DECANATO DE INGENIERÍA E INFORMÁTICA

Evaluación de riesgos de tecnología de la información en una zona franca de equipos electrónicos, periodo septiembre- diciembre, año 2019

Trabajo de grado para optar por el título en:

Ingeniería en Sistemas de Computación

Sustentantes:

Br. Francisco Alberto Deño Disla	2012-0878
Br. Víctor Manuel De la Cruz Flores	2014-1762

"Los conceptos expuestos en esta investigación son de la exclusiva responsabilidad de sus autores"

Asesor (a):

Ing. Edgar Morrobert

Santo Domingo, D.N.
República Dominicana
Noviembre, 2019

EVALUACIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN EN UNA ZONA FRANCA DE EQUIPOS ELECTRÓNICOS, PERIODO SEPTIEMBRE- DICIEMBRE, AÑO 2019

ÍNDICE DE CONTENIDO

DEDICATORIAS IX

AGRADECIMIENTOS XI

RESUMEN EJECUTIVO XIII

INTRODUCCIÓN XIV

CAPITULO I 1

ASPECTOS INTRODUCTORIOS DEL PROBLEMA DE INVESTIGACIÓN 1

1.1. Selección del tema 2
1.2. Planteamiento del problema 2
1.3. Justificación 2
1.4. Objetivos de la investigación 3
1.4.1. Objetivo General 3
1.4.2. Objetivos específicos 4
1.5. Alcance 4
1.6. Métodos de investigación 4
1.6.1. Observación 4
1.6.2. Inductivo 5
1.7. Tipos de investigación 5
1.7.1. Investigación descriptiva 5
1.7.2. Investigación explicativa 5
1.8. Resumen capítulo I 6

CAPITULO II 7

EVALUACIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN EN UNA ZONA FRANCA 7

2.1 Evaluación de riesgos 8
2.2. Tecnología de la información 9
2.2.1. Componentes de tecnología de la información 11
2.2.2. Características de las tecnologías de la información 15

2.2.3. Papel de la tecnología de la información en las empresas 16
2.3. Zona franca 17
2.3.1. Características 18
2.3.2. Beneficios 18
2.3.3. Clasificación de las zonas francas 19
2.3.4. Clasificación de los usuarios de las zonas francas 20
2.3.5. Zonas francas en la República Dominicana 20
2.4. Equipos electrónicos 22
2.4.1. Mantenimiento de los equipos electrónicos 22
2.4.2. Propósitos y objetivos del mantenimiento de equipos electrónicos 23
2.4.3. Clasificación de los equipos electrónicos 24
CAPITULO III 25
GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27005:2011 25
3.1. Norma ISO/IEC 27005:2011 26
3.1.1. Ciclo PHVA o Deming. 26
3.1.2. Metodología de gestión del riesgo en la seguridad de la información 29
3.2. Establecimiento del contexto 40
3.3. Identificación de riesgos 42
3.3.1. Identificación de activos 42
3.3.2. Identificación de las amenazas 43
3.3.3. Identificación de controles existentes 44
3.4. Análisis del riesgo 46
3.5. Evaluación de riesgos 46
3.5.1. Identificación de las consecuencias 47
3.5.2. Evaluación de las consecuencias 49
3.6. Metodologías 51
3.6.1. Metodología de análisis cualitativo de riesgos 51
3.6.2. Metodología de análisis cuantitativo de riesgos. 52
CAPITULO IV 54
CONTEXTO DE LA TECNOLOGÍA DE LA INFORMACIÓN EN LA ZONA FRANCA OBJETO DEL ESTUDIO 54

4.1 Entendimiento de Tecnología de la Información en la Zona Franca 55
4.1.1. Infraestructura de TI 55
4.2. Desarrollo y cambio a Sistemas 63
4.2.1. Solicitud de cambios 63
4.2.2. Metodología de desarrollo 64
4.2.3. Control de versiones 64
4.2.4. Pruebas y aceptación de los cambios 64
4.2.5. Pase de los cambios a producción 65
4.3. Gobierno de TI 66
4.3.1. Estructura Organizacional 66
4.3.2. Políticas y Procedimientos 67
4.3.3. Gestión de Proyectos 67
4.3.4. Gestión Presupuestaria 68
4.3.5. Inventario de Recursos HW y SW 68
4.3.6. Gestión de relación con Terceros 69
4.4. Operaciones de TI 69
4.4.1. Respaldo de datos y sistemas 69
4.4.2. Plan de Recuperación ante Desastres 70
4.4.3. Monitoreo de Recursos 70
4.4.4. Soporte a Usuarios 70
4.5. Seguridad en base a la tecnología 71
4.5.1. Seguridad Física 71
4.5.2. Controles Ambientales 72
4.5.3. Seguridad Lógica 72
4.5.4. Autenticación (Red y Sistema) 73
4.5.5. Protección Código Malicioso 73
4.5.6. Seguridad Perimetral 73
4.5.7. Ciberseguridad 73
4.6 Criterio metodológico para la evaluación de los riesgos de tecnología de la información. 74
4.6.1 Criterios de probabilidad 74
4.6.2 Criterios de Impacto 75
4.6.3 Criterio de evaluación del riesgo 76

4.6.4 Riesgos de Tecnología de la información levantados en la zona franca 79
4.6.5 Evaluación de los riesgos de la zona franca 79
4.6.6 Relación de controles implementados 81
CAPITULO V 82
SOLUCIONES A LOS RIESGOS DE TECNOLOGÍA 82
DE LA INFORMACIÓN INVESTIGADOS EN LA ZONA FRANCA 82
5.1. Implicaciones de los riesgos de TI en la gestión de la zona franca.....83
5.2. Informe de Observaciones de Riesgos de TI.....83
5.2.1 Control de Actividades en el Data Center 83
5.2.2 Control de Robo o Divulgación de datos críticos de la empresa.....84
5.2.3 Control de disponibilidad de las informaciones y de continuidad de las operaciones 85
5.2.4 Control de documentación de políticas y procedimientos.....86
5.2.5 Control de Indisponibilidad de recursos Económicos 87
5.2.6 Control de Continuidad del Negocio 88
5.2.7 Control de interrupción de los servicios y/o de las operaciones de la empresa ...88
5.2.8 Control de registro de entradas y salidas del personal en los controles de accesos 89
5.2.9 Control de vulnerabilidades en los sistemas de información 90
5.2.10 Control de ataque de Malware y Spyware.....91
5.2.11 Control de penetración no autorizado a los recursos tecnológicos.....91
CONCLUSIÓN 93
RECOMENDACIONES 95
REFERENCIAS BIBLIOGRAFICAS.....96
ANEXOS.....99

INDICE DE TABLAS

Tabla 1. ESCALA DE VALORACIÓN DEL RIESGO.....33

Tabla 2. CRITERIOS DE VALORACIÓN DE ACTIVOS 36

Tabla 3. DESCRIPCIÓN DE LOS DISPOSITIVOS SERVIDORES.....57

Tabla 4. ESCALA DE PROBABILIDAD DEL RIESGO 74

Tabla 5. ESCALA DE IMPACTO DEL RIESGO 75

Tabla 6. MEDIDAS DE RIESGOS 76

Tabla 7. RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN ZONA FRANCA (2019) 78

Tabla 8. MATRIZ DE EVALUACIÓN DE RIESGOS 80

Tabla 9. CONTROLES IMPLEMENTADOS A LOS RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN ZONA FRANCA (2019).....81

ÍNDICE DE GRÁFICOS

Ilustración 1. CICLO PHVA. 28

Ilustración 2. PROCESO DE GESTIÓN DEL RIESGO ISO/IEC 31000:2009.....30

Ilustración 3. PROCESO DE GESTIÓN DEL RIESGO ISO/IEC 27005:2011.....31

Ilustración 4. MAPA DE CALOR.....34

Ilustración 5. CADENA DE IDENTIFICACIÓN DE ACTIVOS 43

Ilustración 6. CADENA DE IDENTIFICACIÓN DE LAS AMENAZAS 44

Ilustración 7. CADENA DE IDENTIFICACIÓN DE CONTROLES EXISTENTES 45

Ilustración 8. CADENA DE IDENTIFICACIÓN DE LAS CONSECUENCIAS 48

Ilustración 9. CADENA DE EVALUACIÓN DE LAS CONSECUENCIAS 50

Ilustración 10. TOPOLOGÍA DE RED 62

Ilustración 11. ESTRUCTURA DE CARGOS.....66

DEDICATORIAS

Dedico este trabajo principalmente a **Dios**, por haberme dado la vida y permitirme el haber llegado hasta este momento tan importante de mi formación profesional.

A mi familia, por el apoyo incondicional, el amor y confianza que permitieron que pudiera culminar mi carrera profesional.

A mi padre**, Fernando A. Deño** que a pesar de que ya no está con nosotros, siento que está conmigo siempre y aunque nos faltaron muchas cosas por vivir juntos, sé que este momento hubiera sido tan especial para el como lo es para mí.

A mi tío **Domingo Eduardo Reynoso** quien ha sido como un padre, sirviendo de ejemplo para el desarrollo de mi vida personal y profesional.

A todas las personas especiales que me acompañaron en esta etapa, aportando a mi formación tanto profesional y como ser humano.

A la universidad APEC, a la Facultad de Ingeniería, a mis profesores y todo el personal quienes con la enseñanza de sus valiosos conocimientos aportaron día a día para mi crecimiento profesional, a cada una por su paciencia, dedicación, apoyo incondicional y amistad.

Francisco Alberto Deño

DEDICATORIAS

Dedicado a **Dios** por el regalo de la vida y guiarme en el desarrollo de ella, permitirme llegar a concluir esta meta.

A mis padres **Basilio De la Cruz** y **Trinidad Flores** por ese apoyo incondicional que siempre me han brindado, han sido los forjadores de quien soy y mi inspiración por ser cada día mejor.

A mis hermanos **Héctor De la Cruz** y **Kelvin De la Cruz** por su acostumbrada ayuda durante mis años de preparación profesional que aún no terminan.

A mi hijo **Luis Manuel** que me impulso a concluir esta meta y esta le servirá de ejemplo en el mañana.

A mi compañera de vida **Zulenmi Carvajal**, que ha estado conmigo en los momentos más turbulentos motivándome y ayudándome.

Víctor Manuel De la Cruz Flores

AGRADECIMIENTOS

Le agradezco a **Dios** por haberme permitido culminar mi carrera universitaria, por ser mi fortaleza en los momentos de debilidad y por brindarme una vida llena de aprendizajes, experiencias y sobre todo de felicidad.

A mi madre **Ana Mercedes**, por a pesar de todos los inconvenientes siempre estar ahí apoyándome y motivándome para culminar mis estudios. A mis tías **Marina Disla** y **Xiomara Peláez**, dos mujeres esenciales en mi vida, las cuales agradezco por el amor recibido, la dedicación y la paciencia con la que cada día se preocupaban para que hoy en día pudiera alcanzar esta meta.

A mis hermanas y primas, en especial a **Mariely Mañan** y **Claribel Terrero** las cuales han sido mi mayor impulso en este proceso y las cuales me han apoyado en cada decisión y cada proyecto.

A mi amigo **Jhonatan Martínez**, el cual ha estado en todo el trayecto de mi vida dándome un apoyo incondicional y estando presente en todo momento. Hoy en día me siento feliz porque logramos esta meta juntos.

Quiero exaltar la labor de mis amigos **Ariel Febles**, **Elisardo Félix** y resaltar el apoyo de la señorita **Diana Martínez**, los cuales estuvieron presentes durante toda o la mayor parte de la realización y el desarrollo de esta tesis.

A nuestro asesor, **Profesor Edgar Morrobert**, el cual fue nuestra guía para hoy poder culminar nuestros estudios, donde compartió de sus conocimientos no tan solo en este trabajo final si no a lo largo de nuestra carrera universitaria.

Francisco Alberto Deño

AGRADECIMIENTOS

Mi agradecimiento a la Universidad UNAPEC por haberme permitido formarme en ella.

Gracias al **Ing. Edgar Morrobert** por ser el asesor y guía para completar esta tesis.

Gracias al cuerpo docente de la universidad por sus enseñanzas.

Gracias a mis familiares y amigo por ayudarme a dar este gran paso, ser profesional.

Víctor Manuel De la Cruz Flores

RESUMEN EJECUTIVO

Todas las actividades que se desarrollan para la producción de bienes y servicios tienen unos riesgos asociados en la ejecución de sus procesos, que se obtienen de los contextos externo o interno de la empresa. En el caso de los riesgos relacionados por la utilización de la tecnología de la información, se hace necesario generar herramientas de gestión que garanticen la continuidad del negocio, en esta investigación se busca evaluar los riesgos de tecnología de la información en una zona franca de equipos electrónicos, para un periodo de septiembre a diciembre del año 2019. Para tales fines se utilizó la Norma ISO/IEC 27005: 2011 Gestión de riesgos de la Seguridad la Información.

El punto de partida fue la identificación de los activos de tecnología de la información de la zona franca de equipos electrónicos, utilizada para todas sus operaciones, además de la evaluación de las medidas de seguridad implementadas, para de este modo establecer controles y evaluar los existentes, finalmente se realizó una evaluación de riesgos, identificando los activos críticos, así como las amenazas a las que están expuestos.

En esta investigación se hizo énfasis en determinar los riesgos en base a su probabilidad de ocurrencia y el impacto asociado que generaría en la producción de la zona franca. Los resultados de esta investigación constituyen un factor clave del éxito medular para la empresa, ya que la misma tiene sus procesos automatizados en un 100%.

Esta investigación fue producto de un estudio de campo que se llevó a cabo mediante procedimientos científicos tales como observaciones, recolección de información y datos en general de la zona franca de equipos electrónicos.

Los resultados que arroja el estudio determinaron.

- Razonamiento de los riesgos críticos de la zona franca.
- Evaluación de los riesgos de la tecnología de la información.
- Establecimiento de controles.

INTRODUCCIÓN

La zona franca donde se realizó esta investigación que tiene como intención evaluar los riesgos de tecnología de la información en un periodo de septiembre a diciembre del año 2019, se dedica al reacondicionamiento de equipos electrónicos para la venta internacional, la misma tiene facilidades tributarias (exenciones) que les brinda el Gobierno Dominicano para un tema de empleos RD.

Esta zona franca utiliza en un 100% la Tecnología de la Información y Comunicaciones (TIC) en el proceso de producción, reacondicionamiento de equipos electrónicos y en los procesos administrativos. En adición a esto, los riesgos sobre los objetivos de la seguridad de la información (disponibilidad, confidencialidad e integridad) se hacen presentes. Por tal razón, realizar evaluaciones periódicas, y objetivas, para determinar el nivel de riesgo al que están expuestos estos objetivos, debe ser una prioridad para lograr los objetivos que se establecen en la empresa.

En esta investigación se establecerá el contexto de los riesgos de TIC de la zona franca, se determinarán todos los activos de tecnología de la información, se evaluaran los riesgos asociados en base a la probabilidad e impacto, basados en la norma ISO/IEC 27005:2011 de Gestión de Riesgos de Seguridad de la Información, se analizaran los controles existentes y se realizará una propuesta de mejora basado en los hallazgos, esto permitirá implementar acciones de tratamiento de estos riesgos, que una vez implementados podrán disminuir el nivel de incertidumbre con que puede estar operando la empresa.

Esta zona franca tiene como característica critica que debe cumplir con acuerdos y normativas de aceptación de Estados Unidos, lo que demanda un nivel de eficacia en la operatividad de su producción, por ende, un riesgo de seguridad de la información impacta directamente en que no se cumpla con este apartado que puede repercutir en el colapso de la zona franca de equipos electrónicos.

El contenido de esta investigación está presentando en un informe que consta cinco capítulos básicos: Introducción, información general de la investigación: Justificación, Antecedentes, preguntas y objetivos, el planteamiento del problema de investigación. El Marco metodológico el cual contiene, tipo de investigación, técnicas e instrumentos de recolección de datos, método de estudio, diseño de investigación, procedimientos para la recolección de datos, técnicas empleadas en el proceso, procedimientos para el análisis de datos, técnicas empleadas en el proceso, validez y confiabilidad delimitación, limitaciones y contexto de investigación.

La información ha sido segmentada de la siguiente forma: Capítulo I. Aspectos introductorios del problema de investigación. Capitulo II. Evaluación de riesgos de tecnología de la información en una zona franca de equipos electrónicos. Capitulo III. Gestión de riesgos de seguridad de la información ISO/IEC 27005:2011. Capitulo IV. Contexto de la Tecnología de la información en zona franca de equipos electrónicos, objeto del estudio y Capítulo V. Soluciones a los riesgos de tecnología de la información investigados en la zona franca. Se dedica un apartado a la bibliografía básica de los temas abordados.

CAPITULO I

ASPECTOS INTRODUCTORIOS DEL PROBLEMA DE INVESTIGACIÓN

1.1. Selección del tema

EVALUACIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN EN UNA ZONA FRANCA DE EQUIPOS ELECTRÓNICOS, PERIODO SEPTIEMBRE-DICIEMBRE, AÑO 2019.

1.2. Planteamiento del problema

En las zonas francas de equipos electrónicos se incrementan cada día más los riesgos tecnológicos, debido a que al pasar el tiempo aumentan el número de aplicaciones y herramientas de tecnología, que incluyen nuevos riesgos, que requieren ser adecuadamente gestionados. Es por esto la necesidad de realizar una evaluación de riegos de tecnología de la información.

La zona franca objeto de estudio nunca ha realizado una evaluación de los riesgos de la Tecnología de la Información (TI) que utiliza, por lo que no tiene cuantificado el nivel de impacto que tendría sobre sus operaciones la materialización de determinados riesgos.

La investigación se realizará en la zona franca que por motivos de confidencialidad se omitirá el nombre de esta. Está se encuentra ubicada en la ciudad de Santo Domingo, República Dominicana.

Las informaciones presentadas tendrán efecto durante el periodo de tiempo Septiembre - Diciembre del año 2019.

1.3. Justificación

Se adopta la definición propuesta por Bosque et. Al (2004) en donde, el Riesgo Tecnológico hace referencia a la probabilidad de sufrir daños o pérdidas económicas, ambientales y humanas como consecuencia del funcionamiento deficiente o accidente de una tecnología aplicada en una actividad humana. (Negrete, 2015).

Tener en conocimiento el nivel de riesgo en que está operando una determinada organización, le permite a sus directos tomar decisiones más certeras para el logro de los objetivos estratégicos que se hayan definido para dicha organización. Todo proceso tiene asociado determinados riesgos inherentes y en Tecnología de la Información se pueden citar los relacionados a afectar los objetivos de la seguridad de la información: Disponibilidad, Integridad y Confidencialidad.

En la industria de las zonas francas de equipos electrónicos, las fuentes que pueden afectar estos objetivos tienen sus orígenes, principalmente, en la gestión de los accesos físicos y lógicos a los entornos donde se manejan las informaciones, propias de la organización, así como de sus clientes y partes interesadas.

Basado en lo que se describe anteriormente este trabajo de grado tiene como finalidad realizar un proceso de evaluación de riesgos de tecnología de la información en una zona franca de equipos electrónicos para presentar las recomendaciones que consideramos apropiadas para tratar apropiadamente estos riesgos.

1.4. Objetivos de la investigación

1.4.1. Objetivo General

Evaluar los riesgos de tecnología de la información en una Zona Franca de Equipos Electrónicos, ubicada en la cuidad de Santo Domingo, Rep. Dom. Periodo septiembre-diciembre, año 2019.

1.4.2. Objetivos específicos

1. Analizar en forma detallada el ambiente de TI de la Zona Franca, agrupando por área de controles generales los procesos que se realizan en esta.

2. Determinar los criterios para cualificar las probabilidades de ocurrencia de los riesgos de TI identificados.

3. Determinar los criterios para cuantificar las probabilidades de ocurrencia de los riesgos de TI identificados.

4. Determinar los criterios para cualificar el impacto, para el negocio de la Zona Franca, de los riesgos de TI identificados.

5. Determinar los criterios para cuantificar el impacto, para el negocio de la Zona Franca, de los riesgos de TI identificados.

1.5. Alcance

La investigación se realiza en las instalaciones de una zona franca la cual se dedica a la reparación y al remanufacturado de dispositivos electrónicos, localizada en la cuidad de Santo Domingo, Rep. Dom. Periodo septiembre- diciembre, año 2019.

1.6. Métodos de investigación

1.6.1. Observación

En base a lo expresado por Fernández Collado y Baptista Lucio (2014) “La recolección se basa en instrumentos estandarizados. Es uniforme para todos los casos. Los datos se obtienen por observación, medición y documentación. Se utilizan instrumentos que han demostrado ser válidos y confiables en estudios previos o se generan nuevos basados en la

revisión de la literatura y se prueban y ajustan. Las preguntas, ítems o indicadores utilizados son específicos con posibilidades de respuesta o categorías predeterminadas".

1.6.2. Inductivo

Es el método de investigación del cual se parte del análisis de lo particular hasta llegar a conclusiones generales, es decir, va de lo particular a lo general, Sampieri (2007).

1.7. Tipos de investigación

1.7.1. Investigación descriptiva

Muy frecuentemente el propósito del investigador es describir situaciones y eventos. Esto es, decir cómo es y se manifiesta determinado fenómeno. Los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, comunidades o cualquier otro fenómeno que sea sometido a análisis (Dankhe, 1986). Miden y evalúan diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar. Desde el punto de vista científico, describir es medir. (Sampieri, 1997)

Para poder evaluar los riesgos de tecnología de la información, se utilizará el estudio descriptivo, ya que a través de este podemos investigar en detalle, los eventos físicos y lógicos encontrados en las Zonas Francas de equipos electrónicos. Esto, con el propósito de medir las vulnerabilidades de una infraestructura tecnológica.

1.7.2. Investigación explicativa

Están dirigidos a responder a las causas de los eventos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se da éste, o por qué dos o más variables están relacionadas. Además de que proporcionan un sentido de entendimiento del fenómeno a que hacen referencia. (Sampieri, 1997).

Por medio del estudio explicativo, se podrá entender las diferentes debilidades de los sistemas de información relacionadas a las variables de control existentes en las Zonas Francas de Equipos Electrónicos, tales como procesos de seguridad y control al acceso de la información.

1.8. Resumen capítulo I

Las zonas francas son empresas que se destinan a la industrialización de productos con fines de exportación o servicios como servicio al cliente vía telefónica, los llamados call center. Este tipo de empresa tienen facilidades tributarias (exenciones) que les brinda el Gobierno Dominicano, a los fines de dinamizar su crecimiento y fortalecerlas como fuentes de empleo. Las zonas francas de equipos electrónicos están dedicadas al reacondicionamiento de equipos electrónicos de manera que puedan estar disponibles para la venta.

