTROL**

### **A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN**

<b>A.12.1 Requerimientos de seguridad de los sistemas</b>	Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.
A.12.1.1 Análisis y especificación de Los requerimientos de seguridad	Control: Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.

<b>A.12.2 Procesamiento correcto en las aplicaciones</b>	Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.
A.12.2.1 Validación de data de Insumo	Control: El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
A.12.2.2 Control de procesamiento interno	Control: Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.
A.12.2.3 Integridad del mensaje	Control: Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
A.12.2.4 Validación de data de output	Control: Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
<b>A.12.4 Seguridad de los archivos del sistema</b>	Objetivo: Garantizar la seguridad de los archivos del sistema
A.12.4.1 Control de software operacional	Control: Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
<b>A.12.5 Seguridad en los procesos de desarrollo y soporte</b>	Objetivo: Mantener la seguridad del software e información del sistema de aplicación

A.12.5.1 Procedimientos de control de cambio	Control: La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
A.12.5.2 Revisión técnica de las aplicaciones después de cambios en el sistema operativo	Control: Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
<b>Elaborado por:</b> Los Autores	

**Tabla 35 - Acciones y Controles – Riesgo: Suplantación de identidad**

<b>RIESGO: SUPLANTACIÓN DE IDENTIDAD</b>	
<b>Activo al que afecta:</b> Aplicaciones informáticos, Personas.	
<b>ACCIONES – CONTROL</b>	
<b>A.8 SEGURIDAD DE LOS RECURSOS HUMANOS</b>	
<b>A.8.3 Terminación o cambio del empleo</b>	Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.
A.8.3.3 Eliminación de derechos de acceso	Control: Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
<b>A.11 CONTROL DE ACCESO</b>	

<b>A.11.2 Gestión del acceso del usuario</b>	Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no autorizado a los sistemas de información.
A.11.2.1 Inscripción del usuario	Control: Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2 Gestión de privilegios	Control: Se debe restringir y controlar la asignación y uso de los privilegios.
<b>A.11.3 Responsabilidades del usuario</b>	Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.
A.11.3.1 Uso de clave	Control: Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2 Equipo de usuario desatendido	Control: Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido
<b>A.11.5 Control de acceso al sistema de operación</b>	Objetivo: Evitar acceso no autorizado a los sistemas operativos.
A.11.5.2 Identificación y autenticación del usuario	Control: Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.
A.11.5.5 Sesión inactiva	Control: Las sesiones inactivas deben cerrarse después de un período de inactividad definido.

**Elaborado por:** Los Autores

**Tabla 36 - Acciones y Controles – Riesgo: Uso no previsto de recursos**

<b>RIESGO: USO NO PREVISTO DE RECURSOS.</b>	
<b>Activo al que afecta:</b>	Redes, Equipos informáticos, Aplicaciones informáticos, Servicios.
<b>ACCIONES – CONTROL</b>	
<b>A.7 GESTIÓN DE ACTIVOS</b>	
<b>A.7.1 Responsabilidad por los activos</b>	Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.
A.7.1.3 Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
<b>A.10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES</b>	
<b>A.10.7 Gestión de medios</b>	Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no autorizada de los activos; y la interrupción de las actividades comerciales.
A.10.7.1 Gestión de los medios removibles	Control: Deben existir procedimientos para la gestión de medios removibles.
<b>Elaborado por:</b> Los Autores	

**Tabla 37 - Acciones y Controles – Riesgo: Difusión de software dañino**

<b>RIESGO: DIFUSIÓN DE SOFTWARE DAÑINO.</b>	
<b>Activo al que afecta:</b>	Redes, Equipos informáticos, Aplicaciones informáticos, Servicios.
<b>ACCIONES – CONTROL</b>	
<b>A.10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES</b>	



<b>A.10.4 Protección contra software malicioso y código móvil</b>	Objetivo: Proteger la integridad del software y la información.
A.10.4.1 Controles contra software malicioso	Control: Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
<b>Elaborado por:</b> Los Autores	

**Tabla 38** - Acciones y Controles – Riesgo: Vulnerabilidad de los programas

<b>RIESGO: VULNERABILIDAD DE LOS PROGRAMAS.</b>	
<b>Activo al que afecta:</b> Aplicaciones informáticos, Servicios.	
<b>ACCIONES – CONTROL</b>	
<b>A.10 GESTIÓN DE LAS COMUNICACIONES Y OPERACIONES</b>	
<b>A.10.3 Planeación y aceptación del sistema</b>	Objetivo: Minimizar el riesgo de fallas en los sistemas.
A.10.3.1 Gestión de capacidad	Control: Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.3.2 Aceptación del sistema	Control: Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
<b>A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN</b>	
<b>A.12.6 Gestión de vulnerabilidad técnica</b>	Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.

A.12.6.1 Control de vulnerabilidades Técnicas	Control: Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
---	---

**Elaborado por:** Los Autores

**Tabla 39 - Acciones y Controles – Riesgo: Desastres industriales (Fugas de Amoniaco)**

<b>RIESGO: DESASTRES INDUSTRIALES (FUGAS DE AMONIACO).</b>	
<b>Activo al que afecta:</b> Personas.	
<b>ACCIONES – CONTROL</b>	
<b>A.9 SEGURIDAD FÍSICA Y AMBIENTAL</b>	
<b>A.9.1 Áreas seguras</b>	Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.
A.9.1.3 Seguridad de oficinas, habitaciones y medios	Control: Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4 Protección contra amenazas externas y ambientales	Control: Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.9.1.5 Trabajo en áreas seguras	Control: Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.

**Elaborado por:** Los Autores

**Tabla 40 - Acciones y Controles – Riesgo: Indisponibilidad del personal**

<b>RIESGO: INDISPONIBILIDAD DEL PERSONAL.</b>	
<b>Activo al que afecta:</b> Personas.	
<b>ACCIONES – CONTROL</b>	
<b>A.14 GESTIÓN DE LA CONTINUIDAD COMERCIAL</b>	
<b>A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial</b>	Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.
A.14.1.3 Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Control: Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
<b>Elaborado por:</b> Los Autores	

**Tabla 41 - Acciones y Controles – Riesgo: Manipulación de equipos**

<b>RIESGO: MANIPULACIÓN DE EQUIPOS</b>	
<b>Activo al que afecta:</b> Redes, Equipos informáticos, Aplicaciones informáticos.	
<b>ACCIONES – CONTROL</b>	
<b>A.7 GESTIÓN DE ACTIVOS</b>	
<b>A.7.1 Responsabilidad por los activos</b>	Objetivo: Lograr y mantener la protección apropiada de los activos organizacionales.
A.7.1.1 Inventarios de activos	Control: Todos los activos deben estar claramente identificados; y se debe elaborar y

	mantener un inventario de todos los activos importantes.
A.7.1.2 Propiedad de los activos	Control: Toda la información y los activos asociados con los medios de procesamiento de la información deben ser ‘propiedad’ de una parte designada de la organización.
A.7.1.3 Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
<b>Elaborado por:</b> Los Autores	

**Tabla 42 - Acciones y Controles – Riesgo: Manipulación de programas**

<b>RIESGO: MANIPULACIÓN DE PROGRAMAS</b>	
<b>Activo al que afecta:</b> Aplicaciones informáticos, Servicios.	
<b>ACCIONES – CONTROL</b>	
<b>A.12 ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN</b>	
<b>A.12.5 Seguridad en los procesos de desarrollo y soporte</b>	Objetivo: Mantener la seguridad del software e información del sistema de aplicación
A.12.5.1 Procedimientos de control de cambio	Control: La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
<b>Elaborado por:</b> Los Autores	

**Tabla 43** - Acciones y Controles – Riesgo: Restauración fallida de los respaldos

<b>RIESGO: RESTAURACIÓN FALLIDA DE RESPALDOS</b>	
<b>Activo al que afecta</b>	Equipos informáticos, Aplicaciones informáticas, Servicios.
<b>ACCIONES – CONTROL</b>	
<b>A.10 GESTION DE LAS COMUNICACIONES Y OPERACIONES</b>	
<b>A.10.5 Respaldo (back-up)</b>	Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.
A.10.5.1 Back-up o respaldo de la información	Control: Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
<b>Elaborado por:</b> Los Autores	

## **CAPÍTULO 5**

### **CONCLUSIONES Y RECOMENDACIONES**

#### **5.1 Conclusiones**

En la evaluación realizada en la empresa se lograron detectar 16 diferentes riesgos que pueden llegar a afectar a 38 activos, para lo cual se seleccionó los controles idóneos en referencia a la norma ISO27001 explicando de forma clara el objetivo de la misma y la respectiva salvaguarda.

Se llega a la conclusión que se deberá implementar los controles seleccionados para el área de TI y a su vez tratar de prever una o varias situaciones que deriven en un siniestro, fallo o daño que pueda generar una paralización parcial o definitiva en las operaciones de la empresa en el ámbito informático.

#### **5.2 Recomendaciones**

Se recomienda que para alcanzar una seguridad de la información aceptable, la empresa deberá aplicar los controles antes mencionados para cada uno de los riesgos encontrados.

Se deberá exigir que los usuarios cumplan con dichos controles para que la empresa no tenga ningún fallo en la parte de informática, llevar controles diarios de los progresos con los controles seleccionados, hacer un buen inventario de activos actualizados, ordenamiento de direcciones ip, estandarización de nombres de usuarios y equipos, monitorear la red para que esta no se vea vulnerable ante ataques que provengan del exterior de la empresa para esto se recomienda el uso de los software especializados Belarc Advisor y Wireshark.

## **CAPÍTULO 6**

### **PROPUESTA**

#### **6.1 Datos informativos**

##### **ACTIVIDAD DE LA EMPRESA**

La empresa LacteoSA es una industria dedicada a la producción y distribución de productos lácteos a nivel nacional. Esta organización está comprometida a elaborar y procesar productos de calidad para mantener su nivel competitivo en el mercado ecuatoriano.

##### **MISION**

Estamos comprometidos a elaborar productos lácteos de excelente calidad que sean la primera elección de los consumidores y clientes del País, empleando la mejor materia prima, recursos tecnológicos de vanguardia y un equipo humano profesional, ético y altamente productivo.

##### **VISION**

Ser la empresa líder con mayor demanda de sus productos, avanzado hacia un desarrollo y fortalecimiento integral, con permanente innovación ideológica, intelectual y tecnológica; ayudando a combatir la desnutrición de la comunidad actual y de las futuras generaciones.

#### **6.2 Antecedentes de la propuesta**

En las empresas, es de vital importancia mantener un aseguramiento de información en los activos que esta maneja, es por esto necesario que la gerencia se preocupe en determinar riesgos presentes que pueden causar daños en las actividades diarias de la organización.

En el departamento de TI de la empresa en estudio, existen políticas establecidas formalmente, pero a pesar de esto, estas no han sido efectivas para poder mantener la correcta seguridad de la información, y los activos se han visto en riesgo ante amenazas internas y externas.

A pesar de los problemas que han existido en la organización, el departamento no se ha preocupado por realizar un análisis para determinar los riesgos latentes en la empresa. Por ende no existen medidas de cómo actuar ante posibles fallos para asegurar la continuidad del negocio.

### **6.3 Justificación**

Es importante señalar que las políticas y procedimientos definidos en los controles propuestos, son la base para mantener una correcta seguridad en la información que maneja la organización. Además promueve la continuidad del negocio con planes de contingencia y ayuda a la gerencia a saber cómo actuar en caso de que se presenten imprevistos en las actividades del día a día.

El departamento de TI contiene activos muy importantes para la organización. Estos activos manejan información que debe de ser resguardada y protegida ante posibles desastres que se presenten en el desarrollo de las actividades diarias de la empresa. La mejor forma de salvaguardar la información valiosa de la empresa, es que el departamento tenga establecidas políticas y procedimientos que permitan brindar una correcta seguridad de la información. Para esto, es recomendable establecer controles basados en estándares que permitan determinar riesgos y cómo actuar ante amenazas presentadas en la organización.

En el análisis de riesgo realizado, se pudo verificar que existen activos del departamento de TI que están expuestos a amenazas, y que si estas ocurren, degradarían el activo de forma crítica. Un ejemplo claro de esto es la infraestructura donde se



encuentran los servidores (cuarto de servidores) el cual no se encuentra debidamente adecuado para la protección de los equipos.

Los controles propuestos y las recomendaciones de los mismos presentadas en el informe, permitirá a la directiva de la organización, integrar una serie de acciones encaminadas a proteger la información y los activos que contienen la misma.

#### **6.4 Objetivos**

El informe realizado tiene como objetivo principal presentar los resultados de las amenazas a las cuales se encuentra expuesto el departamento de TI y los activos del mismo. Además propone una serie de actividades con el fin de ayudar a la directiva a establecer los controles propuestos para mantener una correcta seguridad de la información en el departamento de TI de la organización.

Para que tenga validez y cumpla de mejor manera con su objetivo, las recomendaciones de este informe requieren que sean analizadas por la directiva de la empresa, tomando la decisión de implementar los controles o no, luego de tener claro los beneficios que brindará a la organización. Así también se puede mencionar los siguientes objetivos específicos:

- Indicar las características que debe poseer el cuarto de servidores, tomando en cuenta que este es el activo más crítico de la organización.
- Proponer la creación de políticas que ayuden a mantener la disponibilidad, integridad y confidencialidad de la información utilizada en la organización.
- Proponer la creación de procedimientos que permitan cumplir con las políticas establecidas y con esto aseguren el cumplimiento de su objetivo.

## **6.5 Análisis de factibilidad**

Este informe de evaluación detalla los problemas encontrados en el departamento de TI y recomienda una serie de instrucciones que permite orientar de mejor forma a la implementación de los controles propuestos. Para mantener una seguridad óptima en la información y en los activos que manejan la misma, es necesario realizar un análisis de riesgo y, dependiendo de los resultados, establecer una serie de controles adecuados. Estos controles deben ser implementados de manera correcta, y así, puedan garantizar de forma efectiva la seguridad de la información.

Para establecer estos controles, es recomendable basarse en una serie de instructivos que permitan determinar los lineamientos y objetivos sobre la seguridad de la información. Es por eso que basado en el análisis de riesgo realizado en los capítulos anteriores, se desarrolló este informe que propone recomendaciones que servirán para orientar a la organización, para la correcta implantación de los controles.

La propuesta de la presente Tesis, que se refiere a la elaboración de un informe de evaluación de seguridad de la información, es factible de llevarse a la práctica por cuanto, este fue desarrollado basándose en los resultados del análisis de riesgo realizado, y que ayudó a determinar las falencias y amenazas que ponen en riesgo los activos del departamento de TI y la información manejada por los mismos dentro de la organización.

## **6.6 Fundamentación**

En el informe se estableció como marco referencial las Normas ISO27001, y la Norma Técnica Peruana NTP-ISO/IEC 17799 para la elaboración de la investigación y comparación de la empresa. Basado en estos lineamientos se pudo detectar vulnerabilidades, amenazas y escoger sus controles o salvaguardas correspondientes.

Para realizar las técnicas de recolección de información, cuadros de calificaciones, porcentajes, estimaciones, identificación de activos de forma ordenada, clasificada y normada se usó La Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información MAGERIT V3.0.

De esta manera se mantiene una concordancia del informe con las Normas ISO y el manejo óptimo de los recursos de la empresa guiada por una buena identificación de los procedimientos que indica MAGERIT.

Es así que, las recomendaciones del informe que mostraremos a continuación se basan estrictamente en Normas ISO para su buen funcionamiento y buenos resultados una vez aplicados en la empresa.

## **6.7 Metodología, modelo operativo**

A continuación, se detalla el informe de evaluación de seguridad que se elaboró a partir de los controles seleccionados, luego de haber realizado el análisis de riesgo de los activos del departamento de TI de la organización.

### **6.7.1 Título del informe**

Informe de evaluación de seguridad en la información basada en la norma ISO 27001 en el departamento de TI de una empresa de lácteos.

### **6.7.2 Introducción**

El presente informe se desarrolló con el fin de ayudar al departamento de TI a mejorar las políticas de seguridad existentes y la falta de procedimientos, las cuales no brindaban un apoyo al momento de controlar las amenazas y vulnerabilidades.

Este trabajo ayudará a la organización al momento de crear procedimientos y replantear políticas apegadas a los estándares de seguridad de la ISO, y con esto mejorar la protección y salvaguardar la integridad de la información, las cual es vital para toda empresa.

### **6.7.3 Antecedentes**

En las empresas, es de vital importancia mantener un aseguramiento de información en los activos que esta maneja, es por esto necesario que la gerencia se preocupe en determinar riesgos presentes que pueden causar daños en las actividades diarios de la organización.

En el departamento de TI de la empresa en estudio, existen políticas establecidas formalmente, pero a pesar de esto, estas no han sido efectivas para poder mantener la correcta seguridad de la información, y los activos se han visto en riesgo ante amenazas internas y externas.

A pesar de los problemas que han existido en la organización, el departamento no se ha preocupado por realizar un análisis para determinar los riesgos latentes en la empresa. Por ende no existen medidas de cómo actuar ante posibles fallos para asegurar la continuidad del negocio.

### **6.7.4 Objetivo**

El informe realizado tiene como objetivo principal presentar los resultados de las amenazas a las cuales se encuentra expuesto el departamento de TI y los activos del mismo. Además propone una serie de actividades con el fin de ayudar a la directiva a establecer los controles propuestos para mantener una correcta seguridad de la información en el departamento de TI de la organización.

Para que tenga validez y cumpla de mejor manera con su objetivo, las recomendaciones de este informe requieren que sean analizadas por la directiva de la empresa, tomando la decisión de implementar los controles o no, luego de tener claro los beneficios que brindará a la organización. Así también se puede mencionar los siguientes objetivos específicos:

- Indicar las características que debe poseer el cuarto de servidores, tomando en cuenta que este es el activo más crítico de la organización.
- Proponer la creación de políticas que ayuden a mantener la disponibilidad, integridad y confidencialidad de la información utilizada en la organización.
- Proponer la creación de procedimientos que permitan cumplir con las políticas establecidas y con esto aseguren el cumplimiento de su objetivo.

#### **6.7.5 Alcance**

El alcance de este informe se basa netamente en brindar recomendaciones para que el departamento de TI pueda generar políticas y procedimientos que mitiguen las falencias o carencias de controles en los activos de la organización.

#### **6.7.6 Hallazgos y recomendaciones**

##### **HALLAZGO 1: Falta de un plan de análisis de riesgos sobre los activos y sistemas de información computarizados**

Se pudo determinar que en la empresa no existe un plan de análisis de riesgo para determinar de forma correcta y periódica las amenazas que afectarían a los activos de la organización. Esto se determinó ya que el departamento de TI no tiene definido los riesgos que pueden afectar cada activo de la empresa.

Se realizó el análisis de riesgo basado en la metodología Magerit para determinar los riesgos que tiene cada activo. (**Ver Anexo A.11**)

## **Recomendaciones**

Se recomienda elaborar un plan de análisis de riesgo para poder determinar de forma efectiva los riesgos que afronta cada activo, y de esta forma salvaguardar la seguridad de la información de los mismos.

### **HALLAZGO 2: Deficiencias en infraestructura que brinda seguridad física a los activos del departamento y al entorno. (Ver Anexo A.4)**

- Condiciones inadecuadas de temperatura y humedad: Se encontró que el cuarto de servidores no tiene una buena temperatura la cual perjudicaría la integridad físicas de los mismos.
- Daños por agua: Se encontró deficiencias en la impermeabilización del cielo falso que está encima del cuarto de servidores y esto provoca filtración de agua que ocasionaría daños físicos; además en el cuarto contiguo a la data center se filtró agua ocasionando daños en la pared que da hacia el cuarto de servidores.
- Fuego: No se encontró algún sistema contra incendios (Extintores, detectores de humo, alarmas)
- Corte de suministro eléctrico: No se encontró una correcta protección de los equipos antes las fallas de corte de energía por parte del servicio público.
- Desastres industriales (Fuga de amoníaco): Se determinó que las áreas de trabajo de TI son inseguras por cuanto puede ocurrir fugas de amoníaco que perjudiquen a la salud de los trabajadores, además no se encontró algún plan de contingencia si llegase a ocurrir dicho siniestro.
- Robo: Se determinó que existe muy poca seguridad al momento de acceder al cuarto de servidores (Puertas Dañadas, Cielo raso faltante).

## **Recomendaciones**

Se recomienda implementar los siguientes controles basados en la Norma ISO/IEC 27001-2005:

### **Perímetro de seguridad física**

**(Ver Anexo A.12 - Dominio (9), Objetivo de control (1), Control (1))**

Deben de existir perímetros de seguridad (tales como paredes, tarjetas de control de entrada) para proteger áreas que contengan información de recursos y medios de procesamiento de información.

Los siguientes puntos deben ser considerados al momento de establecer perímetros de seguridad físicos para que estos sean apropiados:

- a) El perímetro de seguridad debe de estar claramente definido y el lugar y fuerza del perímetro dependerá de los requerimientos de seguridad del activo dependiendo de los resultados de la evaluación de riesgos.
- b) El perímetro de un edificio o un lugar que contenga activos de tratamiento de información, debe de tener solidez física (debe de contar con zonas que no puedan derribarse fácilmente). El lugar debe de contar con muros sólidos y las puertas exteriores deben estar protegidas contra accesos no autorizados (mecanismos de control, alarmas, rejas, etc.). Las puertas y ventanas deben permanecer cerradas con llave cuando estén desatendidas.
- c) Deberá de existir medios de control de acceso físico al lugar. Dicho acceso deberá restringirse sólo al personal autorizado.
- d) Las barreras físicas deben extenderse desde el suelo real hasta el techo real, para evitar contaminación del entorno o entradas no autorizadas.
- e) Las puertas para incendios deben de tener alarma, ser monitoreadas y probadas para mantener el nivel requerido de resistencia en concordancia con los estándares apropiados.

- f) Se deberá instalar mecanismos de detección de intrusos. Estos deben ser regularmente probados para cubrir todas las puertas externas y ventanas de acceso, las áreas no ocupadas deben de tener una alarma todo el tiempo.
- g) Los recursos de procesamiento de información utilizados por la organización, deben ser físicamente separados de los que son utilizados por terceros.

### **Controles físicos de entrada**

**(Ver Anexo A.12 - Dominio (9), Objetivo de control (1), Control (2))**

Las áreas de seguridad deben ser protegidas por controles de entrada adecuados que aseguren el acceso sólo al personal autorizado.