El uso de la Tecnología de la Información y Comunicaciones (TIC) en las zonas francas de equipos electrónicos puede ser considerado como alto. En adición, los riesgos sobre los objetivos de la seguridad de la información (disponibilidad, confidencialidad, integridad) se hacen presentes en esta industria. Por tal razón, realizar evaluaciones periódicas, y objetivas, para determinar el nivel de riesgo al que están expuestos estos objetivos, debe ser una prioridad para lograr los objetivos que se establecen este tipo de empresas.

Este trabajo incluye todos los aspectos necesarios para lograr determinar el contexto de riesgos de TIC de la zona franca objeto de estudio y con su desarrollo se obtendrán las acciones de tratamiento de estos riesgos, que una vez implementados podrán disminuir el nivel de incertidumbre con que puede estar operando el objeto de estudio.

CAPITULO II

EVALUACIÓN DE RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN EN UNA ZONA FRANCA

2.1 Evaluación de riesgos

El riesgo es considera y definido como una amenaza que tiende a explotar los ámbitos de la vulnerabilidad de un activo el cual puede ser dañado. Por su parte, los riesgos de seguridad de la información y la tecnología de las comunicaciones, se define como las amenazas que puede sufrir la infraestructura de los equipos tecnológicos, sobre toda el área de data center principal de dicha estructura, lugar donde se encuentran alojados diversidad de servidores.

El objetivo principal que se persigue mediante la evaluación de riesgos es el de proteger a la organización o institución, dicha protección no solo encaminada a los elementos informáticos, sino que también procura proteger a toda la organización como una función esencial de la empresa.

En este mismo tenor, es importante señalar, que la evaluación de riesgos es el proceso mediante el cual se pretende detectar, identificar, evaluar, controlar y en este mismo orden, aplicar ideales y tomar decisiones, para la prevención y reducción de riesgos que pueda vulnerar los equipos electrónicos. Es por esto que, a través de la implementación de las evaluaciones de riesgos, se puede controlar y prevenir el impacto negativo de factores externos sobre los equipos, así como las probabilidades e incidencias de que estos se vean afectados por dichos factores.

No obstante, a pesar de la importancia que poseen los sistemas de evaluación de riesgos cabe mencionar, que no existe un método concreto de cómo gestionar dichos riesgos, por lo cual, de acuerdo con las necesidades de cada equipo y cada empresa, lo ideal es el desarrollo de un proceso estructurado, sistemático y riguroso de análisis de riesgos para la creación del plan de tratamiento y prevención de estos.

Bien es cierto que la gestión del riesgo es una actividad recurrente dentro de las empresas, que se refiere al análisis, a la planificación, solución, ejecución, el control y el seguimiento de todas las medidas implantadas y la política de seguridad que ha sido impuesta en torno a los equipos electrónicos al igual que a la preservación de la información, por lo cual, los

desarrolladores de dichos sistemas de evaluación de riesgos, deben velar por que los mismos se adapten a las necesidades de la empresa y los equipos que se utilizan dentro de la mismo, debido a que son los indicadores de riesgo los que muestran si la empresa se encuentra sujeta o tiene alta probabilidad de ser sometida a un riesgo, por lo cual, un sistema no adecuado puede repercutir en que dichos indicadores de riesgo nos muestren las necesidades reales de la institución en torno a los riesgos que en la misma se presentan.

2.2. Tecnología de la información

Para Raffino (2018), la tecnología es un conjunto de nociones y conocimientos utilizados para lograr un objetivo preciso, que dé lugar a la solución de un problema específico del individuo o a la satisfacción de alguna de sus necesidades. Es un concepto extremadamente amplio que es capaz de abarcar una inmensa variedad de aspectos que pueden ir de la electrónica al arte o la medicina.

La tecnología de la información es considerada como la aplicación de equipos electrónicos mediante los cuales los negocios y las empresas logran almacenar, recuperar, transmitir y manipular datos.

La frase tecnología de la información es proveniente del inglés “Information Technology”, y se hace conocido a través del administrador de computadoras Jim Domsic (1985), con la finalidad de darle un término más actualizado al procesamiento de datos.

La tecnología de la información es un término que comprende todo lo que está vinculado con el almacenamiento, protección, procesamiento y transmisión de la información. Este concepto engloba todo lo relacionado con la informática, la electrónica y las telecomunicaciones. Los avances tecnológicos como el Internet, las comunicaciones móviles, los satélites, entre otros. Han hecho significativos cambios en el sistema económico y social, influyendo en las relaciones sociales. Venemedia 2019.

El término es utilizado como sinónimo para los computadores, y las redes de computadoras, pero también abarca otras tecnologías de distribución de información, tales como la televisión y los teléfonos. Múltiples industrias están asociadas con las tecnologías de la información, incluyendo hardware y software de computador, electrónica, semiconductores, internet, equipos de telecomunicación, e-commerce y servicios computacionales.

Es en este mismo orden que la tecnología de la información permite capturar, almacenar, transmitir, gestionar, consultar informaciones de las organizaciones, sus clientes y las partes interesadas (accionistas, proveedores, entre otras). Las características relacionadas a la manera en que hoy día se manejan las Tecnología de la Información crean nuevas amenazas y vulnerabilidades, que aumentan el desafío de mantener la adecuada gestión de la seguridad de la información, en cualquiera de sus estados.

La tecnología de la información abarca el dominio completo de la información, que incluye al hardware, al software, a los periféricos y a las redes. Un elemento se orienta dentro de la categoría de las TI cuando se usa con el propósito de almacenar, proteger, recuperar y procesar datos electrónicamente.

En la actualidad y gracias a las tecnologías de la información los individuos pueden comunicarse y recibir información en tiempo real, cosa que era imposible hacer hace unos años atrás. Estamos viviendo en la era de la información, y a nivel empresarial, una organización debe estar al día con relación a las nuevas tecnologías ya que esto va a repercutir en su desempeño, el poder manejar herramientas que logren disminuir los costos operativos de la empresa es de vital importancia al igual que el poder entregar los productos en menor tiempo, y el brindarles a los clientes un servicio de calidad y con resultados óptimos.

La mejor manera de que una empresa sea mucho más competitiva a nivel nacional e internacional es manejando las tecnologías de la información, adquiriendo equipos de alta tecnología y mejorando los procesos de TI, simultáneamente ir capacitando a su personal

para que este sea capaz de poder manejar todo lo relacionado con los equipos tecnológicos que se encuentren dentro de la organización.

Dentro de la tecnología podemos marcar de las predecesoras, la que se usan en el teléfono, radio y televisión. Dentro de las recientes consideraremos las que se refieren a comunicaciones móviles.

Podemos citar como ejemplo el mismo tipo de tecnologías que se utilizan para trasmitir la voz puede también trasmitir el fax, datos y el vídeo de compresión digital. Las redes se marcarán como aquellas que utilizan una conexión a través de cable de fibra óptica, cable de cobre, cable coaxial, conexiones inalámbricas, telefonía celular y los enlaces por satélite.

Los hardware de equipos se referirán a la parte física que constituyen los dispositivos. Tenemos como ejemplos los ordenadores y todos los equipos que se utilizan para la conectividad de la red y para la comunicación. Los programas informáticos (software) por su parte que son el fluido de todos estos elementos.

2.2.1. Componentes de tecnología de la información

Los múltiples factores con cualidad tecnológica explican la convergencia de la electrónica, la informática y las telecomunicaciones en las Tecnología de la Información y la Comunicación. Todas parten de tres hechos fundamentales: Los tres campos de actividad se caracterizan por utilizar un soporte físico común, como es la microelectrónica, llamado el hardware. Por el gran componente del software incorporado, por el uso intensivo de la infraestructura de comunicaciones, que permiten la distribución (deslocalización), de los distintos elementos de proceso de la información en ámbitos geográficos distintos. Revista educativa (2019).

La microelectrónica, es frecuentemente denominada hardware, está residente en todas las funcionalidades del proceso de información. Soluciona los problemas relacionados con la interacción con el entorno como la adquisición y la presentación de la información,

mediante dispositivos como transductores, tarjetas de sonido, tarjetas gráficas, entre otros. Su mayor potencialidad está en la función de tratamiento de la información.

La unidad fundamental de tratamiento de la información es el microprocesador, que es el órgano que interpreta las órdenes del software, las procesa y genera una respuesta. La microelectrónica está presente en todas las funciones de comunicación, almacenamiento y registro.

El software es responsable de trasladar las órdenes que el usuario da a una computadora al lenguaje de ejecución de órdenes que entiende la máquina.

Está presente en todas las funcionalidades del proceso de la información, pero especialmente en el tratamiento de la información. El hardware sólo entiende un lenguaje que es el de las señales eléctricas en forma de tensiones eléctricas.

Las infraestructuras de comunicaciones constituyen pues el otro elemento base del proceso de información, desde el momento en que alguna de las funcionalidades resida en un lugar físicamente separado de las otras. Para acceder a esta función hay que utilizar redes de comunicación por las que viaja la información, debiéndose asegurar una seguridad, calidad, inexistencia de errores, rapidez, entre otros. Universidad de Cauca 2019.

En general, las tecnologías de la información constan de los siguientes elementos que se combinan para proporcionar al usuario servicios a través de diversas aplicaciones.

La variedad de aplicaciones es una integración de las tecnologías cuya finalidad es que el acceso y uso de los servicios sea intuitivo y sencillo para el usuario, evitando de esta forma cualquier complejidad tecnológica en el servicio. Los tres componentes son:

- Hardware.
- Software.
- Infraestructuras de telecomunicaciones.

Hardware: Son todos los componentes físicos y accesorios del ordenador (hardware es un término inglés que puede traducirse como "lo duro"). Es el soporte físico que ayuda al tratamiento de la información. Más conocido con el nombre de PC (Personal Computer o equivalentemente, computadora u ordenador personal) para identificarla.

Software: Es el conjunto de programas informáticos; son programas o instrucciones escritas en un lenguaje que puede interpretar el ordenador (la palabra anglosajona software significa "lo blando"). Los programas de software se basan en la utilización de códigos de números.

Los programas de software más extendidos son los sistemas operativos, procesadores de texto, hojas de cálculo, bases de datos, programas de diseño gráfico, entre otros.

El software es el elemento clave que permite la compenetración entre hombre y la máquina.

Software: Es el soporte lógico, un conjunto de instrucciones escritas en lenguajes de programación y traducidas posteriormente a dígitos binarios para que sean entendidas por el hardware. Está presente en todas las funcionalidades del proceso de la información, pero especialmente en el tratamiento de la información.

La tecnología software está presente en todos los procesos de información, ya que dichas funciones son realizadas cada vez con mayor intensidad por ordenadores.

Los distintos componentes bases del software son:

a) Sistemas Operativos: Responsables del control de las complejas arquitecturas que pueden construirse con los componentes microelectrónicos y facilitar interfaces amigables con el usuario.

b) Middleware: La parte de la arquitectura encargada de abstraer a las aplicaciones de los detalles de las plataformas de explotación, mediante las Application Programs Interfaces (APIs).

c) Cliente/Servidor: Es la arquitectura que reparte la carga de trabajo entre la estación de usuario y la estación central.

d) Bases de Datos: Se utilizan para el manejo, manipulación y administración de información.

e) Programas de Aplicación: Software para la realización de tareas variadas como puedan ser hojas de cálculo, proceso de textos, aplicaciones de gestión comercial, científicas, de diseño, entre otros.

f) Lenguajes de Programación y Herramientas para la Ingeniería Software: Son el conjunto de lenguajes y herramientas de ayuda al desarrollo de la realización de aplicaciones específicas.

Las tecnologías de la información se caracterizan porque, conforme avanza su desarrollo, el componente de software constituye un porcentaje mayor del valor añadido incorporado a los productos. Así, por ejemplo, se calcula que el software constituye el 80% del coste de las infraestructuras de telecomunicaciones.

Infraestructuras de Telecomunicaciones: Transportan la información desde un punto a otro, a través de un conjunto de equipos y medios de acceso, transmisión y conmutación.

Proporcionan la capacidad necesaria para mantener una comunicación, ya sea ésta en forma de voz, datos o imágenes. Esta definición incluye todas las necesidades que impone una comunicación, como son tener acceso a la red de comunicación, transportar la información y poner en comunicación al emisor y al receptor.

2.2.2. Características de las tecnologías de la información

Innovación: Señala que es tan rápido el proceso de innovación de la tecnología que rebosa al contexto prevaleciente, en ocasiones por su poca capacidad para absorber la tecnología, o en muchas de las ocasiones cuando se incorpora una tecnología a cualquier empresa, esta tecnología ya está siendo remodelada y trasformada.

Interconexión: Describe las diferentes formas de conexiones, vía hardware y que se permitirá el acto de la comunicación en el que se han desarrollado nuevas realidades expresivas y comunicativas.

Diversidad: Esto significa que no existe una única tecnología disponible, sino que, por el contrario, se tiene una variedad de ellas.

Inmaterialidad: Esto hace referencia a que la materia prima en torno a la cual desarrollan su actividad es la información, e información en múltiples códigos y formas, tales como: visuales, auditivas, audiovisuales, textuales de datos estacionarios y en movimiento.

Interactividad: El control de la comunicación se centra más en el receptor, descargando un papel importante en la construcción del mensaje, el rol del trasmisor evoluciona.

Instantaneidad: Esta elimina las barreras de espacio y tiempo.

Generación de nuevos lenguajes expresivos: Esto es que permiten nuevas realidades expresivas, como es el caso de los multimedia e hipermedia, que ocasionan nuevos

dominios alfabéticos, que potencializan la alfabetización en el lenguaje informático y multimedia.

Ruptura de la linealidad expresiva: Los mensajes tienden a organizarse no de forma lineal, sino de manera hipertextual, lo que da como resultado consecuencias significativas, tales como son la desestructuración del discurso, la transferencia del peso de la comunicación del autor al texto, el desafío de pasar de la distribución de la información a su gestión, y la construcción del significado de forma diferente en función de la navegación hipertextual realizada por el receptor.

Elevados parámetros de calidad, imagen y sonido: La calidad con que pueden transferir la información, y se ha logrado por la digitalización de las señales visuales, auditivas y de datos y por los avances significativos en el hardware usado para las comunicaciones.

Potenciación, audiencia segmentaria y diferenciada: Es la especialización de los programas y medios en función de las características y demandas de los receptores, esto indica en el caso de los medios televisivos, que pueden provocar una segmentación de audiencias, según la conveniencia.

También el caso de las redes sociales o comunidades virtuales rompen el concepto de cultura de masas y se superpone la cultura de la fragmentación de las audiencias en función de los intereses y actitudes de los que participen.

2.2.3. Papel de la tecnología de la información en las empresas

La tecnología de la información juega un papel fundamental dentro de las empresas, esto en virtud de las reducciones en los costos de la producción, repercute en mejoras organizacionales a nivel de estructura, influye a su vez en la extensión comercial de la empresa y en el desarrollo de la imagen, así como el posicionamiento de esta en el mercado de una forma más específica se puede mencionar que:

- Información, bajada de los costes.
- Deslocalización de la producción (centros de atención a clientes).
- Mejor conocimiento del entorno, mejora de la eficacia de las tomas de decisiones.
- A nivel de la estructura de la empresa y de la gestión del personal.
- Organización menos jerarquizada, repartición sistemática y práctica de la información.
- Mejor gestión de los recursos humanos.
- A nivel comercial.
- Extensión del mercado potencial (comercio electrónico).
- Una bajada de los costes logísticos.
- Desarrollo de las innovaciones en servicios y respuestas a las necesidades de los consumidores.
- Mejora de la imagen de marca de la empresa (empresa innovadora).

Quedando claramente expuesto que la tecnología de la información colabora con la evolución de las empresas y su transformación, dotándolas de más confianza, autonomía de gestión y reivindicación cívica frente a la sociedad, lo cual ha desencadenado en el empoderamiento de las empresas.

2.3. Zona franca

Para Lynne Markus y Daniel Robey (2009) una zona franca es un territorio delimitado de un país donde se goza de algunos beneficios tributarios, como la exención del pago de derechos de importación de mercancías, así como exoneraciones de algunos impuestos o una diferente regulación de estos.

El área geográfica destinada a la zona franca tiene como finalidad atraer inversiones extranjeras, conectar la economía nacional con la internacional.

En pocas palabras podemos decir que una zona franca es un área de terreno de una nación, físicamente delimitada y sujeta a un régimen fiscal y aduanero especial. Dicho territorio, está dedicado a la producción y comercialización de bienes para la exportación, así como a la prestación de servicios vinculados con el comercio internacional.

2.3.1. Características

Muchos gobiernos de países establecen zonas francas en regiones apartadas o extremas, con el fin de atraer allí a población y promover el desarrollo económico de la región. En las zonas francas suelen crearse grandes centros de compra, y también se instalan con frecuencia industrias maquiladoras, plantas procesadoras o almacenes especiales para la mercancía en tránsito.

A veces esas zonas francas son llamadas puertos libres, por una analogía con los puertos libres conocidos desde hace mucho tiempo, los puertos libres de tasas aduaneras o con regulaciones de tasas favorables; por ejemplo, el puerto libre de Trieste. A menudo, los puertos libres son parte de las zonas económicas.

Otras características importantes de las zonas francas es que estas:

- Deben poseer al menos 20 hectáreas de territorio
- Deber estar dotadas de infraestructura
- Debe poseer patrimonio
- Debe poseer un patrimonio líquido determinado

2.3.2. Beneficios

- Captan nuevas inversiones de capital
- Generar empleos formales
- Generan empleos calificados
- Consolidan la plataforma logista de una nación

- Generar encadenamientos productivos
- Aportan al desarrollo económico del país

2.3.3. Clasificación de las zonas francas

Zona franca permanente: es la que posee un área delimitada del territorio nacional, en la que se instalan múltiples usuarios industriales o comerciales, los cuales gozan de un tratamiento tributario, aduanero y de comercio exterior especial, según sea el caso.

Zona franca permanente especial: es la que posee el área delimitada del territorio nacional, en la que se instala un único usuario industrial, el cual goza de un tratamiento tributario, aduanero y de comercio exterior especial.

Zona franca transitoria: es el área delimitada (transitoria) del territorio nacional, donde se celebran ferias, exposiciones, congresos y seminarios de carácter nacional e internacional, que revistan importancia para la economía y/o el comercio internacional, y que gozan de un tratamiento tributario, aduanero y de comercio exterior especial.

En virtud de si las zonas francas pertenecen al estado, a una empresa privada, a una asignación específica de producción o poseen más de una de estas mismas características, se pueden clasificar a su vez en:

- Zonas francas privadas
- Zonas francas estatales
- Zonas francas especiales
- Zonas francas mixtas

2.3.4. Clasificación de los usuarios de las zonas francas

Usuario operador: persona jurídica autorizada para dirigir, administrar, supervisar, promocionar y desarrollar una o varias zonas francas, así como para calificar a sus usuarios.

Usuario industrial de bienes: persona jurídica instalada exclusivamente en una o varias zonas francas, autorizada para producir, transformar o ensamblar bienes, mediante el procesamiento de materias primas o de productos semielaborados.

Usuario industrial de servicio: persona jurídica autorizada para desarrollar:

- Logística, manipulación, distribución, empaque, reempaque, envase, etiquetado o clasificación.
- Telecomunicaciones, sistemas de tecnología de la información para captura, procesamiento, almacenamiento y transmisión de datos
- Investigación científica y tecnológica.

Usuario comercial: persona jurídica autorizada para desarrollar actividades de mercadeo, comercialización, almacenamiento o conservación de bienes, en una o varias zonas francas.

2.3.5. Zonas francas en la República Dominicana

Las zonas francas en la República Dominicana datan del año 1969 con la instalación de una Zona Franca Industrial en la ciudad de La Romana. La segunda zona franca del territorio nacional dominicano nació en el año 1972 con el auspicio del sector público a través de la Corporación de Fomento Industrial (CFI), entidad descentralizada del Estado que en el presente sigue encargada de su administración y operación. Esta segunda zona está ubicada en la ciudad de San Pedro de Macorís. Es en ese mismo orden, en el año 1973 cuando surge la tercera zona franca del país localizada en la ciudad de Santiago de los Caballeros.

El Consejo Nacional de Zona Francas de Exportación de la República Dominicana (2019) establece que, a partir del año 1973, las tres Zonas Francas existentes empiezan a crecer de manera sostenida. Es así como en la década de 1973 – 1983, las empresas establecidas pasaron de 15 a 101. El auge de la demanda de naves industriales prosiguió con mayor intensidad durante los años 1986, 1987 y 1988, cuando la República Dominicana registró el proceso de instalación de zonas francas más importante en el área del Caribe y Centroamérica, superando a todas las naciones del área.

Actualmente en base al Reporte de Estadísticas Zonas Francas República Dominicana (2017) el sector de Zonas Francas de la República Dominicana posee unos 150,000 empleados en toda la geografía nacional, distribuidos de la siguiente manera: 46% Región Norte, 12% Región Este, 25% Distrito Nacional y 17% Región Sur. Las exportaciones realizadas por las zonas francas durante el año 2014 sobrepasaron los US$5.2 millones de dólares.

En la actualidad, la República Dominicana cuenta con uno de los programas de zonas francas más dinámicos y exitosos en toda el área de Centroamérica y el Caribe. Dicho programa ha demostrado ser una alternativa efectiva y rentable para las empresas extrajeras, principalmente por la cercanía del país a los Estados Unidos.

Para Ibidem (2019), estos centros de producción permiten que compañías extranjeras y locales puedan establecer operaciones y se beneficien de incentivos impositivos y de facilidades de importación. Hoy en día operan en el país un total de 68 parques de zonas francas, diseminados en todo el territorio nacional, los cuales albergan alrededor de 645 empresas y aportan más de 160,000 empleos.

Actualmente en la República Dominicana, las Zonas Francas se han convertido en uno de los sectores más dinámicos de la economía dominicana y en vínculo estratégico con los más importantes mercados internacionales. Con cerca de 614 empresas establecidas en 60 parques industriales. La actividad que mayormente se ha desarrollado dentro de las zonas francas es la confección textil, encontrándose nuestro país entre los primeros en volúmenes

de exportación de este renglón al mercado de los Estados Unidos. Otras actividades de importancia son la fabricación de calzados, manufactura de joyas, ensamblaje de componentes electrónicos, entre otros.

2.4. Equipos electrónicos

Para Ibidem (2019), un aparato electrónico consiste en una combinación de componentes electrónicos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas. Los aparatos electrónicos a diferencia de los eléctricos utilizan la electricidad para el almacenamiento, transporte o transformación de información.

En este orden, son considerados como equipos electrónicos todo aparato que se encuentre elaborado mediante la utilización de componentes electrónicos, tales como los denominados transistores, circuitos integrados, resistencias, capacitores, entre otros. Es decir, que se constituyen como equipos electrónicos aquella combinación de componentes electrónicos que se encuentran organizados en circuitos, los cuales se encuentran destinados a controlar y aprovechar las señales electrónicas, estos utilizan la electricidad para lograr almacenar, transportar o transformar información.