Para implementar este control, deben de considerarse los siguientes puntos:

- a) Se deben de supervisar las visitas a áreas seguras, a menos que el acceso haya sido aprobado previamente, y se debe de registrar la fecha y momento de entrada y salida. Los visitantes sólo tendrán acceso para propósitos específicos, y se le deberá dar las instrucciones sobre los requisitos de seguridad del área y los procedimientos de emergencia.
- b) Se debería utilizar controles de autenticación, por ejemplo, tarjetas con números de identificación personal (PIN), para controlar y validar el acceso sólo al personal autorizado a la información sensible y sus recursos. Se debe de mantener un registro auditable de todos los accesos, con las medidas de seguridad apropiadas.
- c) Se debe de exigir a todo el personal, que posea alguna forma de identificación visible y se le pedirá que solicite a los extraños y a cualquiera que no lleve dicha identificación.



- d) Se deberá garantizar el acceso restringido al personal de apoyo de terceros, solo cuando este sea requerido.
- e) Se deberá revisar y actualizar regularmente los derechos de acceso a las áreas de seguridad.

### **Protección contra las amenazas externas y de origen ambiental**

**(Ver Anexo A.12 - Dominio (9), Objetivo de control (1), Control (4))**

Se debe aplicar protección física del fuego, inundación, terremoto, explosión, malestar civil y otras situaciones de desastre natural o humano.

Se debe de considerar amenazas de seguridad presentadas por premisas vecinas, tales como un incendio en el edificio vecino, goteo de agua en el techo o en pisos ubicados por debajo del nivel de la tierra o una explosión en la calle.

Los siguientes puntos deberán ser considerados para evitar daños por parte de fuego, inundaciones, temblores, explosiones y otras formas de desastre natural o humano:

- a) Materiales peligrosos y combustibles se deben de almacenar en lugares distantes del área segura.
- b) El equipo y los medios de respaldo deberían de estar alejados del área principal, para evitar que se dañen por algún desastre.
- c) Debe de existir equipo apropiado contra incendio y estar ubicado adecuadamente.

### **Emplazamiento y protección de Equipos**

**(Ver Anexo A.12 - Dominio (9), Objetivo de control, (2) Control (1))**

El equipo debe situarse en lugares donde se pueda reducir el riesgo de amenazas del entorno y permita mantener una protección adecuada.

Se deberán considerar los siguientes puntos para mantener una protección correcta de los equipos:

- a) Los equipos deben de situarse donde se minimicen los accesos innecesarios a las áreas de trabajo.
- b) Los equipos de procesamiento y almacenamiento de información que manejan datos sensibles, se deben de instalar en lugares donde se evite el riesgo de que personas no autorizadas vean los procesos durante su uso.
- c) Los elementos que requieran especial protección se deberán de aislar.
- d) Los controles deben ser adoptados para minimizar los riesgos de amenazas como robo, incendio, humo, explosivos, polvo, agua, vibraciones, radiaciones electromagnéticas y vandalismo.
- e) La empresa debe de incluir en sus políticas la prohibición de fumar, beber y comer cerca de los equipos de tratamiento de información.
- f) Se deberá revisar periódicamente las condiciones ambientales que puedan afectar a los equipos de tratamiento de información.
- g) Debe de existir protección contra la luz en todos los edificios y filtros de luz en todas las líneas de poder y comunicación.
- h) Se debe de considerar métodos de protección especial para los equipos que operen en ambientes industriales.

Los equipos que procesen información sensible deben ser protegidos para minimizar el riesgo de pérdida de información.

## **Instalaciones de Suministro**

**(Ver Anexo A.12 - Dominio (9), Objetivo de control (2), Control (2))**

Se deberán de proteger los equipos contra fallos eléctricos u otras anomalías causadas por fallas en los servicios públicos.

Todos los servicios de apoyo, como la electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado deben de ser los adecuados para los sistemas que están sirviendo. Los equipos de apoyo deben ser inspeccionados regularmente y probados apropiadamente para asegurar el funcionamiento correcto y reducir el riesgo causado por alguna falla o anomalía.

Se sugiere instalar un Sistema de alimentación ininterrumpida (U.P.S.) para asegurar el funcionamiento de los equipos que soportan operaciones críticas del negocio o para el cierre ordenado de los mismos. En caso de que exista un fallo prolongado de energía, se recomienda instalar un generador de respaldo. Si se utiliza un generador de energía, se debería disponer de una reserva suficiente de combustible para asegurar la disponibilidad del funcionamiento del mismo durante un tiempo prolongado. Los equipos UPS y los generadores deben ser revisados regularmente para asegurar su correcto funcionamiento.

Deben de existir instalados interruptores de emergencia cerca de las puertas de emergencia de la sala de cómputo, para facilitar una desconexión rápida en casos de emergencia.

El suministro de agua debe ser estable y adecuado. Un problema con el suministro de agua, puede dañar los equipos o hacer que los sistemas contra incendio no funcionen efectivamente. Deberá de instalarse (de ser requerido) un sistema de alarmas para detectar problemas de funcionamiento.

Los equipos de comunicación deben de conectarse al proveedor al menos por dos rutas para prevenir fallos en conexiones del servicio de voz.

### **Seguridad del cableado**

**(Ver Anexo A.12 - Dominio (9), Objetivo de control (2), Control (3))**

Se debe de proteger contra daños el cableado de energía y comunicaciones que transportan datos o soporten procesos de información.

Se deberá de considerar los siguientes puntos para la seguridad en el cableado:

- a) Las líneas de energía y comunicaciones deberán ser enterradas, de ser posible, o adoptarse medidas de protección alternativas.
- b) La red cableada deberá ser protegida contra daños usando conductos y evitando rutas a través de áreas públicas.
- c) Se debe de separar los cables de comunicación de los de energía para evitar interferencias.
- d) Los cables deben ser identificados para minimizar errores de manejo como el de parchar cables de una red incorrecta.
- e) Se deberá considerar medidas adicionales tales como:
  - 1) Instalación de conductos blindados y cajas cerradas en los puntos de inspección y terminación.
  - 2) Uso de medios de transmisión alternativos.
  - 3) Uso de fibra óptica.
  - 4) Uso de escudo electromagnético para proteger los cables.
  - 5) Acceso controlado para parchar paneles y cuartos de cable.

## **Mantenimiento de los equipos**

**(Ver Anexo A.12 - Dominio (9), Objetivo de control (2), Control (4))**

Se debe de ejecutar mantenimientos adecuados a los equipos para asegurar su disponibilidad e integridad permanente.

Se debe de considerar las siguientes pautas para el mantenimiento de equipos:

- a) Se deben de ejecutar mantenimientos a los equipos de acuerdo a los intervalos y especificaciones dadas por el fabricante o suministrador.
- b) La reparación y mantenimiento de los equipos solo lo debe realizar el personal de mantenimiento debidamente autorizado.
- c) Se debe de documentar todos los fallos presentados por el equipo, así como todos los mantenimientos preventivos y correctivos.
- d) Se debe definir controles apropiados para que, cuando el equipo sea programado para un mantenimiento, sea despejada la información sensible del mismo.
- e) Se deberá de cumplir todos los requisitos impuestos por las políticas de los seguros.

### **HALLAZGO 3: Falta de procedimientos para la ejecución de actividades diarias de un empleado.**

- Errores de usuario: No se encontraron documentos que definan los procedimientos de operación de cada empleado para poder ejecutar su trabajo de forma correcta. Además el departamento carece de un proceso disciplinario formal para los empleados que han cometido una falta que atente con la seguridad de la información

## **Recomendaciones**

Se recomienda implementar los siguientes controles basados en la Norma ISO/IEC 27001-2005:

### **Funciones y responsabilidades**

**(Ver Anexo A.12 - Dominio (8), Objetivo de control (1), Control (1))**

Todas las funciones y responsabilidades de los empleados, contratistas y terceros deben de ser definidas y documentadas bajo los lineamientos de la política de seguridad de la organización.

Las funciones de seguridad y responsabilidades deben de cumplir los siguientes requisitos:

- Ser definidas bajo los lineamientos de la política de seguridad de la organización
- Ejecutar procesos particulares o actividades
- Asegurar que la responsabilidad sea asignada a un individuo para que este pueda tomar decisiones
- Deben proteger a los activos de un acceso no autorizado, modificación, destrucción o interferencia
- Reportar eventos o riesgos de seguridad para la organización

Las funciones de seguridad y responsabilidades deben ser comunicadas a los candidatos al trabajo durante el proceso de selección.

## **Concienciación, formación y capacitación en seguridad de la información**

**(Ver Anexo A.12 - Dominio (8), Objetivo de control (2), Control (2))**

Todo el personal de la organización debe recibir capacitación apropiada sobre el conocimiento y actualizaciones de las políticas y procedimientos organizacionales que sean relevantes para la función de su trabajo.

La capacitación sobre el conocimiento debe de empezar con una inducción formal del proceso designado para incluir la política de seguridad de la organización, antes de dar acceso a la información o al servicio.

La capacitación en curso debe incluir requisitos de seguridad, responsabilidades legales y controles del negocio, así como buenas prácticas para el uso correcto de los recursos que se usan para el procesamiento de la información.

## **Proceso disciplinario**

**(Ver Anexo A.12 - Dominio (8), Objetivo de control (2), Control (3))**

Debe de existir un proceso formal disciplinario para los empleados que han cometido una falta en la seguridad de la información.

El proceso disciplinario se debe de ejecutar siempre y cuando se verifique que la falta de seguridad ha ocurrido. El proceso disciplinario debe de asegurar un correcto y justo tratamiento de los empleados que son sospechosos de cometer alguna falta en la seguridad.

Este proceso debe de tomar en consideración factores como la naturaleza, la gravedad de la apertura y su impacto en el negocio, si es que el violador estuvo propiamente entrenado, así como otros factores si son requeridos. En caso de ser mala conducta por

parte del empleado, el proceso debe de permitir, en caso de ser necesario, el retiro de sus labores, derechos de accesos y privilegios.

### **Documentación de los procedimientos de operación**

**(Ver Anexo A.12 - Dominio (10), Objetivo de control (1), Control (1))**

Se debe publicar los procedimientos de operación documentados y estar disponibles a los usuarios que lo requieran, además se debe darles mantenimiento periódicamente.

Se debe definir procedimientos de actividades asociadas al procesamiento de información y sus recursos, tales como procedimientos de encendido y apagado, mantenimiento de equipos, backups, manipulación de correos y seguridad.

Estos procedimientos deben detallar específicamente la ejecución de cada tarea, incluyendo:

- a) Proceso y utilización correcta de la información.
- b) Requisitos de planificación, indicando las dependencias con otros sistemas, estableciendo tiempos de inicio y fin.
- c) Backups.
- d) Instrucciones de manejo de errores.
- e) Reinicio del sistema y procedimientos de recuperación.
- f) Contactos de apoyo en caso de dificultades inesperadas operacionales o técnicas.
- g) Gestión de información de registros de auditoría.



#### **HALLAZGO 4: Incumplimiento de política para la eliminación de ex-empleados de la organización y bloqueos en equipos desatendidos.**

- Suplantación de identidad: Se encontró un incumplimiento de la política para la eliminación de empleados que ya dejan de pertenecer a la organización. Esto es riesgoso en cuanto a que puede existir una suplantación de identidad al momento de acceder a información a la cual el ex-empleado tenía acceso. También no se encontraron procedimientos que describan el proceso para establecer bloqueos en los equipos desatendidos por parte del usuario.

#### **Recomendaciones**

Se recomienda implementar los siguientes controles basados en la Norma ISO/IEC 27001-2005:

#### **Retirada de los derechos de acceso**

**(Ver Anexo A.12 - Dominio (8), Objetivo de control (3), Control (3))**

Los derechos de acceso de los empleados, contratistas o usuarios de terceros a la información y a las instalaciones de procesamiento de información, deben de ser removidos en caso de la culminación del empleo, contrato o acuerdo, o deben de ser ajustados en caso de cambio.

En la culminación, se debe reconsiderar los derechos de acceso de una persona a los activos asociados con los sistemas de información. Esto determinará si es necesario retirar los derechos de acceso. Cuando ocurre el cambio de un empleo, este debe ser reflejado en el retiro de todos los derechos de acceso que no fueron aprobados para el nuevo empleado.

Los derechos de acceso deben ser removidos o adaptados, incluyendo acceso físico y lógico, tarjetas de identificación, llaves, suscripciones y cualquier documento que lo identifique como un miembro actual de la empresa. En el caso de los empleados, contratistas o usuarios de terceros que sean retirados de la organización y que estos

posean contraseñas para acceder a los activos, estas deben ser cambiadas. Los derechos de acceso deben de ser removidos o cambiados antes de que el empleo termine o cambie, tomando en cuenta factores de riesgo como:

- Si la finalización o cambio es iniciado por el empleado o por la gerencia y la razón de la finalización
- Las responsabilidades actuales del empleado
- El valor de los activos que accede actualmente

### **Registro de usuario**

**(Ver Anexo A.12 - Dominio (11), Objetivo de control (2), Control (1))**

Se debería formalizar un procedimiento de registro de altas y bajas de usuarios para garantizar el acceso a los sistemas y servicios de información multiusuario.

Se debería controlar el acceso a los servicios de información multiusuario mediante un proceso formal de registro que debería incluir:

- a) La utilización de un identificador único para cada usuario, de esta forma puede vincularse a los usuarios y responsabilizarles de sus acciones. Se debería permitir el uso de identificadores de grupo cuando sea conveniente para el desarrollo del trabajo y estos deben ser aprobados y documentados.
- b) La comprobación de la autorización del usuario por el propietario del servicio para utilizar el sistema o el servicio de información. También puede ser conveniente que la gerencia apruebe por separado los derechos de acceso.
- c) Verificación de la adecuación del nivel de acceso asignado al propósito del negocio y su consistencia con la política de seguridad de la organización.
- d) La entrega a los usuarios de una relación escrita de sus derechos de acceso.

- e) La petición a los usuarios para que reconozcan con su firma la comprensión de las condiciones de acceso.
- f) La garantía de que no se provea acceso al servicio hasta que se hayan completado los procedimientos de autorización.
- g) El mantenimiento de un registro formalizado de todos los autorizados para usar el servicio.
- h) La eliminación inmediata de las autorizaciones de acceso a los usuarios que dejan la organización o cambien de trabajo en ella.
- i) La revisión periódica y eliminación de identificadores y cuentas de usuario redundantes.
- j) La garantía de no reasignación a otros usuarios de los identificadores de usuario redundantes.

### **Gestión de privilegios**

**(Ver Anexo A.12 - Dominio (11), Objetivo de control (2), Control (2))**

Debería restringirse y controlarse el uso y asignación de privilegios.

Se debería controlar la asignación de privilegios por un proceso formal de autorización en los sistemas multiusuario. Se deberían considerar los pasos siguientes:

- a) Identificar los privilegios asociados a cada elemento del sistema, por ejemplo, el sistema operativo, el sistema gestor de base de datos y cada aplicación; así como las categorías de empleados que necesitan de ellos.
- b) Asignar privilegios a los individuos según los principios de “necesidad de su uso” y “caso por caso” y en línea con la política de control de acceso, por ejemplo, el requisito mínimo para cumplir su función sólo cuando se necesite.

- c) Mantener un proceso de autorización y un registro de todos los privilegios asignados. No se otorgarán privilegios hasta que el proceso de autorización haya concluido.
- d) Promover el desarrollo y uso de rutinas del sistema para evitar la asignación de privilegios a los usuarios.
- e) Promover el desarrollo y uso de programas que evitan la necesidad de correr con privilegios.
- f) Asignar los privilegios a un identificador de usuario distinto al asignado para un uso normal.

### **Uso de contraseñas**

**(Ver Anexo A.12 - Dominio (11), Objetivo de control (3), Control (1))**

Los usuarios deberían seguir buenas prácticas de seguridad para la selección y uso de sus contraseñas.

Todos los usuarios deberían ser informados acerca de:

- a) Mantener la confidencialidad de las contraseñas.
- b) Evitar guardar registros (papel, archivos de software o dispositivos) de las contraseñas, salvo si existe una forma segura de hacerlo y el método de almacenamiento ha sido aprobado.
- c) Cambiar las contraseñas si se tiene algún indicio de su vulnerabilidad o de la del sistema.
- d) Seleccionar contraseñas de buena calidad, con una longitud mínima caracteres, que sean:
  - 1) Fáciles de recordar.

- 2) No estén basadas en algo que cualquiera pueda adivinar u obtener usando información relacionada con el usuario, por ejemplo, nombres, fechas de nacimiento, números de teléfono, etc.
  - 3) No sean vulnerables a ataques de diccionario (no consisten en palabras incluidas en diccionarios).
  - 4) Estén carentes de caracteres consecutivos repetidos o que sean todos números o todas letras.
- 
- e) Cambiar las contraseñas a intervalos de tiempo regulares o en proporción al número de accesos (las contraseñas de las cuentas con privilegios especiales deberían cambiarse con más frecuencia que las normales), evitando utilizar contraseñas antiguas o cíclicas.
  - f) Cambiar las contraseñas temporales asignadas para inicio, la primera vez que se ingrese al sistema.
  - g) No incluir contraseñas en ningún procedimiento automático de conexión, que, las deje almacenadas permanentemente.
  - h) No compartir contraseñas de usuario individuales.
  - i) No utilizar la misma contraseña para propósitos personales o de negocio.

Si los usuarios necesitan acceder a múltiples servicios o plataformas y se les pide que mantengan contraseñas múltiples, deberían ser aconsejados sobre la posibilidad de usar una sola contraseña de calidad para todos los servicios, que brinde un nivel razonable de protección para la contraseña almacenada.

### **Equipo de usuario desatendido**

**(Ver Anexo A.12 - Dominio (11), Objetivo de control (3), Control (2))**

Los usuarios deberían asegurar que los equipos informáticos desatendidos estén debidamente protegidos.

Todos los usuarios y proveedores de servicios deberían conocer los requisitos de seguridad y los procedimientos para proteger los equipos desatendidos, así como sus responsabilidades para implantar dicha protección. Se les debería recomendar:

- a) Cancelar todas las sesiones activas antes de marcharse, salvo si se dispone de una herramienta de bloqueo general, por ejemplo, una contraseña para protector de pantalla.
- b) Desconectar (log-off) los servidores o los computadores centrales cuando se ha terminado la sesión (y no sólo apagar el terminal o el computador personal).
- c) Proteger el terminal o el puesto de trabajo cuando no estén en uso con un bloqueador de teclado o una medida similar, por ejemplo, una contraseña de acceso.

### **Identificación y autenticación del usuario**

**(Ver Anexo A.12 - Dominio (11), Objetivo de control (5), Control (2))**

Todos los usuarios deberían disponer de un identificador único para su uso personal y debería ser escogida una técnica de autenticación adecuada para verificar la identidad de estos.

Este control debe ser aplicado para todos los tipos de usuario (incluidos los administradores de red y de bases de datos, los programadores de sistemas y el personal técnico de apoyo).

Los ID de los usuarios deben ser utilizados para seguir la pista de las actividades de cada responsable individual. Las actividades regulares del usuario no deben ser realizadas desde cuentas privilegiadas.

En circunstancias excepcionales que se justifiquen por sus ventajas pueden usarse identificadores de usuario compartidos para un grupo de usuarios o un trabajo específico. En estos casos se debería necesitar la aprobación escrita de la gerencia. Puede necesitarse la implantación de controles adicionales para la responsabilidad.

Los ID's genéricos utilizados por individuos deben ser solo permitidos donde las funciones o acciones llevadas a cabo no requieren ser trazadas (como la lectura) o cuando existan otros controles establecidos (contraseñas genéricas utilizadas solamente por un grupo de personas a la vez y conectándose en dicho momento).

Donde se requiera una fuerte autenticación e identificación, se pueden utilizar métodos alternativos a las contraseñas como medios criptográficos, tarjetas inteligentes o medios biométricos.

#### **Desconexión automática de sesión**

**(Ver Anexo A.12 - Dominio (11), Objetivo de control (5), Control (5))**

Las sesiones se deberían desactivar tras un periodo definido de inactividad.

Este dispositivo de desactivación debería borrar la pantalla y cerrar la aplicación y las sesiones de conexión a red tras dicho periodo definido de inactividad. El tiempo de desactivación debería reflejar los riesgos de seguridad del área, la clasificación de la información que se maneja, las aplicaciones que se utilizan y los riesgos relacionados con los usuarios de los equipos.

Muchos computadores personales suelen tener limitado de alguna forma este dispositivo que borra la pantalla para evitar el acceso no autorizado, pero no cierra la aplicación o las sesiones de conexión a red.

## **HALLAZGO 5: Falta de procedimientos para el cumplimiento del correcto uso de los equipos por parte de los usuarios y que son responsabilidad del departamento de TI**

- Uso no previsto de recursos: No se encontraron documentos que definan las reglas para el uso aceptable de los recursos por parte del usuario.
- Manipulación de equipos: Se encontró riesgo en cuanto al mal uso de los recursos administrados por parte del usuario.
- Difusión de software dañino: No existen procedimientos documentados para el uso de medios removibles por parte del usuario. Esto puede causar que los equipos se infecten de virus si alguno de estos medios removibles se encuentra infectado.

### **Recomendaciones**

Se recomienda implementar los siguientes controles basados en la Norma ISO/IEC 27001-2005:

### **Inventarios de activos**

**(Ver Anexo A.12 - Dominio (7), Objetivo de control (1), Control (1))**

Todos los activos deben ser claramente identificados. Se debe elaborar y mantener actualizado un inventario de los activos más importantes.

La organización debe de identificar todos los activos de y la documentación de los mismos. Se debe de elaborar un inventario de activos que debe de incluir la información necesaria para poder recuperarse de un desastre. Esta información debe de incluir:

- Tipo de Activo
- Formato



- Ubicación
- Información de respaldo
- Información de Licencia
- Valor dentro del Negocio

Adicionalmente, los propietarios y la clasificación de la información debe ser aceptada y documentada para cada activo. Se deben de identificar los niveles de protección basado en la importancia del activo y su valor dentro del negocio.

### **Propiedad de los activos**

**(Ver Anexo A.12 - Dominio (7), Objetivo de control (1), Control (2))**

Todos los activos asociados con el proceso de información deben de tener un responsable dentro de la organización.

Cada propietario de los activos debe ser responsable de:

- Asegurar que la información y los activos de procesamiento de la misma sea apropiadamente clasificadas.
- Definir y revisar periódicamente las restricciones de acceso y clasificaciones, basándose en políticas de control aplicables.

### **Uso aceptable de los activos**

**(Ver Anexo A.12 - Dominio (7), Objetivo de control (1), Control (3))**

Se deben definir las reglas para el uso aceptable de la información y de los activos asociados con el procesamiento de la información. Estas reglas deben de ser identificadas, documentadas e implementadas.

Todo el personal de la organización, contratistas y terceras partes deberán de regirse a las reglas definidas para un uso aceptable de la información y de los activos asociados con el procesamiento de la información. Esto incluye:

- Reglas para uso de Internet y correo electrónico
- Normas para el uso de aparatos móviles, especialmente para el uso fuera de la organización.

Todo el personal que haga uso de los activos de la organización o tenga acceso a los mismos, debe de estar al tanto de las reglas definidas para el uso de la información y de los activos asociados con el procesamiento de la información. Estas reglas o guías deben de ser provistas por la gerencia relevante.

### **Controles contra el código malicioso**

**(Ver Anexo A.12 - Dominio (10), Objetivo de control (4), Control (1))**

Se deberá implementar controles para detectar y prevenir software malicioso, así como procedimientos adecuados para concientizar a los usuarios.

La protección contra software malicioso deberá de basarse en sistemas adecuados de acceso, controles de gestión de cambios y la conciencia de la seguridad. Los siguientes puntos deberán ser considerados:

- a) Establecer una política formal que requiera el cumplimiento de las licencias de software y prohibición del uso de software no autorizado.
- b) Establecer una política formal de protección contra los riesgos relacionados con la obtención de archivos o cualquier otro medio, indicando las medidas protectoras a seguir.

- c) Realizar revisiones periódicas del software y datos manejados en los sistemas que soportan procesos críticos de la organización.
- d) Instalar y actualizar frecuentemente software de detección y reparación de virus. Estos análisis se deben realizar de forma rutinaria y como un control preventivo; las revisiones deberán incluir:
  - ✓ Verificación de archivos electrónicos de origen desconocido o no autorizado. Comprobar la existencia de virus antes de utilizar dichos archivos.
  - ✓ Verificación de todo archivo adjunto en un correo electrónico o descarga realizada por el usuario. Esta comprobación se debe realizar en lugares como: servidores de correo, computadores personales o entrada a la red de la organización.
  - ✓ Verificación de códigos maliciosos en las páginas web.
- e) Establecer procedimientos y responsabilidades de administración para utilizar protección de antivirus, información de los ataques de virus y recuperación de la información.
- f) Definir planes de continuidad del negocio apropiados para recuperarse de los ataques de virus.
- g) Implementar procedimientos para recolección de información periódicamente, tales como suscripción a listas de correo o verificaciones de páginas Web que contenga información sobre nuevos virus.
- h) Definir procedimientos para comprobar la información relativa al software malicioso y asegurar que las alertas son reales. Se deberá advertir al personal sobre los virus reales y los falsos avisos de virus, y de cómo actuar al momento de que se presenten estos casos.

## **Gestión de soportes extraíbles**

**(Ver Anexo A.12 - Dominio (10), Objetivo de control (7), Control (1))**

Debería haber procedimientos para la gestión de los medios informáticos removibles.

Se deberían considerar las siguientes pautas para la gestión de los medios removibles:

- a) Se deberían borrar cuando no se necesiten más, los contenidos previos de todo medio reutilizable del que se desprenda la organización.
- b) Donde sea necesario y práctico, todo medio desechado por la organización debería requerir autorización y se debería guardar registro de dicha remoción para guardar una pista de auditoria.
- c) Todos los medios se deberían almacenar a salvo en un entorno seguro, de acuerdo con las especificaciones de los fabricantes.
- d) La información almacenada en el medio, que requiere estar disponible mayor tiempo que el tiempo de vida del medio (en concordancia con las especificaciones del productor) debe ser también almacenada con el fin de no perder dicha información debido al deterioro del medio.
- e) El registro de los medios removibles debe ser considerado para limitar la oportunidad de pérdida de datos.
- f) Los medios removibles deben ser solo activados si existe una razón de negocio para hacerlo.

Se deberían documentar claramente todos los procedimientos y niveles de autorización.

## **HALLAZGO 6: Falta de procedimientos para mantenimiento y actualizaciones de equipos y aplicaciones.**

- Caída del sistema por agotamiento de recursos: No se encontró documentado un plan de mantenimiento para los activos más importantes de la organización. Esto puede repercutir al funcionamiento inadecuado del mismo.
- Errores de mantenimiento y actualizaciones de programas: No existe definidos procedimientos que indiquen como realizar el mantenimiento de los equipos y programas que contienen los mismos.
- Vulnerabilidades de los programas: No existe información documentada sobre vulnerabilidades técnicas presentadas en los sistemas presentes de la organización.
- Manipulación de los programas: No se ha encontrado procedimientos formales que indiquen un control de cambios que el personal de TI realiza sobre los programas de la organización

### **Recomendaciones**

Se recomienda implementar los siguientes controles basados en la Norma ISO/IEC 27001-2005:

#### **Mantenimiento de los equipos**

**(Ver Anexo A.12 - Dominio (9), Objetivo de control (2), Control (4))**

Se debe de ejecutar mantenimientos adecuados a los equipos para asegurar su disponibilidad e integridad permanente.

Se debe de considerar las siguientes pautas para el mantenimiento de equipos:

- a) Se deben de ejecutar mantenimientos a los equipos de acuerdo a los intervalos y especificaciones dadas por el fabricante o suministrador.

- b) La reparación y mantenimiento de los equipos solo lo debe realizar el personal de mantenimiento debidamente autorizado.
- c) Se debe de documentar todos los fallos presentados por el equipo, así como todos los mantenimientos preventivos y correctivos.
- d) Se debe definir controles apropiados para que, cuando el equipo sea programado para un mantenimiento, sea despejada la información sensible del mismo.
- e) Se deberá de cumplir todos los requisitos impuestos por las políticas de los seguros.

### **Gestión de capacidades**

**(Ver Anexo A.12 - Dominio (10), Objetivo de control (3), Control (1))**

Se le debe dar buen uso a los recursos y a las proyecciones realizadas de capacidades adecuadas futuras a través de monitoreo certificando así que el sistema funcione acorde a lo requerido.

Se deben identificar todos los requisitos de capacidad para cada actividad a ejecutarse sea ésta nueva o que ya esté vigente. Con el fin de asegurar que los requisitos se cumplan, se debe realizar monitoreo de los sistemas y de ser necesario mejorar la disponibilidad y eficiencia de los mismos.

Se deberá instalar controles de detección con el objetivo de detectar problemas en un tiempo determinado.

Se debe considerar los requisitos de las recientes actividades al momento de realizar las proyecciones, así como las tendencias actuales del manejo de la información.

Se deberá prestar atención a los recursos con costos altos o tiempos de llegada largo; para esto, la utilización de los recursos claves del sistema serán monitoreados por la gerencia con la información obtenida se deberá identificar y evitar los cuellos de botella que representen una amenaza a la seguridad del sistema.

### **Aceptación del sistema**

**(Ver Anexo A.12 - Dominio (10), Objetivo de control (3), Control (2))**

Se deberá establecer medidas de aceptación para sistemas de información nuevos o versiones mejoradas, realizando las pruebas adecuadas de los mismos antes de su aceptación.

Los requisitos y criterios de aceptación de los nuevos sistemas, deben de estar claramente definidos, documentados y probados, la responsabilidad de esta tarea será de los administradores. Los nuevos sistemas, actualizaciones o nuevas versiones solo serán migrados a producción luego de obtener una aceptación formal de los mismos.

Se deberá considerar los siguientes puntos:

- a) Requisitos de capacidad y rendimiento de los computadores.
- b) Procedimientos de recuperación de errores, así como los planes de contingencia.
- c) Preparación y prueba de procedimientos operativos de rutina.
- d) Conjunto acordado de controles y medidas de seguridad instalados.
- e) Plan de continuidad de negocio
- f) Manual de procedimiento eficaz
- g) Resultados de que la instalación del nuevo sistema no producirá errores sobre los existentes.

- h) Evidencias del efecto que causará el nuevo sistema en la seguridad de la organización.
- i) Formación en la producción o utilización de los nuevos sistemas.

En los desarrollos importantes, se deberá consultar al responsable de operaciones y los usuarios que participarán en el sistema para asegurar la eficacia operacional del diseño propuesto.

### **Análisis y especificación de los requisitos de seguridad**

**(Ver Anexo A.12 - Dominio (12), Objetivo de control (1), Control (1))**

Los enunciados de los requisitos de negocio para sistemas nuevos o mejoras a sistemas existentes deberían especificar los requisitos de control.

Las especificaciones deberían considerar los controles automatizados a ser incorporados en el sistema y la necesidad de controles manuales de apoyo. Se deberían aplicar consideraciones similares cuando se evalúen, desarrollen o compren paquetes de software para aplicaciones de negocio.

Los requisitos y controles de seguridad deberían reflejar el valor de los activos de información implicados y el posible daño a la organización que resultaría de fallos o ausencia de seguridad.

Los requisitos del sistema para la seguridad de información y procesos para implementar la seguridad deben ser integrados en las etapas iniciales de los proyectos de sistema de información. Los controles introducidos en la etapa de diseño son significativamente menos costos de implementar y mantener que los que se incluyen durante o después de la implementación.



Si los productos son comprados, se debe realizar una prueba formal y un proceso de adquisición. Los contratos con el proveedor deben indicar los requisitos de seguridad. Si los requisitos no satisfacen la funcionalidad de la seguridad en un producto se debe reconsiderar los riesgos introducidos y los controles asociados antes de comprar el producto. Donde se suministre una funcionalidad adicional que cause un riesgo en la seguridad, se debe desactivar o se debe revisar la estructura del control propuesto para determinar si se puede tomar ventaja de la funcionalidad disponible.

### **Validación de los datos de entrada**

**(Ver Anexo A.12 - Dominio (12), Objetivo de control (2), Control (1))**

Se deberían validar los datos de entrada a las aplicaciones del sistema para garantizar que son correctas y apropiadas.

Se deberían aplicar verificaciones a la entrada de las transacciones, de los datos de referencia (por ejemplo nombres y direcciones, límites de crédito, números de clientes) y de las tablas de parámetros (por ejemplo precios de venta, tasas de cambio de divisas, tasas de impuestos).

Los controles siguientes deberían ser considerados:

- a) Entrada duplicada u otras verificaciones, como verificación de fronteras o campos limitados para especificar los rangos de los datos de entrada, para detectar los errores siguientes:
  - 1) valores fuera de rango.
  - 2) caracteres inválidos en los campos de datos.
  - 3) datos que faltan o están incompletos.
  - 4) datos que exceden los límites de volumen por exceso o defecto.
  - 5) datos de control no autorizado o inconsistente.
  
- b) Revisión periódica del contenido de los campos clave o los archivos de datos para confirmar su validez e integridad.

- c) inspección de los documentos físicos de entrada para ver si hay cambios no autorizados a los datos de entrada (todos deberían estar autorizados).
- d) Procedimientos para responder a los errores de validación.
- e) Procedimientos para comprobar la integridad de los datos de entrada.
- f) Definición de las responsabilidades de todos los implicados en el proceso de entrada de datos.
- g) Creación de un registro de actividades envueltas en el procesamiento de los datos de entrada.

### **Control de procesamiento interno**

**(Ver Anexo A.12 - Dominio (12), Objetivo de control (2), Control (2))**

Se deberían incorporar a los sistemas comprobaciones de validación para detectar cualquier tipo de corrupción de información a través de errores del proceso o por actos deliberados.

El diseño de las aplicaciones debería asegurar la implantación de restricciones que minimicen el riesgo de los fallos del proceso con pérdidas de integridad. Áreas de riesgo específicas a considerar serían:

- a) El uso en los programas de funciones ‘añadir’ y ‘borrar’ para cambiar los datos.
- b) Los procedimientos para evitar programas que corran en orden equivocado o después del fallo de un proceso anterior.
- c) El uso de programas correctos de recuperación después de fallas para asegurar el proceso correcto de los datos.
- d) La protección contra ataques utilizando corridas o desbordes de buffers.

Se debería tener preparado una lista de verificación apropiada, tener las actividades documentadas y los resultados deben mantenerse seguros. A continuación se dan ejemplos de comprobaciones que pueden incorporarse:

- a) Controles de sesión o de lotes, para conciliar los cuadros de los archivos tras las actualizaciones de las transacciones.
- b) Controles para comprobar los cuadros de apertura contra los cuadros previos del cierre, como:
  - 1) Controles de pasada en pasada.
  - 2) Totales de actualización de archivos.
  - 3) Controles de programa a programa.
- c) Validación de los datos generados por el sistema.
- d) Comprobaciones de la integridad, autenticidad u otro aspecto de seguridad de datos o del software transferido entre el computador central y las computadoras remotas.
- e) Totales de comprobación de registros y archivos.
- f) Comprobaciones que aseguren que los programas de las aplicaciones se ejecutan en el momento adecuado.
- g) Comprobaciones que aseguren que los programas se ejecutan en el orden correcto, que finalizan en caso de falla y que no sigue el proceso hasta que el problema se resuelve.
- h) Crear un registro de las actividades envueltas en el procesamiento.

## **Integridad de los mensajes**

**(Ver Anexo A.12 - Dominio (12), Objetivo de control (2), Control (3))**

Se debería identificar los requerimientos para asegurar la autenticación y protección de la integridad de los mensajes en aplicaciones y se deberían de identificar e implementar controles apropiados.

Una evaluación de riesgos de seguridad debe ser llevada a cabo para determinar si la integridad de los mensajes es requerida e identificar el método más apropiado para su implementación.

## **Validación de los datos de salida**

**(Ver Anexo A.12 - Dominio (12), Objetivo de control (2), Control (4))**

Se deberían validar los datos de salida de un sistema de aplicación para garantizar que el proceso de la información ha sido correcto y apropiado a las circunstancias.

La validación de salidas puede incluir:

- a) Validaciones de verosimilitud para comprobar que los datos de salida son razonables.
- b) Cuentas de control de conciliación para asegurar el proceso de todos los datos.
- c) Suministro de suficiente información al lector o a un sistema de proceso subsiguiente para poder determinar la exactitud, completitud, precisión y clasificación de la información.
- d) Procedimientos para contestar los cuestionarios de validación de salidas.
- e) Definición de las responsabilidades de todos los implicados en el proceso de salida de datos.

- f) Creación de un registro de actividades en el proceso de validación de los datos de salida.

### **Control de software en explotación**

**(Ver Anexo A.12 - Dominio (12), Objetivo de control (4), Control (1))**

Deberían existir procedimientos para controlar la instalación del software en sistemas operacionales.

Para minimizar el riesgo de corrupción deberían considerarse los siguientes controles:

- a) La actualización de las librerías de programas operativos sólo se debería realizar por el administrador capacitado previa autorización de la gerencia.
- b) Los sistemas operativos deberían tener sólo código ejecutable y no desarrollo de código o compiladores.
- c) No se debería implantar código ejecutable en un sistema operativo mientras no se tenga evidencia del éxito de las pruebas, la aceptación del usuario y la actualización de las librerías de programas fuente. Deben ser realizadas en un sistema separado.
- d) Se debería utilizar un sistema de control de configuración para mantener un control de todo el software implementado así como la documentación del sistema.
- e) Debería existir una estrategia de restauración no actualizada antes de que se implementen los cambios.
- f) Se debería mantener un registro de auditoría de todas las actualizaciones a las librerías de programas en producción.
- g) Se deberían retener las versiones anteriores de software como medida de precaución para contingencias.

- h) Las versiones antiguas de software deben ser archivadas junto con toda la información requerida, los parámetros, procedimientos, detalles de configuración y software de soporte, durante el tiempo en que los datos sean retenidos.

El software adquirido que se use en sistemas operativos se debería mantener en el nivel de soporte del proveedor. A través del tiempo, los vendedores de software cesaran de suministrar versiones antiguas. La organización debe considerar los riesgos de confiar en un software que no cuente con soporte.

Cualquier decisión de actualización debe tomar en cuenta los requisitos del negocio para dicho cambio y la seguridad del nuevo lanzamiento, como por ejemplo la introducción de una nueva funcionalidad de seguridad o el número y severidad de los problemas de seguridad que afectan esta versión. Los parches de software deben ser aplicados cuando ayuden a remover o reducir las vulnerabilidades.

Sólo se debería permitir acceso físico o lógico a los proveedores cuando sea imprescindible por motivos de soporte, y con aprobación de la gerencia. Las actividades de los proveedores deberían ser supervisadas y controladas.

El software de computación debe recaer en software y módulos suministrados externamente los cuales deben ser monitoreados y controlados para evitar cambios no autorizados que puedan introducir debilidades en la seguridad.

### **Procedimientos de control de cambio**

**(Ver Anexo A.12 - Dominio (12), Objetivo de control (5), Control (1))**

La implementación de cambios debe ser controlada usando procedimientos formales de cambio.

Para minimizar la corrupción de los sistemas de información, se deberían mantener estrictos controles sobre la implantación de cambios. La introducción de nuevos sistemas y cambios mayores al sistema existente debe seguir un proceso formal de documentación, especificación, prueba, control de calidad e implementación.

Este proceso debe incluir una evaluación de riesgos, un análisis de los impactos de los cambios y una especificación de los controles de seguridad necesarios. Este proceso debe también asegurar que no se comprometa la seguridad y los procedimientos de control existentes, que a los programadores de soporte se les da acceso solo a las partes del sistema necesarias para su trabajo y que se debe tener una aprobación y acuerdo formal para cualquier cambio.

La aplicación y sus procedimientos de control de cambios deberían estar integrados siempre que sea posible. Este proceso debería incluir:

- a) El mantenimiento de un registro de los niveles de autorización acordados.
- b) La garantía de que los cambios se realizan por usuarios autorizados.
- c) La revisión de los controles y los procedimientos de integridad para asegurarse que los cambios no los debilitan.
- d) La identificación de todo el software, información, entidades de bases de datos y hardware que requiera mejora.
- e) La obtención de la aprobación formal para propuestas detalladas antes de empezar el trabajo.
- f) La garantía de la aceptación por el usuario autorizado de los cambios antes de cualquier implantación.
- g) La garantía de actualización de la documentación del sistema al completar cualquier cambio y del archivo o destrucción de la documentación antigua.

- h) El mantenimiento de un control de versiones de toda actualización del software.
- i) El mantenimiento de un seguimiento de auditoría de todas las peticiones de cambio.
- j) La garantía del cambio de la documentación operativa y de los procedimientos de usuario en función de la necesidad.
- k) La garantía de la adecuación del tiempo de implantación de los cambios para no dificultar los procesos de negocio implicados.

**Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo  
(Ver Anexo A.12 - Dominio (12), Objetivo de control (5), Control (2))**

Se deberían revisar y probar las aplicaciones del sistema cuando se efectúen cambios, para asegurar que no impactan adversamente en el funcionamiento o en la seguridad.

Este proceso debería cubrir:

- a) La revisión de los procedimientos de control de la aplicación y de la integridad para asegurar que los cambios en el sistema operativo no han sido comprometidos.
- b) La garantía de que el plan de soporte anual y el presupuesto cubren las revisiones y las pruebas del sistema que requieran los cambios del sistema operativo.
- c) La garantía de que la modificación de los cambios del sistema operativo se realiza a tiempo para que puedan hacerse las revisiones apropiadas antes de su implantación.
- d) La garantía de que se realizan los cambios apropiados en los planes de continuidad del negocio.



Se le debe dar la responsabilidad, a un grupo específico o individuo, de monitorear las vulnerabilidades y los lanzamientos de parches y arreglos por parte de los vendedores.

### **Control de vulnerabilidades técnicas**

**(Ver Anexo A.12 - Dominio (12), Objetivo de control (6), Control (1))**

Se debe obtener a tiempo la información sobre las vulnerabilidades técnicas de los sistemas información utilizadas. Igualmente, se debe evaluar la exposición de la organización a tales vulnerabilidades y las medidas apropiadas para tratar a los riesgos asociados.

Un inventario actual y completo de activo es un prerrequisito para una efectiva gestión de vulnerabilidades técnicas. La información específica requerida para apoyar la gestión de vulnerabilidades técnicas incluye al vendedor de software, número de versiones, el estado actual de despliegue (por ejemplo que software es instalado en que sistema) y las personas dentro de la organización responsables del software.

Una acción apropiada y a tiempo debe ser tomada en cuenta en respuesta a la identificación de vulnerabilidades técnicas potenciales. Las siguientes pautas deben seguirse para establecer un proceso de gestión de vulnerabilidades técnicas efectivas:

- a) La organización debe definir y establecer los roles y responsabilidades asociados con la gestión de vulnerabilidades técnicas, incluyendo el monitoreo de vulnerabilidades, la evaluación de la vulnerabilidad de riesgo, el parchado, el seguimiento de activos y cualquier otra responsabilidades coordinadas.
- b) Los recursos de información que se utilizaran para identificar las vulnerabilidades técnicas relevantes y para mantener precaución sobre ellos se deben identificar para el software y otras tecnologías; estos recursos de

información deben ser actualizados basados en cambios de inventario o cuando un recurso nuevo o más útil se encuentre.

- c) Se debería definir una línea de tiempo para reaccionar ante notificaciones de vulnerabilidades técnicas potenciales y relevantes.
- d) Una vez identificada las vulnerabilidades técnicas potenciales, la organización debe identificar los riesgos asociados y las acciones a ser tomadas en cuenta. Esta acción puede implicar el parchado de sistemas vulnerables y/o la aplicación de otros controles.
- e) Dependiendo en que tan urgente sea necesario tratar una vulnerabilidad técnica, la acción a ser tomada en cuenta debe ser llevada a cabo de acuerdo a controles relacionados con la gestión de cambios o siguiendo los procedimientos de respuesta ante incidentes en la seguridad de información.
- f) Si un parche se encuentra disponible, se deben tratar los riesgos asociados con la instalación (los riesgos planteados por la vulnerabilidad deben ser comparados con los riesgos de instalación del parche).
- g) Los parches deben ser probados y evaluados antes de que sean instalados con el fin de asegurar que sean efectivos y que no resulten en efectos secundarios que no puedan ser tolerados. Si no existe ningún parche disponible, se deberían considerar otros controles como:
  - 1) Apagar los servicios y capacidades relacionadas con la vulnerabilidad.
  - 2) Adaptar o tratar los controles de acceso, por ejemplo los firewall en los bordes de red.
  - 3) Monitoreo creciente para detectar o prevenir ataques actuales.
  - 4) Aumento en la precaución de la vulnerabilidad.
- h) Un registro de ingreso debe ser mantenido para todos los procedimientos emprendidos.

- i) Se debería monitorear y evaluar la gestión de procesos en la vulnerabilidad técnica con el fin de asegurar su efectividad y eficiencia.
- j) Los sistemas en alto riesgo deben ser tratados primero.

**HALLAZGO 7: Falta de documentación para restaurar respaldos correctamente.**

- Restauración fallida de respaldos: No se encontraron procedimientos para poder restaurar los respaldos realizados en caso de que se necesiten.

**Recomendaciones**

Se recomienda implementar los siguientes controles basados en la Norma ISO/IEC 27001-2005:

**Copias de seguridad de la información**

**(Ver Anexo A.12 - Dominio (10), Objetivo de control (5), Control (1))**

Se deberían hacer regularmente copias de seguridad de toda la información esencial del negocio y del software, en concordancia con la política acordada de recuperación.