2.4.1. Mantenimiento de los equipos electrónicos

El buen funcionamiento de los equipos es un factor decisivo en la rentabilidad y competitividad global de una empresa, para las empresas es importante mantener todo funcionando sin problemas y eficientemente para minimizar el tiempo de inactividad de la producción y evitar eventos imprevistos. Por lo tanto, es necesario tener un buen control de calidad.

Dentro de las empresas, a través del manteniendo de los equipos electrónicos se persigue reducir los riesgos de paradas de producción, y aumenta la vida útil de los mismos, evitando un mayor coste de reparaciones futuras.

2.4.2. Propósitos y objetivos del mantenimiento de equipos electrónicos

Propósitos y objetivos que se persiguen y se pretenden obtener mediante la ejecución del mantenimiento de equipos electrónicos son:

- Configurar circuitos electrónicos reconociendo su estructura en bloques.
- Calcule los parámetros de los circuitos electrónicos analógicos y digitales identificando los valores de las etapas de entrada-salida y de acondicionamiento y procesamiento de la señal.
- Verificar el funcionamiento de los circuitos analógicos y de la electrónica digital micro programable utilizando equipos de medición y sistemas de software para el análisis y la configuración.
- Elaborar el presupuesto de mantenimiento, comparando los aspectos técnicos y económicos para ofrecer la mejor solución.
- Organizar y gestionar las intervenciones de mantenimiento correctivo en función del nivel de servicio y optimizar los recursos humanos y materiales.
- Gestionar el suministro y almacenamiento de materiales y equipos, definiendo la logística asociada y controlando los stocks.
- Desarrollar intervenciones de mantenimiento de acuerdo con la documentación técnica y las condiciones de los equipos o sistemas.
- Diagnosticar disfunciones o averías en equipos o sistemas, en función de los síntomas detectados, la información proporcionada por el usuario, la información técnica y el historial de instalación.
- Supervisar y/o ejecutar procesos de mantenimiento preventivo, correctivo y predictivo, controlando el tiempo y la calidad de los resultados.
- Realizar la puesta en marcha de los equipos y sistemas electrónicos, asegurando su funcionamiento dentro de los parámetros técnicos de aceptación y asegurando las condiciones de calidad y seguridad.

2.4.3. Clasificación de los equipos electrónicos

2.4.3.1. Según los materiales

Grandes electrodomésticos: los grandes electrodomésticos son aquellos que poseen una mayor demanda de corriente eléctrica circulando en su sistema para su correcto funcionamiento.

Pequeños electrodomésticos: son aquellos que necesitan de una menor demanda de voltaje o de electricidad para su correcto funcionamiento.

2.4.3.2. Según la posición

Equipos de informática y telecomunicaciones: son aquellos equipos electrónicos que han sido diseñados para la transmisión de información.

Aparatos electrónicos de consumo: son aquellos equipos electrónicos que han sido diseñados para el consumo de los usuarios, entre estos podemos encontrar los televisores, los radios, entre otros.

Herramientas electrónicas o eléctricas: son maquinarias utilizadas como herramientas de trabajo, tales como taladros, sierras eléctricas y máquinas de coser, tomando en cuenta que no pertenecen a esta categoría las maquinarias industriales que permanecen de forma fija dentro de las empresas.

Aparatos médicos: son todos los aparatos que poseen componentes eléctricos o electrónicos utilizados en el sector salud.

CAPITULO III

GESTIÓN DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN ISO/IEC 27005:2011

3.1. Norma ISO/IEC 27005:2011

La primera versión de la norma fue publicada el 4 de junio del año 2008. La misma establece los lineamientos para la gestión del riesgo en la seguridad de la información, sin apartarse de los conceptos generales especificados en la Norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Primero a esta primera versión, posterior a la publicación de la ISO/IEC 27001:2005, BSI (British Standards Institution, Institución de Estándares Británica) publicó la norma BS7799-3:2006, enfocada en la gestión de riesgos de seguridad de los sistemas de información.

La comprensión de los conceptos, modelos, procesos y términos descritos en la norma ISO/IEC 27001:2005 e ISO/IEC 27002:2013 es importante para un completo entendimiento de la norma ISO/IEC 27005:2011, que es aplicable a todo tipo de organizaciones (por ejemplo, empresas comerciales, agencias gubernamentales, organizaciones sin fines de lucro, entre otras), que tienen la intención de gestionar los riesgos que puedan comprometer la organización de la seguridad de la información. ISO/IEC 27000:2011.

La ISO Norma ISO/IEC 27005:2011, se definió para la administración de riesgos informáticos, y se encuentra alineada a la Norma ISO/IEC 31000:2009, la cual se desarrolló para la administración de riesgos en cualquier área de una organización y como otras normas ISO, tiene como metodología de implementación y mejora continúa basada en el ciclo PHVA (Planear-Hacer-Verificar-Actuar).

3.1.1. Ciclo PHVA o Deming

El ciclo PHVA fue desarrollado en 1920 por Walter Shewhart y popularizado por Edwars Deming, razón por la cual es llamado el ciclo de Deming. El enfoque de este ciclo es establecer y gestionar un sistema de gestión en cualquier nivel de la organización, de tal

forma que el proceso donde se implemente sea sostenible y se encuentre en mejora continua.

La implementación del ciclo PHVA en cualquier sistema de gestión se basa en 4 fases Universidad de Washington (2011), que son las siguientes:

Planificación (Plan): Identificar primero cuál es el problema. El uso de herramientas como los diagramas de Causa y Efecto o el análisis de los 5 (cinco) porqués ayuda a la identificación del problema raíz. Los resultados de estas herramientas sirven de insumo para diseñar un mapa del proceso, con el fin de atacar el problema.

Hacer (Do): Esta fase involucra, inicialmente la reunión de posibles soluciones al problema y posterior, realizar un análisis de estas soluciones para seleccionar aquella que más se adapte a las necesidades y recursos de la organización, y por último desarrollar programas piloto para implementar la solución seleccionada. Esta fase no es explícitamente llevar a producción la solución, en esta fase se "intenta" y se prueba o se realiza test de lo propuesto.

Verificar (Check): Se realiza la medición de la ejecución del piloto implementado en la fase de Hacer. Se recogen y analizan los resultados de ese piloto, con el fin de establecer, de ser necesario, mejoras en el proceso y de esta forma definir el alcance y las áreas de implementación. Es posible repetir la fase Hacer, posterior al análisis de los resultados.

Actuar (Act): Por último, posterior a la implementación completa del proceso, el ciclo de Deming, es un ciclo de mejora continua, lo que significa que se hace necesario, volver a la primera fase Planificación, y estar en constante planificación, ejecución y validación de mejoras el proceso.

GRÁFICO I: CICLO PHVA

Ilustración 1. CICLO PHVA.

Fuente: https://www.gestiopolis.com/el-phva-y-las-normas-iso-9000

Las etapas de la norma ISO/IEC 27005:2011 son para Ramírez & Ortiz (2011):

- Establecimiento de plan de comunicación interno y externo.
- Definición del contexto organizacional interno y externo.
- Valoración de riesgos tecnológicos.
- Tratamiento de riesgos tecnológicos.
- Monitoreo y mejora continua del proceso de gestión.

A continuación, se presentan las actividades del Proceso Gestión del Riesgo para la alineación y operativización del ciclo de Deming PHVA basada en la ISO/IEC 27005:2011.

PLANEAR:

1. Definir el Plan de Gestión del Riesgo.
2. Valoración del riesgo:
   2.1. Identificar el riesgo.
   2.2. Estimación del Riesgo.
   2.3 Evaluación del Riesgo.
3. Plan de Tratamiento del Riesgo.

3.1. Aceptación del Riesgo.

HACER

1. Implementar el Plan de Tratamiento.
2. Implementar el Plan de Divulgación del Riesgo.

VERIFICAR.

1. Monitorear y Revisar el Riesgo.

ACTUAR.

1. Mantener y Mejorar el Proceso de Gestión del Riesgo.

3.1.2. Metodología de gestión del riesgo en la seguridad de la información

Criterio basado en la Norma ISO/IEC 27005:2011 que establece que la identificación de un incidente en el contexto tecnológico es considerada como la materialización de un riesgo. Y la materialización de un riesgo, no importando si éste es reincidente o es identificado por primera vez, implica la definición e implementación de un procedimiento de gestión de riesgos en el contexto tecnológico.

El objetivo principal de una gestión de riesgos es la identificación de las necesidades de una organización en el cumplimiento de los requisitos de un Sistema de Gestión de Seguridad de la Información.

El proceso de gestión de riesgos en área de Seguridad de la Información y en toda organización contribuye con a:

- La identificación de los riesgos
- Valoración de los riesgos de acuerdo con su probabilidad e impacto en la organización.
- Definición de la priorización de los planes de acción o tratamiento del riesgo.

- Participación de los interesados (stakeholders) en la toma de decisiones sobre la gestión del riesgo.
- Eficacia en el monitoreo y cumplimiento de los planes de acción definidos.

Para lograr lo antes expuesto es necesario implementar una metodología que resguarde los principios a fin de la gestión del riesgo, regularmente sobre los incidentes de seguridad derivados de la seguridad y gestión de eventos de información. La metodología seleccionada se basa en Norma ISO/IEC 27005:2011, el modelo sugerido por la norma se visualiza en la siguiente imagen:

Descripción general del proceso de gestión de riesgos de seguridad de la información:

GRÁFICO II: PROCESO DE GESTIÓN DEL RIESGO ISO/IEC

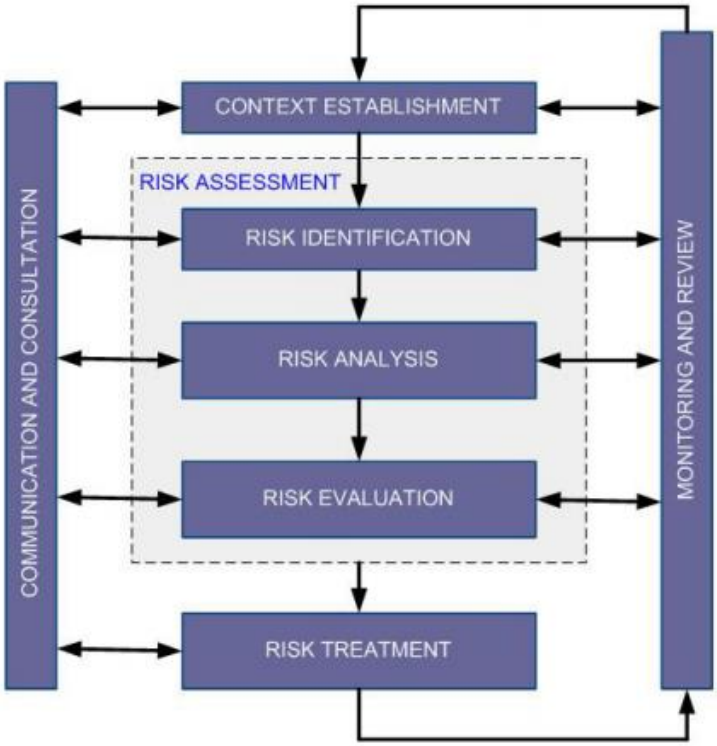

Ilustración 2. PROCESO DE GESTIÓN DEL RIESGO ISO/IEC

Fuente: Norma ISO/IEC 27005:2011.

El proceso de gestión de riesgos de seguridad de la información puede ser iterativo para la evaluación de riesgos y / o actividades de tratamiento de riesgos. Un enfoque iterativo para realizar una evaluación de riesgos puede aumentar la profundidad y detalle de la evaluación en cada iteración.

Como se puede visualizar el proceso es iterativo para las actividades de valoración y tratamiento del riesgo. De forma general, inicialmente se define el contexto, posterior se realiza la identificación del riesgo (esto incluye la identificación de los activos), luego se realiza una estimación del riesgo, si se tiene información suficiente, se pasa al tratamiento del riesgo, de lo contrario se realiza una valoración o evaluación del riesgo.

GRÁFICO III: PROCESO DE GESTIÓN DEL RIESGO ISO/IEC 27005:2011

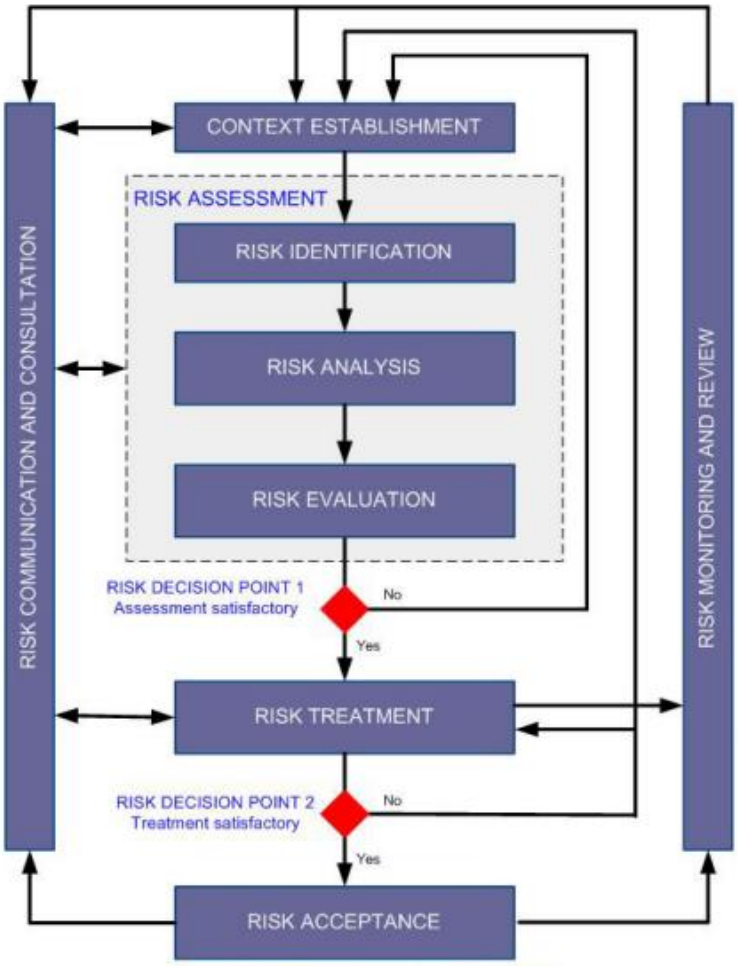

Ilustración 3. PROCESO DE GESTIÓN DEL RIESGO ISO/IEC 27005:2011

Fuente: Norma ISO/IEC 27005:2011.

Si la evaluación del riesgo no es suficiente se realiza otra iteración, hasta que se contenga la información necesaria para los planes de tratamiento; finalizados los planes de tratamiento, los cuales son monitoreados durante su implementación, se busca conseguir que la valoración del riesgo se encuentre dentro de los niveles de aceptación del mismo. Cada una de las actividades debe ser reportada a los directores y stakeholders del contexto definido en el primer paso del proceso.

ESQUEMA, DEFINICIÓN E IMPLEMENTACIÓN DE LA METODOLOGÍA

TABLA I: ESCALA DE VALORACIÓN DEL RIESGO

Valoración	Definición
Riesgo Extremo	Se estima que este nivel de riesgo supera el Nivel de Aceptación de la entidad. Su nivel es considerable teniendo en cuenta la frecuencia de materialización del riesgo y el impacto generado. Para los riesgos ubicados en este nivel, se debe generar una respuesta con planes de acción inmediatos.
Riesgo Critico	Es un riesgo elevado y requiere mitigación dentro de los límites de tiempo determinados (mediano plazo), aunque se encuentre de los niveles de aceptación de la entidad.
Riesgo Tolerable	Se considera un nivel de riesgo normal con el que la entidad puede coexistir, para los riesgos ubicados en este nivel, no se descartan acciones de mejora en un tiempo discrecional y definido por la entidad, con el fin de ubicarlos en un nivel de severidad menor.
Riesgo Aceptable	Indica un nivel de riesgo, en donde la relación de impacto y probabilidad es muy baja y pueden ser gestionados con procedimientos rutinarios.

Tabla 1. ESCALA DE VALORACIÓN DEL RIESGO

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

Mapa de Calor

En base en las definiciones anteriores de la escala de probabilidad y de impacto, se define el mapa de calor para la Entidad, el cual permite identificar de forma visual la evaluación o valoración del riesgo según su impacto y su probabilidad, y de esta manera identificar el perfil del riesgo de los incidentes de seguridad procedentes de la seguridad y gestión de eventos de información.

GRÁFICO IV: MAPA DE CALOR

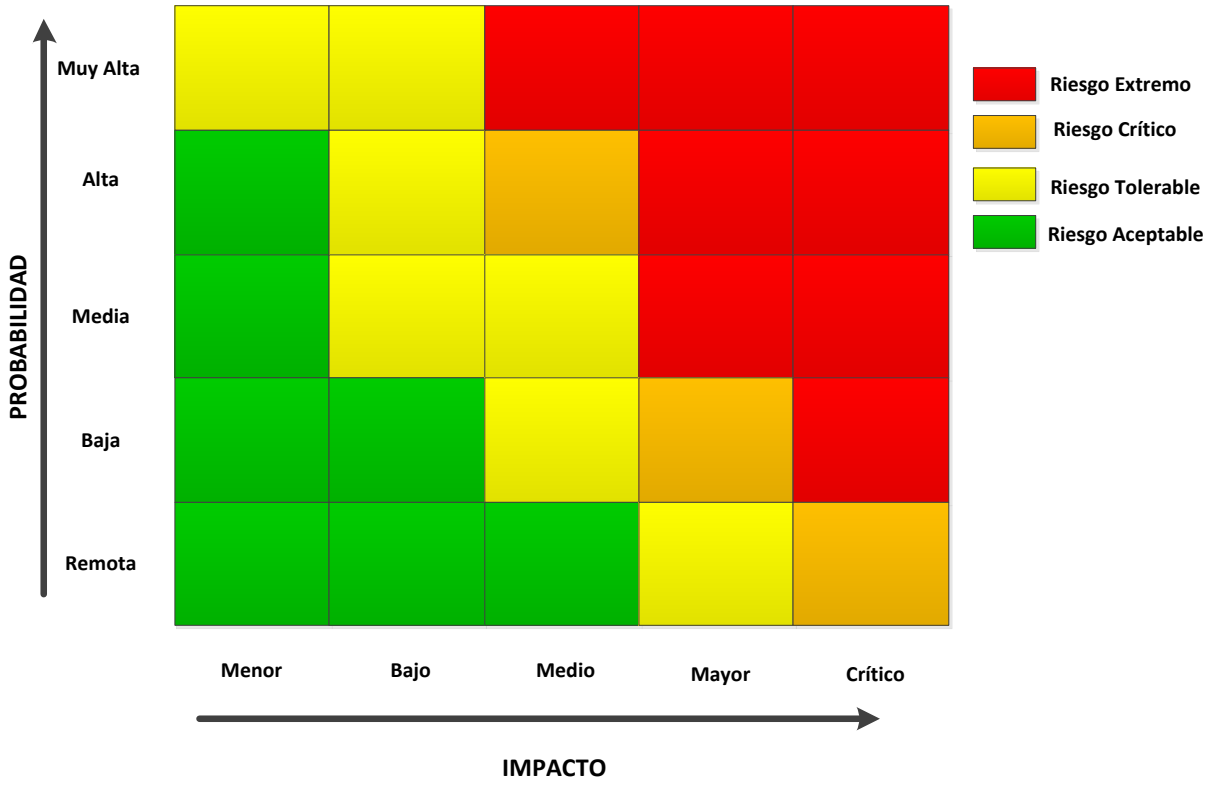

Ilustración 4. MAPA DE CALOR

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

Criterios de aceptación del riesgo

El nivel de aceptación de riesgos de TI de la Zona Franca corresponde a los riesgos que posterior a su evaluación se encuentran ubicados en las zonas de Riesgo Tolerable y Aceptable.

Los riesgos que no se encuentren en el nivel de aceptación de riesgos de la empresa, deben definir un plan de tratamiento a corto plazo (6 meses) y mediano plazo (un año), para Riesgo Extremo y Riesgo Crítico, respectivamente.

Identificación de los activos

Los activos por valorar son todos aquellos servicios y/o componentes tecnológicos configurados, para la valoración de cada activo se deben tener en cuenta los siguientes criterios de confidencialidad, integridad y disponibilidad de la información:

TABLA II: CRITERIOS DE VALORACIÓN DE ACTIVOS

Criterio	Confidencialidad	Integridad	Disponibilidad
Alto	Administra o procesa información confidencial y su uso inadecuado puede generar graves consecuencias para la entidad (demandas, pérdidas económicas, de reputación o imagen, entre otros.)	La información que administra o procesa apoya la toma de decisiones estratégicas de la entidad. No se admiten errores, los errores deben ser solucionados de inmediato.	Apoya los procesos críticos de la empresa y se requiere de una recuperación inmediata en caso de falla.
Medio	Administra o procesa información interna y su uso inadecuado puede generar medianas consecuencias para la empresa (Reclamaciones de las áreas que soporta).	La información que administra o procesa apoya la toma de decisiones de las áreas de la empresa. Permite una brecha en los errores de la información. Los errores pueden ser solucionados a corto plazo.	Apoya los procesos no críticos de la empresa y permite su recuperación en un tiempo no mayor a 2 días.
	El activo administra o procesa información pública y su divulgación no le genera consecuencias	La información que administra o procesa apoya la toma de decisiones de las áreas de	Apoya los procesos no críticos de la empresa y permite su recuperación en un tiempo superior a 2

Bajo	negativas a la empresa.	la compañía. Permite una brecha en los errores de la información. Los errores pueden ser solucionados a mediano plazo.	días.

Tabla 2. CRITERIOS DE VALORACIÓN DE ACTIVOS

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

Identificación de los riesgos

Posterior a la valoración de los activos, la identificación de los riesgos se basa en los incidentes que se han registrado en la empresa. Todo incidente resultante, en primera instancia, se considera un incidente de seguridad de la información, y debido a su presencia tiene como consecuencia la materialización de un riesgo.

Para la identificación de los riesgos, se deben tener en cuenta las vulnerabilidades asociadas a los activos identificados y con base en la experiencia de Analista de Riesgos, se deben definir e implementar los controles necesarios para el tratamiento del riesgo, según los resultados de la evaluación.

Evaluación del Riesgo

En esta fase se evalúa el riesgo según la valoración de los activos, la valoración en cuento a impacto y probabilidad de los riesgos identificados durante la implementación de la evaluación de los riesgos, basándose en el modelo definido para la estimación del riesgo (Cualitativo).

Para esta evaluación también se deben tener en cuenta los controles que se tienen implementados con miras a la reducción de la valoración del riesgo.