Adecuados servicios de respaldo deben ser provistos para asegurar que toda la información esencial del negocio pueda recuperarse tras un desastre o un fallo de los medios.

Los siguientes puntos de la recuperación de información deben ser considerados:

- a) Definir el nivel necesario de recuperación de la información.
- b) Almacenar un nivel mínimo de información de respaldo, junto a los registros exactos y completos de las copias de seguridad y a procedimientos documentados de recuperación.

- c) La extensión y frecuencia de los respaldos deben reflejar las necesidades de la organización, los requisitos de seguridad de la información envuelta, y la criticidad de la información para la operación continua de la organización.
- d) Los respaldos deben estar almacenados en una locación remota, en una distancia suficiente para escapar de cualquier daño frente a un desastre en el local principal.
- e) Se debería dar a la información de respaldo un nivel adecuado de protección física y del entorno, un nivel consistente con las normas aplicadas en el local principal. Se deberían extender los controles y medidas aplicados a los medios en el local principal para cubrir el local de respaldo.
- f) Los medios de respaldo se deberían probar regularmente, donde sea factible, para asegurar que son fiables cuando sea preciso su uso en caso de emergencia.
- g) Se deberían comprobar y probar regularmente los procedimientos de recuperación para asegurar que son eficaces y que pueden cumplirse en el tiempo establecido por los procedimientos operativos de recuperación.
- h) En situaciones donde la confidencialidad sea importante, los respaldos deben ser protegidos por medios de encriptación.

Deben probarse regularmente arreglos individuales de las copias de seguridad de los sistemas para asegurar que estos reúnen los requisitos de los planes de continuidad del negocio. Para los sistemas críticos, los arreglos auxiliares deben cubrir toda la información de los sistemas, aplicaciones y datos necesarios de recuperarse del sistema completo en caso de un desastre.

El periodo de retención para la información esencial del negocio, y también cualquier requisito permanente para las copias de los archivos debe determinarse.

## **HALLAZGO 8: Falta de adiestramiento al personal ante posible ausencia del mismo.**

- Indisponibilidad del personal: No existen planes de continuidad del negocio ante la ausencia de un empleado de la organización.

### **Recomendaciones**

Se recomienda implementar los siguientes controles basados en la Norma ISO/IEC 27001-2005:

### **Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información**

**(Ver Anexo A.12 - Dominio (14), Objetivo de control (1), Control (3))**

Se deberían desarrollar planes de mantenimiento y recuperación de las operaciones del negocio, para asegurar la disponibilidad de información al nivel y en las escalas de tiempo requeridas, tras la interrupción o la falla de sus procesos críticos.

El proceso de planificación de la continuidad del negocio debería considerar los siguientes aspectos:

- a) La identificación de los procedimientos de emergencia y los acuerdos de todas las responsabilidades.
- b) La identificación de las pérdidas aceptables de información y servicios.
- c) La implementación de procedimientos que permiten la recuperación y restauración de las operaciones de negocio y la disponibilidad de información en escalas de tiempo requerido. Se necesita particular atención para la evaluación de las dependencias de negocio externas e internas y de los contratos vigentes.
- d) Los procedimientos operacionales de seguimiento para completar la restauración y recuperación.

- e) La documentación de los procedimientos y procesos acordados.
- f) La formación apropiada del personal en los procedimientos y procesos de emergencia acordados, incluyendo la gestión de crisis.
- g) La prueba y actualización de los planes.

El proceso de planificación se debería centrar en los objetivos requeridos del negocio, por ejemplo, en la recuperación de servicios específicos a los clientes en un plazo aceptable.

Se deberían considerar los servicios y recursos necesarios para conseguirlo, incluyendo el personal, los recursos no informáticos y los contratos de respaldo de los dispositivos informáticos. Estos contratos pueden incluir arreglos con terceros en la forma de acuerdos recíprocos o servicios de suscripciones comerciales.

Lo planes de continuidad del negocio deben tratar las vulnerabilidades organizacionales y por lo tanto deben contener información sensible que necesita ser protegida apropiadamente. Las copias de los planes de continuidad del negocio deben ser guardadas en una locación remota, a una distancia suficiente para escapar de cualquier daño de un desastre en el sitio principal.

La gerencia debe asegurar que las copias de los planes de continuidad de negocio estén actualizadas y protegidas con el mismo nivel de seguridad aplicada al sitio principal.

Otro material necesario para ejecutar los planes e continuidad debe ser también almacenado en la locación remota.

Si se utilizan locaciones alternativas temporales, el nivel de control de seguridad implementada debe ser equivalente al sitio principal.

### **6.7.7 Conclusión**

Para este informe realizado se puede concluir que se deberá de seguir las recomendaciones dadas para implementar los controles propuestos en base al análisis de riesgo realizado. Se determina que si los riesgos detectados, no son tratados de forma correcta, estos podrían causar un daño severo en los activos del departamento y así interrumpir la continuidad del negocio de la organización.

### **6.8 Administración**

La presente propuesta será administrada por:

- El Jefe del Departamento de Tecnología de Información:
  - Ing. José Torres Manso
  
- Los Proponente:
  - Sr. Jorge Valdiviezo Troya
  - Sr. Roberto Rodríguez Poveda

## BIBLIOGRAFÍA

- AENOR, C. M. (2014). La norma ISO 27001 del Sistema de Gestión de la Seguridad de la Información. *Asociación Española para la Calidad (AEC)*, 40-46.
- Alan Calder, S. W. (2012). *IT Governance: An International Guide to Data Security and ISO27001/ISO27002*. USA: Kogan Page.
- Alberto Prieto, A. L. (2002). *Introducción a la Informática 3ª Edición*. España: McGraw-Hill.
- Angelica Mosquera Quinto, a. G. (2011). *Guía de referencia: los antivirus y sus tendencias futuras*. Colombia.
- Arribas, J. D. (2006). *Conocimientos Básicos de Informática*. Sevilla-España: Editorial MAD.
- bsi. (2013). *bsi*. Obtenido de <http://www.bsigroup.es/es/certificacion-y-auditoria/Sistemas-de-gestion/estandares-esquemas/Seguridad-de-la-Informacion-ISOIEC27001/>
- Carlos, U. J. (2008). *Dirección y gestión de los sistemas de información en la empresa*. Madrid: ESIC.
- (1996). *Cuadernos de Documentación Multimedia Vol. 5*. España.
- Gutierrez Cervantes, X. (s.f.). *Fuentes primarias y secundarias en un trabajo de investigación*. Obtenido de [http://www.ehowenespanol.com/fuentes-primarias-secundarias-investigacion-info\\_354586/](http://www.ehowenespanol.com/fuentes-primarias-secundarias-investigacion-info_354586/)
- Hesselbach, X. (2002). *Análisis de redes y sistemas de comunicaciones*. Barcelona-España: Edicions UPC.
- iso27000.es. (2012). *ISO 27000.es*. Obtenido de <http://www.iso27000.es/sgsi.html>
- Kosutic, C. D. (2014). *27001 Academy*. Obtenido de <http://www.iso27001standard.com/es/que-es-iso-27001/>



- Michelena, A. V. (2003). *Enredados. El mundo de la Internet*. Lima-Peru: Editorial Grijei.
- Pérez, E. H. (2003). *Tecnologías y redes de transmisión de datos*. Mexico DF - Mexico: Limusa.
- ROYER, J.-M. (2004). *Seguridad informática, riesgos, amenazas, prevención y soluciones*. Barcelona-España: Ediciones ENI.

## ANEXOS

### A.1 Imágenes de plantillas, encuestas y checklist realizadas

#### A.1.1 Plantilla de Levantamiento de Activos - APLICACIONES - SOFTWARE

#### ACTUALIZACIONES SISTEMA OPERATIVO


### LEVANTAMIENTO DE ACTIVOS - APLICACIONES

Nombre: Jose Torres  
 Departamento: Sistemas

APLICACIONES	
CODIGO: <u>API-001</u>	NOMBRE: <u>Software Actualizaciones</u>
DESCRIPCION: <u>Software que envia Actualizaciones del sistema a las maquinas</u>	
RESPONSABLE: <u>Sistemas</u>	
TIPO: <u>Aplicaciones Informaticas</u>	

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD	1	<u>Porque disponibilidad baja</u>
INTEGRIDAD	2	<u>La integridad es requerida</u>
CONFIDENCIALIDAD	2	<u>La informacion es de acceso privado</u>

DEPENDENCIA DE ACTIVOS INFERIORES	
activo: <u>EQUI-004</u>	grado: <u>alto</u>
<u>¿por qué?: Es necesario el equipo para q funcione el programa</u>	
activo: <u>EQUI-010</u>	grado: <u>alto</u>
<u>¿por qué?: Necesita la conexión con las maquinas para su correcta actualización</u>	
activo: <u>SRV-013</u>	grado: <u>Alto</u>
<u>¿por qué?: Necesita internet para que se actualice</u>	

  
 FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS. ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

A.1.2 Plantilla de Levantamiento de Activos - SERVICIOS - TRANSACCIÓN DE PAGO A PROVEEDORES


**LEVANTAMIENTO DE ACTIVOS - SERVICIOS**

Nombre: Jameth Cortava  
 Departamento: Contabilidad

SERVICIOS	
CODIGO: <u>SE R V - 001</u>	NOMBRE: <u>Transacción Pago a Proveedores</u>
DESCRIPCIÓN: <u>Proceso por el cual se le conciben los costos por pagar a los proveedores por medio de transferencias, concaración o cheques</u>	
RESPONSABLE: <u>Jameth Cortava</u>	
TIPO: <u>Servicio</u>	

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD	}	<u>Es muy necesario para la empresa debe tener los mejores costos lo debe tener la alta calidad</u>
INTEGRIDAD	}	
CONFIDENCIALIDAD	}	

DEPENDENCIA DE ACTIVOS INFERIORES	
activo: <u>Servicio de contabilidad</u>	grado: <u>Medio</u>
¿por qué?: <u>Debido que el sistema debe estar actualizado y libre de errores</u>	
activo: <u>Servicio de compras</u>	grado: <u>Alto</u>
¿por qué?: <u>El sistema debe estar conectado siempre</u>	
activo:	grado:
¿por qué?:	

  
INDUSTRIAS LÁCTEAS S.A.  
INDULAC  
 -----  
INDULAC FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS. ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

A.1.3 Plantilla de Levantamiento de Activos - EQUIPOS INFORMÁTICOS - ESTACIONES DE TRABAJO – COMPUTADORA


**LEVANTAMIENTO DE ACTIVOS – EQUIPOS INFORMATICOS**

Nombre: Ponameth Montezuma  
 Departamento: Contabilidad

EQUIPOS INFORMATICOS		
CODIGO: <u>Equi - 011</u>	NOMBRE: <u>PC</u>	
DESCRIPCION: Equipo con características comunes: Procesador Intel (P) Core (TM) i3 Memoria RAM de 512 GB Disco duro de 500 GB Sistema Operativo Windows 7 Profesional		
RESPONSABLE: <u>Ponameth Montezuma</u>		
UBICACION: <u>Area Contabilidad</u>		
NUMERO: <u>7</u>		
TIPO: <u>Equipo</u>		

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD	3	<u>Nunca disponible en el trabajo</u>
INTEGRIDAD	3	
CONFIDENCIALIDAD	3	<u>Se le da clasificacion de alta seguridad</u>

DEPENDENCIA DE ACTIVOS INFERIORES	
activo: <u>Inteligencia Humana</u>	grado: <u>Alto</u>
¿por qué?: <u>La computadora debe estar conectada a la red</u>	
activo: <u>Software de Actualización</u>	grado: <u>A Bn</u>
¿por qué?: <u>La computadora de estos actualizaciones</u>	
activo:	grado:
¿por qué?:	

  
 INDUSTRIAS LASCORAS S.A.  
 INDLASC  
 -----  
 FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS. ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

A.1.4 Plantilla de Levantamiento de Activos – REDES DE COMUNICACIÓN -  
CABLEADO ESTRUCTURADO


**LEVANTAMIENTO DE ACTIVOS- REDES DE COMUNICACION**

Nombre: Jose Torres  
Departamento: Sistema

REDES DE COMUNICACIÓN		
CÓDIGO: <u>Rede 001</u>	NOMBRE: <u>Cable Estructurado</u>	
DESCRIPCIÓN: <u>Compuesto por cable utp categoría 6A y fibra optica</u>		
RESPONSABLE: <u>Sistema</u>		
UBICACIÓN: <u>Sistema</u>		
NUMERO: <u>1</u>		
TIPO: <u>Redes de comunicaciones</u>		

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD	3	<u>Requiso disponibilidad alta</u>
INTEGRIDAD	3	<u>La integridad es requerida</u>
CONFIDENCIALIDAD	3	<u>La informacion es de datos valiosos</u>

DEPENDENCIA DE ACTIVOS INFERIORES	
activo: <u>INST-001</u>	grado: <u>Alto</u>
¿por qué?: <u>La instalación es requerida para el correcto funcionamiento</u>	
activo:	grado:
¿por qué?:	
activo:	grado:
¿por qué?:	

  
 -----  
 FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, **ACEPTA Y AVALA** TODOS LOS DATOS PROPORCIONADOS, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

A.1.5 Plantilla de Levantamiento de Activos - INSTALACIONES - DATA CENTER  
PLANTA


**LEVANTAMIENTO DE ACTIVOS - INSTALACIONES**

Nombre: Car. Rodriguez  
 Departamento: Sistemas

INSTALACIONES		
CODIGO: <u>INST-001</u>	NOMBRE: <u>Data center plant</u>	
DESCRIPCION:		
RESPONSABLE: <u>Car. Rodriguez</u>		
UBICACION: <u>Sistem</u>		
NUMERO: <u>1</u>		
TIPO: <u>Instalación</u>		

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD	2	<u>Requisito de capacidad de red.</u>
INTEGRIDAD	3	<u>Es integrada</u>
CONFIDENCIALIDAD	3	<u>Se refiere a los datos propios</u>

DEPENDENCIA DE ACTIVOS INFERIORES	
activo:	grado:
¿por qué?:	
activo:	grado:
¿por qué?:	
activo:	grado:
¿por qué?:	

  
 FIRMA DE ACEPTACION

---

AL FIRMAR ESTA ENCUESTA, **ACEPTA Y AVALA** TODOS LOS DATOS PROPORCIONADOS, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA.

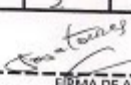
A.1.6 Plantilla de Levantamiento de Activos - PERSONAS - USUARIOS DE LA ORGANIZACIÓN

**LEVANTAMIENTO DE ACTIVOS - PERSONAS**

Nombre: Jose Torres  
 Departamento: \_\_\_\_\_

PERSONAS	
CODIGO: <u>1525-0001</u>	NOMBRE: <u>Usuarios de la Organización</u>
DESCRIPCION: <u>Usuarios que tienen acceso a Equipos Informativos y que se encuentran en los niveles de la administración</u>	
NUMERO: <u>Sistema</u>	
TIPO: <u>Usuarios</u>	

VALORACION	VALOR	JUSTIFICACION
DISPONIBILIDAD	3	<u>requiere disponibilidad alta</u>
INTEGRIDAD	3	<u>la integridad es indispensable</u>
CONFIDENCIALIDAD	3	<u>la información es restringida</u>

  
 -----  
 FIRMA DE ACEPTACION

AL FIRMAR ESTA ENCUESTA, **ACEPTA Y AVALA** TODOS LOS DATOS PROPORCIONADOS, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

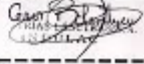


### A.1.7 CheckList – Routers

**Lista de Verificación - Router**

Nombre: Carra Pedregalqui  
 Departamento: Sistemas  
 Cargo: Coordinador de Área

CHECK LIST - ROUTER			
PREGUNTA	ALTO	MEDIO	BAJO
¿Se siguió algún estándar para la ubicación del dispositivo? (Medidas)		✓	
¿Este dispositivo esta en un lugar adecuado? (gabinete, cuarto de telecomunicaciones, etc.)	✓		
¿Tienen acceso a este dispositivo únicamente personal autorizado?	✓		
¿Es segura la ubicación del dispositivo frente a desastres naturales u otras eventualidades? (fugas de agua)			✓
¿El dispositivo tiene una alimentación de energía auxiliar?	✓		
¿Existe documentación acerca de la configuración actual del router?			✓
¿Posee un dispositivo similar a este almacenado como respaldo?		✓	
¿Se han borrado los usuarios y contraseñas que vienen por defecto en el router?	✓		
¿Se tiene ya un proveedor en caso de que se necesite renovar este equipo? (precios, tiempo, existencia)	✓		
¿Los banners que se muestran en el router no muestran información propia de la empresa?			✓
¿Existe alguna política para la administración de contraseñas de este dispositivo?	✓		
¿La persona que realiza las configuraciones del router posee alguna certificación?			✓
¿Se han realizan pruebas de hackeo ético para identificar las vulnerabilidades de este dispositivo?			✓
¿La persona que realiza las configuraciones del router tiene trabajo fijo en la empresa?			✓
¿En caso de fallo o falta de este dispositivo el negocio puede continuar?			✓
¿Se han realizan pruebas de hackeo ético para identificar las vulnerabilidades de este dispositivo?			✓

  
 FIRMA DE ACEPTACION

AL FIRMAR ESTE CHECK LIST, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**. ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA




### A.1.8 CheckList – Switchs

**Lista de Verificación - Switch**

Nombre: Carla Rodríguez  
 Departamento: Sistema  
 Cargo: Coordinadora de Area

CHECK LIST - SWITCH			
PREGUNTA	ALTO	MEDIO	BAJO
¿Se siguió algún estándar para la ubicación del dispositivo? (Medidas)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿Este dispositivo esta en un lugar adecuado? (gabinete, cuarto de telecomunicaciones, etc.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Tienen acceso a este dispositivo únicamente personal autorizado?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Es segura la ubicación del dispositivo frente a desastres naturales u otras eventualidades? (fugas de agua)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿El dispositivo tiene una alimentación de energía auxiliar?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Existe documentación acerca de la configuración actual del switch?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿Posee un dispositivo similar a este almacenado como respaldo?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿Se han borrado los usuarios y contraseñas que vienen por defecto en el switch?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Se tiene ya un proveedor en caso de que se necesite renovar este equipo? (precios, tiempo, existencia)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Los banners que se muestran en el switch no muestran información propia de la empresa?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿Existe alguna política para la administración de contraseñas de este dispositivo?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿La persona que realiza las configuraciones del switch posee alguna certificación?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿Se han realizan pruebas de hackeo ético para identificar las vulnerabilidades de este dispositivo?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿La persona que realiza las configuraciones del switch tiene trabajo fijo en la empresa?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿En caso de fallo o falta de este dispositivo el negocio puede continuar?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿Los puertos que no están siendo usados están correctamente bloqueados?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

  
 FIRMA DE ACEPTACION

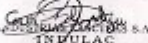
AL FIRMAR ESTE CHECK LIST, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

A.1.9 CheckList – PC

**Lista de Verificación - PC**

Nombre: Caron Belenizky  
 Departamento: Sistemas  
 Cargo: Coordinador de Area

CHECK LIST - PC			
PREGUNTA	ALTO	MEDIO	BAJO
¿Este dispositivo esta en un lugar protegido de robo?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿Tienen acceso a este dispositivo únicamente personal autorizado?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿Es segura la ubicación del dispositivo frente a desastres naturales u otras eventualidades?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿La persona que realiza las configuraciones del dispositivo posee conocimientos técnicos a cerca de este?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿El dispositivo tiene una alimentación de energía auxiliar?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Existe documentación acerca de la configuración actual del computador?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿Hay computadores de respaldo en caso de la ausencia de este?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Se tiene ya un proveedor en caso de que se necesite renovar este equipo? (precios, tiempo, existencia)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿En caso de fallo o falta de este dispositivo el negocio puede continuar?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿Se realiza mantenimiento periódico a este equipo?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

  
 TNPULAC  
 FIRMA DE ACEPTACION


AL FIRMAR ESTE CHECK LIST, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**. ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

A.1.10 CheckList – Servidores

**Lista de Verificación - Servidores**

Nombre: Geor Rodríguez  
 Departamento: Sistemas  
 Cargo: Coordinador de Srv

CHECK LIST - SERVIDORES			
PREGUNTA	ALTO	MEDIO	BAJO
¿Este dispositivo esta en un lugar adecuado? (tiene protección física)	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿Tienen acceso a este dispositivo únicamente personal autorizado?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Es segura la ubicación del dispositivo frente a desastres naturales u otras eventualidades?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿La persona que realiza las configuraciones del dispositivo posee conocimientos técnicos a cerca de este?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿El dispositivo tiene una alimentación de energía auxiliar?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Existe documentación acerca de la configuración actual del dispositivo?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Posee un dispositivo similar a este almacenado como respaldo?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿Se tiene ya un proveedor en caso de que se necesite renovar este equipo? (precios, tiempo, existencia)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿En caso de fallo o falta de este dispositivo el negocio puede continuar?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿Se realiza mantenimiento periódico a este equipo?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

  
 FIRMADO EN: 13/01/2017

-----  
 FIRMA DE ACEPTACIÓN


AL FIRMAR ESTE CHECK LIST, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**. ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

A.1.11 CheckList – Cableado y Redes

**Lista de Verificación – Cableado y Redes**

Nombre: César Beltrán  
 Departamento: Sistemas  
 Cargo: Coordinador de Área

CHECK LIST - CABLEADO			
PREGUNTA	ALTO	MEDIO	BAJO
¿Se ha seguido algún estándar para la implementación de cableado estructurado?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿Se han realizado pruebas de cables certificados?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
¿Existen enlaces redundantes en los enlaces de mayor importancia?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
¿Existen puntos de acceso a la red que no estén debidamente protegidos?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
¿En caso de fallo o falta de este dispositivo el negocio puede continuar?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

  
 INDIPLAC S.A.  
 INDIPLAC


-----  
 FIRMA DE ACEPTACION

AL FIRMAR ESTE CHECK LIST, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA

Nombre: César Beltrán  
 Departamento: Sistemas  
 Cargo: Coordinador de Área

CHECK LIST - REDES			
PREGUNTA	ALTO	MEDIO	BAJO
¿Existe un inventario sobre los dispositivos de redes y telecomunicaciones, así también como del personal a cargo de estos?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

  
 INDIPLAC S.A.  
 INDIPLAC

-----  
 FIRMA DE ACEPTACION

AL FIRMAR ESTE CHECK LIST, **ACEPTA Y AVALA TODOS LOS DATOS PROPORCIONADOS**, ESTA INFORMACION SERA UTILIZADA UNICAMENTE PARA EFECTO DE INVESTIGACION DE TESIS UNIVERSITARIA



**A.2 Imágenes data center**

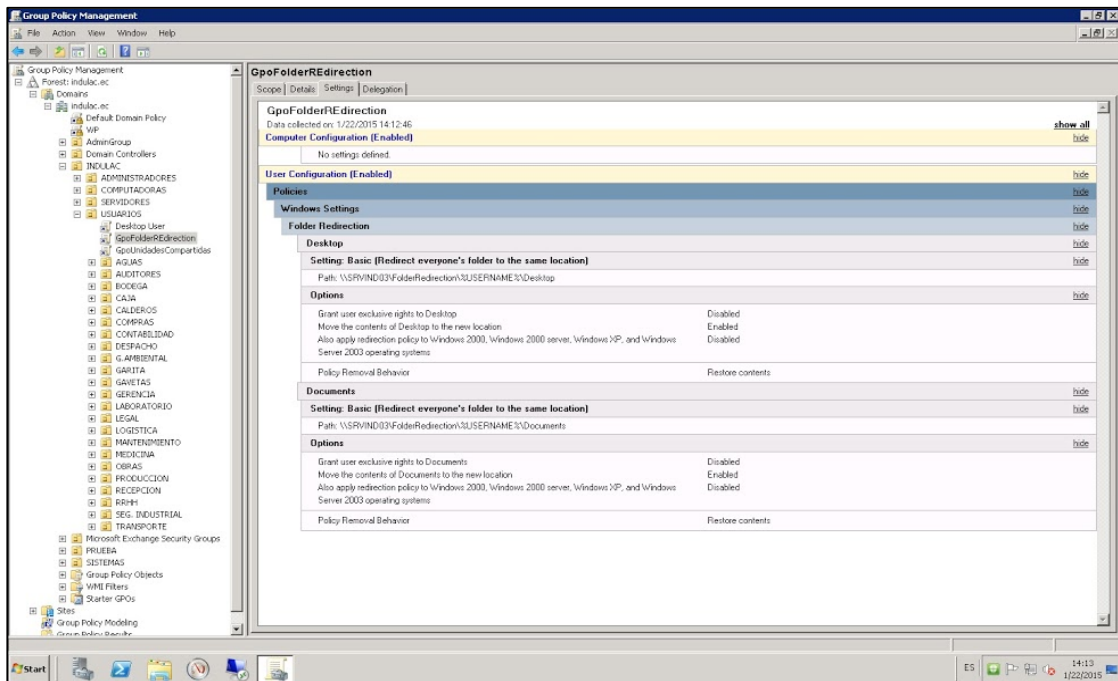
**A.2.1 Servidor en rack de comunicaciones**



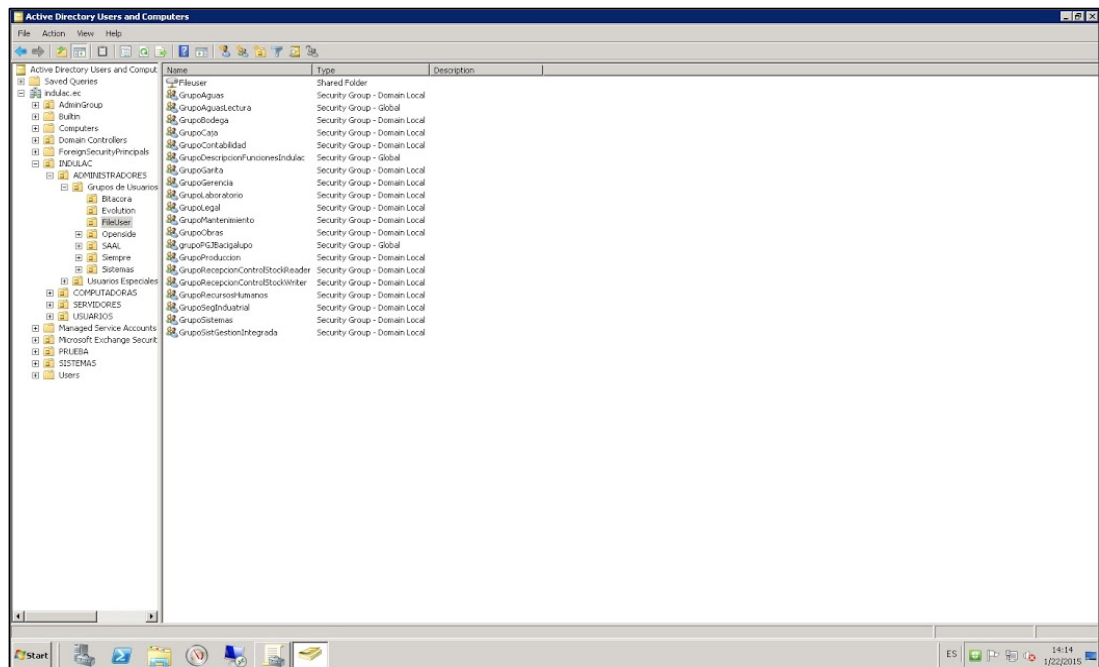


## A.3 Imágenes de servidores (software)

### A.3.1 Servidor de Carpetas Compartidas – Folder Redirection

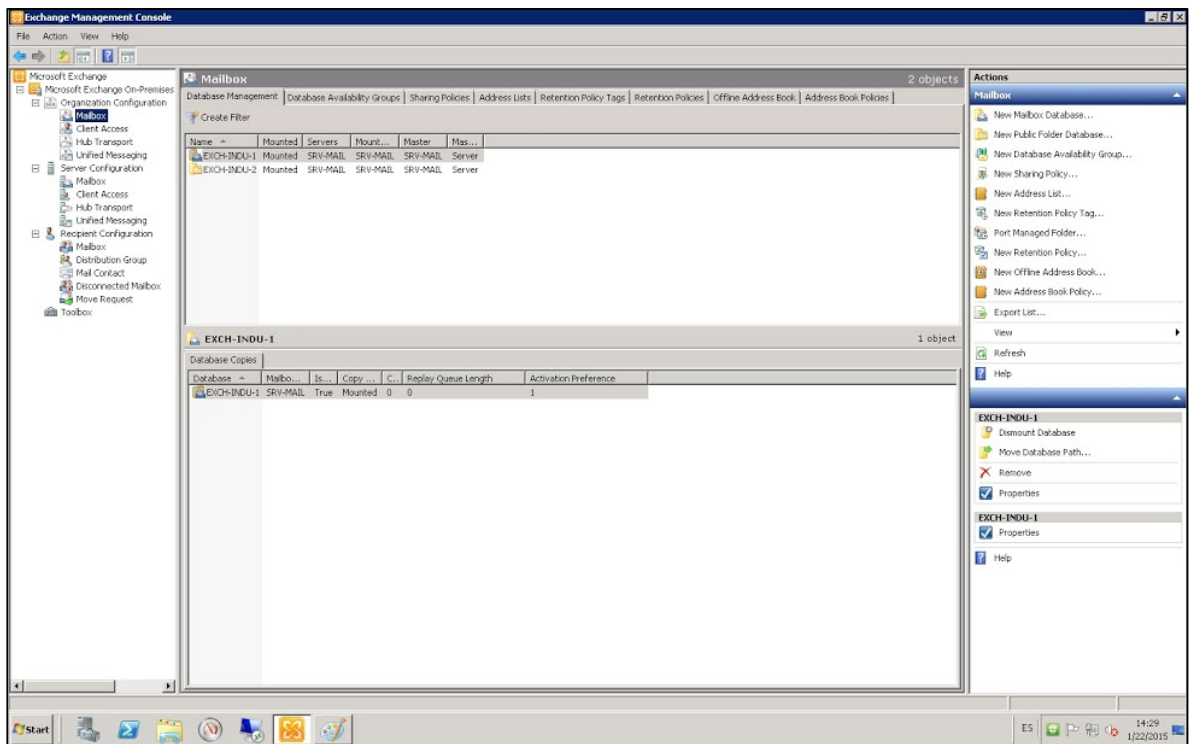
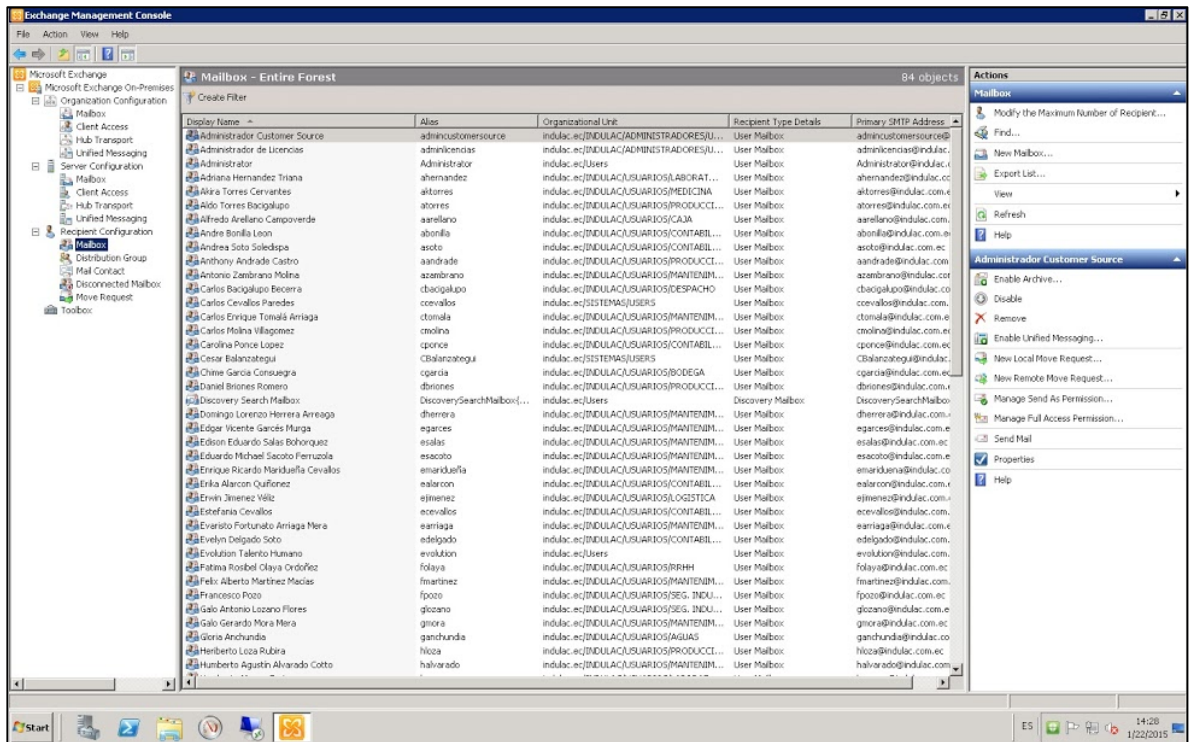


### A.3.2 Servidor de Directorio Activo



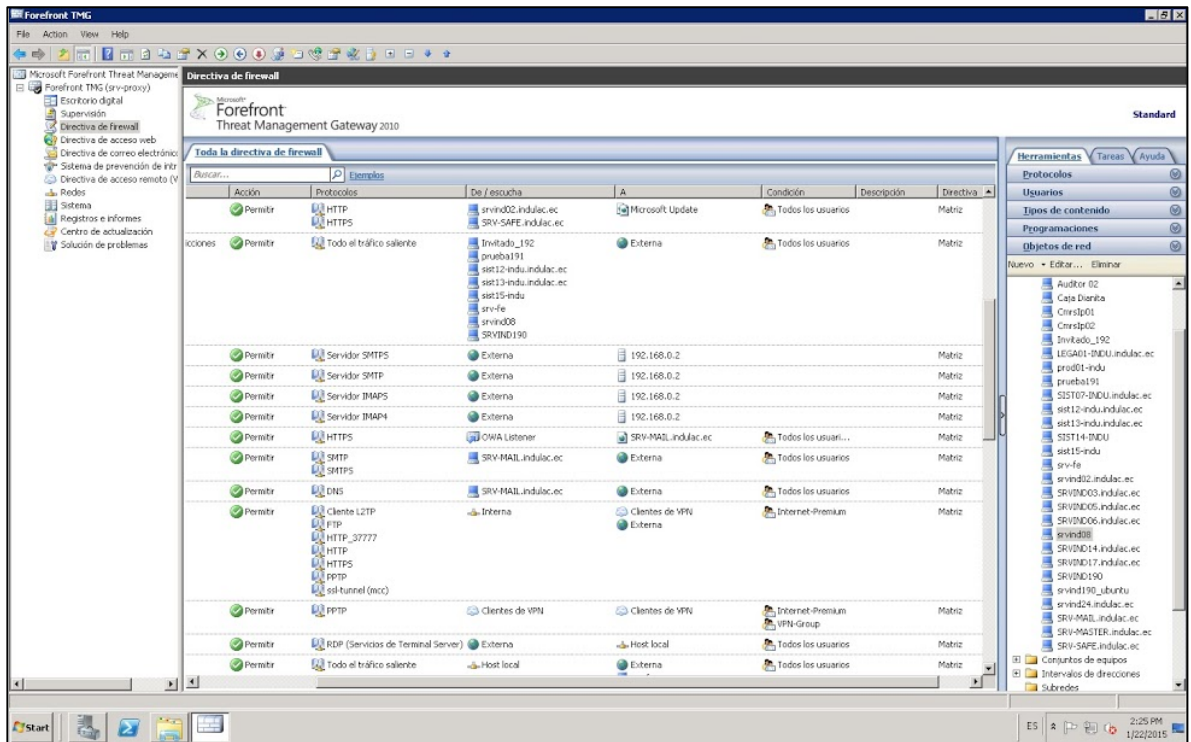


### A.3.3 Servidor de Exchange Server

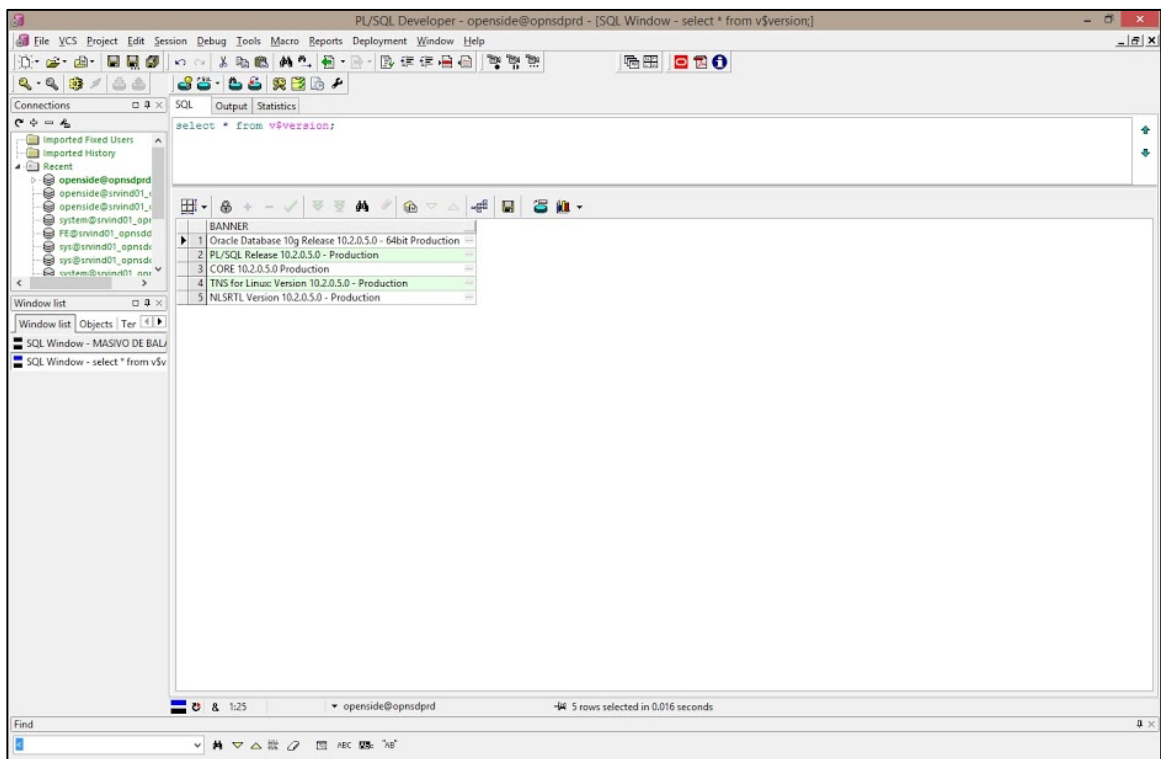




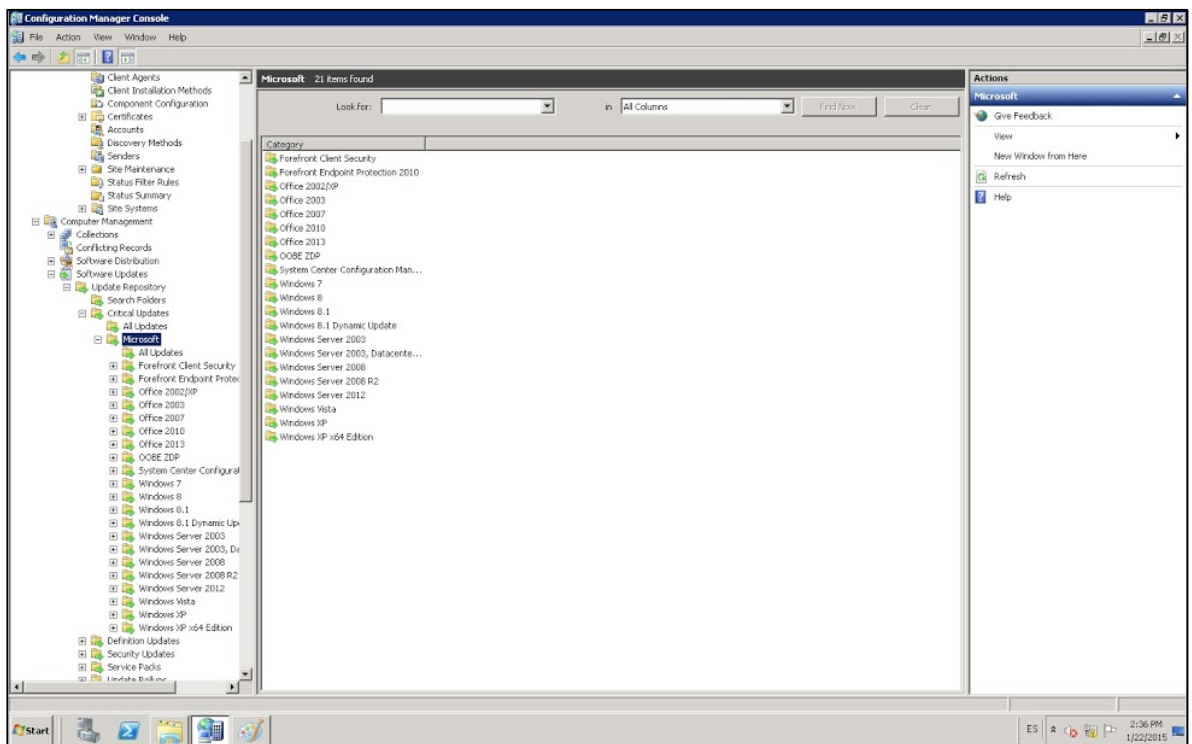
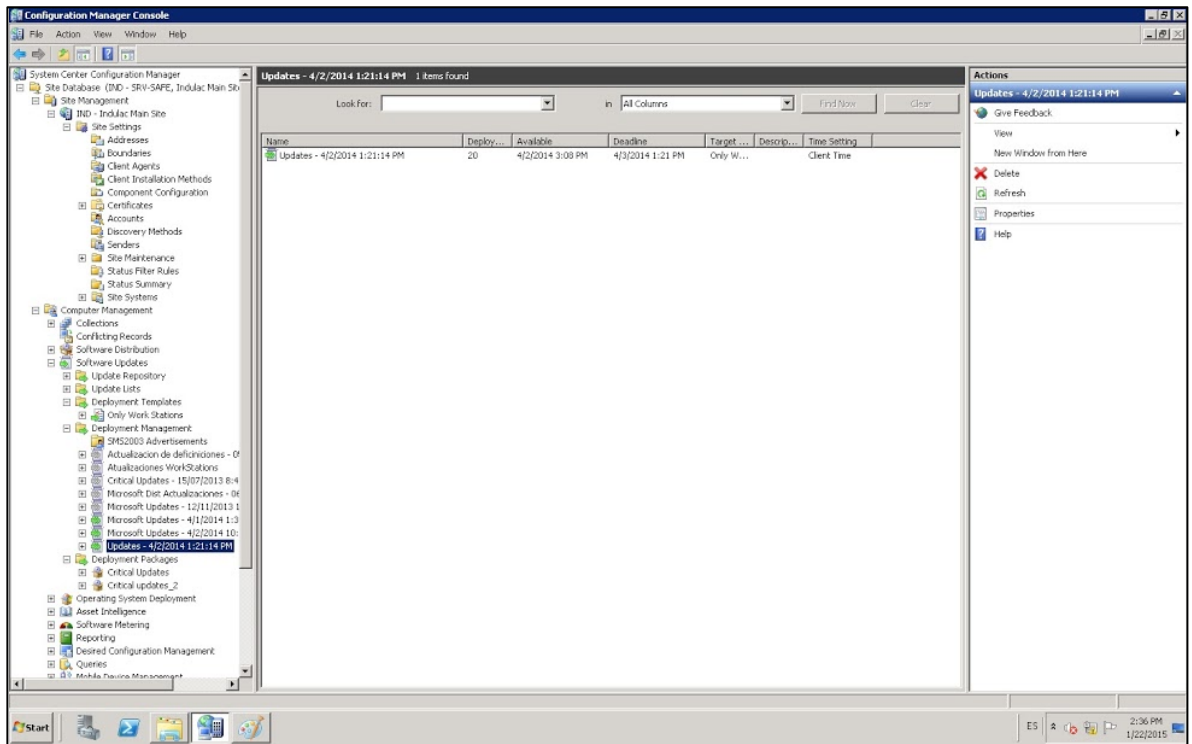
### A.3.4 Servidor de Forefront (Firewall-proxy)