Tratamiento del Riesgo

Para los riesgos que como resultado de su evaluación se encuentren valorados como Riesgo Extremo o Riesgo Crítico, debe definirse obligatoriamente un plan de tratamiento. Para aquellos Riesgos Extremos, este plan de tratamiento debe ser definido e implementado a corto plazo (6 meses, máximo); y, para los Riesgos Críticos, el plazo se encuentra entre 6 meses y máximo 1 año. Estos planes tienen como objetivo realizar un tratamiento de los riesgos según las siguientes opciones:

Reducción del Riesgo (Mitigación): Implementación de controles los cuales minimizan la frecuencia de la probabilidad y/o reducen el impacto del riesgo. El plan se define con acompañamiento del Analista de Riesgos de la Dirección de Seguridad de la Información y es implementado por el área responsable y/o dueño del sistema donde se identificó el riesgo.

Retención del Riesgo (Aceptación): Los riesgos son aceptados, de forma objetiva y con conocimiento de las áreas responsables del sistema o activo, donde se identificó el riesgo. Esta aceptación debe satisfacer las políticas de la empresa y debe basarse en los criterios de aceptación de la misma.

Para el caso de los riesgos en el nivel Riesgo Extremo, no deberían ser aceptados, sin embargo, el área de Tecnología de la Información decide aceptar el riesgo.

Evitación del Riesgo: Es la decisión de no implementar la actividad o la acción la cual es causa del riesgo. Para los riesgos que provienen de los incidentes de seguridad, esta opción de tratamiento se estimaría que es poco útil, debido a la materialización del riesgo.

Transferencia del Riesgo: Para el caso que el riesgo provenga de alguno de los proveedores o fabricantes de los sistemas. En este caso el riesgo debe ser transferido al proveedor o fabricante. Esto indica que es posible que el proveedor requiera realizar un análisis de riesgos según sus políticas, lo que podría generar la aparición de nuevos riesgos o la

alteración en la valoración de estos. Sin embargo, se debe definir en conjunto con el proveedor las acciones necesarias para el tratamiento del riesgo. Independientemente de la opción seleccionada para el tratamiento del riesgo, se deben indicar las acciones necesarias para implementar el plan.

Aceptación del Riesgo

Para los riesgos que se encuentren valorados como Riesgo Tolerable o Riesgo Aceptable, se recomienda definir planes de tratamiento a largo plazo (a partir de un año en adelante).

Comunicación del Riesgo

El proceso de comunicación es transversal a todas las anteriores fases descritas del modelo de Gestión de Riesgos. Durante todo el ciclo de vida de la Gestión de Riesgos, deben estar involucrados las áreas de Tecnología de la Información las cuales podrían ser impactadas por los riesgos identificados a partir de los incidentes de seguridad materializados.

Dentro de esta comunicación se debe concienciar no al área de Tecnología de la Información, sino a la Alta Gerencia, que el proceso de Gestión de Riesgos de TI, para la evaluación de los riesgos de seguridad, son un componente que permitirá la consecución de los objetivos estratégicos de la empresa.

La comunicación efectiva, se realizará en cada una de las sesiones de trabajo en cada fase del modelo.

Monitoreo y Revisión del Riesgo

Esta fase involucra, en primera medida, la evaluación de la eficacia de la implementación del modelo de Gestión de Riesgos, además de la identificación de las mejoras que se necesite realizar al mismo. Y por otro lado es el monitoreo de los riesgos identificados, la actualización de los controles definidos, modificación, en caso de requerirse, de los

criterios de valoración del riesgo, su impacto, su probabilidad, la identificación de nuevas amenazas y vulnerabilidades.

Monitoreo y Revisión del Proceso

De forma semestral el área de Seguridad debe definir el alcance de la Gestión de Riesgos, teniendo en cuenta: Criticidad de los activos y riesgos identificados

Validación de los tiempos de respuesta en cada una de las fases, cuando se requiere dar una comunicación desde el área de Seguridad de la Información a las áreas involucradas en el proceso. Se deben validar las herramientas que respaldan el proceso, incluyendo las actualizaciones que se requieran sobre estas para la mejora del desempeño del proceso. Validar el alcance en temas legales del proceso de Gestión de Riesgos (Cumplimiento de Regulaciones Internas o Externas) Validación de los criterios de valoración de activos, de activos, niveles de aceptación de riesgos. Validación de la documentación y de las políticas que respaldan la ejecución del proceso.

Monitoreo y Revisión de Los Factores de Riesgo

Este monitoreo consiste en el constante seguimiento sobre los siguientes puntos: Planes de Tratamiento de nuevas amenazas sobre los activos configurados por la empresa. Impacto y probabilidad de la materialización del riesgo. Identificación de nuevas causas de materialización del riesgo o deficientes implementaciones de los controles. Actualización de las valoraciones de los riesgos.

3.2. Establecimiento del contexto

Esta etapa de la gestión del riesgo tiene por objetivo comparar los niveles de riesgos identificados en la fase anterior con los criterios de evaluación y aceptación del riesgo. Estos criterios son definidos durante la definición del contexto y deben estar alineados con los objetivos de la organización.

Se establece en la Norma ISO/IEC 27005:2011, lo siguiente:

En el 3.4. Contexto externo: Se debe establecer el entorno externo en el que la organización busca alcanzar sus objetivos.

NOTA El contexto externo puede incluir: Lo cultural, social, político, legal, regulatorio, financiero, tecnológico, económico, natural y entorno competitivo, ya sea internacional, nacional, regional o local; conductores impulsores y tendencias claves que tienen impacto en los objetivos de la organización; y relaciones y percepciones y valores de partes interesadas externas.

En el 3.5. Contexto interno: Es en el que la organización busca alcanzar sus objetivos.
NOTA El contexto interno puede incluir:

- Gobernanza, estructura organizativa, roles y responsabilidades.
- Políticas, objetivos y las estrategias que existen para lograrlos.
- Las capacidades, entendidas en términos de recursos y conocimiento (por ejemplo, capital, tiempo, personas, procesos, sistemas y tecnologías).
- Sistemas de información, flujos de información y procesos de toma de decisiones (tanto formales como informales).
- Relaciones y percepciones y valores de los interesados internos.
- La cultura de la organización.
- Normas, directrices y modelos adoptados por la organización.
- Forma y alcance de las relaciones contractuales.

Entrada: Toda la información sobre la organización relevante para el contexto de gestión de riesgos de seguridad de la información.

Acción: Se debe establecer el contexto externo e interno para la gestión de riesgos de seguridad de la información, que implica establecer los criterios básicos necesarios para la gestión de riesgos de seguridad de la información (7.2), definiendo el alcance y límites (7.3), y establecer una organización apropiada que opere la seguridad de la información, gestión de riesgos (7.4).

Guía de implementación: Es esencial determinar el propósito de la gestión de riesgos de seguridad de la información, ya que esto afecta el proceso y el establecimiento del contexto en particular. Este propósito puede ser:

- Apoyo a un SGSI.
- Cumplimiento legal y evidencia de diligencia debida.
- Preparación de un plan de continuidad del negocio.
- Preparación de un plan de respuesta a incidentes.
- Descripción de los requisitos de seguridad de la información de un producto, servicio o mecanismo.

La guía de implementación para los elementos de establecimiento de contexto necesarios para soportar un SGSI se discute más a fondo en Cláusulas 7.2, 7.3 y 7.4 a continuación.

NOTA ISO/IEC 27001:2005 no utiliza el término "contexto". Sin embargo, toda la Cláusula 7 se relaciona con los requisitos. “Definir el alcance y los límites del SGSI” [4.2.1 a)], “definir una política del SGSI” [4.2.1 b)] y “definir el riesgo enfoque de evaluación [4.2.1 c)], especificado en ISO/IEC 27001:2005.
Producto: La especificación de criterios básicos, el alcance y los límites, y la organización de la información y los procesos de gestión de riesgos de seguridad.

3.3. Identificación de riesgos

Se realiza para conocer y determinar los posibles eventos con potencial para causar pérdidas, se debe hacer el levantamiento de cómo esto puede suceder.

Los resultados de esta etapa serán los datos de entrada de la etapa de estimación del riesgo.

Es relevante que la organización identifique a sus fuentes de riesgo, sus causas y consecuencias. El objetivo es generar una lista completa de los riesgos basados en eventos que tienen la capacidad de crear, aumentar, evitar, reducir, acelerar o retrasar el logro de sus objetivos.

En la fase de análisis del riesgo, el primer paso es la identificación del riesgo. Esta identificación se lleva a cabo de manera que pueda conocer y determinar los posibles eventos que tienen un potencial para causar pérdida, así como elevar la forma en que esto puede suceder.

3.3.1. Identificación de activos

Activo es cualquier elemento de valor para la organización, cualquier elemento tangible (como hardware) o intangible (por ejemplo, la propiedad intelectual), recurso o la habilidad que tiene valor o sea crítico para la existencia de la organización, y que por lo tanto necesita protección.

Se requiere un nivel de detalle que permita el suministro de información adecuada y suficiente para el análisis y evaluación del riesgo.

La primera información sobre cada activo es: ¿quién es su responsable?”
Identificación de activos: Activos primarios o activos de soporte y de infraestructura
Con la información recogida durante la fase de definición de contexto, como el alcance, lista de componentes y responsables, entre otros, se inicia la identificación de los activos.

En la actividad de la identificación de los activos:

Entrada: Se contempla los resultados de la etapa de definición del alcance.

Acción: Desarrollo de la actividad de identificación de los activos. La identificación de los activos debe ser hecha a un nivel de detalle que permite el suministro de información adecuada y suficiente para el análisis y evaluación del riesgo. Como el proceso define la necesidad de varias iteraciones, el detalle puede ser profundizado en cada iteración.

Salida: Lista de los activos considerados sensibles para la organización y también una lista de los negocios relacionados a estos activos.

GRÁFICO V: CADENA DE IDENTIFICACIÓN DE ACTIVOS

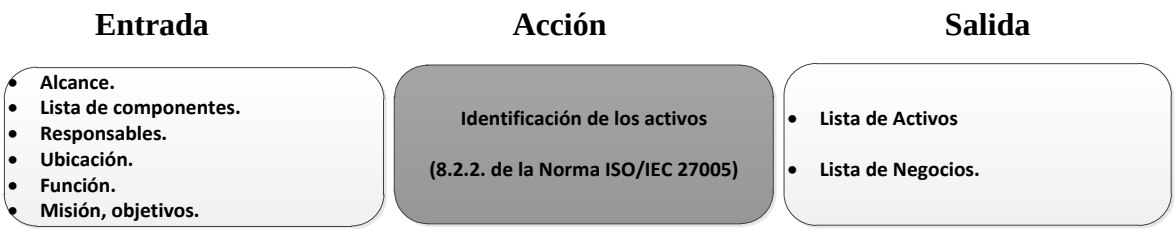

Ilustración 5. CADENA DE IDENTIFICACIÓN DE ACTIVOS

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

3.3.2. Identificación de las amenazas

Amenaza es cualquier evento que explota vulnerabilidades, con potencial de causar incidentes no deseados, que podrían resultar en daño para un sistema u organización.

En la identificación de las amenazas son realizadas acciones para identificar dentro del alcance las amenazas existentes en la organización.

De esta actividad de identificación de las amenazas, el equipo de análisis tendrá como:

Entrada: la información de su historial, obtenidas de los incidentes ocurridos, de observaciones realizadas por los responsables y usuarios de los activos, y aún a través de información recolectada de catálogos externos de amenazas.
Acción: identificación de las amenazas y sus fuentes. La fuente de amenaza está relacionada a su agente, entidad que puede causar una amenaza explotando o evidenciando alguna vulnerabilidad. Uno de los principales y más peligrosas agentes de amenaza es el ser humano.
Salida: una lista de amenazas con la identificación del tipo y de la fuente de las amenazas.

GRÁFICO VI: CADENA DE IDENTIFICACIÓN DE LAS AMENAZAS

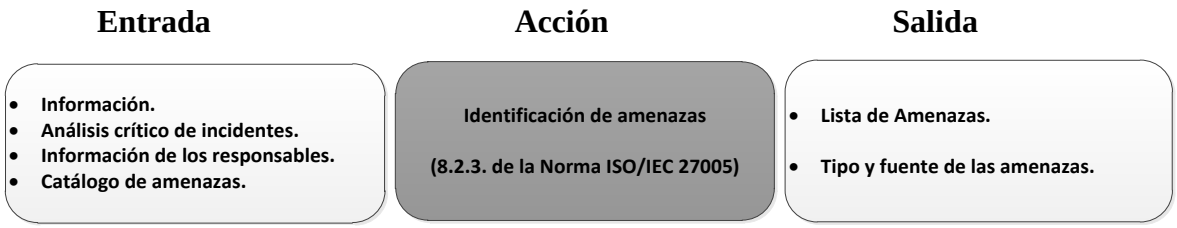

Ilustración 6. CADENA DE IDENTIFICACIÓN DE LAS AMENAZAS

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

3.3.3. Identificación de controles existentes

El control es cualquier procedimiento administrativo, físico u operacional capaz de tratar los riesgos de la ocurrencia de un incidente de seguridad.

El objetivo es identificar en el ambiente del alcance los controles planeados para la implementación y los controles existentes, ya desplegados y en uso.

Entrada: Documentaciones de los controles ya existentes y los planes de implementación de control para el tratamiento del riesgo.
Acción: Identificación de los controles implementados y planificados.

Salida: Lista de todos los controles existentes y planeados, su implementación y estado de uso.

Objetivos de la identificación de controles:
Evitar costos y reproceso con duplicación de controles y asegurar que los controles existentes están funcionando de manera correcta y tratando el riesgo de forma deseada.

Actividades de la identificación de controles:

- Reuniones con los responsables por la seguridad de la información.
- Entrevistas con los usuarios para identificación de los controles existentes.

Analizar de manera crítica la documentación sobre los controles existentes.
• Realizar cuestionarios y listas de verificación.
• Hacer inspecciones físicas, visitas y observaciones en los locales.

Controles complementares pueden ser necesarios para el tratamiento eficaz del riesgo.
Controles ineficaces o insuficientes deben ser removidos y reemplazados.
Controles previstos se deben evaluar si realmente serán capaces de hacer frente a los riesgos a los que se refieren al cumplimiento.

GRÁFICO VII: CADENA DE IDENTIFICACIÓN DE CONTROLES EXISTENTES

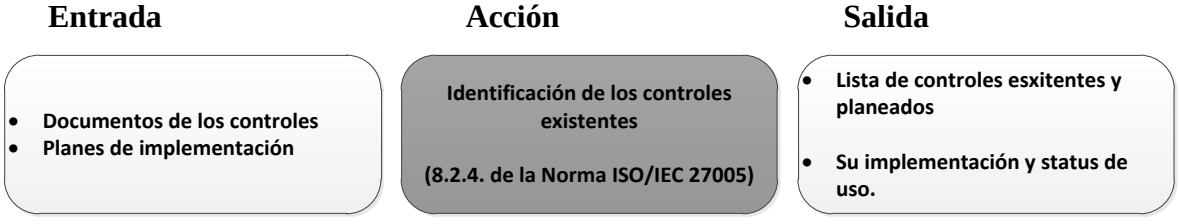

Ilustración 7. CADENA DE IDENTIFICACIÓN DE CONTROLES EXISTENTES

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

3.4. Análisis del riesgo

El análisis del riesgo es un proceso formal para identificar las amenazas y vulnerabilidades, y a partir de esta identificación categorizar el riesgo involucrado y determinar el tratamiento apropiado.

En la secuencia de este proceso, después del conocimiento del contexto del ambiente en el que se realizará el análisis del riesgo, se deben identificar los activos, las amenazas, los controles existentes y también aquellos que necesitan ser implementados. El paso para desarrollar consiste en identificar las vulnerabilidades y las consecuencias que pueden ser causadas, en caso de que las vulnerabilidades sean explotadas.

3.5. Evaluación de riesgos

El proceso de gestión del riesgo de seguridad de la información consta de seis grandes actividades:

- Definición del contexto
- Análisis y Evaluación del riesgo.
- Tratamiento del riesgo.
- Aceptación del riesgo.
- Comunicación del riesgo.
- Seguimiento y análisis crítico.

Para evaluar los riesgos se comprenden las siguientes fases:

Identificación del riesgo: Donde son determinados los eventos que pueden causar potenciales pérdidas.

Análisis del riesgo: Donde se determina la probabilidad de ocurrencia de los eventos.

Evaluación del riesgo: Ordena los riesgos de acuerdo con los criterios de evaluación establecidos en la definición de contexto.

Para llevar el proceso de evaluación del riesgo debe establecerse un patrón o criterio que sirve de base para que las cosas y las personas puedan ser comparadas y juzgadas.

Los criterios para la evaluación del riesgo que se utilizan para evaluar los riesgos de seguridad deben considerar lo siguiente:

- El valor estratégico del proceso.
- La criticidad de los activos.
- El histórico de ocurrencia de los eventos de seguridad.
- El valor del activo para el proceso.
- La probabilidad de ocurrencias y otros, de acuerdo con la organización y el alcance.

3.5.1. Identificación de las consecuencias

Un escenario es nada más que la descripción de una amenaza explorando una o más vulnerabilidades en un incidente de seguridad de la información.

Dentro de las consecuencias operacionales, podemos citar como ejemplos las siguientes:

- La oportunidad perdida.
- Salud y seguridad de los profesionales involucrados.
- Tiempo de investigación y tiempo de reparación.
- Tiempo perdido de trabajo.
- Costo financiero para reparar el daño.
- Imagen y reputación.

El control es cualquier procedimiento administrativo, físico u operacional capaz de tratar los riesgos de la ocurrencia de un incidente de seguridad. Ejemplos de controles incluyen políticas, procedimientos, estructuras organizacionales, antivirus, parches, cerraduras, extintor de incendio y backups, entre otros.

Se entiende por consecuencias, el resultado de un incidente o evento que puede tener un impacto en los objetivos de la organización. En esta parte del análisis del riesgo, una consecuencia puede ser, por ejemplo:

- La pérdida de eficacia en el funcionamiento operacional de los sistemas;
- La inestabilidad en el funcionamiento de sistemas;
- Condiciones adversas de operación;
- Pérdida de la oportunidad de negocios;
- Imagen y reputación afectadas;
- Violación de obligaciones reglamentarias;
- Pérdidas financieras;
- La pérdida de datos e información;
- La pérdida de vidas humanas;
- Pérdida de competitividad
- Entre muchos otros, de acuerdo con los negocios de la Zona Franca.

GRÁFICO VIII: CADENA DE IDENTIFICACIÓN DE LAS CONSECUENCIAS

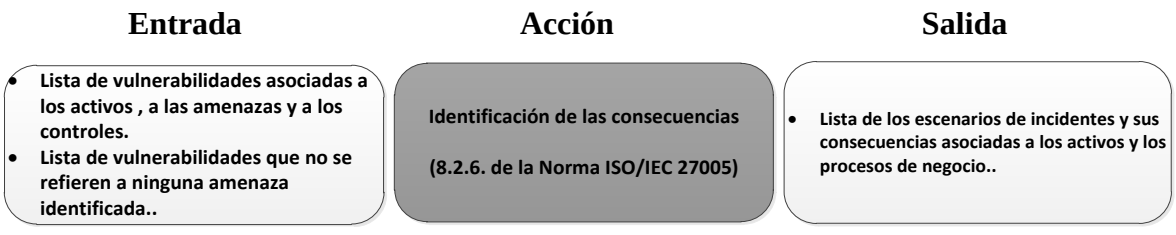

Ilustración 8. CADENA DE IDENTIFICACIÓN DE LAS CONSECUENCIAS

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

3.5.2. Evaluación de las consecuencias

El propósito es evaluar el impacto en los negocios de la organización teniendo en cuenta las consecuencias de una violación de la seguridad de la información.

El orden de los activos puede hacerse de dos maneras:

- A través del valor de reposición del activo.
- A través de las consecuencias para el negocio.

La valoración de los activos y su clasificación por la criticidad son factores importantes para la determinación del impacto de un escenario de incidente. El incidente puede afectar a más de un activo, debido a la interdependencia de los activos.

Las consecuencias se pueden expresar en términos de criterios financieros, técnicos, humanos, del impacto en los negocios, entre otros criterios. Se debe realizar la preparación de la lista de consecuencias evaluadas referentes a un escenario de incidente, en relación con los activos y criterios de impacto.

La actividad de la evaluación de las consecuencias tiene como objetivo evaluar los impactos sobre los negocios de la organización, teniendo en cuenta las consecuencias de una violación de seguridad de la información, tales como: la pérdida o degradación de la disponibilidad de los activos, la pérdida de la confidencialidad o la pérdida de integridad. Para esta evaluación, el equipo de análisis tendrá en cuenta los criterios y factores y adoptará una de las metodologías de apreciación: cualitativa o cuantitativa.

Entrada: Resultados de la etapa de identificación del riesgo.

Acción: Exactamente el desarrollo de la actividad de evaluación de las consecuencias sobre el negocio de la organización.

Salida: Lista de las consecuencias relativas a un escenario de incidente, estando relacionado a los activos y criterios de impacto.

GRÁFICO IX: CADENA DE EVALUACIÓN DE LAS CONSECUENCIAS

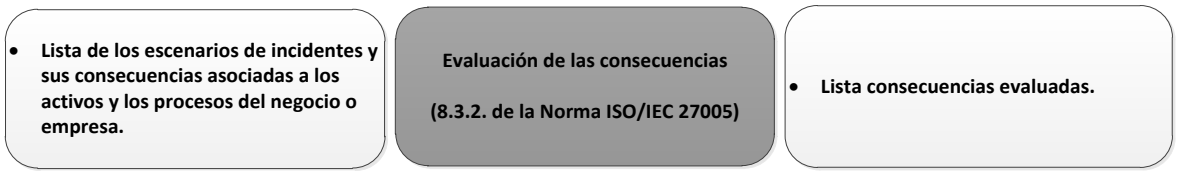

Ilustración 9. CADENA DE EVALUACIÓN DE LAS CONSECUENCIAS

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

Una de las primeras acciones es el ordenamiento de los activos de acuerdo con su criticidad e importancia para el logro de los objetivos de negocio de la organización. Es posible hacer esto de dos maneras:

1. A través del valor de reposición del activo: Donde se determina el costo financiero de recuperación o reposición del activo y también del valor de la información que contenga. Por ejemplo, un servidor de correo electrónico de una organización se quemó y tiene su costo de reposición estimado en US$ 5 mil. En la metodología cualitativa el valor es alto y en la metodología cuantitativa el valor es US$ 5 mil.

2. A través de las consecuencias al negocio: El valor se determina por el impacto de las consecuencias en los negocios. Normalmente este valor es más significativo que sólo el valor del activo. Siguiendo con el ejemplo del servidor de correo electrónico quemado del apartado anterior, se identificó que la organización trabaja con ventas de artículos deportivos hechos a mano, y sus ventas se realizan a través de e-mail, incluyendo el proceso de pago.

   El servidor tomó cinco días para ser restablecido y configurado, y el propietario estima que dejó de vender alrededor de US$ 20 mil por cada día parado. En la

metodología cualitativa el valor es elevado y en la metodología cuantitativa el valor es de US$ 100 mil (5 días de paro x US$ 20 mil por día).