### A.3.5 Servidor de ORACLE



### A.3.6 Servidor de Actualizaciones



#### **A.4 Imágenes de las instalaciones**

##### **A.4.1 Imágenes de las instalaciones – Amenaza Daño por Agua**



##### **A.4.2 Imágenes de las instalaciones – Amenaza Condiciones inadecuadas de temperatura y humedad**

###### **A.4.2.1 Imágenes de las instalaciones – Paredes con humedad**





**A.4.2.2 Imágenes de las instalaciones – Cielo raso con humedad - Figura 1**



**A.4.2.2 Imágenes de las instalaciones – Cielo raso con humedad - Figura 2**



**A.4.2.3 Imágenes de las instalaciones – Poco servicio de aire acondicionado**



**A.4.2.4 Imágenes de las instalaciones – Oxidación de Rack de comunicaciones**





**A.4.3 Imágenes de las instalaciones – Amenaza Robo**



**A.4.4 Imágenes de las instalaciones – Defecto de infraestructura**



### A.5 Identificación de activos

CODIGO	NOMBRE	CODIGO	DESCRIPCION	CANTIDA D	CLASIFICACIÓN	DEPARTAMENT O
SERV-001	TRANSACCION DE PAGO A PROVEEDORES	SERV-001	PROCESO POR EL CUAL SE LE CANCELAN LAS CUENTAS POR PAGAR A LOS PROVEEDORES POR MEDIO DE TRANSFERENCIAS BANCARIAS O CHEQUES	1	SERVICIO	CONTABILIDAD
SERV-002	TRANSACCION DE PAGO DE NOMINAS	SERV-002	PROCESO EN EL CUAL SE PAGA LA NOMINA A LOS EMPLEADOS POR MEDIO DE TRANSFERENCIAS BANCARIAS	1	SERVICIO	TALENTO HUMANO
SERV-003	TRANSACCION DE REGISTRO DE INVENTARIO A BODEGA	SERV-003	PROCESO POR EL CUAL SE REGISTRAN LAS ENTRADAS Y SALIDAS DE DIFERENTES ARTICULOS A BODEGA	1	SERVICIO	LOGISTICA
SERV-004	TRANSACCION DE REGISTRO DE FACTURA Y COBRANZA	SERV-004	PROCESO EN EL CUAL SE REGISTRAN LAS FACTURAS DE VENTAS Y SE REALIZA EL	1	SERVICIO	VENTAS



			COBRO DE LAS MISMAS			
SERV-005	TRANSACCION DE COTIZACIONES Y COMPRAS	SERV-005	PROCESO EN EL QUE SE REALIZA COTIZACIONES Y COMPRAS DE LOS DIFERENTES ARTICULOS O SERVICIOS QUE NECESITA LA ORGANIZACIÓN	1	SERVICIO	COMPRAS
SERV-006	TELEFONÍA FIJA	SERV-006	central que permite la comunicación telefónica	1	SERVICIO	SISTEMAS
SERV-007	SOPORTE TÉCNICO	SERV-007	soporte brindado al personal de la organización	1	SERVICIO	SISTEMAS
SERV-008	SOPORTE OPENSIDE	SERV-008	soporte brindado a la aplicación administrativa manejada en la compañía	1	SERVICIO	SISTEMAS
SERV-009	SOPORTE EVOLUTION	SERV-009	soporte brindado a la aplicación de Recursos Humanos manejada en la compañía	1	SERVICIO	SISTEMAS
SERV-010	MOTOR DE BASE DE DATOS	SERV-010	BASE DE DATOS ORACLE STANDARD EDITION 9i	1	SERVICIO	SISTEMAS
SERV-011	DIRECTORIO ACTIVO	SERV-011	SERVICIO QUE PERMITE CREAR, ADMINISTRAR Y ELIMINAR LOS USUARIOS,	1	SERVICIO	SISTEMAS

			GRUPOS DE USUARIOS Y POLITICAS QUE SE UTILIZARAN EN LA RED DENTRO DE LA ORGANIZACIÓN.			
SERV-012	CORREO ELECTRONICO	SERV-012	EXCHANGE SERVER 2010 STANDARD EDITION	1	SERVICIO	SISTEMAS
SERV-013	SERVICIO DE INTERNET	SERV-013	SERVICIO QUE BRINDA UN PROVEEDOR EXTERNO	1	SERVICIO	SISTEMAS
SERV-014	SERVICIO DE REDIRECCIONAMIENTO DE CARPETAS	SERV-014	SERVICIO QUE RESPALDA LOS ARCHIVOS QUE LOS USUARIOS GUARDAN EN EL "ESCRITORIO" Y "MIS DOCUMENTOS". LOS ARCHIVOS SON RESPALDADOS EN UN SERVIDOR	1	SERVICIO	SISTEMAS
SERV-015	NETWORKING	SERV-015	DIRECCIONAMIENTO IP, PERMISOS DE REDES	1	SERVICIO	SISTEMAS
REDE-001	CABLEADO ESTRUCTURADO	REDE-001	CONFORMADA POR CABLE UTP CATEGORIA 6A Y FIBRA OPTICA, PUNTOS DE RED	1	REDES DE COMUNICACIONES	SISTEMAS
INST-001	DATA CENTER PLANTA	INST-001	INFRAESTRUCTURA DE LA PLANTA EN LA CUAL SE	1	INSTALACIONES	SISTEMAS

			ENCUENTRAN LOS SERVIDORES			
PERS-001	USUARIOS DE LA ORGANIZACIÓN	PERS-001	USUARIOS QUE TIENEN ACCESO A EQUIPOS INFORMATICOS Y QUE SE ENCUENTRAN CREADOS DENTRO DEL DIRECTORIO ACTIVO	40	PERSONAS	
APLI-001	SOFTWARE ACTUALIZACIONES SISTEMA OPERATIVO	APLI-001	SOFTWARE QUE ENVIA ACTUALIZACIONES DEL SISTEMA A LAS MAQUINAS QUE SE ENCUENTRAN EN EL DIRECTORIO ACTIVO	1	APLICACIONES INFORMÁTICAS	SISTEMAS
APLI-002	SOFTWARE PROXY - FIREWALL	APLI-002	TMG FOREFRONT PROTECTION. SOFTWARE QUE ADMINISTRA REGLAS DE ACCESO A INTERNET Y TAMBIEN RESTRINGUE EL ACCESO A USUARIOS NO AUTORIZADOS	1	APLICACIONES INFORMÁTICAS	SISTEMAS
APLI-003	NORMAS, POLITICAS Y PROCEDIMIENTOS DEL AREA	APLI-003	políticas y procedimientos sobre el buen uso de los equipos de la compañía	6	APLICACIONES INFORMÁTICAS	SISTEMAS

APLI-004	MANUALES	APLI-004	manuales guardados sobre el funcionamiento e instalación de las aplicaciones de la compañía	20	APLICACIONES INFORMÁTICAS	SISTEMAS
APLI-005	APLICACIONES ADMINISTRATIVAS Y RECURSOS HUMANOS	APLI-005	OPENSIDE - EVOLUTION	2	APLICACIONES INFORMÁTICAS	SISTEMAS
APLI-006	RESPALDO DE SERVIDORES	APLI-006	SOFTWARE QUE GUARDA RESPALDOS DIARIOS DE CONFIGURACIONES Y ARCHIVOS DE LOS SERVIDORES	1	APLICACIONES INFORMÁTICAS	SISTEMAS
APLI-007	SOFTWARE CAMARAS IP	APLI-007	SOFTWARE QUE ADMINISTRA LAS CAMARAS INSTALADAS EN LA ORGANIZACIÓN	1	APLICACIONES INFORMÁTICAS	SISTEMAS
APLI-008	ANTIVIRUS	APLI-008	SOFTWARE QUE PERMITE DETECTAR Y ELIMINAR VIRUS QUE SE ENCUENTREN EN LOS EQUIPOS DE LA ORGANIZACIÓN	1	APLICACIONES INFORMÁTICAS	SISTEMAS
EQUI-001	SERVIDOR DE DIRECTORIO ACTIVO	EQUI-001	Procesador Intel® Xeon® E5320 1.86GHz Memoria RAM de 2GB HP Disco Duro de	1	EQUIPOS INFORMÁTICOS	SISTEMAS

			70GB HP LOGICAL VOLUMEN SCSI Sistema Operativo Windows Server 2008 R2 standard Edition			
EQUI-002	SERVIDOR DE CORREO ELECTRÓNICO	EQUI-002	Procesador Intel® Xeon® E5620 (4 core, 2.40 GHz, 12MB L3, 80W) Memoria RAM de 10GB HP Disco Duro de 500GB HP LOGICAL VOLUMEN SCSI Sistema Operativo Windows Server 2008 R2 standard Edition	1	EQUIPOS INFORMÁTICOS	SISTEMAS
EQUI-003	SERVIDOR DE INTERNET PROXY – FIREWALL	EQUI-003	Procesador Intel® Xeon® E5430 2,66GHz Memoria RAM de 4GB HP Disco Duro de 130GB HP LOGICAL VOLUMEN SCSI Sistema Operativo Windows Server 2008 R2 standard Edition	1	EQUIPOS INFORMÁTICOS	SISTEMAS

EQUI-004	SERVIDOR DE CARPETAS COMPARTIDAS	EQUI-004	Procesador Intel® Xeon® E5645 2.40GHz Memoria RAM de 10GB HP Disco Duro de 1.36TB HP LOGICAL VOLUMEN SCSI Sistema Operativo Windows Server 2008 R2 standard Edition	1	EQUIPOS INFORMÁTICOS	SISTEMAS
EQUI-005	SERVIDORES DE APLICACIÓN Y BASE DE DATOS	EQUI-005	Procesador Intel® Xeon® E5645 2.40GHz Memoria RAM de 10GB HP Disco Duro de 1.36TB HP LOGICAL VOLUMEN SCSI Sistema Operativo Windows Server 2008 R2 standard Edition	2	EQUIPOS INFORMÁTICOS	SISTEMAS
EQUI-006	SERVIDOR DE RESPALDO	EQUI-006	Procesador CORE 2 DUO 2,8 GHz Memoria RAM de 2GB DDR2 KINSTONG 667Mhz Disco Duro de 4TB Sistema Operativo Ubuntu	1	EQUIPOS INFORMÁTICOS	SISTEMAS

			Server 12.04			
EQUI-007	SERVIDOR DE ACTUALIZACIONES Y ANTIVIRUS	EQUI-007	Procesador Intel® Xeon® E5430 2,66GHz Memoria RAM de 10GB HP Disco Duro de 675GB HP LOGICAL VOLUMEN SCSI Sistema Operativo Windows Server 2012 SE	1	EQUIPOS INFORMÁTICOS	SISTEMAS
EQUI-008	SERVIDORES PARA CÁMARAS IP	EQUI-008	Procesador Intel® Core™ i5-2400 (6M Cache, up to 3.40 GHz) Memoria RAM de 2GB DD 24TB SATA II Sistema Operativo propio del fabricante	2	EQUIPOS INFORMÁTICOS	SISTEMAS
EQUI-009	ROUTER DE COMUNICACIONES	EQUI-009	Router Cisco dado por el ISP	1	EQUIPOS INFORMÁTICOS	SISTEMAS
EQUI-010	SWITCH DE COMUNICACIONES	EQUI-010	Switch Cisco que interconectan la red Interna	14	EQUIPOS INFORMÁTICOS	SISTEMAS
EQUI-011	ESTACIONES DE TRABAJO - COMPUTADORA	EQUI-011	Equipos con características comunes: Procesador Intel(R) Core(TM) i3	7	EQUIPOS INFORMÁTICOS	CONTABILIDAD

			Memoria RAM de 2GB DD 500GB Sistema Operativo Windows 7			
EQUI-012	ESTACIONES DE TRABAJO - COMPUTADORA	EQUI-012	Equipos con características comunes: Procesador Intel(R) Core(TM) i3 Memoria RAM 2GB DD 500GB Sistema Operativo Windows 7	4	EQUIPOS INFORMÁTICOS	TALENTO HUMANO
EQUI-013	ESTACIONES DE TRABAJO - COMPUTADORA	EQUI-013	Equipos con características comunes: Procesador Intel(R) Core(TM) i3 Memoria RAM de 2GB DD 500GB Sistema Operativo Windows 7	4	EQUIPOS INFORMÁTICOS	PRODUCCION
EQUI-014	ESTACIONES DE TRABAJO - COMPUTADORA	EQUI-014	Equipos con características comunes: Procesador Intel(R) Core(TM) i3 Memoria RAM de 2GB	15	EQUIPOS INFORMÁTICOS	SISTEMAS



			DD 500GB Sistema Operativo Windows 7			
EQUI-015	ESTACIONES DE TRABAJO - COMPUTADORA	EQUI-015	Equipos con características comunes: Procesador Intel(R) Core(TM) i3 Memoria RAM de 2GB DD 500GB Sistema Operativo Windows 7	3	EQUIPOS INFORMÁTICOS	LOGISTICA
EQUI-016	ESTACIONES DE TRABAJO - COMPUTADORA	EQUI-016	Equipos con características comunes: Procesador Intel(R) Core(TM) i3 Memoria RAM 2GB DD 500GB Sistema Operativo Windows 7	2	EQUIPOS INFORMÁTICOS	VENTAS
EQUI-017	ESTACIONES DE TRABAJO - COMPUTADORA	EQUI-017	Equipos con características comunes: Procesador Intel(R) Core(TM) i3 Memoria RAM de 2GB Disco Duro de	2	EQUIPOS INFORMÁTICOS	COMPRAS

			500GB Sistema Operativo Windows 7			
EQUI-018	DISCOS DUROS USB DE RESPALDOS	EQUI-018	DISCOS DUROS EXTERNOS UTILIZADOS PARA RESPALDOS DE INFORMACIÓN	3	EQUIPOS INFORMÁTICOS	SISTEMAS

### A.6 Identificación de amenazas

CLASIFICACIÓN	AMENAZA	VULNERABILIDAD	GRUPO DE ACTIVO QUE PUEDE AFECTAR
AMENAZAS DE ORIGEN NATURAL	Fuego Daños por agua Desastres naturales (Terremotos)	Falta de protección contra fuego Falta de protección estructural contra agua Problemas origen estructural donde se encuentre el activo	Equipos informáticos Instalaciones Redes de Comunicaciones
AMENAZAS DE ORIGEN INDUSTRIAL	Desastres industriales (Fuga de amoniaco) Corte de suministro eléctrico Condiciones inadecuadas de temperatura y humedad	Falta de controles ante posible fuga Funcionamiento inadecuado de los UPS Mal funcionamiento de climatización en la empresa	Equipos informáticos Instalaciones; Personas Redes de Comunicaciones
CAUSADAS POR LAS PERSONAS DE FORMA ACCIDENTAL	Errores de Usuario Difusión de software dañino Fugas de información Vulnerabilidades de los programas Caída del sistema por agotamiento de recursos Restauración fallida de respaldos Errores mantenimiento actualización programas Errores de mantenimiento actualización de equipos Indisponibilidad del personal	Falta de capacitación Falta o fallo en antivirus Inexistentes controles de aseguramiento de información Problemas con actualización o software no depurado Equipos con características mínimas para el trabajo Falta procedimientos generar respaldos y restaurar los mismos Controles bajos o nulos de actualización de software Controles bajos o nulos de actualización de equipos Bajos o nulos controles de control de personal	Servicios Aplicaciones informáticas Personas Equipos informáticos Redes de Comunicaciones
CAUSADAS	Uso no previsto de los recursos	Falta de políticas sobre usos de los recursos y controles de	

POR LAS PERSONAS DE FORMA DELIBERADA	Suplantación de Identidad	acceso	Equipos informáticos Servicios Aplicaciones informáticas Redes de Comunicaciones Personas
	Modificación deliberada de la información	Falta de controles de acceso del personal Falta de procedimientos y control de cambios en la información	
	Divulgación de información	Almacenamiento no protegido	
	Robo	Falta controles de entrada y salida de recursos	
Manipulación de programas manipulación de equipos Ingeniería Social	Falta de controles de modificación de programas Falta de controles de manipulación de equipos Falta de procedimientos para el acceso a la información		

## A.7 Criterios de valoración

### A.7.1 Criterios de valoración de activos

DIMENSIÓN	VALOR	CLASE	DESCRIPCIÓN
<b>Disponibilidad</b>	1	Bajo	Los procesos de la empresa no se ven afectados si esta información no se encuentra disponible
	2	Mediano	Si la información no se encuentra disponible puede que afecte a los procesos que la utilizan. Sin embargo, existen métodos de contingencia para el desarrollo de las operaciones o el proceso podría esperar hasta que se encuentre disponible la información
	3	Alto	Los procesos de la organización pueden llegar a tener un fatal efecto si esta información no se encuentra disponible en el momento que se la necesita
<b>Integridad</b>	1	No requerida	Esta información es utilizada para consultas
	2	Requerida	Se requiere integridad en la información pero si el contenido de esta llega a ser falsificado, las operaciones no se verían afectadas gravemente
	3	Obligatoria	Puede causar un efecto falta en las operaciones de la empresa si la integridad de esta información se perdiera
<b>Confidencialidad</b>	1	Acceso Publica	Información que puede ser revelada a terceras partes.
	2	Acceso Privado	Información que solo puede ser revelada al personal de la empresa. Si el contenido fuera revelado a terceras partes, no hubiera mucho efecto en las operaciones de la empresa.
	3	Restringido	Información que solo es revelada a partes específicas y departamentos de la organización. Si el contenido es revelado a personal no autorizado, puede haber un gran efecto en las operaciones de la empresa.

### A.7.2 Criterios de valoración de amenazas

DIMENSIÓN	VALOR	CLASE	DESCRIPCIÓN
DEGRADACIÓN DEL ACTIVO	1	Bajo	Si ocurre la amenaza, el activo no se vería degradado gravemente
	2	Regular	Si la amenaza ocurre, el activo se vería degradado de manera regular
	3	Alto	Si la amenaza ocurre, el activo se vería degradado gravemente
PROBABILIDAD DE OCURRENCIA	1	Bajo	Existe una baja probabilidad. La frecuencia de ocurrencia es una vez al año o menos.
	2	Medio	Existe una probabilidad moderada. La frecuencia de ocurrencia es una vez cada 6 meses o menos.
	3	Alto	Existe una alta probabilidad. La frecuencia de ocurrencia es una vez al mes o más.

### A.7.3 Criterios de valoración de vulnerabilidades

DIMENSIÓN	VALOR	CLASE	DESCRIPCIÓN
Control de seguridad	1	Alto	Controles establecidos y adecuados para combatir la amenaza
	2	Medio	Control medio de seguridad
	3	Bajo	Escasos o inexistentes controles de seguridad

### A.8 Valoración de activos

CODIGO	ACTIVO	CLASIFICACIÓN	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
SERV-001	TRANSACCION DE PAGO A PROVEEDORES	SERVICIO	3	3	3
SERV-002	TRANSACCION DE PAGO DE NOMINAS	SERVICIO	3	3	3
SERV-003	TRANSACCION DE REGISTRO DE INVENTARIO A BODEGA	SERVICIO	3	3	3
SERV-004	TRANSACCION DE REGISTRO DE FACTURA Y COBRANZA	SERVICIO	3	3	3
SERV-005	TRANSACCION DE COTIZACIONES Y COMPRAS	SERVICIO	3	3	3
SERV-006	TELEFONÍA FIJA	SERVICIO	3	3	3

SERV-007	SOPORTE TÉCNICO	SERVICIO	3	2	2
SERV-008	SOPORTE OPENSIDE	SERVICIO	3	3	3
SERV-009	SOPORTE EVOLUTION	SERVICIO	3	3	3
SERV-010	MOTOR DE BASE DE DATOS	SERVICIO	3	3	3
SERV-011	DIRECTORIO ACTIVO	SERVICIO	3	2	2
SERV-012	CORREO ELECTRONICO	SERVICIO	3	3	3
SERV-013	SERVICIO DE INTERNET	SERVICIO	3	2	2
SERV-014	SERVICIO DE REDIRECCIONAMIENTO DE CARPETAS	SERVICIO	3	3	3
SERV-015	NETWORKING	SERVICIO	3	3	3
REDE-001	CABLEADO ESTRUCTURADO	REDES DE COMUNICACIONES	3	3	3
INST-001	DATA CENTER PLANTA	INSTALACIONES	2	3	3
PERS-001	USUARIOS DE LA ORGANIZACIÓN	PERSONAS	3	3	3
APLI-001	SOFTWARE ACTUALIZACIONES SISTEMA OPERATIVO	APLICACIONES INFORMÁTICAS	1	2	2
APLI-002	SOFTWARE PROXY - FIREWALL	APLICACIONES INFORMÁTICAS	2	2	3
APLI-003	NORMAS, POLITICAS Y PROCEDIMIENTOS DEL AREA	APLICACIONES INFORMÁTICAS	3	3	2
APLI-004	MANUALES	APLICACIONES INFORMÁTICAS	3	3	3
APLI-005	APLICACIONES ADMINISTRATIVAS Y RECURSOS HUMANOS	APLICACIONES INFORMÁTICAS	3	3	3
APLI-006	RESPALDO DE SERVIDORES	APLICACIONES INFORMÁTICAS	3	3	3
APLI-007	SOFTWARE CAMARAS IP	APLICACIONES INFORMÁTICAS	2	3	2
APLI-008	ANTIVIRUS	APLICACIONES INFORMÁTICAS	2	2	1

EQUI-001	SERVIDOR DE DIRECTORIO ACTIVO	EQUIPOS INFORMÁTICOS	3	2	3
EQUI-002	SERVIDOR DE CORREO ELECTRÓNICO	EQUIPOS INFORMÁTICOS	3	2	3
EQUI-003	SERVIDOR DE INTERNET PROXY – FIREWALL	EQUIPOS INFORMÁTICOS	3	2	3
EQUI-004	SERVIDOR DE CARPETAS COMPARTIDAS	EQUIPOS INFORMÁTICOS	2	2	3
EQUI-005	SERVIDORES DE APLICACIÓN Y BASE DE DATOS	EQUIPOS INFORMÁTICOS	3	3	3
EQUI-006	SERVIDOR DE RESPALDO	EQUIPOS INFORMÁTICOS	3	3	3
EQUI-007	SERVIDOR DE ACTUALIZACIONES Y ANTIVIRUS	EQUIPOS INFORMÁTICOS	1	2	2
EQUI-008	SERVIDORES PARA CÁMARAS IP	EQUIPOS INFORMÁTICOS	2	3	2
EQUI-009	ROUTER DE COMUNICACIONES	EQUIPOS INFORMÁTICOS	3	3	2
EQUI-010	SWITCH DE COMUNICACIONES	EQUIPOS INFORMÁTICOS	3	3	2
EQUI-011	ESTACIONES DE TRABAJO - COMPUTADORA - CONTABILIDAD	EQUIPOS INFORMÁTICOS	3	3	3
EQUI-012	ESTACIONES DE TRABAJO - COMPUTADORA - TALENTO HUMANO	EQUIPOS INFORMÁTICOS	3	3	3
EQUI-013	ESTACIONES DE TRABAJO - COMPUTADORA - PRODUCCION	EQUIPOS INFORMÁTICOS	3	3	3
EQUI-014	ESTACIONES DE TRABAJO - COMPUTADORA - SISTEMAS	EQUIPOS INFORMÁTICOS	3	3	3
EQUI-015	ESTACIONES DE TRABAJO - COMPUTADORA - LOGISTICA	EQUIPOS INFORMÁTICOS	3	3	3
EQUI-016	ESTACIONES DE TRABAJO - COMPUTADORA - VENTAS	EQUIPOS INFORMÁTICOS	3	3	3
EQUI-017	ESTACIONES DE TRABAJO - COMPUTADORA - COMPRAS	EQUIPOS INFORMÁTICOS	3	3	3
EQUI-018	DISCOS DUROS USB DE RESPALDOS	EQUIPOS INFORMÁTICOS	2	3	3

## A.9 Valoración de amenazas

ACTIVO	AMENAZA			VULNERABILIDAD	
	DESCRIPCION	DEGRADACIÓN DE ACTIVO	PROBABILIDAD DE OCURRENCIA	DESCRIPCION	CONTROL DE SEGURIDAD
TRANSACCION DE PAGO A PROVEEDORES	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	3
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	3	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	2	ALMACENAMIENTO NO PROTEGIDO	1
TRANSACCION DE PAGO DE NOMINAS	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	3
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
TRANSACCION DE REGISTRO DE INVENTARIO A BODEGA	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	3

	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	3
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
TRANSACCION DE REGISTRO DE FACTURA Y COBRANZA	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	3
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
TRANSACCION DE COTIZACIONES Y COMPRAS	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
TELEFONÍA FIJA	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	2
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2



	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
SOPORTE TÉCNICO	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	3
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2
	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	3
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
	ERRORES DE USUARIO	2	2	FALTA DE CAPACITACION	3
SOPORTE OPENSIDE	FUGAS DE INFORMACIÓN	1	2	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1
SOPORTE EVOLUTION	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2

	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
MOTOR DE BASE DE DATOS	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
DIRECTORIO ACTIVO	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	3	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
CORREO ELECTRONICO	ERRORES DE USUARIO	1	3	FALTA DE CAPACITACION	2
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	3	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
SERVICIO DE	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	1

INTERNET	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2
	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
SERVICIO DE REDIRECCIONAMIENTO DE CARPETAS	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	2
	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
NETWORKING	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
CABLEADO ESTRUCTURADO	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	2
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	1	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1

	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	1	2	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	2	1	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
DATA CENTER PLANTA	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	2	2	FUNCIONAMIENTO INADECUADO DE LOS UPS	1
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	2	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2
SOFTWARE ACTUALIZACIONES SISTEMA OPERATIVO	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2
	DIFUCION DE SOFTWARE DAÑINO	2	1	FALTA O FALLO EN ANTIVIRUS	2
	FUGAS DE INFORMACIÓN	2	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	VULNERABILIDADES DE LOS PROGRAMAS	2	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	2
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	3
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
	MANIPULACIÓN DE PROGRAMAS	2	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2
SOFTWARE PROXY -	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1
	DIFUCION DE SOFTWARE DAÑINO	3	2	FALTA O FALLO EN ANTIVIRUS	2

FIREWALL	FUGAS DE INFORMACIÓN	2	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	VULNERABILIDADES DE LOS PROGRAMAS	2	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	2
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
	MANIPULACIÓN DE PROGRAMAS	2	2	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2
NORMAS, POLITICAS Y PROCEDIMIENTOS DEL AREA	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	1
	DIFUCION DE SOFTWARE DAÑINO	2	2	FALTA O FALLO EN ANTIVIRUS	1
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2
	VULNERABILIDADES DE LOS PROGRAMAS	1	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	1
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
MANIPULACIÓN DE PROGRAMAS	1	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2	
MANUALES	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	1
	DIFUCION DE SOFTWARE DAÑINO	2	2	FALTA O FALLO EN ANTIVIRUS	1
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2
	VULNERABILIDADES DE LOS PROGRAMAS	1	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	1

	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	1
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	2	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
	MANIPULACIÓN DE PROGRAMAS	1	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2
APLICACIONES ADMINISTRATIVAS Y RECURSOS HUMANOS	ERRORES DE USUARIO	1	3	FALTA DE CAPACITACION	2
	DIFUCION DE SOFTWARE DAÑINO	3	1	FALTA O FALLO EN ANTIVIRUS	1
	FUGAS DE INFORMACIÓN	2	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	VULNERABILIDADES DE LOS PROGRAMAS	2	2	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	3
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	3
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	2
	SUPLANTACIÓN DE IDENTIDAD	1	3	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	2	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
	MANIPULACIÓN DE PROGRAMAS	1	2	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	1
RESPALDO DE SERVIDORES	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2
	DIFUCION DE SOFTWARE DAÑINO	2	1	FALTA O FALLO EN ANTIVIRUS	1
	FUGAS DE INFORMACIÓN	2	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	VULNERABILIDADES DE LOS PROGRAMAS	1	2	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	1
	RESTAURACIÓN FALLIDA DE RESPALDOS	1	1	FALTA DE PROCEDIMIENTOS PARA GENERAR RESPALDOS Y RESTAURAR LOS MISMOS	3
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	2

	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2
	MANIPULACIÓN DE PROGRAMAS	2	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	1
SOFTWARE CAMARAS IP	ERRORES DE USUARIO	2	1	FALTA DE CAPACITACION	3
	DIFUCION DE SOFTWARE DAÑINO	3	1	FALTA O FALLO EN ANTIVIRUS	1
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	VULNERABILIDADES DE LOS PROGRAMAS	2	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	2
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	2
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
	MANIPULACIÓN DE PROGRAMAS	2	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	1
ANTIVIRUS	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2
	DIFUCION DE SOFTWARE DAÑINO	3	2	FALTA O FALLO EN ANTIVIRUS	2
	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	VULNERABILIDADES DE LOS PROGRAMAS	2	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	2
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	2
	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2
	MODIFICACION DELIVERADA DE LA	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS	1

	INFORMACIÓN		EN LA INFORMACIÓN		
	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1
	MANIPULACIÓN DE PROGRAMAS	2	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2
SERVIDOR DE DIRECTORIO ACTIVO	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2
	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
SERVIDOR DE CORREO ELECTRÓNICO	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2



	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
SERVIDOR DE INTERNET PROXY – FIREWALL	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2
	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
	SERVIDOR DE CARPETAS COMPARTIDAS	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO
DAÑOS POR AGUA		3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
DESASTRES NATURALES (TERREMOTOS)		3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
DESASTRES INDUSTRIALES (FUGA DE AMONIACO)		1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
CORTE DE SUMINISTRO ELECTRICO		3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD		3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS		2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2

	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2
	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
SERVIDORES DE APLICACIÓN Y BASE DE DATOS	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2
	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
SERVIDOR DE RESPALDO	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2

	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2
	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
SERVIDOR DE ACTUALIZACIONES Y ANTIVIRUS	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIAO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2
	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	2
SERVIDORES PARA CÁMARAS IP	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIAO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2

	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	1
	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
ROUTER DE COMUNICACIONES	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIAO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	1
	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
SWITCH DE COMUNICACIONES	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2

	AMONIACO)				
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	1
	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
ESTACIONES DE TRABAJO	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	2
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2
	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2
	USO NO PREVISTO DE RECURSOS	2	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	3	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	3
DISCOS DUROS USB	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3
	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2

DE RESPALDOS	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2
	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	1
	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	1
	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2
	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	1
	USO NO PREVISTO DE RECURSOS	2	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1
	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1
	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1
	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1
USUARIOS DE LA ORGANIZACIÓN	FUGAS DE INFORMACIÓN	1	2	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1
	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	3	2	FALTA DE CONTROLES ANTE POSIBLE FUGA	3
	INDISPONIBILIDAD DEL PERSONAL	1	3	BAJOS O NULOS CONTROLES DE CONTROL DE PERSONAL	2
	INGENIERIA SOCIAL	1	2	FALTA DE PROCEDIMIENTOS PARA EL ACCESO A LA INFORMACIÓN	1

### A.10 Riesgos vs activos afectados

RIESGO	ACTIVOS QUE AFECTA
<p style="text-align: center;"><b>CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD</b></p>	<p>CABLEADO ESTRUCTURADO            DATA CENTER PLANTA            SERVIDOR DE DIRECTORIO ACTIVO            SERVIDOR DE CORREO ELECTRÓNICO            SERVIDOR DE INTERNET PROXY – FIREWALL            SERVIDOR DE CARPETAS COMPARTIDAS            SERVIDORES DE APLICACIÓN Y BASE DE DATOS            SERVIDOR DE RESPALDO            SERVIDOR DE ACTUALIZACIONES Y ANTIVIRUS            SERVIDORES PARA CÁMARAS IP            ROUTER DE COMUNICACIONES            SWITCH DE COMUNICACIONES            ESTACIONES DE TRABAJO            DISCOS DUROS USB DE RESPALDOS</p>
<p style="text-align: center;"><b>DAÑOS POR AGUA</b></p>	<p>CABLEADO ESTRUCTURADO            DATA CENTER PLANTA            SERVIDOR DE DIRECTORIO ACTIVO            SERVIDOR DE CORREO ELECTRÓNICO            SERVIDOR DE INTERNET PROXY – FIREWALL            SERVIDOR DE CARPETAS COMPARTIDAS            SERVIDORES DE APLICACIÓN Y BASE DE DATOS            SERVIDOR DE RESPALDO            SERVIDOR DE ACTUALIZACIONES Y ANTIVIRUS            SERVIDORES PARA CÁMARAS IP            ROUTER DE COMUNICACIONES            SWITCH DE COMUNICACIONES            ESTACIONES DE TRABAJO            DISCOS DUROS USB DE RESPALDOS</p>
<p style="text-align: center;"><b>FUEGO</b></p>	<p>CABLEADO ESTRUCTURADO</p>

	<p>DATA CENTER PLANTA  SERVIDOR DE DIRECTORIO ACTIVO  SERVIDOR DE CORREO ELECTRÓNICO  SERVIDOR DE INTERNET PROXY – FIREWALL  SERVIDOR DE CARPETAS COMPARTIDAS  SERVIDORES DE APLICACIÓN Y BASE DE DATOS  SERVIDOR DE RESPALDO  SERVIDOR DE ACTUALIZACIONES Y ANTIVIRUS  SERVIDORES PARA CÁMARAS IP  ROUTER DE COMUNICACIONES  SWITCH DE COMUNICACIONES  ESTACIONES DE TRABAJO  DISCOS DUROS USB DE RESPALDOS</p>
<p><b>CORTE DE SUMINISTRO ELECTRICO</b></p>	<p>CABLEADO ESTRUCTURADO  SERVIDOR DE DIRECTORIO ACTIVO  SERVIDOR DE CORREO ELECTRÓNICO  SERVIDOR DE INTERNET PROXY – FIREWALL  SERVIDOR DE CARPETAS COMPARTIDAS  SERVIDORES DE APLICACIÓN Y BASE DE DATOS  SERVIDOR DE RESPALDO  SERVIDOR DE ACTUALIZACIONES Y ANTIVIRUS  SERVIDORES PARA CÁMARAS IP  ROUTER DE COMUNICACIONES  SWITCH DE COMUNICACIONES  ESTACIONES DE TRABAJO  DISCOS DUROS USB DE RESPALDOS</p>
<p><b>CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS</b></p>	<p>TRANSACCION DE PAGO A PROVEEDORES  TRANSACCION DE PAGO DE NOMINAS  TRANSACCION DE REGISTRO DE INVENTARIO A BODEGA  TRANSACCION DE REGISTRO DE FACTURA Y COBRANZA  SERVICIO DE INTERNET  SERVIDOR DE CORREO ELECTRÓNICO  SERVIDOR DE CARPETAS COMPARTIDAS  ESTACIONES DE TRABAJO  DISCOS DUROS USB DE RESPALDOS</p>



<b>ERRORES DE USUARIO</b>	SOPORTE TÉCNICO SOPORTE OPENSIDE CORREO ELECTRONICO APLICACIONES ADMINISTRATIVAS Y RECURSOS HUMANOS SOFTWARE CAMARAS IP
<b>ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS</b>	SOFTWARE ACTUALIZACIONES SISTEMA OPERATIVO SOFTWARE PROXY - FIREWALL APLICACIONES ADMINISTRATIVAS Y RECURSOS HUMANOS RESPALDO DE SERVIDORES
<b>SUPLANTACIÓN DE IDENTIDAD</b>	TRANSACCION DE PAGO A PROVEEDORES TRANSACCION DE REGISTRO DE INVENTARIO A BODEGA CORREO ELECTRONICO APLICACIONES ADMINISTRATIVAS Y RECURSOS HUMANOS
<b>USO NO PREVISTO DE RECURSOS</b>	TELEFONÍA FIJA SOPORTE TÉCNICO SERVICIO DE REDIRECCIONAMIENTO DE CARPETAS
<b>DIFUCION DE SOFTWARE DAÑINO</b>	SOFTWARE PROXY - FIREWALL ANTIVIRUS
<b>VULNERABILIDADES DE LOS PROGRAMAS</b>	APLICACIONES ADMINISTRATIVAS Y RECURSOS HUMANOS SOFTWARE CAMARAS IP
<b>DESASTRES INDUSTRIALES (FUGA DE AMONIACO)</b>	USUARIOS DE LA ORGANIZACIÓN
<b>INDISPONIBILIDAD DEL PERSONAL</b>	USUARIOS DE LA ORGANIZACIÓN
<b>MANIPULACION DE EQUIPOS</b>	ESTACIONES DE TRABAJO
<b>MANIPULACIÓN DE PROGRAMAS</b>	SOFTWARE PROXY - FIREWALL
<b>RESTAURACIÓN FALLIDA DE RESPALDOS</b>	RESPALDO DE SERVIDORES

## A.11 Análisis de riesgo

ACTIVO	VALOR DEL ACTIVO			AMENAZA			VULNERABILIDAD		VALORACION DEL RIESGO		
	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD	DESCRIPCION	DEGRADACIÓN DE ACTIVO	PROBABILIDAD DE OCURRENCIA	DESCRIPCION	CONTROL DE SEGURIDAD	DISPONIBILIDAD	INTEGRIDAD	CONFIDENCIALIDAD
TRANSACCION DE PAGO A PROVEEDORES	3	3	3	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1	4,5	4,5	4,5
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	3	3
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	3	9	9	9
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	3	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2	12	12	12
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	2	ALMACENAMIENTO NO PROTEGIDO	1	4,5	4,5	4,5
TRANSACCION DE PAGO DE NOMINAS	3	3	3	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1	4,5	4,5	4,5
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	3	3
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS	3	9	9	9

			RECURSOS			PARA EL TRABAJO					
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2	6	6	6
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	3	3	3
TRANSACCION DE REGISTRO DE INVENTARIO A BODEGA	3	3	3	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1	4,5	4,5	4,5
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	3	3
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	3	13,5	13,5	13,5
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	3	13,5	13,5	13,5
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	3	3	3
TRANSACCION DE REGISTRO DE FACTURA Y COBRANZA	3	3	3	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1	4,5	4,5	4,5
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	3	3
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	3	13,5	13,5	13,5

	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	3
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	3	3	3
TRANSACCION DE COTIZACIONES Y COMPRAS	3	3	3	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1	4,5	4,5	4,5
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	3	3
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	4,5	4,5	4,5
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	4,5	4,5	4,5
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	3	3	3
TELEFONÍA FIJA	3	3	3	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2	6	6	6
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	3	3
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	3	3	3
	3	3	3	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y	2	9	9	9

							CONTROLES DE ACCESO				
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2	6	6	6
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	6	6
SOPORTE TÉCNICO	3	2	2	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	3	13,5	9	9
	3	2	2	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2	6	4	4
	3	2	2	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2	6	4	4
	3	2	2	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	3	13,5	9	9
	3	2	2	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	2	2
	3	2	2	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	4	4
	3	2	2	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	4	4
SOPORTE OPENSIDE	3	3	3	ERRORES DE USUARIO	2	2	FALTA DE CAPACITACION	3	18	18	18
	3	3	3	FUGAS DE INFORMACIÓN	1	2	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	4,5	4,5	4,5
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2	6	6	6
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE	1	1	FALTA DE CONTROLES DE	2	6	6	6

				IDENTIDAD			ACCESO DEL PERSONAL				
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	6	6
SOPORTE EVOLUTION	3	3	3	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1	4,5	4,5	4,5
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2	6	6	6
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2	6	6	6
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	3
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	6	6
MOTOR DE BASE DE DATOS	3	3	3	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2	6	6	6
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2	6	6	6
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	4,5	4,5	4,5
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2	6	6	6
	3	3	3	MODIFICACION	1	1	FALTA DE PROCEDIMIENTOS Y	2	6	6	6

				DELIVERADA DE LA INFORMACIÓN			CONTROL DE CAMBIOS EN LA INFORMACIÓN				
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	3	3	3
DIRECTORIO ACTIVO	3	2	2	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2	6	4	4
	3	2	2	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	2	2
	3	2	2	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	3	2	2
	3	2	2	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	2	2
	3	2	2	SUPLANTACIÓN DE IDENTIDAD	1	3	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	6	4	4
	3	2	2	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1	3	2	2
	3	2	2	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	3	2	2
CORREO ELECTRONICO	3	3	3	ERRORES DE USUARIO	1	3	FALTA DE CAPACITACION	2	12	12	12
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	3	3
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	4,5	4,5	4,5
	3	3	3	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4,5	4,5	4,5
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	3	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2	12	12	12
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1	3	3	3

	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	3	3	3
SERVICIO DE INTERNET	3	2	2	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	1	3	2	2
	3	2	2	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2	6	4	4
	3	2	2	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2	9	6	6
	3	2	2	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4,5	3	3
	3	2	2	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	4,5	3	3
	3	2	2	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1	3	2	2
	3	2	2	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	4	4
SERVICIO DE REDIRECCIONAMIENTO DE CARPETAS	3	3	3	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1	4,5	4,5	4,5
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2	6	6	6
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	4,5	4,5	4,5
	3	3	3	USO NO PREVISTO DE RECURSOS	1	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	2	9	9	9
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	4,5	4,5	4,5
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	3	3	3



NETWORKING	3	3	3	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2	6	6	6
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	3	3
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	4,5	4,5	4,5
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	3
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	6	6
CABLEADO ESTRUCTURADO	3	3	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	2	12	12	12
	3	3	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	12	12	12
	3	3	3	DESASTRES NATURALES (TERREMOTOS)	1	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	3	3	3
	3	3	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	6	6	6
	3	3	3	CORTE DE SUMINISTRO ELECTRICO	1	2	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	9	9	9
	3	3	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	2	1	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	9	9	9
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	1	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	4,5	4,5	4,5

DATA CENTER PLANTA	2	3	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	12	18	18
	2	3	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	8	12	12
	2	3	3	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	4	6	6
	2	3	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	4	6	6
	2	3	3	CORTE DE SUMINISTRO ELECTRICO	2	2	FUNCIONAMIENTO INADECUADO DE LOS UPS	1	4	6	6
	2	3	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	2	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	8	12	12
	2	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2	4	6	6
SOFTWARE ACTUALIZACIONES SISTEMA OPERATIVO	1	2	2	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2	2	4	4
	1	2	2	DIFUSION DE SOFTWARE DAÑINO	2	1	FALTA O FALLO EN ANTIVIRUS	2	3	6	6
	1	2	2	FUGAS DE INFORMACIÓN	2	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	1,5	3	3
	1	2	2	VULNERABILIDADES DE LOS PROGRAMAS	2	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	2	3	6	6
	1	2	2	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	3	6	12	12
	1	2	2	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	1	2	2
	1	2	2	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2	2	4	4

	1	2	2	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1	1	2	2
	1	2	2	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	1	2	2
	1	2	2	MANIPULACIÓN DE PROGRAMAS	2	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2	3	6	6
SOFTWARE PROXY - FIREWALL	2	2	3	ERRORES DE USUARIO	1	2	FALTA DE CAPACITACION	1	3	3	4,5
	2	2	3	DIFUCION DE SOFTWARE DAÑINO	3	2	FALTA O FALLO EN ANTIVIRUS	2	10	10	15
	2	2	3	FUGAS DE INFORMACIÓN	2	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	3	3	4,5
	2	2	3	VULNERABILIDADES DE LOS PROGRAMAS	2	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	1	3	3	4,5
	2	2	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	2	8	8	12
	2	2	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	2	2	3
	2	2	3	SUPLANTACIÓN DE IDENTIDAD	1	2	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	4,5
	2	2	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	4	4	6
	2	2	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	2	2	3
	2	2	3	MANIPULACIÓN DE PROGRAMAS	2	2	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2	8	8	12
NORMAS, POLITICAS Y PROCEDIMIENTOS DEL AREA	3	3	2	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	1	3	3	2
	3	3	2	DIFUCION DE SOFTWARE DAÑINO	2	2	FALTA O FALLO EN ANTIVIRUS	1	6	6	4
	3	3	2	FUGAS DE	1	1	INEXISTENTES CONTROLES DE	2	6	6	4

			INFORMACIÓN			ASEGURAMIENTO DE INFORMACION					
	3	3	2	VULNERABILIDADES DE LOS PROGRAMAS	1	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	1	3	3	2
	3	3	2	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	1	3	3	2
	3	3	2	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	2
	3	3	2	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	2
	3	3	2	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	4
	3	3	2	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	6	4
	3	3	2	MANIPULACIÓN DE PROGRAMAS	1	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2	6	6	4
MANUALES	3	3	3	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	1	3	3	3
	3	3	3	DIFUCION DE SOFTWARE DAÑINO	2	2	FALTA O FALLO EN ANTIVIRUS	1	6	6	6
	3	3	3	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	2	6	6	6
	3	3	3	VULNERABILIDADES DE LOS PROGRAMAS	1	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	1	3	3	3
	3	3	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	1	3	3	3
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3

	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	3
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	2	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1	4,5	4,5	4,5
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	6	6
	3	3	3	MANIPULACIÓN DE PROGRAMAS	1	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2	6	6	6
APLICACIONES ADMINISTRATIVAS Y RECURSOS HUMANOS	3	3	3	ERRORES DE USUARIO	1	3	FALTA DE CAPACITACION	2	12	12	12
	3	3	3	DIFUCION DE SOFTWARE DAÑINO	3	1	FALTA O FALLO EN ANTIVIRUS	1	6	6	6
	3	3	3	FUGAS DE INFORMACIÓN	2	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	4,5	4,5	4,5
	3	3	3	VULNERABILIDADES DE LOS PROGRAMAS	2	2	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	3	18	18	18
	3	3	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	3	18	18	18
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	2	6	6	6
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	3	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2	12	12	12
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	2	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1	4,5	4,5	4,5
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	6	6
	3	3	3	MANIPULACIÓN DE PROGRAMAS	1	2	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	1	4,5	4,5	4,5
	RESPALDO DE SERVIDORES	3	3	3	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2	6	6
3		3	3	DIFUCION DE	2	1	FALTA O FALLO EN ANTIVIRUS	1	4,5	4,5	4,5