La valoración de los activos y su clasificación por la criticidad son importantes para la determinación del impacto de un escenario de incidente, pues el incidente todavía puede afectar más de un activo, debido a la interdependencia de los activos. Por lo tanto, la evaluación de las consecuencias está fuertemente relacionada con la valoración de activos. Recuerde que las consecuencias podrían ser expresadas en términos de criterios monetarios, técnicos, humanos, del impacto en los negocios u otros criterios importantes para la organización.

3.6. Metodologías

3.6.1. Metodología de análisis cualitativo de riesgos

El análisis cualitativo se basa en la evaluación, a través de atributos calificadores y descriptivos, de la intensidad de las consecuencias y la probabilidad de ocurrencia del riesgo identificado. En la metodología cualitativa no se asigna valores financieros a los activos, consecuencias o controles, sino que se utilizan escalas de atributos a través de valores descriptivos relativos.

Esta estimación es considerada demasiado subjetiva, siendo ideal para una verificación inicial de los riesgos, cuando no se dispone de suficientes datos numéricos.

Ejemplos del uso del análisis cualitativo:

Para probabilidad:

- Alta, media y baja.
- Raro, poco probable, posible, probable y casi cierto.
- Remotamente posible, ocasionalmente, a menudo, varias veces al mes.
- Improbable, probable y cierto.
- Pequeña, mediana y grande.
- Bajo, medio, alto, muy alto y elevado.

- Improbable, remota, ocasional, probable, frecuente.

Para consecuencias (impactos):

- Alta, media y baja.
- Irrelevante, Insignificante, Marginal, Crítico, Extremo y catastrófica;
- Extremo, alto, medio, bajo y despreciable;
- Grande, mediana, pequeña y banales;
- Trastornos muy graves, graves, limitados, ligeros y muy ligeros;

3.6.2. Metodología de análisis cuantitativo de riesgos.

En la metodología de análisis cuantitativo es utilizada una escala de valores numéricos con el objetivo de intentar calcular valores numéricos para cada uno de los componentes recolectados durante las actividades de identificación del riesgo. Un enfoque cuantitativo se adopta cuando hay un escenario que permita definir los valores financieros, aunque sea aproximado de los activos priorizados, así como los impactos.

Por ejemplo, se estima que el valor real de cada activo en función del costo de reemplazo o del costo asociado a la pérdida de productividad, y otros valores de acuerdo con el tipo de Zona Franca.

Esta manera de calcular puede ser empleada para el levantamiento estimado del costo de los controles y otros valores identificados en la etapa anterior. El análisis cuantitativo se debe usar datos históricos y datos precisos y auditables. Si no existe tal información, este tipo de cálculo se convierte en falso.

Ejemplos de uso de este análisis cuantitativo:

Para probabilidad:

- 50%;
- 0,2;
- 0,75

Para consecuencias (impactos):

- Valor de reposición del activo: US$ 12.000;
- Valor de mantenimiento del activo;
- Costo de implantación del control;
- Valor de la sanción por incumplimiento de contrato;
- Perjuicio por las horas de inactividad.

CAPITULO IV

CONTEXTO DE LA TECNOLOGÍA DE LA INFORMACIÓN EN LA ZONA FRANCA OBJETO DEL ESTUDIO

4.1 Entendimiento de Tecnología de la Información en la Zona Franca

Como parte del Entendimiento del Ambiente de TI de la empresa, realizamos entrevistas a su Encargado de Tecnología de la Información. Las informaciones obtenidas se presentan a continuación:

4.1.1. Infraestructura de TI

La infraestructura de TI en la zona franca está conformada por múltiples dispositivos y plataformas los cuales permiten la operatividad de la empresa. La zona franca establecida en la avenida las américas consta de dos edificios con una distancia de 3,350 metros cuadrados, en donde su infraestructura tiene un promedio de 25 departamentos y unos 1,700 empleados divididos en dos turnos los cuales trabajan de manera conjunta para la remano facturación de teléfonos celulares.

La infraestructura cuenta con tres data center, en donde el data center principal tiene alojados los principales Servidores, Switchs, firewall, Central telefónicas, DVR cámaras seguridad, UPS y equipos de comunicaciones. Este data center establece una conectividad a través de fibra óptica mono modo hacia los demás data center. Existe un cableado estructurado de Data CAT6 el cual se despliega en bandejas de escalerillas desde los cuartos de comunicaciones de cada nivel hacía las estaciones de trabajo, mesas de producción y los diversos puntos que necesitan conectividad cableada. Dicho cableado está organizado dentro de Racks y gabinetes PANDUIT conectados hacia los dispositivos de comunicación.

La empresa posee dos (2) ups principales individuales, en donde un UPS APC SYMMETRA PX con capacidades de 100KVA sirve para la distribución de energía hacia las computadoras y dispositivos de la planta de producción y un UPS APC SYMMETRA PX con capacidad de 20KVA sirve para el suministro de energía a los servidores, equipos de comunicación y dispositivos críticos que no pueden persistir sin energía eléctrica.

Adicional a esto, cada data center tienen instalados tomas de electricidad alimentadas de los dos ups principales, en donde se conectan estas dos tomas a un ATS, el cual permite tener redundancia en caso de cualquier fallo de electricidad en los ups y así puedan quedar energizados los dispositivos hasta resolver cualquier inconveniente. Adicional a esto la empresa tiene instalada dos (2) plantas eléctricas con capacidad de 500kw en modo de backup para funcionar si se presenta cualquier falla eléctrica en el sector.

Los tres data center tienen instalados aires de precisión APC inRow cooling SC ACRP100 con el objetivo de mantener las variables de temperatura ambientales de los equipos que están instalados dentro del área, permitiendo así el buen funcionamiento de los equipos críticos que mantienen la operatividad de la empresa. También se tienen instalados termostato para poder visualizar la temperatura del área.

El acceso a los data center es restringido. Solo el personal de seguridad y TI tiene acceso a dichas áreas. En cada data center está instalado un sistema de control de acceso STAND ALONE, el cual a través de tarjetas RFID da acceso al área al personal autorizado. La administración de este sistema de control de acceso se dificulta debido a que este tipo de sistema se maneja de manera independiente lo cual quiere decir que a la hora de realizar un cambio en el equipo o la desactivación de una tarjeta debe de hacerse manualmente en cada una de las puertas.

Los data center están monitoreados por cámaras de seguridad desde el departamento seguridad y monitoreo.

La empresa tiene instalados un circuito cerrado de video vigilancia CCTV, con un alrededor de 200 cámaras de seguridad distribuidas dentro de las instalaciones de los dos edificios, monitoreadas por el departamento de Monitoreo. Dentro de este departamento se encuentran instaladas un aproximado de 15 televisores los cuales despliegan la imagen de cada una de las cámaras instaladas dentro y fuera de las instalaciones. El departamento cuanta con un personal externo el cual está conformado por tres operadores de cámaras de

video vigilancia y un supervisor los cuales observan atentamente para detectar cualquier actividad delictiva, conductas sospechosas o inusuales y cualquier otra incidencia.

Los operadores son responsables de manejar las cámaras de seguridad y equipos de video vigilancia, a la vez de observar las áreas asignadas a estos y de llevar un registro de los acontecimientos o incidencias que se presentan en la empresa.

La tecnología que utilizan para las cámaras de seguridad es una tecnología análoga CCTV. En cada data center se encuentra instalado un gabinete de comunicaciones con una capacidad de 12U, en los cuales están instalados los DVR marca DAHUA de 32 canales. El cableado utilizado para las cámaras es un cableado coaxial SIAMES RG59, que se distribuye desde los data center hacia los distintos puntos donde se encuentran las cámaras de seguridad. Los tipos de cámaras utilizados dentro de las instalaciones son: Domo, Bullet y PTZ, con resoluciones de 1080P y 720P.

El área de TI administra los equipos de video vigilancia, en donde crea y da permisos a los usuarios que tienen acceso a los diferentes DVR instalados en la infraestructura. La compañía de equipos electrónicos poseía (6) seis servidores físicos dentro de su data center principal los cuales se detallan a continuación:

TABLA III: DESCRIPCIÓN DE LOS DISPOSITIVOS SERVIDORES

Marca y Modelo	Sistema Operativo	Procesador	Memoria	Hard Drive	Funcion
HP PROLIANT DL360 G7	Windows Server 2012 standard	2 X Xeon E5630 2.53 GHz	8 GB DDR3 DIMM ECC	1 TB a 7,200 RPM	Domain Controller 01
Dell PowerEdge R230	Windows Server 2012 standard	Intel Xeon E3-1220 v5 a 3.0 GHz	8 GB UDIMM 2133 Mt/s	1 TB a 7,200 RPM	Domain Controller 02
Dell PowerEdge R230	Windows Server 2012 standard	Intel Xeon E3-1220 v5 a 3.0 GHz	8 GB UDIMM 2133 Mt/s	1 TB a 7,200 RPM	FTP Server
Dell PowerEdge R230	Windows Server 2012 standard	Intel Xeon E3-1220 v5 a 3.0 GHz	8 GB UDIMM 2133 Mt/s	1 TB a 7,200 RPM	FTP Server, Spiceworks
Dell PowerEdge R230	Ubuntu Server	Intel Xeon E3-1220 v5 a 3.0 GHz	8 GB UDIMM 2133 Mt/s	1 TB a 7,200 RPM	Test Server
Dell PowerEdge R230	Windows Server 2012 standard	Intel Xeon E3-1220 v5 a 3.0 GHz	8 GB UDIMM 2133 Mt/s	1 TB a 7,200 RPM	Hyper-V

Tabla 3. DESCRIPCIÓN DE LOS DISPOSITIVOS SERVIDORES

Fuente: Elaboración propia, a partir de la entrevista al Gerente de TI.

Estos servidores están instalados dentro de un gabinete de comunicaciones y conectados a unos ATS, los cuales se alimentan de circuitos eléctricos de UPS con el fin de tener redundancia ante cualquier fallo eléctrico.

Estos servidores se encuentran fuera de garantía, lo que implica que de ocurrir una falla de hardware se vieran afectados los usuarios que dependen de este servidor.

Dentro de la tabla de servidores mostrada anteriormente se puede mencionar que la compañía tiene un servidor principal con el rol de Controlador de Dominio primario en donde se aloja la base de datos de Directorio Activo con los datos de todos los empleados de la empresa, a la vez este ejecuta la aplicación XWINSCT que se utiliza para la administración de los relojes de ponche, la misma es administrada por la compañía ABC software la cual se integra con el sistema SPN para procesar la nómina de pago sobre la base de horas marcadas y/o controlar las asistencias de los empleados en la compañía. Adicional a esto el servidor tiene instalado el aplicativo SIGA el cual maneja la parte financiera, contable, de compras y contrataciones.

El segundo servidor realiza la función de Controlador de Dominio secundario recibiendo una replicación exacta del controlador de dominio principal, sirviendo como respaldo en caso de que el primer servidor fallara.

El tercer servidor tiene instalado el servicio de FTP server, en el cual se alojan informaciones de los diferentes departamentos de la empresa, permitiendo esto que se comparta la información de las diferentes áreas que trabajen de la mano.

El cuarto servidor tiene instalado la plataforma de Ticket Spiceworks, el cual cuenta con las características de administración de inventario, monitoreo de la red, help desk o mesa de ayuda entre otros. Adicional a esto el servidor ejecuta el servicio de FTP en donde se alojan los diferentes archivos de los empleados.

El quinto servidor sirve como servidor de prueba para el área de desarrollo de software bajo una plataforma Linux.

El sexto servidor tiene como función principal la virtualización de otros servidores apoyándose sobre el rol de hipervisor que ofrece la herramienta Hyper-V. Entre los servidores virtualizados podemos encontrar un equipo con la versión de sistema operativo Windows Server 2012 que se encarga de ejecutar el sistema de gestión humana llamado SPN, instalado y administrado por la compañía Gestión Informática.

Cabe destacar que estos servidores responden a las peticiones de múltiples dispositivos de la empresa los cuales operan con múltiples plataformas como: Windows en versiones 7, 8.1 y 10, MAC OS en versiones soportadas por los dispositivos y Linux como ultima plataforma.

4.1.1.1. Sistemas de Información

La empresa cuenta con los sistemas de recursos humanos implementados por la empresa Gestión Informática, la cual desplegó el software SPN que gestiona los procesos de recursos humanos, administrativo y financiero.

A la vez la empresa ABC Software brinda los servicios de implementación de sistemas de control de asistencia, XWINSCT es el software de asistencia muy completo para procesar nómina de pago sobre la base de horas marcadas y/o controlar las asistencias de los empleados de la empresa.

La compañía utiliza el Sistema Integrado de Gestión Administrativa- SIGA la cual es una herramienta informática que simplifica y automatiza los procesos administrativos de la empresa y que sigue las normas establecida por los Órganos Rectores de los Sistemas Administrativos del Estado. Este se utiliza para la parte contable y financiera, manejando también la parte de compra y contrataciones.

4.1.1.2. Procesamiento y Almacenamiento

Para el procesamiento de la información se utilizan las aplicaciones creadas y mantenidas por el departamento de desarrollo de software, las cuales conectan a diferentes plataformas a través de APIs (Application Programming Interface) las cuales se integran según las necesidades de cada módulo a sub-sistemas de inventario, proceso, supervisión de planta, entre otros, con arquitectura de micro-servicios. Las APIs pasan las informaciones a diferentes bases de datos en diferentes plataformas (Azure, AWS, Local) para mantener la persistencia y congruencia de los datos a largo plazo, cabe destacar que cada uno de estos servicios tienen sus propios features e implementaciones para manejar la permanencia de los datos a largo plazo (SSD HDD Disk, HDD RAIDs, entre otros).

Adicional a estas aplicaciones la empresa cuenta con un sistema de Cloud Storage en donde utilizan la herramienta de Dropbox para compartir la información de las diferentes áreas las cuales trabajan en conjunto.

También se cuenta con varios servidores con el feature de FTP (File Transport Protocol) en donde se tienen carpetas por departamento y en las cuales los usuarios con los permisos correspondientes tienen acceso a leer y escribir datos.

4.1.1.3. Telecomunicaciones

La empresa tiene contratados los servicios de comunicación de las proveedoras Claro y Columbus Network / C&W Business, los cuales proveen la conectividad a internet. Dichas proveedoras envían un servicio de línea dedicado a través de fibra óptica hacia las instalaciones, en donde se conectan desde los transceiver de fibra óptica suministrados por las compañías de telecomunicación hacia un Firewall Fortinet 800D. La velocidad contratada por la empresa de telecomunicaciones claro dominicana es de 100Mbps/100Mbps velocidad simétrica la cual funciona como enlace principal, mientras que las velocidades contratadas por la compañía C&W Business es de 50Mbps/50Mbps velocidad simétrica.

La empresa cuenta con un appliance Fortinet 800D el cual tiene configurado un balanceo de carga de los dos enlaces WAN que suministran los proveedores de servicios, en adición a esto el equipo tiene las configuraciones y políticas de acceso a la red. La conectividad hacia la red LAN se establece desde el firewall hacia el switch core principal a través de un pathcore de fibra.

El switch core principal establece la interconexión a través de patchcore de fibra conectados a un FDP (Fiber Distribution Panel) que se encuentra en el gabinete principal y este a su vez se conecta hacia otros FDP ubicados en los distintos gabinetes de comunicaciones y desde aquí se establece una conexión por patchcore de fibra hacia los switches de acceso.

Dentro de las instalaciones se tiene una solución WIFI desplegada por equipos de la marca Aruba, en donde hay un aproximado de 20 AP (Access Point) distribuidos en todo el plantel, los cuales brindan una cobertura de aproximadamente un 98% de la planta fisica, estos equipos son gestionados a través de una controladora virtual la cual permite una fácil administración de la solución.

La compañía tiene instalada una Central Telefónica ZYCOO la cual asegura el servicio de telefonía IP en los diferentes departamentos pudiendo realizar llamadas tanto internas como externas. Esta solución se integra a la vez con la plataforma de teléfonos Cordless la cual permite que los empleados se desplacen entre los diferentes departamentos haciendo uso de teléfonos inalámbricos IP.

4.1.1.4. Red y Plataformas

La infraestructura de red implementada se apoya principalmente en el uso de la topología estrella, en la cual todos los nodos están conectados directamente y brindando la ventaja de que si una computadora o nodo falla esta no afecta el funcionamiento del resto de la red.

GRÁFICO X: TOPOLOGÍA DE RED

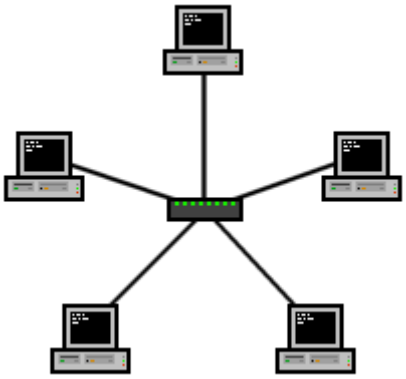

Ilustración 10. TOPOLOGÍA DE RED

Fuente: Elaboración propia, a partir de la entrevista al Encargado TI.

La empresa cuenta con un direccionamiento IP clase A, el cual esta segmentado a través del uso de VLAN para separar el tráfico de la red de los distintos departamentos. El rol de DHCP está habilitado en el switch core principal el cual distribuye las IP hacia los distintitos equipos de la red.

Se pueden encontrar dentro de la empresa múltiples plataformas que soportan la operativa del negocio en el cual se destacan plataformas Windows sobre la cual se ejecutan la mayoría de las aplicaciones del área de producción, a su vez se utilizan aplicativos bajo la plataforma Linux como es el caso de Blancco Software el cual se utiliza para el borrado de información de los teléfonos celulares, dentro de la empresa abundan dispositivos Apple el cual utiliza su plataforma de Mac OS.

La compañía tiene un licenciamiento corporativo de licencias Microsoft Windows en la versión de Sistemas operativos Windows 7 Enterprise para todas las computadoras y para los servidores de plataformas Windows en versiones Windows Server 2012 Standard se adquirió una licencia por equipo.

Las Bases de datos instaladas en los servidores utilizan una versión de Microsoft SQL Server 2012 Express la cual solo permite un almacenamiento de 10GB en las bases de datos ejecutadas dentro de estos.

4.1.1.5. Sistemas de Gestión de Bases de Datos

En el apartado de base de datos la empresa cuenta con tres diferentes infraestructuras para soportar las diferentes tecnologías de base de datos que soportan los diferentes sistemas existentes; Primero cuenta con servidores locales en donde se soportan bases de datos con tecnología Microsoft SQL Server, en segundo lugar se cuenta con la plataforma Microsoft Azure para soportar las bases de datos con tecnología Microsoft SQL Server y tercero se cuenta con la plataforma AWS (Amazon Web Services) que contiene servidores RDS (Relational Database Service) con tecnologia MySQL.

4.1.1.6. Emails

La plataforma de correos utilizada por la empresa es Microsoft Office 365, en la cual se aprovecha las ventajas que esta plataforma ofrece con sus aplicaciones tales como Outlook, OneDrive, Word, Excel, PowerPoint, OneNote, SharePoint, Microsoft Teams y Yammer, entre otros. A la vez esta brinda una administración centralizada en la nube y libre de infraestructura y mantenimiento de equipos.

4.2. Desarrollo y cambio a Sistemas

4.2.1. Solicitud de cambios

La solicitud de cambios comienza con un email enviado por el cliente al sistema automático de ticket llamado Jira, una vez enviado es recibido por el sistema para luego ser categorizado por el personal de soporte en niveles 1, 2 y 3 dependiendo de la complejidad del mismo, donde el nivel 1 es el más simple y puede ser atendido por el personal de soporte y los niveles 2 y 3 se escalan al departamento de desarrollo y cambio, debido a que requieren un proceso más complejo que involucra análisis, diseño, desarrollo y pruebas.

4.2.2. Metodología de desarrollo

La empresa utiliza la metodología AGILE & SCRUM para el desarrollo y mantenimiento de los aplicativos. Donde los desarrollos y cambios se dividen por ciclos llamados Sprints, los cuales contienen todo el proceso desde el análisis hasta los feedback de los clientes en el desarrollo y mantenimiento del software.

4.2.3. Control de versiones

Para el control de versiones de los sistemas se utiliza la tecnología git, la cual procura eficiencia y confiabilidad del mantenimiento de versiones sin importar que el aplicativo tenga un gran número de archivos en el código fuente.

La metodología aplicada en la compañía para el manejo del repositorio git es gitflow, la cual divide los desarrollos en features creando ramas para cada uno de ellos, así mismo también existen ramas para cambios inmediatos en el ambiente para corregir algún error que afecte el sistema y necesite una corrección inmediata siendo llamados hotfix.

4.2.4. Pruebas y aceptación de los cambios

En este aspecto, en el departamento de desarrollo existe un personal dedicado a QA (Quality Assurance), el cual cumple con la función de determinar la calidad y la usabilidad de los desarrollos de software, esto sucede una vez es entregado el requerimiento a ellos por el desarrollador vía Jira.

Una vez el analista de QA tiene el requerimiento y lo evalúa haciendo pruebas de diferentes indoles dependiendo de las características propias del desarrollo que está evaluando en el momento, este puede aprobar el mismo debido a que no contiene errores o puede regresar el requerimiento al desarrollador con la lista y detalles de los errores encontrados para que el requerimiento posteriormente sea devuelto con los errores corregidos, reiniciando otra vez

las pruebas continuando el flujo y así una y otra vez hasta que no allá errores encontrados en el desarrollo.

Como segunda etapa de las pruebas todos los desarrollos aprobados se integran en un ambiente de preproducción, donde se identifica si existe conflicto entre los diferentes desarrollos a liberar en la nueva versión.

4.2.5. Pase de los cambios a producción

El proceso de pase de cambios a producción comienza con el registro de todos los requerimientos de desarrollo aprobados en el backlog de la versión a hacer la liberación. Se procede a notificar vía correo a los involucrados con un tiempo de anticipación de no menos de tres días.

Una vez notificado el personal se procede en el día acordado a esperar que los sistemas ya no estén en uso fuera del horario laboral, comenzando así con el proceso de pase del código a los ambientes de producción, después los analistas de QA asignados al pase se encargan de hacer pruebas de regresión para evaluar todos los módulos del sistema en el ambiente de producción, en caso de suceder algún inconveniente se notifica a los desarrolladores asignados al pase.

Luego los desarrolladores tendrán un máximo de dos horas para resolver el inconveniente, de manera que de no poder solucionar el problema se procede a realizar la reversión a la versión anterior del aplicativo. En caso de que los analistas de QA no encuentren problemas en la regresión o que los desarrolladores logren resolver cualquier problema notificado se procede a enviar una notificación vía correo electrónico a los departamentos afectados por los cambios liberados de la nueva versión en producción.

4.3. Gobierno de TI

4.3.1. Estructura Organizacional

El organigrama de la empresa en donde se refleja su estructura y diseño organizacional se muestra a continuación:

GRÁFICO XI: ESTRUCTURA DE CARGOS

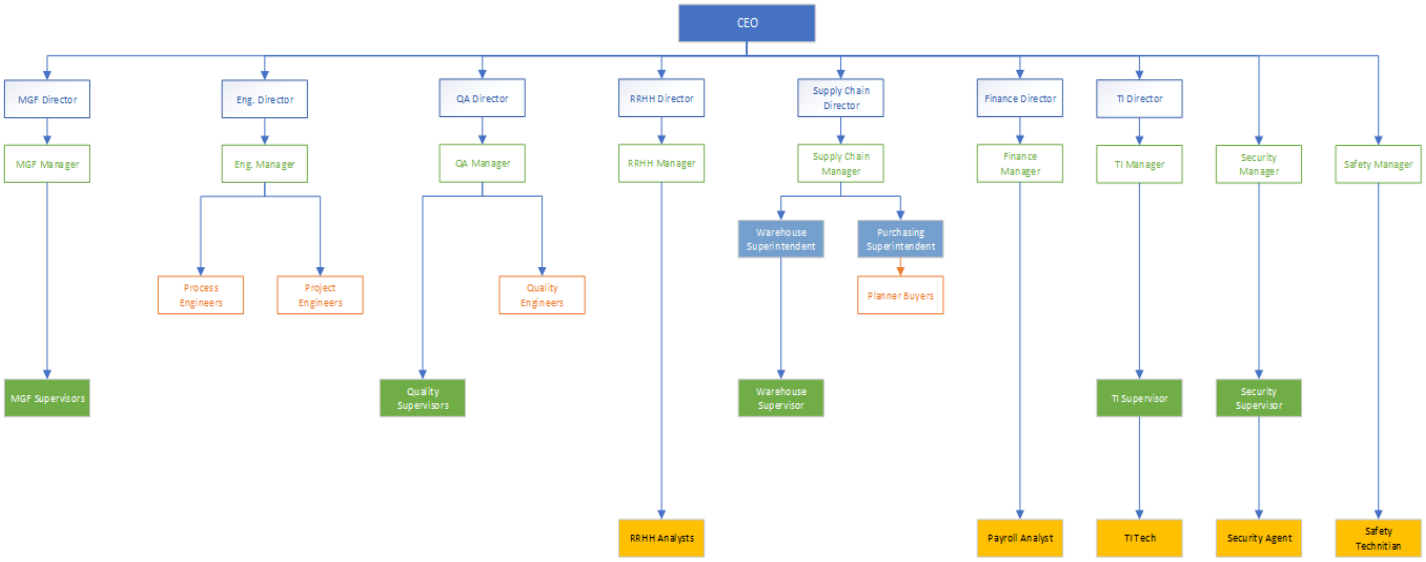

Ilustración 11. ESTRUCTURA DE CARGOS

Fuente: Manual de Recursos Humanos, versión 2019.

La compañía es dirigida por un CEO (Chief Executive Officer) al cual se reportan todos los directores y gerentes, los mismos envían reportes semanales donde reflejan los avances o retrasos de las metas establecidas mensualmente.

Cada área cuenta con un personal de supervisión, estos se reportan a sus gerentes expresándoles las necesidades o mejoras que necesitan realizar para eficientizar los procesos que agregan valor al negocio.

En el caso del departamento de tecnología, está organizado por un director el cual analiza los reportes del Gerente en base a decisiones tomadas para el trabajo del supervisor y los IT support.

Cada colaborador dentro de la empresa realiza un papel importante para la ejecución de los procesos de trabajo los cuales permiten lograr sus metas.

4.3.2. Políticas y Procedimientos

Dentro de la organización se encuentra un área de control de documentación, la cual maneja el flujo de la información y toda la documentación de las políticas y procedimientos. Esta área es quien controla los niveles de permisos en los documentos a cada usuario por departamentos, teniendo así el control de quien debe tener acceso a los diferentes directorios alojados en los servidores de la empresa.

Las policitas y procedimientos de TI (Tecnología de la Información) no se han desarrollado en base a las funciones y procedimientos de la empresa, hasta el momento solo se cuenta con las políticas y procedimientos internos referentes al negocio.

4.3.3. Gestión de Proyectos

Al momento de la introducción de un nuevo proyecto o cliente en la empresa, se convoca una reunión con los gerentes de cada departamento, dígase el área de Finanzas, Recursos Humanos, Desarrollo de Software, Ingeniería, Producción, Calidad, Logística y Tecnología de Información.

En esta primera intervención el gerente de proyecto desglosa el Project Charter, donde se detalla los requerimientos del proyecto, demanda, alcance y presupuesto estimado, a la vez, tiempo de ejecución del mismo y la fecha estimada de cierre de este.

Esto desglose busca como finalidad que los representantes de cada departamento puedan realizar un levantamiento de los recursos que disponen para la realización del proyecto y a la vez utilizar la información para evaluar las barreras que le impiden o no, la materialización de este. Esto suele ejecutarse al inicio del turno, dando la oportunidad de una segunda intervención al final de este con el levantamiento completado.

Con la data colectada, al finalizar el turno en la segunda reunión que se lleva a cabo, se toman las mejores decisiones que como equipo consideran para la materialización y agilización del proyecto, una vez tomada las decisiones correspondientes, se procede a listar las tareas que surgen de dichas decisiones, donde el gerente de proyecto da seguimiento a cada responsable para el cumplimiento del tiempo establecido.

4.3.4. Gestión Presupuestaria

La estructura de la empresa se maneja a través de proyectos, los cuales definen la inversión en el momento de ejecución, es decir, dentro de la planificación no se cuenta con una gestión de presupuesto establecida. Esto impide realizar la previsión de gastos e ingresos durante un periodo de tiempo determinado. La empresa maneja los fondos según la necesidad y la prioridad de los clientes.

4.3.5. Inventario de Recursos HW y SW

El inventario de los dispositivos de tecnología está bajo la responsabilidad del área de TI, la cual tiene una documentación manual en un documento Excel donde se especifican la ubicación, nombre de dispositivo, marca, modelo, capacidad, entro otros. En dicho documento a la vez se encuentra un inventario de Software el cual detalla las versiones de producto y los Product Key (llave de producto) de las distintas aplicaciones tercerizadas que utiliza la empresa.

La plataforma de Ticket Spiceworks a su vez contiene la característica de inventario la cual crea una lista de los activos a partir del escaneo en red, donde conteniendo toda la

información relacionada a los dispositivos y el hardware. En el caso de Spiceworks, el inventario todavía es capaz de almacenar información más relevante, es decir, no solo los activos de la red, sino también datos sobre muebles, suministros de oficina y más. Este escaneo de red ocurre a través de protocolos de administración remota: WMI (Windows Management I), SSH (Secure Shell) y (SNMP) Protocolo simple de administración de red.

4.3.6. Gestión de relación con Terceros

La empresa actualmente tienes varios servicios contratados de personal externo, los cuales trabajan en el desarrollo de las funciones de la empresa. En base a la relación con terceros, la empresa no cuenta con un personal para la supervisión de estos, es decir, cada área que recibe los servicios de un tercero vela por asegurar que los servicios contratados se estén ejecutando y estén funcionando correctamente.

4.4. Operaciones de TI

4.4.1. Respaldo de datos y sistemas

La compañía actualmente no cuenta con un sistema o dispositivo que respalde los datos que se ejecutan dentro de las instalaciones, es decir, no existe un plan de backup manual o automático para salvaguardar los datos que se alojan en los servidores locales, a le vez no contienen una documentación de las configuraciones que actualmente se ejecutan en los equipos de la red. Esto representa una debilidad ante cualquier evento que provocara la perdida de información.

A la vez, tampoco existe una herramienta de recuperación de datos al momento que ocurriera una eliminación de información importante para la organización.

4.4.2. Plan de Recuperación ante Desastres

Plan de recuperación ante desastres es un proceso de recuperación que cubre los datos, el hardware y el software crítico, para que un negocio pueda comenzar de nuevo sus operaciones en caso de un desastre natural o causado por humanos.

Teniendo en cuenta la definición anterior, esto es algo de suma importancia para la seguridad de una empresa, sin embargo, no hay un plan de recuperación ante tales eventualidades, es decir, en el caso de perder información por un desastre natural, la empresa quedaría expuesta a una reconstrucción de datos desde la etapa inicial, lo cual representa pérdidas para la estabilidad y seguridad de la organización como tal.

4.4.3. Monitoreo de Recursos

La detección oportuna de fallas y el monitoreo de los elementos que conforman una red de computadoras son actividades de gran relevancia para el departamento de IT. De esto se deriva la importancia de contar con un esquema capaz de notificar las fallas en la red y de mostrar el comportamiento mediante el análisis y recolección de tráfico.

En la empresa no cuenta con un sistema de monitorización de recursos, el cual pueda alertar o notificar sobre las fallas en los diferentes dispositivos que estén dentro de la red, actualmente para poder visualizar algún inconveniente en un equipo o sistema, este debe ser reportado por el usuario para dar el soporte necesitado.

4.4.4. Soporte a Usuarios

El departamento de tecnología cuenta con ocho IT support, los cuales dan soporte a las diversas plataformas que se manejan dentro de la empresa. El proceso para realizar una solicitud o reportar inconveniente es a través de un correo electrónico, el cual automáticamente genera un ticket dentro del sistema Spicework. De esta manera los IT support pueden verificar los tickets y asignarlos según la prioridad del problema reportado.

En caso de no poder resolver algún inconveniente, este se escala a un siguiente nivel para la solución inmediata del problema.

4.5. Seguridad en base a la tecnología

4.5.1. Seguridad Física

Dentro de las instalaciones la empresa cuenta con un departamento de seguridad, el cual vela por el cumplimiento de las reglas dentro del plantel. Dicho departamento es responsable de los accesos a la planta del personal interno y externo a las diferentes áreas. Al momento de un personal externo entrar a las instalaciones se toman los datos de la persona y luego es acompañado por un personal de seguridad o TI hasta el área en el cual necesitan acceder.

Las áreas de Data Center son monitoreadas a través de cámaras de seguridad las 24 horas, los 7 días de la semana. Dicho personal a la vez es responsable de que ningún personal tanto interno como externo entre a las instalaciones con algún dispositivo de almacenamiento y otros objetos no permitidos. Esto con el objetivo de que ninguna persona pueda sustraer alguna información de la empresa.

Cada uno de los data center tienen una puerta la cual está controlado por un sistema de control de acceso el cual solo tienen acceso el personal de TI, esto con el objetivo de proteger las áreas que contienen información y medios de procesamiento de información.

El departamento de seguridad no lleva un control de registros de entrada a los data center y los conceptos de los trabajos que se realizan a determinadas horas lo cual es un riesgo de seguridad.

4.5.2. Controles Ambientales

Dentro de las instalaciones de la zona franca se tiene un control de temperatura el cual no permite que se genere humedad y altas temperaturas en las diversas áreas donde se trabaja con los dispositivos electrónicos, esto con el objetivo de evitar daños severos a los diferentes dispositivos.

Dentro de los data center están instalados aires de precisión los cuales mantienen un nivel de temperatura óptimas, permitiendo así que los equipos puedan trabajar en las mejores condicione. De esta manera se reduce las posibilidades de sobrecalentamiento o condiciones de humedad extremas que puedan conducir a fallos en los sistemas y en los componentes del hardware de los equipos. Dentro de estas áreas se encuentran instalados relojes de termostato los cuales indican la temperatura actual del área, a la vez se tienen detectores de humo los cuales alertan en caso de que se ocasione algún incendio.

4.5.3. Seguridad Lógica

La zona franca no posee un departamento de seguridad electrónica el cual proteja la compañía de posibles ataques informáticos los cuales puedan poner en riesgo la operatividad del negocio, es el departamento de TI el cual se encarga de restringir el acceso a los programas y archivos, tratando así de gestionar la seguridad en los datos. Los equipos de seguridad como el firewall son administrado por el área de TI, en donde el personal de esta área crea y aplican las políticas de seguridad a la vez de gestionar los permisos de acceso a los diferentes sistemas.

Cabe destacar que la empresa no cuenta con una herramienta para analizar el tráfico de la red en tiempo real, la cual pudiera detectar un tráfico malicioso y así poder tomar las medidas oportunas para evitar daños a los sistemas y la perdida de información.
Actualmente los colaboradores de las áreas administrativas tienen acceso a los diferentes servidores de correo, la cual representa una vulnerabilidad ya que a través de estos servidores de correo pueden sustraer información sensitiva de la empresa.

4.5.4. Autenticación (Red y Sistema)

La autenticación de los usurarios es manejada a través del directorio activo, el cual contiene un base de datos de todo el personal de la empresa, en este a su vez se realiza una clasificación de los tipos de usuario y sus objetivos de acceso a los sistemas. También establece los permisos por usuarios para los diferentes directorios compartidos de la red.

4.5.5. Protección Código Malicioso

La empresa no cuenta con ningún programa de antivirus el cual pueda detectar y eliminar cualquier código malicioso, actualmente todos los servidores y computadoras solo poseen el antivirus gratuito que trae de manera integrada los sistemas operativos de Microsoft Windows Defender, a los cuales no se le da ningún seguimiento en cuento a las actualizaciones.

4.5.6. Seguridad Perimetral

La seguridad perimetral para proteger la red privada de la empresa esta manejada por el firewall, en donde se han aplicado algunas medidas de seguridad. Dentro de la configuración de los equipos de red no existe ninguna configuración de políticas de accesos tales como listas de acceso o Acces List para controlar el tráfico en que viajen los paquetes. Los equipos de comunicación no tienen habilitado el protocolo SSH para establecer una conexión más segura y se carece de VPN para la conexión remota de los usuarios lo cual limita a la hora de trabajar fuera del plantel.

4.5.7. Ciberseguridad

La compañía de equipos electrónicos no cuenta con un personal de protección para los sistemas de archivos de información, el cual pueda prevenir todo tipo de amenaza que puedan poner en riesgo la información que es procesada, transportada y almacenada en los dispositivos de la empresa.

4.6 Criterio metodológico para la evaluación de los riesgos de tecnología de la información

4.6.1 Criterios de probabilidad

La probabilidad se estima de la frecuencia de ocurrencia de un riesgo en un periodo específico. La escala de probabilidad definido por la Entidad se relaciona en la siguiente tabla:

TABLA IV: ESCALA DE PROBABILIDAD DEL RIESGO.

Nivel	Criterio cualitativo	Descripción	Frecuencia
1	**Remota**	Muy baja probabilidad de ocurrencias excepcionales. El evento puede ocurrir sólo bajo circunstancias	1 vez por año
2	**Baja**	Limitada probabilidad de ocurrencia. El evento puede ocurrir muy esporádicamente.	1 vez por semestre
3	**Moderada**	Mediana probabilidad de ocurrencia. El evento ocurrirá en algún momento.	Entre 2 y 5 por trimestre
4	**Alta**	Significativa probabilidad de ocurrencia. El evento ocurrirá casi en cualquier circunstancia.	Entre 6 y 12 por mes
5	**Muy Alta**	Muy alta probabilidad de ocurrencia. Se espera la ocurrencia del evento en la mayoría de los casos.	Más de 12 veces por mes

Tabla 4. ESCALA DE PROBABILIDAD DEL RIESGO

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

4.6.2 Criterios de Impacto

Los criterios de impacto se definen en función de la afectación de la confidencialidad, integridad y disponibilidad de la información, en caso de la materialización del riesgo:

TABLA V: ESCALA DE IMPACTO DEL RIESGO.

Nivel	Criterio cualitativo	Descripción
1	**Bajo**	No hay afectación en la confidencialidad, integridad y disponibilidad de la información, por ser información pública de la Entidad
2	**Menor**	Afectación en la confidencialidad, integridad y disponibilidad de la información pública de la Entidad
3	**Medio**	Afectación en la confidencialidad, integridad y/o disponibilidad de la información de uso interno de la Entidad o de terceros
4	**Mayor**	Afectación en la confidencialidad, integridad y/o disponibilidad de la información privada de la entidad o de terceros, sin implicaciones legales o de carácter de reputación de la entidad.
5	**Crítico**	Afectación en la confidencialidad, integridad y/o disponibilidad de la información privada de la Entidad o de terceros, con implicaciones legales o de carácter de reputación de la entidad.

Tabla 5. ESCALA DE IMPACTO DEL RIESGO

Fuente: Elaboración propia a partir de la Norma ISO/IEC 27005:2011.

4.6.3 Criterio de evaluación del riesgo

Se obtiene de la multiplicación de la probabilidad por impacto, y el resultado conforme a esta tabla es la valoración del riesgo.

Nota: Por razones de falta de autorización de la Zona Franca, no se pudieron realizar pruebas de funcionalidad de los controles implementados.

TABLA VI: MEDIDAS DE RIESGOS

Categorización	Puntuación
Bajo	De 1 a 5
Tolerable o medio	De 6 a 13
Crítico o alto	De 14 a 19
Extremo	De 20 a 25

Tabla 6. MEDIDAS DE RIESGOS

Fuente: Elaboración propia a partir del levantamiento de los riesgos en la zona franca (2019).

TABLA VII: RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN ZONA FRANCA (2019)

Ref.	Nombre de Riesgo	Descripción de Riesgo
R1	Riesgo de control de las actividades realizadas en el Data Center, por terceros.	No se mantienen registros de las actividades que dentro del Data Center realizan los terceros a los que se les otorga acceso a este.
R2	Riesgo para la seguridad de la información y confidencialidad de la empresa.	No existe una política de seguridad dentro de las instalaciones para controlar el acceso a correos personales, al mismo tiempo no existe un control para los usuarios que acceden a páginas o plataformas de envíos de archivo, representando esto un riesgo para la empresa ya que pueden extraer información sensitiva de la misma.
R3	Riesgo de disponibilidad de las informaciones y de continuidad de las operaciones.	La empresa no cuenta con herramientas para realizar BackUp automáticos de los aplicativos alojados en los servidores, al igual que de la información en general que manejan los usuarios de la organización en los dispositivos de almacenamiento. No existe un directorio el cual contenga los respaldos de configuración de los equipos de telecomunicaciones.
R4	Riesgo de errores en la ejecución de las actividades del área.	El Departamento de TI carece de políticas y procedimientos por escrito de todas las operaciones tecnológicas que realiza la empresa, tanto para los usuarios internos como externo, lo que puede evidenciar mal manejo de la información de cómo opera el departamento ya que no hay protocolo de como ejecutar acciones en equipos y situaciones que se presenten.
R5	Riesgos de indisponibilidad de recursos económicos.	La compañía actualmente no asigna una porción presupuestaria para el área de TI, lo que impide realizar la previsión de gastos del departamento con relación a las compras de suministros y de equipos. La empresa maneja los fondos según la necesidad y las prioridades de las áreas de producción, lo que impide una planificación en el desarrollo de proyectos tecnológicos los cuales aportarían mejoras a los procesos y la erradicación de problemas futuros, manteniendo así la

		infraestructura actualizada con relación a la vanguardia tecnológica.
R6	Riesgo de Recuperación de los procesos de TI	La Zona Franca no tiene definido un Plan de Recuperación ante Desastres (DRP, por sus siglas en inglés).
R7	Riesgo de indisponibilidad de los recursos de red y servicios.	La empresa no cuenta con un software de monitoreo para alertar o notificaciones sobre fallas en los equipos críticos, servidores y congestión de la red, lo que dificulta la detención temprana de problemas tanto en los equipos como en el tráfico de datos en la institución como entre localidades.
R8	Riesgo de control de entradas y salidas del personal en los controles de accesos.	Los controles de acceso no facilitan un registro ni reporte de entrada y salida de cada personal el cual tiene acceso, estos equipos solo admiten autenticación por tarjetas RFID y clave lo cual representa un riesgo si un personal pierde su tarjeta.
R9	Riesgo de disponibilidad de recursos y servicios de TI.	La zona franca no tiene definido procedimientos para la gestión (identificación, seguimiento, tratamiento, etc.) de las vulnerabilidades de los recursos de TI, incluyendo sus sistemas de información.
R10	Riesgo para la seguridad de la información (confidencialidad, disponibilidad y la integridad)	La empresa no cuenta con ningún programa de detección de virus o código malicioso el cual pueda eliminar cualquier amenaza que atente contra la información del negocio.
R11	Riesgo de penetración no autorizado a los recursos tecnológicos.	Aunque la empresa cuenta con un Firewall no se han realizado pruebas de penetración para validar que tan seguros esta los datos en la red de la empresa.

Tabla 7. RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN ZONA FRANCA (2019)

Fuente: Elaboración propia, a partir de la entrevista al Encargado TI.

4.6.4 Riesgos de Tecnología de la información levantados en la zona franca

Riesgos de TI zona Franca:

Los Riesgo de TI en el negocio están asociados al uso de propiedad, operación, participación, influencia y la adopción de la tecnología de la información de la empresa donde su objetivo está en estado o efecto de incertidumbre.

Los riesgos en la zona franca según la aplicación de la tecnología de la información caben destacar los siguientes:

4.6.5 Evaluación de los riesgos de la zona franca

Tabla VIII: MATRIZ DE EVALUACIÓN DE RIESGOS

Ref.	RIESGO	PROBABILIDAD (1-5)	IMPACTO (1-5)	Medida del Riesgo (1-25)
R1	Riesgo (no existe) bitácora de registro de acceso a data center del personal interno o externo.	**3**	**4**	**12** TOLERABLE O MEDIO
R2	Riesgo para la Seguridad de la información o confidencialidad de la empresa.	**3**	**5**	**15** CRITICO O ALTO
R3	Riesgo de disponibilidad de las informaciones y de continuidad de las operaciones.	**3**	**5**	**15** CRITICO O ALTO
R4	Riesgo de no documentación de políticas y procedimientos.	**4**	**4**	**16** CRITICO O ALTO
R5	Riesgos de Indisponibilidad de recursos Económicos.	**4**	**5**	**13** TOLERABLE O MEDIO

R6	Riesgo de Continuidad del Negocio.	**4**	**4**	**16** CRITICO O ALTO
R7	Riesgo de indisponibilidad de los recursos de red y servicios.	**4**	**4**	**16** CRITICO O ALTO
R8	Riesgo de no registro de entradas y salidas del personal en los controles de accesos.	**3**	**4**	**12** TOLERABLE O MEDIO
R9	Riesgo de no control de vulnerabilidades en los sistemas de información.	**3**	**5**	**15** CRITICO O ALTO
R10	Riesgo de ataque de Malware y Spyware	**4**	**4**	**16** CRITICO O ALTO
R11	Riesgo de penetración no autorizado a los recursos tecnológicos.	**3**	**5**	**15** CRITICO O ALTO

Tabla 8. MATRIZ DE EVALUACIÓN DE RIESGOS

Fuente: Elaboración propia a partir del levantamiento de los riesgos en la zona franca (2019).