			SOFTWARE DAÑINO								
	3	3	3	FUGAS DE INFORMACIÓN	2	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	4,5	4,5	4,5
	3	3	3	VULNERABILIDADES DE LOS PROGRAMAS	1	2	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	1	4,5	4,5	4,5
	3	3	3	RESTAURACIÓN FALLIDA DE RESPALDOS	1	1	FALTA DE PROCEDIMIENTOS PARA GENERAR RESPALDOS Y RESTAURAR LOS MISMOS	3	9	9	9
	3	3	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	2	9	9	9
	3	3	3	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	3
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	3
	3	3	3	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	6	6	6
	3	3	3	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	2	6	6	6
	3	3	3	MANIPULACIÓN DE PROGRAMAS	2	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	1	4,5	4,5	4,5
SOFTWARE CAMARAS IP	2	3	2	ERRORES DE USUARIO	2	1	FALTA DE CAPACITACION	3	9	13,5	9
	2	3	2	DIFUCION DE SOFTWARE DAÑINO	3	1	FALTA O FALLO EN ANTIVIRUS	1	4	6	4
	2	3	2	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	2	3	2
	2	3	2	VULNERABILIDADES DE LOS PROGRAMAS	2	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	2	6	9	6

	2	3	2	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	2	4	6	4
	2	3	2	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	2	3	2
	2	3	2	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	2	3	2
	2	3	2	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	2	4	6	4
	2	3	2	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	2	3	2
	2	3	2	MANIPULACIÓN DE PROGRAMAS	2	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	1	3	4,5	3
ANTIVIRUS	2	2	1	ERRORES DE USUARIO	1	1	FALTA DE CAPACITACION	2	4	4	2
	2	2	1	DIFUCION DE SOFTWARE DAÑINO	3	2	FALTA O FALLO EN ANTIVIRUS	2	10	10	5
	2	2	1	FUGAS DE INFORMACIÓN	1	1	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	2	2	1
	2	2	1	VULNERABILIDADES DE LOS PROGRAMAS	2	1	PROBLEMAS CON ACTUALIZACION O SOFTWARE NO DEPURADO	2	6	6	3
	2	2	1	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE PROGRAMAS	2	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE SOFTWARE	2	6	6	3
	2	2	1	USO NO PREVISTO DE RECURSOS	1	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	2	2	1
	2	2	1	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	2	4	4	2
	2	2	1	MODIFICACION DELIVERADA DE LA INFORMACIÓN	1	1	FALTA DE PROCEDIMIENTOS Y CONTROL DE CAMBIOS EN LA INFORMACIÓN	1	2	2	1

	2	2	1	DIVULGACIÓN DE INFORMACIÓN	1	1	ALMACENAMIENTO NO PROTEGIDO	1	2	2	1
	2	2	1	MANIPULACIÓN DE PROGRAMAS	2	1	FALTA DE CONTROLES DE MODIFICACIÓN DE PROGRAMAS	2	6	6	3
SERVIDOR DE DIRECTORIO ACTIVO	3	2	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	18	12	18
	3	2	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	12	8	12
	3	2	3	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	6	4	6
	3	2	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	6	4	6
	3	2	3	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	18	12	18
	3	2	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	15	10	15
	3	2	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	6	4	6
	3	2	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2	6	4	6
	3	2	3	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4,5	3	4,5
	3	2	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	2	3
	3	2	3	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	6	4	6
	3	2	3	MANIPULACION DE	2	1	FALTA DE CONTROLES DE	1	4,5	3	4,5



				EQUIPOS			MANIPULACIÓN DE EQUIPOS				
SERVIDOR DE CORREO ELECTRÓNICO	3	2	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	18	12	18
	3	2	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	12	8	12
	3	2	3	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	6	4	6
	3	2	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	6	4	6
	3	2	3	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	18	12	18
	3	2	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	15	10	15
	3	2	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2	12	8	12
	3	2	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2	6	4	6
	3	2	3	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4,5	3	4,5
	3	2	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	2	3
	3	2	3	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	6	4	6
3	2	3	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1	4,5	3	4,5	
SERVIDOR DE INTERNET PROXY –	3	2	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	18	12	18

FIREWALL	3	2	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	12	8	12
	3	2	3	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	6	4	6
	3	2	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	6	4	6
	3	2	3	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	18	12	18
	3	2	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	15	10	15
	3	2	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	6	4	6
	3	2	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2	6	4	6
	3	2	3	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4,5	3	4,5
	3	2	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	2	3
	3	2	3	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	6	4	6
	3	2	3	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1	4,5	3	4,5
SERVIDOR DE CARPETAS COMPARTIDAS	2	2	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	12	12	18
	2	2	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	8	8	12
	2	2	3	DESASTRES NATURALES	3	1	PROBLEMAS DE ORIGEN	1	4	4	6

			(TERREMOTOS)			ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO					
	2	2	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	4	4	6
	2	2	3	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	12	12	18
	2	2	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	10	10	15
	2	2	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2	8	8	12
	2	2	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2	4	4	6
	2	2	3	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	3	4,5
	2	2	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	2	2	3
	2	2	3	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	4	4	6
	2	2	3	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1	3	3	4,5
SERVIDORES DE APLICACIÓN Y BASE DE DATOS	3	3	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	18	18	18
	3	3	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	12	12	12
	3	3	3	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	6	6	6

	3	3	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	6	6	6
	3	3	3	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	18	18	18
	3	3	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	15	15	15
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	4,5	4,5	4,5
	3	3	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2	6	6	6
	3	3	3	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4,5	4,5	4,5
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	3
	3	3	3	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	6	6	6
	3	3	3	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1	4,5	4,5	4,5
SERVIDOR DE RESPALDO	3	3	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	18	18	18
	3	3	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	12	12	12
	3	3	3	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	6	6	6
	3	3	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	6	6	6

	3	3	3	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	18	18	18
	3	3	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	15	15	15
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	4,5	4,5	4,5
	3	3	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2	6	6	6
	3	3	3	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4,5	4,5	4,5
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	3
	3	3	3	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	6	6	6
	3	3	3	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1	4,5	4,5	4,5
SERVIDOR DE ACTUALIZACIONES Y ANTIVIRUS	1	2	2	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	6	12	12
	1	2	2	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	4	8	8
	1	2	2	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	2	4	4
	1	2	2	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	2	4	4
	1	2	2	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	6	12	12
	1	2	2	CONDICIONES	3	2	MAL FUNCIONAMIENTO DE	2	5	10	10

			INADECUADAS DE TEMPERATURA Y HUMEDAD			CLIMATIZACION EN LA EMPRESA					
	1	2	2	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	1,5	3	3
	1	2	2	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2	3	6	6
	1	2	2	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	1,5	3	3
	1	2	2	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	1	2	2
	1	2	2	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	2	4	4
	1	2	2	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	2	3	6	6
SERVIDORES PARA CÁMARAS IP	2	3	2	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	12	18	12
	2	3	2	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	8	12	8
	2	3	2	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	4	6	4
	2	3	2	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	4	6	4
	2	3	2	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	12	18	12
	2	3	2	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	10	15	10

	2	3	2	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	3	4,5	3
	2	3	2	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	2	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	1	3	4,5	3
	2	3	2	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	3	4,5	3
	2	3	2	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	2	3	2
	2	3	2	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	4	6	4
	2	3	2	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1	3	4,5	3
ROUTER DE COMUNICACIONES	3	3	2	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	18	18	12
	3	3	2	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	12	12	8
	3	3	2	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	6	6	4
	3	3	2	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	6	6	4
	3	3	2	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	18	18	12
	3	3	2	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	15	15	10
	3	3	2	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	6	6	4

	3	3	2	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	1	3	3	2
	3	3	2	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4,5	4,5	3
	3	3	2	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	2
	3	3	2	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	6	6	4
	3	3	2	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1	4,5	4,5	3
SWITCH DE COMUNICACIONES	3	3	2	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	18	18	12
	3	3	2	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	12	12	8
	3	3	2	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	6	6	4
	3	3	2	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	6	6	4
	3	3	2	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	18	18	12
	3	3	2	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	15	15	10
	3	3	2	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	1	6	6	4
	3	3	2	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	1	3	3	2



				EQUIPOS								
	3	3	2	USO NO PREVISTO DE RECURSOS	2	1	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4,5	4,5	3	
	3	3	2	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	2	
	3	3	2	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	6	6	4	
	3	3	2	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1	4,5	4,5	3	
ESTACIONES DE TRABAJO	3	3	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	2	12	12	12	
	3	3	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	12	12	12	
	3	3	3	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	6	6	6	
	3	3	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	6	6	6	
	3	3	3	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	2	18	18	18	
	3	3	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	2	15	15	15	
	3	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	2	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2	12	12	12	
	3	3	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	2	6	6	6	
	3	3	3	USO NO PREVISTO DE RECURSOS	2	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y	1	6	6	6	

							CONTROLES DE ACCESO				
	3	3	3	SUPLANTACIÓN DE IDENTIDAD	1	1	FALTA DE CONTROLES DE ACCESO DEL PERSONAL	1	3	3	3
	3	3	3	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	6	6	6
	3	3	3	MANIPULACION DE EQUIPOS	2	3	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	3	22,5	22,5	22,5
DISCOS DUROS USB DE RESPALDOS	2	3	3	FUEGO	3	1	FALTA DE PROTECCION CONTRA FUEGO	3	12	18	18
	2	3	3	DAÑOS POR AGUA	3	1	FALTA DE PROTECCION ESTRUCTURAL CONTRA AGUA	2	8	12	12
	2	3	3	DESASTRES NATURALES (TERREMOTOS)	3	1	PROBLEMAS DE ORIGEN ESTRUCTURAL EN EL EDIFICIO DONDE SE ENCUENTRE EL ACTIVO	1	4	6	6
	2	3	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	1	1	FALTA DE CONTROLES ANTE POSIBLE FUGA	2	4	6	6
	2	3	3	CORTE DE SUMINISTRO ELECTRICO	3	3	FUNCIONAMIENTO INADECUADO DE LOS UPS	1	6	9	9
	2	3	3	CONDICIONES INADECUADAS DE TEMPERATURA Y HUMEDAD	3	2	MAL FUNCIONAMIENTO DE CLIMATIZACION EN LA EMPRESA	1	5	7,5	7,5
	2	3	3	CAIDA DEL SISTEMA POR AGOTAMIENTO DE RECURSOS	2	1	EQUIPOS CON CARACTERISTICAS MINIMAS PARA EL TRABAJO	2	6	9	9
	2	3	3	ERRORES DE MANTENIMIENTO ACTUALIZACIÓN DE EQUIPOS	1	1	CONTROLES BAJOS O NULOS DE ACTUALIZACION DE EQUIPOS	1	2	3	3
	2	3	3	USO NO PREVISTO DE RECURSOS	2	2	FALTA DE POLITICAS SOBRE USOS DE LOS RECURSOS Y CONTROLES DE ACCESO	1	4	6	6
	2	3	3	SUPLANTACIÓN DE	1	1	FALTA DE CONTROLES DE	1	2	3	3

				IDENTIDAD			ACCESO DEL PERSONAL				
	2	3	3	ROBO	3	1	FALTA DE CONTROLES DE ENTRADA Y SALIDA DE RECURSOS A LA ORGANIZACIÓN	1	4	6	6
	2	3	3	MANIPULACION DE EQUIPOS	2	1	FALTA DE CONTROLES DE MANIPULACIÓN DE EQUIPOS	1	3	4,5	4,5
USUARIOS DE LA ORGANIZACIÓN	3	3	3	FUGAS DE INFORMACIÓN	1	2	INEXISTENTES CONTROLES DE ASEGURAMIENTO DE INFORMACION	1	4,5	4,5	4,5
	3	3	3	DESASTRES INDUSTRIALES (FUGA DE AMONIACO)	3	2	FALTA DE CONTROLES ANTE POSIBLE FUGA	3	22,5	22,5	22,5
	3	3	3	INDISPONIBILIDAD DEL PERSONAL	1	3	BAJOS O NULOS CONTROLES DE CONTROL DE PERSONAL	2	12	12	12
	3	3	3	INGENIERIA SOCIAL	1	2	FALTA DE PROCEDIMIENTOS PARA EL ACCESO A LA INFORMACIÓN	1	4,5	4,5	4,5

## A.12 Dominios, objetivos de control y controles de la ISO/IEC 27001:2005.

Dominios (11), Objetivos de control (39) y Controles (133)

- 5. **POLÍTICA DE SEGURIDAD.**
    - 5.1 **Política de seguridad de la información.**
      - 5.1.1 Documento de política de seguridad de la información.
      - 5.1.2 Revisión de la política de seguridad de la información.
  - 6. **ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.**
    - 6.1 **Organización interna.**
      - 6.1.1 Compromiso de la Dirección con la seguridad de la información.
      - 6.1.2 Coordinación de la seguridad de la información.
      - 6.1.3 Asignación de responsabilidades relativas a la seg. de la informac.
      - 6.1.4 Proceso de autorización de recursos para el tratamiento de la información.
      - 6.1.5 Acuerdos de confidencialidad.
      - 6.1.6 Contacto con las autoridades.
      - 6.1.7 Contacto con grupos de especial interés.
      - 6.1.8 Revisión independiente de la seguridad de la información.
    - 6.2 **Terceros.**
      - 6.2.1 Identificación de los riesgos derivados del acceso de terceros.
      - 6.2.2 Tratamiento de la seguridad en la relación con los clientes.
      - 6.2.3 Tratamiento de la seguridad en contratos con terceros.
  - 7. **GESTIÓN DE ACTIVOS.**
    - 7.1 **Responsabilidad sobre los activos.**
      - 7.1.1 Inventario de activos.
      - 7.1.2 Propiedad de los activos.
      - 7.1.3 Uso aceptable de los activos.
    - 7.2 **Clasificación de la información.**
      - 7.2.1 Directrices de clasificación.
      - 7.2.2 Etiquetado y manipulado de la información.
  - 8. **SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.**
    - 8.1 **Antes del empleo.**
      - 8.1.1 Funciones y responsabilidades.
      - 8.1.2 Investigación de antecedentes.
      - 8.1.3 Términos y condiciones de contratación.
    - 8.2 **Durante el empleo.**
      - 8.2.1 Responsabilidades de la Dirección.
      - 8.2.2 Concienciación, formación y capacitación en seg. de la informac.
      - 8.2.3 Proceso disciplinario.
    - 8.3 **Cese del empleo o cambio de puesto de trabajo.**
      - 8.3.1 Responsabilidad del cese o cambio.
      - 8.3.2 Devolución de activos.
      - 8.3.3 Retirada de los derechos de acceso.
  - 9. **SEGURIDAD FÍSICA Y DEL ENTORNO.**
    - 9.1 **Áreas seguras.**
      - 9.1.1 Perímetro de seguridad física.
      - 9.1.2 Controles físicos de entrada.
      - 9.1.3 Seguridad de oficinas, despachos e instalaciones.
      - 9.1.4 Protección contra las amenazas externas y de origen ambiental.
      - 9.1.5 Trabajo en áreas seguras.
      - 9.1.6 Áreas de acceso público y de carga y descarga.
    - 9.2 **Seguridad de los equipos.**
      - 9.2.1 Emplazamiento y protección de equipos.
      - 9.2.2 Instalaciones de suministro.
      - 9.2.3 Seguridad del cableado.
      - 9.2.4 Mantenimiento de los equipos.
      - 9.2.5 Seguridad de los equipos fuera de las instalaciones.
      - 9.2.6 Reutilización o retirada segura de equipos.
      - 9.2.7 Retirada de materiales propiedad de la empresa.
  - 10. **GESTIÓN DE COMUNICACIONES Y OPERACIONES.**
    - 10.1 **Responsabilidades y procedimientos de operación.**
      - 10.1.1 Documentación de los procedimientos de operación.
      - 10.1.2 Gestión de cambios.
      - 10.1.3 Segregación de tareas.
      - 10.1.4 Separación de los recursos de desarrollo, prueba y operación.
    - 10.2 **Gestión de la provisión de servicios por terceros.**
      - 10.2.1 Provisión de servicios.
      - 10.2.2 Supervisión y revisión de los servicios prestados por terceros.
      - 10.2.3 Gestión del cambio en los servicios prestados por terceros.
  - 10.3 **Planificación y aceptación del sistema.**
    - 10.3.1 Gestión de capacidades.
    - 10.3.2 Aceptación del sistema.
  - 10.4 **Protección contra el código malicioso y descargable.**
    - 10.4.1 Controles contra el código malicioso.
    - 10.4.2 Controles contra el código descargado en el cliente.
  - 10.5 **Copias de seguridad.**
    - 10.5.1 Copias de seguridad de la información.
  - 10.6 **Gestión de la seguridad de las redes.**
    - 10.6.1 Controles de red.
    - 10.6.2 Seguridad de los servicios de red.
  - 10.7 **Manipulación de los soportes.**
    - 10.7.1 Gestión de soportes extraíbles.
    - 10.7.2 Retirada de soportes.
    - 10.7.3 Procedimientos de manipulación de la información.
    - 10.7.4 Seguridad de la documentación del sistema.
  - 10.8 **Intercambio de información.**
    - 10.8.1 Políticas y procedimientos de intercambio de información.
    - 10.8.2 Acuerdos de intercambio.
    - 10.8.3 Soportes físicos en tránsito.
    - 10.8.4 Mensajería electrónica.
    - 10.8.5 Sistemas de información empresariales.
  - 10.9 **Servicios de comercio electrónico.**
    - 10.9.1 Comercio electrónico.
    - 10.9.2 Transacciones en línea.
    - 10.9.3 Información públicamente disponible.
  - 10.10 **Supervisión.**
    - 10.10.1 Registros de auditoría.
    - 10.10.2 Supervisión del uso del sistema.
    - 10.10.3 Protección de la información de los registros.
    - 10.10.4 Registros de administración y operación.
    - 10.10.5 Registro de fallos.
    - 10.10.6 Sincronización del reloj.
- 11. **CONTROL DE ACCESO.**
    - 11.1 **Requisitos de negocio para el control de acceso.**
      - 11.1.1 Política de control de acceso.
    - 11.2 **Gestión de acceso de usuario.**
      - 11.2.1 Registro de usuario.
      - 11.2.2 Gestión de privilegios.
      - 11.2.3 Gestión de contraseñas de usuario.
      - 11.2.4 Revisión de los derechos de acceso de usuario.
    - 11.3 **Responsabilidades de usuario.**
      - 11.3.1 Uso de contraseñas.
      - 11.3.2 Equipo de usuario desatendido.
      - 11.3.3 Política de puesto de trabajo despejado y pantalla limpia.
    - 11.4 **Control de acceso a la red.**
      - 11.4.1 Política de uso de los servicios en red.
      - 11.4.2 Autenticación de usuario para conexiones externas.
      - 11.4.3 Identificación de los equipos en las redes.
      - 11.4.4 Protección de los puertos de diagnóstico y configuración remotos.
      - 11.4.5 Segregación de las redes.
      - 11.4.6 Control de la conexión a la red.
      - 11.4.7 Control de encaminamiento (routing) de red.
    - 11.5 **Control de acceso al sistema operativo.**
      - 11.5.1 Procedimientos seguros de inicio de sesión.
      - 11.5.2 Identificación y autenticación de usuario.
      - 11.5.3 Sistema de gestión de contraseñas.
      - 11.5.4 Uso de los recursos del sistema.
      - 11.5.5 Desconexión automática de sesión.
      - 11.5.6 Limitación del tiempo de conexión.
    - 11.6 **Control de acceso a las aplicaciones y a la información.**
      - 11.6.1 Restricción del acceso a la información.
      - 11.6.2 Aislamiento de sistemas sensibles.
  - 11.7 **Ordenadores portátiles y teletrabajo.**
    - 11.7.1 Ordenadores portátiles y comunicaciones móviles.
    - 11.7.2 Teletrabajo.
  - 12. **ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.**
    - 12.1 **Requisitos de seguridad de los sistemas de información.**
      - 12.1.1 Análisis y especificación de los requisitos de seguridad.
    - 12.2 **Tratamiento correcto de las aplicaciones.**
      - 12.2.1 Validación de los datos de entrada.
      - 12.2.2 Control del procesamiento interno.
      - 12.2.3 Integridad de los mensajes.
      - 12.2.4 Validación de los datos de salida.
    - 12.3 **Controles criptográficos.**
      - 12.3.1 Política de uso de los controles criptográficos.
      - 12.3.2 Gestión de claves.
    - 12.4 **Seguridad de los archivos de sistema.**
      - 12.4.1 Control del software en explotación.
      - 12.4.2 Protección de los datos de prueba del sistema.
      - 12.4.3 Control de acceso al código fuente de los programas.
    - 12.5 **Seguridad en los procesos de desarrollo y soporte.**
      - 12.5.1 Procedimientos de control de cambios.
      - 12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
      - 12.5.3 Restricciones a los cambios en los paquetes de software.
      - 12.5.4 Fugas de información.
      - 12.5.5 Externalización del desarrollo de software.
    - 12.6 **Gestión de la vulnerabilidad técnica.**
      - 12.6.1 Control de las vulnerabilidades técnicas.
  - 13. **GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.**
    - 13.1 **Notificación de eventos y puntos débiles de seguridad de la información.**
      - 13.1.1 Notificación de los eventos de seguridad de la información.
      - 13.1.2 Notificación de puntos débiles de seguridad.
    - 13.2 **Gestión de incidentes y mejoras de seguridad de la información.**
      - 13.2.1 Responsabilidades y procedimientos.
      - 13.2.2 Aprendizaje de los incidentes de seguridad de la información.
      - 13.2.3 Recopilación de evidencias.
  - 14. **GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.**
    - 14.1 **Aspectos de seguridad de la información en la gestión de la continuidad del negocio.**
      - 14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.
      - 14.1.2 Continuidad del negocio y evaluación de riesgos.
      - 14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.
      - 14.1.4 Marco de referencia para la planificación de la cont. del negocio.
      - 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.
  - 15. **CUMPLIMIENTO.**
    - 15.1 **Cumplimiento de los requisitos legales.**
      - 15.1.1 Identificación de la legislación aplicable.
      - 15.1.2 Derechos de propiedad intelectual (DPI).
      - 15.1.3 Protección de los documentos de la organización.
      - 15.1.4 Protección de datos y privacidad de la información de carácter personal.
      - 15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.
      - 15.1.6 Regulación de los controles criptográficos.
    - 15.2 **Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.**
      - 15.2.1 Cumplimiento de las políticas y normas de seguridad.
      - 15.2.2 Comprobación del cumplimiento técnico.
    - 15.3 **Consideraciones sobre las auditorías de los sistem. de información.**
      - 15.3.1 Controles de auditoría de los sistemas de información.
      - 15.3.2 Protección de las herramientas de auditoría de los sist. de inform.