4.6.6 Relación de controles implementados

La relación de los controles implementados indica que tanto puede o no afectar un riesgo a la empresa haciendo una comparativa de lo que tiene instalado en ejecución contra lo que puede mitigar este control o si no es lo suficientemente eficaz de prevenir un riego, de esta forma un control no implementado o incompleto pueden incidir varios riegos como lo muestra la siguiente tabla.

TABLA X: CONTROLES IMPLEMENTADOS A LOS RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN ZONA FRANCA (2019)

REF.	Controles Implementado	Referencia de Riesgo
CI-1	Control de acceso en puerta Data Center, solo el personal de TI y seguridad física tienen acceso, pero no es llevado un registro de entrada.	R1, R2, R3, R8
CI-2	Existen los controles de acceso para las áreas críticas de la empresa con la carencia de administración remota, hay que configurar los equipos uno por uno físicamente.	R2, R7, R8, R11
CI-3	Existen controles de antivirus, los propios que trae cada sistema operativo de Windows, Defender, programa de seguridad para prevenir, quitar y poner en cuarentena software espía en Microsoft Windows, pero esta aplicación es considerada antivirus menos efectivo que otros.	R2, R3, R5, R6, R7, R9, R10, R11

Tabla 9. CONTROLES IMPLEMENTADOS A LOS RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN ZONA FRANCA (2019)

Fuente: Elaboración propia, a partir de la entrevista al Encargado TI.

Nota: Por razones de falta de autorización de la Zona Franca no se pudieron realizar pruebas de funcionalidad de los controles implementados.

CAPITULO V

SOLUCIONES A LOS RIESGOS DE TECNOLOGÍA DE LA INFORMACIÓN INVESTIGADOS EN LA ZONA FRANCA

5.1. Implicaciones de los riesgos de TI en la gestión de la zona franca

Las empresas del tipo zona franca miden el estado de sus operaciones cotidianas en el área de producción con niveles de servicios que deben de mantener, un ejemplo de ello para esta empresa de equipos electrónicos es la cantidad de dispositivos que en un día deben de ser remanufacturado y que por la incidencia de uno o varios de los riesgos mencionados en el capítulo IV la producción se vea afectada, lo que acarrearía perdidas en los niveles de servicios al igual que pérdidas millonarias en RD$ pesos, pérdida de clientes, lo que conllevaría el cierre total de la empresa a consecuencia de los riesgos encontrados solo en un departamento, tecnología de la información.

5.2. Informe de Observaciones de Riesgos de TI

Los riesgos descubiertos en esta investigación son no aceptables, es por ello por lo que recomendamos aplicar controles de seguridad para su mitigación.

El plan de tratamiento a los riesgos son los controles para reducir, retener, evitar o compartir los riesgos.

5.2.1 Control de Actividades en el Data Center

Se verificó que no existe una bitácora de acceso a los Data Center de la Zona Franca de Equipos Electrónicos en donde se registren las razones de acceso de terceros a esta área. Esta situación no permite mantener control sobre las actividades que han sido realizadas en la misma, las fechas, tiempos y los datos generales (nombre, empresa, etc.) de las personas a las que se les concedió el acceso, dificultando la probabilidad de poder establecer responsabilidades ante la ocurrencia de algún incidente.

Recomendación:

Gerencia de Tecnología de la Información

1. Implementar un Registro o Bitácora para el acceso del personal interno o tercero, donde se describa el o los nombres del personal entrante, el concepto por el cual deba entrar a esas áreas, notificar la hoy de entrada y salida del área y un campo de firma del responsable del área en el tiempo que este dentro del área. Dicho registro debiese contener los siguientes campos:
    - Fecha de ingreso
    - Nombre del Personal por ingresar
    - Empresa o Departamento
    - Actividad por realizar
    - Hora de ingreso
    - Hora de salida
    - Ingreso o salida de elementos y dispositivos
    - Firma de la persona que ingresa
    - Firma del encargado responsable que autoriza la entrada

    Esta bitácora de registro debe estar establecida por política interna del departamento TI al igual que el llenado del documento, donde conste que todo el personal que ingrese al Data Center tiene que hacer registro de su visita y, en los casos de ser personal interno o externo a la empresa con acceso temporal deben ser acompañado por los responsables del área.

5.2.2 Control de Robo o Divulgación de datos críticos de la empresa

Se verificó que no existen políticas ni procedimientos de seguridad de la información para el acceso a correos personales, al mismo tiempo no existe un control para los usuarios que acceden a paginas o plataformas de envíos de archivo, este riesgo implica que actualmente

hay una brecha de seguridad la cual es susceptible a la extracción de información de información crítica de la empresa.

Recomendación:

Gerencia de Tecnología de la Información

2. Implementar las políticas y procedimientos para el acceso a correos y plataformas de transferencia de archivos, donde se defina los controles para la utilización de las plataformas y la movilización de los archivos de la empresa con el objetivo de salvaguarden la integridad de toda la información de esta. Se debe crear las políticas en el Firewall las cuales bloquen el acceso de correos personales con el fin erradicar el uso de correos externos en el ejercicio de funciones laborales.

   A la vez se debe elaborar e implementar un mecanismo de movilización internar de los documentos para evitar en la medida de lo posible que estos datos viajes a través de plataformas externa en las cuales se pueda perder o sustraer la información.

5.2.3 Control de disponibilidad de las informaciones y de continuidad de las operaciones

Se verificó que actualmente la Zona Franca de Equipos Electrónicos no cuenta con herramientas para la realización de Backup automáticos en los aplicativos y unidades de almacenamientos alojados en los dispositivos y servidores, al mismo tiempo no existe un repositorio donde estén alojados las copias de seguridad o respaldos de las configuraciones de los equipos de la infraestructura tecnológica.

El riesgo de esto implica que ante las ocurrencias de un evento que afectara algún dispositivo de la infraestructura o servicio critico de tecnología no hay garantía de que esto se restablezca en un tiempo oportuno ya que no existe ninguna copia de seguridad de la

información, ni ningún respaldo de archivo de configuración con los parámetros de comunicaciones del funcionamiento los equipos. Teniendo esto como consecuencia la perdida de la información crítica de la empresa y la disminución de las ganancias por la remano facturación de los dispositivos electrónicos.

Recomendación:

Gerencia de Tecnología de la Información

3. Instalar un dispositivo o herramientas automáticas de respaldo de datos (Backup) que garanticen la disponibilidad de la información en caso de alguna perdida de información en las plataformas o servicios principales, teniendo como resultado la estabilidad de los diferente aplicativos y dispositivo de la infraestructura.

   Crear un repositorio en donde se encuentre un backup o respaldo de configuración de los dispositivos de la empresa garantizando la restauración exitosa a la hora de cualquier incidente en los dispositivos o aplicaciones.

5.2.4 Control de documentación de políticas y procedimientos

Se verificó que actualmente no están creadas ni establecidas las políticas y procedimientos que rijan los proceso de TI dentro de las instalaciones de la Zona Franca de Equipos Electrónicos.

El riesgo de esto implica que al ocurrir cualquier eventualidad no existe la documentación de los procesos que los empleados deben cumplir ni las reglas que se deben acatar bajo las normas de la empresa.

Recomendación:

Gerencia de Tecnología de la Información

4. Desarrollar las políticas y procedimientos que definan los procesos de tecnología de la Zona Franca de Equipos Electrónicos, para la capacitación del personal y seguridad de la organización. Se recomienda tener documentado los procedimientos de TI por temas de regulación, mejora de proceso, historial de manejo y actualización de este, el cual sirva de conocimiento general dentro de la zona franca de equipos electrónicos.

5.2.5 Control de Indisponibilidad de recursos Económicos

Se verificó que la compañía no cuenta con un presupuesto asignado al área de TI, el riesgo de esto implica que ante una oportunidad de desarrollo para la mejora en los diferentes procesos de tecnología se vea interrumpida por la falta de recursos económicos que aportarían a la actualización de TI e incluso a la erradicación de problemas persistentes en la zona franca de equipos electrónicos.

Recomendación:

Gerencia de Tecnología de la Información

5. Destinar un presupuesto anual para el desarrollo y mantenimiento de los procesos de tecnología dentro de la Zonas Francas de Equipos Electrónicos. Esto aportaría a la actualización de los equipos, sistemas y controles en TI para el beneficio de la seguridad y mantenimiento tecnológico necesario en la organización.

5.2.6 Control de Continuidad del Negocio

Se verificó que no existe un plan de recuperación de desastre para el departamento de tecnología de la zona franca de equipos electrónicos, el riesgo de esto implica que ante las ocurrencias de un evento que afecte la infraestructura o los servicios de tecnología no hay garantía de que esto se reestablezca en un tiempo oportuno debido a que no existe un plan secuencial de las actividades y los procesos que actualmente se ejecutan en la empresa.

Recomendación:

Gerencia de Tecnología de la Información

6. Crear y establecer un plan de recuperación ante desastres (DRP por sus siglas en ingles Disaster Recovery Plan) para el proceso de recuperación de datos, hardware y software crítico del negocio, donde se puedan reintegrar sus operaciones en caso de desastres naturales o perdida por origen humano, con el fin de tener ventaja en el restablecimiento de las operaciones de la empresa en el menor tiempo posible. Esto debe emplearse en un sitio alterno para la continuidad del negocio en caso de que la catástrofe destruya las instalaciones principales.

   Se recomienda que este plan de continuidad de negocio se ejecute al menos una vez al año para verificar que todo el protocolo de recuperación funcione en condiciones óptimas, teniendo el propósito de reducir los costos de recuperación para la empresa.

5.2.7 Control de interrupción de los servicios y/o de las operaciones de la empresa

Se verificó que la empresa no cuenta actualmente con un sistema de monitoreo, el cual permita notificar al departamento de TI sobre las fallas en la red, servidores o procesos de

las diferentes áreas. Esto dificulta la prevención o solución inmediata departe de TI a los equipos pertinentes como al tráfico de datos críticos en la institución.

Recomendación:

Gerencia de Tecnología de la Información

7. Desarrollar un plan de monitoreo de los recursos de red como son, Router, Switch, Firewall, servidores y equipos críticos para la organización. Implementando un software de monitoreo tales como, SolarWinds, PRTG Network Monitor de Paessler, OpManager entre otras. Donde estas herramientas son configurables con alertas y notificaciones en tiempo real de un evento o incidente en los recursos de la red. Esto aportaría una mejora considerable en el tiempo para detectar el problema o el equipo afectado.

5.2.8 Control de registro de entradas y salidas del personal en los controles de accesos

Se verificó que la entidad no tiene una administración remota individual o por medio de un controlador para un reporte de entrada y salida del personal. Actualmente el proceso de autentificación se maneja por medio de tarjetas RFID y clave. Esto genera una brecha de irregularidad en el registro del personar ya que, en casos de pérdidas de las tarjetas, no se tiene una opción prevista para el reporte de entrada y salida de la empresa. Por otra parte, los dispositivos para estas tarjetas son Stand Alone, significa que al dar un mantenimiento, corrección o revisión se debe realizar físicamente en cada uno de ellos, no se cuenta con una alternativa remota.

Recomendación:

Gerencia de Tecnología de la Información

8. Mejorar los controles de accesos mediante el cambio de estos, ya que estos son sistemas de seguridad críticos para una organización. En el caso de perder una tarjeta de acceso, puede ser tomada por otra persona ajena a la organización e ingresar a las áreas restringidas de la zona franca. Recomendamos un sistema de control con huellas biométricas, con acceso remoto y viable para el reporte de las entradas y salidas de cada personal.

5.2.9 Control de vulnerabilidades en los sistemas de información

Se verificó que la Zona Franca no posee un departamento de seguridad de TI, el cual resguarde los recursos tecnológicos ante ataques informáticos internos o externos, esto ocasiona un riesgo en la operatividad de la empresa como en la información que se maneja.

Recomendación:

Gerencia de Tecnología de la Información

9. Crear un área de seguridad de tecnología como dependencia del departamento de TI, el cual sostenga la seguridad informática de la empresa, y del mismo modo mitigar ataques internos como externos que puedan poner en riesgo y comprometer la información del negocio.

   Se recomienda que, esta área establezca políticas y parámetros de seguridad para los usuarios administrativos y operativos en la manipulación de los equipos a trabajar. Esto quiere decir, aseguramiento por la seguridad perimetral de la red, los accesos de los aplicativos y los controles de accesos a las áreas.

5.2.10 Control de ataque de Malware y Spyware

Se verificó que en la Zona Franca de equipos electrónicos no se cuenta con programas de detección de virus o código malicioso, el cual pueda prevenir una amenaza a los datos de información en la entidad.

Recomendación:

Gerencia de Tecnología de la Información

10. Implementar un administrador de antivirus Enterprise y despliegue del agente en cada uno de los servidores y dispositivos finales, esto con el fin de evitar ataques por parte de programas maliciosos, robos y pérdidas de información. Se recomienda que, las computadoras con el agente instalado sincronicen con el servidor que tendrá instalado el administrador a cargo de enviar las actualizaciones, excepciones y protección de los datos del equipo.

5.2.11 Control de penetración no autorizado a los recursos tecnológicos

Se verificó o que la organización a pesar de tener Firewall no cuenta con pruebas de penetración no autorizada a los recursos de TI. Esto no permite validar la seguridad de los datos en la red de la empresa.

Recomendación:

Gerencia de Tecnología de la Información

11. Al crear un departamento de seguridad TI (recomendación del R9), se anexarían la revisión de estas pruebas en las políticas de seguridad por la confidencialidad, integridad y disponibilidad de los datos.

Además, se recomienda controles de acceso remoto a la red y parámetros de seguridad en el firewall. Y la solicitud de una auditoria a un proveedor externo para las pruebas de penetración a la red perimetral, de esta manera se valida el nivel de control y seguridad en la información crítica de la empresa.

CONCLUSIÓN

Al inicio de esta investigación se estableció como objetivo evaluar los riesgos de tecnología de la información en una Zona Franca de Equipos Electrónicos, ubicada en la cuidad de Santo Domingo, República Dominicana, en un periodo de septiembre a diciembre del año 2019.

En esta investigación se establecieron los siguientes objetivos específicos: Analizar en forma detallada el ambiente de TI de la Zona Franca, agrupando por área de controles generales los procesos que se realizan en esta, determinar los criterios para cualificar las probabilidades de ocurrencia de los riesgos de TI identificados, determinar los criterios para cuantificar las probabilidades de ocurrencia de los riesgos de TI identificados, determinar los criterios para cualificar el impacto, para el negocio de la Zona Franca, de los riesgos de TI identificados y determinar los criterios para cuantificar el impacto sobre el negocio de la Zona Franca, de los riesgos de TI identificados.

Todos los objetivos antes mencionados fueron analizados y establecidos los criterios en el capítulo IV de esta investigación, los mismos eran etapas que debían cumplirse para llegar a este resultado general de la investigación:

Se evaluaron en total 11 riesgos de tecnología de la información de los cuales ocho (8) resultaron ser críticos o alto para un 73% y tres (3) tolerables o medio para un 27%. Dentro de los tolerables o medios encontramos vinculados a: Acceso a data center del personal interno o externo, Indisponibilidad de recursos Económicos, registro de entradas y salidas del personal en los controles de accesos, falta de un plan de recuperación ante desastre.

Los riesgos evaluados como críticos o alto resultaron estar vinculados a lo siguiente: Seguridad de la información o confidencialidad de la empresa, disponibilidad de las informaciones y de continuidad de las operaciones, documentación de políticas y procedimientos, Continuidad del Negocio, indisponibilidad de los recursos de red y

servicios, no control de vulnerabilidades en los sistemas de información, ataque de Malware y Spyware y penetración no autorizado a los recursos tecnológicos.

A través de los resultados de esta investigación la empresa contará con una herramienta objetiva que le permitirá continuar fortaleciendo la gestión, hasta llegar a tener un alto nivel de seguridad de la información integralmente en todos sus recursos, planificación, políticas, procesos, procedimientos, entre otros.

RECOMENDACIONES

Al inicio de esta investigación se estableció como objetivo evaluar los riesgos de tecnología de la información en una Zona Franca de Equipos electrónicos, ubicada en la cuidad de Santo Domingo, República Dominicana, en un periodo de septiembre a diciembre del año 2019.

Dentro de las recomendaciones resultantes de esta investigación destacamos las siguientes:

- Aplicar la norma ISO/IEC 27005:2011 de Gestión de Riesgos de Seguridad de la Información y estándares de seguridad de la información.

- Tomar en consideración los riesgos evaluados en esta investigación.

- Crear planes de mitigación a los riesgos levantados.

- Crear un Plan de Continuidad del Negocio.

- Implementar controles aplicables basados en la Norma ISO 27001:2005 gestión de riesgos de seguridad de los sistemas de información. (solo a nivel de buenas prácticas por el costo de la certificación y que no la requiere a ese nivel por la naturaleza de la empresa).

REFERENCIAS BIBLIOGRAFICAS

Alegsa, L. (2016). *Alegsa*. Obtenido de www.alegsa.com: http://www.alegsa.com.ar/Dic/vulnerabilidad.php

Alegsa, L. (06 de Abril de 2019). *alegsa*. Obtenido de www.alegsa.com: http://www.alegsa.com.ar/Dic/dispositivo_electronico.php

Ariza, M. B. (2007). *Abordaje hermenéutico de la investigación cualitativa. Teorías, procesos, técnicas.* Colombia : Cooperativa de Colombia.

Baray, H. L. (2006). *eumed.* Obtenido de http://www.eumed.net: http://www.eumed.net/libros-gratis/2006c/203/2n.htm

Carvajal, Y. A. (2018). *Editorial Feijóo* . Obtenido de scielo.sld: http://scielo.sld.cu/pdf/caz/v45n1/caz09118.pdf

DGII. (15 de enero de 1990). *DGII.* Obtenido de www.DGII.gov.do: https://dgii.gov.do/legislacion/leyesTributarias/Documents/8-90.pdf

EcuRed. (2008). *ecured*. Obtenido de www.ecured.cu: https://www.ecured.cu/T%C3%A9cnicas_de_Recolecci%C3%B3n_de_Informaci%C3%B3n#T.C3.A9cnicas_de_Verificaci.C3.B3n_Ocular

FERRER, J. (2010). *tecnicas-de-la-investigacion.* Obtenido de metodologia02: http://metodologia02.blogspot.com/p/tecnicas-de-la-investigacion.html

FINAGRO. (2013). *FINAGRO.* Obtenido de FINAGRO: https://www.finagro.com.co/qui%C3%A9nes-somos/activos-de-informaci%C3%B3n

Gardey, A., & Perez Porto, J. (2012). *definicion.de*. Obtenido de www.definicion.de: https://definicion.de/informacion/

Internacional Standard ISO/IEC 27005:2011. Second edition 2011. https://www.saiglobal.com/

ISACA. (2008). *ISACA*. Obtenido de Information Systems Audit and Control Association: https://www.isaca.org/pages/default.aspx

ISO 27001 Security. (2013). *ISO 27001 Security*. Obtenido de ISO 27001 Security: http://www.iso27001security.com/html/27005.html

ISO 27001 Security. (2013). *ISO 27001 Security*. Obtenido de ISO 27001 Security: http://www.iso27001security.com/html/27035.html

MX, E. D. (5 de Septiembre de 2015). *Definición MX*. Obtenido de definicion.mx: https://definicion.mx/evaluacion/

Negrete, J. (24 de Julio de 2015). *redalyc*. Obtenido de http://www.redalyc.org: http://www.redalyc.org/pdf/2233/223353236004.pdf

Orozco, R. L. (2008). *Geocities*. Obtenido de www.geocities.ws: http://www.geocities.ws/roxloubet/investigacionca

Pelekais, C. d. (2000). *Dialnet-MetodosCuantitativos Y Cualitativos*. Obtenido de www.dialnet.unirioja.es: https://dialnet.unirioja.es/descarga/articulo/6436313.pdf

Raffino, M. E. (2018). *concepto*. Obtenido de www.concepto.de: https://concepto.de/metodo-deductivo-2/

Raffino, M. E. (28 de Febrero de 2019). *concepto*. Obtenido de www.concepto.de: https://concepto.de/tecnologia/

Robles, D. (2019). *investigacioncientifica*. Obtenido de www,investigacioncientifica.org: https://investigacioncientifica.org/tipos-de-metodos-de-investigacion/

Rodríguez, G. G. (Febrero de 1996). *Metodología de la Investigación cualitativa.* España : Málaga Aljibe. Obtenido de metodelainv.: http://metodelainv.blogspot.es/

Sampieri, H. (1997). josetavarez. Obtenido de www.josetavarez.net: https://josetavarez.net/Compendio-Metodologia-de-la-Investigacion.pdf

Software ISO Riesgos y Seguridad.https://www.isotools.org/normas/riesgos-y-seguridad/iso-31000/

Velasco, W. V. (septiembre de 2008). *scielo.org*. Obtenido de scielo.org: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

ANEXOS

UNAPEC
UNIVERSIDAD APEC

DECANATO DE INGENIERIA E INFORMATICA

ANTEPROYECTO DE TRABAJO DE GRADO

"EVALUACION DE RIESGOS DE TECNOLOGIA DE LA INFORMACION EN UNA ZONA FRANCA DE EQUIPOS ELECTRONICOS, PERIODO SEPTIEMBRE-DICIEMBRE, AÑO 2019".

Trabajo de grado para optar por el título de Ingeniería en sistemas de computación

Sustentantes:

Francisco Alberto Deño	2012-0878
Luis Antonio Sánchez Suero	2015-0541
Víctor Manuel De la Cruz Flores	2014-1762

Asesor
Edgar Morrobert

DEPARTAMENTO DE SOCIALES
PROYECTO DE TRABAJO DE GRADO
APROBADO
FIRMA
FECHA 23/7/19

Santo Domingo, D. N.

6 de Julio 2019

Indice

II. INTRODUCCIÓN 4

III. JUSTIFICACIÓN 5

IV. DELIMITACIÓN DEL TEMA Y PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN. 6

V. Objetivos Generales y Específicos 7

Objetivo General 7

Objetivos Específicos 7

VI. MARCO TEÓRICO REFERENCIAL 8

Marco Teórico 8

Marco Conceptual 9

VII. DISEÑO METODOLÓGICO: METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN CUANTITATIVA Y/O CUALITATIVA. 12

Tipo de estudio 12

Método de investigación 13

Fuentes y Técnicas de Investigación 14

1. Fuente de investigación 14

2. Técnicas de Investigación 14

VIII. FUENTES DE DOCUMENTACIÓN (FUENTES BIBLIOGRÁFICAS PRIMORDIALES SOBRE EL TEMA). 17

IX. ESQUEMA PRELIMINAR DE CONTENIDO DEL PROYECTO DE GRADO 19

I. TITULO DEL TRABAJO DE GRADO

EVALUACION DE RIESGOS DE TECNOLOGIA DE LA INFORMACION EN UNA ZONA FRANCA DE EQUIPOS ELECTRONICOS, PERIODO SEPTIEMBRE- DICIEMBRE, AÑO 2019.

II. INTRODUCCIÓN

Las zonas francas son empresas que se destinan a la industrialización de productos con fines de exportación o servicios como servicio al cliente vía telefónica, los llamados call center. Este tipo de empresa tienen facilidades tributarias (exenciones) que les brinda el Gobierno Dominicano, a los fines de dinamizar su crecimiento y fortalecerlas como fuentes de empleo. Las zonas francas de equipos electrónicos están dedicadas al reacondicionamiento equipos electrónicos de manera que puedan estar disponibles para la venta.

El uso de la Tecnología de la Información y Comunicaciones (TIC) en las zonas francas de equipos electrónicos puede ser considerado como alto. En adición, los riesgos sobre los objetivos de la seguridad de la información (disponibilidad, confidencialidad, integridad) se hacen presentes en esta industria. Por tal razón, realizar evaluaciones periódicas, y objetivas, para determinar el nivel de riesgo al que están expuestos estos objetivos, debe ser una prioridad para lograr los objetivos que se establecen este tipo de empresas.

Este trabajo incluye todos los aspectos necesarios para lograr determinar el contexto de riesgos de TIC de la zona franca objeto de estudio y con su desarrollo se obtendrán las acciones de tratamiento de estos riesgos, que una vez implementados podrán disminuir el nivel de incertidumbre con que puede estar operando el objeto de estudio.

III. JUSTIFICACIÓN

Se adopta la definición propuesta por Bosque et. Al (2004) en donde, el Riesgo Tecnológico hace referencia a la probabilidad de sufrir daños o pérdidas económicas, ambientales y humanas como consecuencia del funcionamiento deficiente o accidente de una tecnología aplicada en una actividad humana. (Negrete, 2015).

Tener en conocimiento el nivel de riesgo en que está operando una determinada organización, le permite a sus directos tomar decisiones más certeras para el logro de los objetivos estratégicos que se hayan definido para dicha organización. Todo proceso tiene asociado determinados riesgos inherentes y en Tecnología de la Información se pueden citar los relacionados a afectar los objetivos de la seguridad de la información: Disponibilidad, Integridad y Confidencialidad.

En la industria de las zonas francas de equipos electrónicos, las fuentes que pueden afectar estos objetivos tienen sus orígenes, principalmente, en la gestión de los accesos físicos y lógicos a los entornos donde se manejan las informaciones, propias de la organización, así como de sus clientes y partes interesadas.

Basado en lo que se describe anteriormente este trabajo de grado tiene como finalidad realizar un proceso de evaluación de riesgos de tecnología de la información en una zona franca de equipos electrónicos para presentar las recomendaciones que consideramos apropiadas para tratar apropiadamente estos riesgos.

IV. DELIMITACIÓN DEL TEMA Y PLANTEAMIENTO DEL PROBLEMA DE INVESTIGACIÓN.

En las zonas francas de equipos electrónicos se incrementan cada día más los riesgos tecnológicos, debido a que al pasar el tiempo aumentan el número de aplicaciones y herramientas de tecnología, que incluyen nuevos riesgos, que requieren ser adecuadamente gestionados. Es por esto la necesidad de realizar una evaluación de riegos de tecnología de la información.

La zona franca de equipos electrónicos objeto de estudio nunca ha realizado una evaluación de los riesgos de la Tecnología de la Información (TI) que utiliza, por lo que no tiene cuantificado el nivel de impacto que tendría sobre sus operaciones la materialización de determinados riesgos.

La investigación se realizará en la zona franca de equipos electrónicos que por motivos de confidencialidad se omitirá el nombre de esta. Está en la ciudad de Santo Domingo, República Dominicana.

Las informaciones presentadas tendrán efecto durante el periodo de tiempo mayo – agosto del año 2019.

V. Objetivos Generales y Específicos

Objetivo General

Evaluar los riesgos de tecnología de la información en una Zona Franca de Equipos electrónicos, ubicada en la cuidad de Santo Domingo, Rep. Dom.

Objetivos Específicos

1. Analizar en forma detallada del ambiente de TI de la Zona Franca, agrupando por área de controles generales los procesos que se realizan en esta.
2. Determinar los criterios para cualificar las probabilidades de ocurrencia de los riesgos de TI identificados.
3. Determinar los criterios para cuantificar las probabilidades de ocurrencia de los riesgos de TI identificados.
4. Determinar los criterios para cualificar el impacto, para el negocio de la Zona Franca, de los riesgos de TI identificados.
5. Determinar los criterios para cuantificar el impacto, para el negocio de la Zona Franca, de los riesgos de TI identificados.

VI. MARCO TEÓRICO REFERENCIAL

Marco Teórico

La tecnología de la información permite capturar, almacenar, transmitir, gestionar, consultar informaciones de las organizaciones, sus clientes y las partes interesadas (accionistas, proveedores, etc.). Las características relacionadas a la manera en que hoy día se manejan las TI crean nuevas amenazas y vulnerabilidades, que aumentan el desafío de mantener la adecuada gestión de la seguridad de la información, en cualquiera de sus estados. La información puede estar comprometida cuando un tercero no autorizado accede a ella o bien cuando por la ocurrencia de un evento, código malicioso u otra fuente de amenaza, esta información no está disponible para sus usuarios autorizados.

La industria de zonas francas tiene, por lo general, una alta rotación de personal y con la llegada de nuevos colaboradores se hace necesario crearles conciencia sobre la importancia de la seguridad de la información, a la vez que se hace necesario mantener una oportuna evaluación de los controles existentes sobre la seguridad de la información.

Marco Conceptual

Activo de información: Se denomina activo a aquello que tiene algún valor para la empresa y por tanto debe protegerse. De manera que un Activo de Información incluye la información estructurada y no estructurada que se encuentre presente en forma impresa, escrita en papel, transmitida por cualquier medio electrónico o almacenada en equipos de cómputo, incluyendo datos contenidos en registros, archivos y bases de datos. (FINAGRO, 2013).

Amenaza: Una amenaza es la indicación de un potencial evento no deseado, se puede definir como amenaza a todo elemento o acción capaz de atentar contra la seguridad de la información. (ISACA, 2008).

Confidencialidad: Es la propiedad de la información, por la que se garantiza que está accesible únicamente a personal autorizado a acceder a dicha información. (ISACA, 2008).

Control: Aquellos mecanismos y/o procedimientos que regulan el propio funcionamiento del sistema de gestión de la seguridad de la información. (ISACA, 2008).

Disponibilidad: Es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas, procesos o aplicaciones. (ISACA, 2008).

Dispositivo electrónico: es una combinación de componentes electrónicos organizados en circuitos, destinados a controlar y aprovechar las señales eléctricas. (Alegsa, alegsa, 2019)

Evaluación: La evaluación se define como el proceso mediante el cual se intenta determinar el valor de una cosa o persona o el grado de cumplimiento de determinados objetivos. Este término puede utilizarse haciendo referencia a distintos enfoques. (MX, 2015)

Información: está constituida por un grupo de datos ya supervisados y ordenados, que sirven para construir un mensaje basado en un cierto fenómeno o ente. La información permite resolver problemas y tomar decisiones, ya que su aprovechamiento racional es la base del conocimiento. (Gardey & Perez Porto, 2012)

Integridad: Es la capacidad de garantizar que los datos no han sido modificados desde su creación sin autorización. La información que disponemos es válida y consistente. (ISACA, 2008).

Política de seguridad: Una política de seguridad es "la declaración de las reglas que se deben respetar para acceder a la información y a los recursos". Los documentos de una política de seguridad deben ser dinámicos, es decir, ajustarse y mejorarse continuamente según los cambios que se presentan en los ambientes donde se crearon. Las políticas de seguridad deben ser conocidos por todo el personal de una organización. (Velasco, 2008)

Riesgo: Es la materialización de vulnerabilidades identificadas, asociadas con su probabilidad de ocurrencia, amenazas expuestas, así como el impacto negativo que ocasione a las operaciones de negocio. (ISACA, 2008).

Riesgos Tecnológico: Es la probabilidad de sufrir daños o pérdidas humanas, económicas y ambientales como consecuencia del funcionamiento deficiente o accidente de una tecnología aplicada en una actividad. (Carvajal, 2018)

Seguridad de la información: La seguridad de la información es el conjunto de medidas preventivas y reactivas de las organizaciones y sistemas tecnológicos que permiten resguardar y proteger la información buscando mantener la confidencialidad, la disponibilidad e integridad de datos.

La información es poder, y según las posibilidades estratégicas que ofrece tener acceso a cierta información, esta se clasifica como:

- Critica: es indispensable para la operación de la empresa.
- Sensible: debe ser conocida por las personas autorizadas.
- Valiosa: es un activo de la empresa y muy valioso. (ISACA, 2008).

Tecnología: es un conjunto de nociones y conocimientos utilizados para lograr un objetivo preciso, que dé lugar a la solución de un problema especifico del individuo o a la satisfacción de alguna de sus necesidades. Es un concepto extremadamente amplio que es capaz de abarcar una inmensa variedad de aspectos que pueden ir de la electrónica al arte o la medicina. (Raffino, concepto, 2019)

Vulnerabilidad: hace referencia a una debilidad en un sistema permitiendo a un atacante violar la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del sistema o de sus datos y aplicaciones. (Alegsa, Alegsa, 2016)

Zona Franca: Se define la zona franca como un área geográfica del país sometida a los controles aduaneros y fiscales especiales, en la cual se permite la instalación de empresas que destinen su producción o servicios hacia el mercado externo, mediante el otorgamiento de los incentivos necesarios para fomentar su desarrollo. (Ley 08-90, Art. 2)

VII. DISEÑO METODOLÓGICO: METODOLOGÍA Y TÉCNICAS DE INVESTIGACIÓN CUANTITATIVA Y/O CUALITATIVA.

Tipo de estudio

A. Estudio Descriptivo

Muy frecuentemente el propósito del investigador es describir situaciones y eventos. Esto es, decir cómo es y se manifiesta determinado fenómeno. Los estudios descriptivos buscan especificar las propiedades importantes de personas, grupos, -comunidades o cualquier otro fenómeno que sea sometido a análisis (Dankhe, 1986). Miden y evalúan diversos aspectos, dimensiones o componentes del fenómeno o fenómenos a investigar. Desde el punto de vista científico, describir es medir. (Sampieri, 1997)

Para poder evaluar los riesgos de tecnología de la información, se utilizará el estudio descriptivo, ya que a través de este podemos investigar en detalle, los eventos físicos y lógicos encontrados en las Zonas Francas de equipos electrónicos. Esto, con el propósito de medir las vulnerabilidades de una infraestructura tecnológica.

B. Estudio Explicativo:

Están dirigidos a responder a las causas de los eventos físicos o sociales. Como su nombre lo indica, su interés se centra en explicar por qué ocurre un fenómeno y en qué condiciones se da éste, o por qué dos o más variables están relacionadas. Además de que proporcionan un sentido de entendimiento del fenómeno a que hacen referencia. (Sampieri, 1997)

Por medio del estudio explicativo, se podrá entender las diferentes debilidades de los sistemas de información relacionadas a las variables de control existentes en las Zonas Francas de equipos electrónicos, tales como procesos de seguridad y control al acceso de la información.

Método de investigación

A. Metodología Cuantitativo:

Describe, infiere y resuelve problemas usando números. Se hace hincapié en la recopilación de datos numéricos, el resumen de esos datos y el dibujo de inferencias a partir de los datos. (Robles, 2019)

Para poder medir las vulnerabilidades en la infraestructura de la Zona Franca de equipos electrónicos, es necesaria la utilización de datos numéricos para analizar los resultados obtenidos mediante la evaluación de riesgo.

B. Metodología Cualitativo:

Explica y obtiene conocimiento profundo de un fenómeno a través de la obtención de datos extensos narrativos. Es flexible, especificando en términos generales el desarrollo del estudio. Se obtiene a través de la recolección de documentos, observación participativa, entrevistas informales y no estructuradas o notas de campo detalladas y extensas. (Pelekais, 2000)

Este método no se limita a datos numéricos, es decir, nos ayudará a profundizar la evaluación de forma descriptiva y explicativa para un mejor entendimiento del problema y posible solución a la misma.

C. Método Deductivo:

Forma específica de pensamiento o razonamiento, que extrae conclusiones lógicas y válidas a partir de un conjunto dado de premisas o proposiciones. (Raffino, concepto, 2018)

Por medio de la recopilación de datos numéricos y explicativos, se podrá llevar una observación general a una evaluación particular, con el objetivo de lograr un punto de esclarecimiento para la conclusión lógica deseada en este trabajo.

Fuentes y Técnicas de Investigación

1. Fuente de investigación

Las fuentes de investigación utilizadas en este trabajo se basan en fuentes primarias y secundarias, ya que se toma información de libros, documentos oficiales de instituciones públicas, informes técnicos y revistas de autores primarios. Así mismo, se recopila datos de información organizada o elaborada, las cuales son producto de análisis de documentos primarios originales y las entrevistas al personal relacionado a los procesos de TI, al igual que la verificación de controles relacionados a esta.

2. Técnicas de Investigación

La técnica es indispensable en el proceso de la investigación científica, ya que integra la estructura por medio de la cual se organiza la investigación, La técnica pretende los siguientes objetivos:

- Ordenar las etapas de la investigación.
- Aportar instrumentos para manejar la información.
- Llevar un control de los datos.
- Orientar la obtención de conocimientos.

(FERRER, 2010)

En cuanto a las técnicas de investigación, se utilizarán dos formas generales: técnica campo y técnica documental.

Las técnicas de investigación de campo son aquellas que le sirven al investigador para relacionarse con el objeto y construir por sí mismo la realidad estudiada. Tienen el propósito de recopilar información empírica sobre la realidad del fenómeno a estudiar y son útiles para estudiar a fondo un fenómeno en un ambiente determinado. (Orozco, 2008) En este caso, la Zona Franca será el campo de investigación.

Técnicas de investigación documental, también llamadas bibliográficas o en archivos, nos permite adentrarnos en el tema con mayor profundidad. Para Carlos Sandoval, la investigación documental es un instrumento o técnica de investigación, cuya finalidad es obtener datos e información a partir de documentos escritos o no escritos, susceptibles de ser utilizados dentro de los propósitos de un estudio concreto. Mientras más fuentes se utilicen más fidedigno será el trabajo realizado. (Ariza, 2007)

Las diferentes metodologías para utilizar en estas técnicas para la evaluación de riesgos de tecnología de la información en la Zona Franca serán las siguientes:

1. Análisis de Datos:

Al concluir la recolección de datos para este proyecto, la cual se expresa de forma cuantitativa y cualitativa, se procederá al análisis de la información obtenida. En esta etapa se determinará como analizar los datos y que herramientas son necesarias para un resultado verídico.

“Analizar significa establecer categorías, ordenar, manipular y resumir los datos,” (Kerlinger, 1982, p. 96). En esta etapa del proceso de investigación se procede a racionalizar los datos colectados a fin de explicar e interpretar las posibles relaciones que expresan las variables estudiadas. (Baray, 2006)

2. Observación directa:

La observación consiste en la indagación sistemática, dirigida a estudiar los aspectos más significativos de los objetos, hechos, situaciones sociales o personas en el contexto donde se desarrollan normalmente; permitiendo la comprensión de la verdadera realidad del fenómeno. (Rodríguez, 1996)

Uno de los procesos cruciales para la obtención de información, es la observación directa en la Zona Franca, esto servirá de apoyo para los datos verídicos en cuanto a estadística y explicación detallada de los riesgos tecnológicos en la actualidad, y como afectan la seguridad de los datos.

3. Verificación:

Consiste en verificar en la entidad auditada, en forma directa y paralela, como se desarrollan y documentan los procesos, procedimientos, controles, las instalaciones físicas, los movimientos diarios, la relación con el entorno, accionar de sus directivos, trabajadores, etc., permitiendo tener una visión de la organización desde el ángulo que el auditor necesita. (EcuRed, 2008)

Siendo la observación una de las técnicas de investigación para este proyecto, ayudará a que la verificación de los datos en la entidad auditada sea de forma directa. Pues, la relación con el entorno, los movimientos diarios y los procedimientos realizados permitirán una plena evaluación de los riesgos tecnológicos presentes desde el ángulo necesitado para las recomendaciones de lugar.

4. Recopilación Bibliográfica:

Se utilizarán libros y documentos bibliográficos para la investigación de los temas en este proyecto, estas herramientas de búsqueda servirán de base para integrar los datos recopilados de campo con las teorías que competen en el proceso de investigación.

VIII. FUENTES DE DOCUMENTACIÓN (FUENTES BIBLIOGRÁFICAS PRIMORDIALES SOBRE EL TEMA).

Alegsa, L. (2016). *Alegsa*. Obtenido de www.alegsa.com: http://www.alegsa.com.ar/Dic/vulnerabilidad.php

Alegsa, L. (06 de Abril de 2019). *alegsa*. Obtenido de www.alegsa.com: http://www.alegsa.com.ar/Dic/dispositivo_electronico.php

Ariza, M. B. (2007). *Abordaje hermenéutico de la investigación cualitativa. Teorías, procesos, técnicas.* Colombia : Cooperativa de Colombia.

Baray, H. L. (2006). *eumed.* Obtenido de http://www.eumed.net: http://www.eumed.net/libros-gratis/2006c/203/2n.htm

Carvajal, Y. A. (2018). *Editorial Feijóo* . Obtenido de scielo.sld: http://scielo.sld.cu/pdf/caz/v45n1/caz09118.pdf

DGII. (15 de enero de 1990). *DGII.* Obtenido de www.DGII.gov.do: https://dgii.gov.do/legislacion/leyesTributarias/Documents/8-90.pdf

EcuRed. (2008). *ecured*. Obtenido de www.ecured.cu: https://www.ecured.cu/T%C3%A9cnicas_de_Recolecci%C3%B3n_de_Informaci%C3%B3n#T.C3.A9cnicas_de_Verificaci.C3.B3n_Ocular

FERRER, J. (2010). *tecnicas-de-la-investigacion.* Obtenido de metodologia02: http://metodologia02.blogspot.com/p/tecnicas-de-la-investigacion.html

FINAGRO. (2013). *FINAGRO*. Obtenido de FINAGRO: https://www.finagro.com.co/qui%C3%A9nes-somos/activos-de-informaci%C3%B3n

Gardey, A., & Perez Porto, J. (2012). *definicion.de*. Obtenido de www.definicion.de: https://definicion.de/informacion/

ISACA. (2008). *ISACA*. Obtenido de Information Systems Audit and Control Association: https://www.isaca.org/pages/default.aspx

MX, E. D. (5 de Septiembre de 2015). *Definición MX*. Obtenido de definicion.mx: https://definicion.mx/evaluacion/

Negrete, J. (24 de Julio de 2015). *redalyc.* Obtenido de http://www.redalyc.org: http://www.redalyc.org/pdf/2233/223353236004.pdf

Orozco, R. L. (2008). *Geocities*. Obtenido de www.geocities.ws: http://www.geocities.ws/roxloubet/investigacionca

Pelekais, C. d. (2000). *Dialnet-MetodosCuantitativos Y Cualitativos.* Obtenido de www.dialnet.unirioja.es: https://dialnet.unirioja.es/descarga/articulo/6436313.pdf

Raffino, M. E. (2018). *concepto*. Obtenido de www.concepto.de: https://concepto.de/metodo-deductivo-2/

Raffino, M. E. (28 de Febrero de 2019). *concepto*. Obtenido de www.concepto.de: https://concepto.de/tecnologia/

Robles, D. (2019). *investigacioncientifica*. Obtenido de www,investigacioncientifica.org: https://investigacioncientifica.org/tipos-de-metodos-de-investigacion/

Rodríguez, G. G. (Febrero de 1996). *Metodología de la Investigación cualitativa.* España : Málaga Aljibe. Obtenido de metodelainv.: http://metodelainv.blogspot.es/

Sampieri, H. (1997). *josetavarez.* Obtenido de www.josetavarez.net: https://josetavarez.net/Compendio-Metodologia-de-la-Investigacion.pdf

Velasco, W. V. (septiembre de 2008). *scielo.org*. Obtenido de scielo.org: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2008000100008

IX. ESQUEMA PRELIMINAR DE CONTENIDO DEL PROYECTO DE GRADO

INDICE

DEDICATORIA

AGRADECIMIENTOS

INTRODUCCIÓN

CAPITULO I: ASPECTOS INTRODUCTORIOS DEL PROYECTO

1.1 Selección del tema

1.2 Planteamiento del problema

1.3 Justificación

1.4 Objetivos

1.4.1 General

1.4.2 Específicos

1.5 Alcance

1.6 Metodología de investigación

1.6.1 Métodos

1.6.2 Técnicas

CAPITULO II: EVALUACIÓN DEL ESTADO ACTUAL DE LOS RIESGOS TECNOLÓGICOS EN LA ZONA FRANCA.

2.1 Entendimiento Ambiente de TI

2.1.1 Infraestructura de TI

2.1.1.1 Sistemas de Información

2.1.1.2 Procesamiento y Almacenamiento

2.1.1.3 Telecomunicaciones

2.1.1.4 Red y Plataformas

2.1.1.5 Sistemas de Gestión de Bases de Datos

2.1.1.6 Emails

2.2 Desarrollo y cambio a Sistemas

2.2.1 Solicitud de cambios

2.2.2 Metodología de desarrollo

2.2.3 Control de versiones

2.2.4 Pruebas y aceptación de los cambios

2.2.5 Pase de los cambios a producción

2.3 Gobierno de TI

2.3.1 Estructura Organizacional

2.3.2 Políticas y Procedimientos

2.3.3 Gestión de Proyectos

2.3.4 Gestión Presupuestaria

2.3.5 Inventario de Recursos HW y SW

2.3.6 Gestión de relación con Terceros

2.4 Operaciones de TI

2.4.1 Respaldo de datos y sistemas

2.4.2 Plan de Recuperación ante Desastres

2.4.3 Monitoreo de Recursos

2.4.3 Soporte a Usuarios

2.5 Seguridad en base a la tecnología

2.5.1 Seguridad Física

2.5.2 Controles Ambientales

2.5.3 Seguridad Lógica

2.5.4 Autenticación (Red y Sistema)

2.5.5 Protección Código Malicioso

2.5.6 Seguridad Perimetral

2.5.7 Ciberseguridad

CAPITULO III: ANALISIS Y EVALUACION DE RIEGOS

3.1 Criterios para determinar la probabilidad

3.2 Criterios para determinar el impacto

3.3 Criterios para determinar el nivel de riesgo

3.4 Análisis de Riesgo

3.4.1 Identificación de Riesgos

3.4.2 Estimación de Riegos

3.5 Evolución de Riesgos

3.6 Matriz de riesgo

CAPITULO IV: PROPUESTA DE MEJORA EN LOS PROCESOS DE TECNOLOGÍA EN LA ZONA FRANCA.

4.1 Resumen Ejecutivo

4.2 Informe de Observación, riesgos y recomendaciones

4.3 Matriz de Riesgos Proyectados

BIBLIOGRAFIA.