CARRERA DE ANÁLISIS DE SISTEMAS

TEMA:

ESTUDIO DE VULNERABILIDADES Y SEGURIDADES DE LA RED DE LA INDUSTRIA REFEREE CIA. LTDA

AUTORES:

ALVARADO ALVARADO ÁNGEL ALBERTO

QUINTUÑA MORA CINTHYA SILVANA

TRABAJO DE TITULACIÓN PRECIO A LA OBTENCIÓN DEL TÍTULO DE:

TECNÓLOGO EN ANALISIS DE SISTEMAS

TUTOR:

MG. GALO HURTADO

CUENCA-ECUADOR 2019

CARRERA DE ANALISIS DE SISTEMAS

COMITÉ TÉCNICO MULTIDISCIPLINARIO

Certificación de Aprobación del Trabajo de Titulación

Damos fe que el trabajo desarrollado por los estudiantes: **QUINTUÑA MORA CINTHYA SILVANA** y **ALVARADO ALVARADO ÁNGEL ALBERTO** con el título: **"ESTUDIO DE VULNERABILIDADES Y SEGURIDADES DE LA RED DE LA INDUSTRIA REFEREE CIA. LTDA"** cumple con las exigencias metodológicas y técnicas.

Por lo antes mencionado, los TUTORES asignados del COMITÉ TÉCNICO MULTIDISCIPLINARIO resuelve **APROBAR** el Trabajo de Titulación.

Atentamente,

Mgs. Galo Hurtado Crespo.

Ing. Max Zuñiga López

Ing. Juan Pérez Pérez.

Mgs. Juan Hurtado Ortiz.

INSTITUTO SUPERIOR TECNOLÓGICO SUDAMERICANO
COORDINADOR DE CARRERA
DESARROLLO DE SOFTWARE

INSTITUTO DE TECNOLOGIAS SUDAMERICANO

www.sudamericano.edu.ec

DECLARACIÓN DE AUTORÍA DEL TRABAJO

Yo, **QUINTUÑA MORA CINTHYA SILVANA**, estudiante del **Instituto Tecnológico Superior Particular Sudamericano** de la ciudad de Cuenca - Ecuador, que cursó la Tecnología en **ANÁLISIS DE SISTEMAS,** declaro en forma libre y voluntaria que la presente investigación que versa sobre **"ESTUDIO DE VULNERABILIDADES Y SEGURIDADES DE LA RED DE LA INDUSTRIA REFEREE CIA. LTDA."** así como las expresiones vertidas en la misma, son autoría de la compareciente, quien ha realizado en base a recopilación bibliográfica, consultas de internet y consultas de campo.

En consecuencia, asumo la responsabilidad de la originalidad de la misma y el cuidado al remitirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto.

Atentamente,

QUINTUÑA MORA CINTHYA SILVANA

Cédula: 010483115-1

DECLARACIÓN DE AUTORÍA DEL TRABAJO

Yo, **ALVARADO ALVARADO ÁNGEL ALBERTO**, estudiante del **Instituto Tecnológico Superior Particular Sudamericano** de la ciudad de Cuenca - Ecuador, que cursó la Tecnología en **ANÁLISIS DE SISTEMAS,** declaro en forma libre y voluntaria que la presente investigación que versa sobre **"ESTUDIO DE VULNERABILIDADES Y SEGURIDADES DE LA RED DE LA INDUSTRIA REFEREE CIA. LTDA."** así como las expresiones vertidas en la misma, son autoría de la compareciente, quien ha realizado en base a recopilación bibliográfica, consultas de internet y consultas de campo.

En consecuencia, asumo la responsabilidad de la originalidad de la misma y el cuidado al remitirme a las fuentes bibliográficas respectivas para fundamentar el contenido expuesto.

Atentamente,

Angel Alvarado

ALVARADO ALVARADO ÁNGEL ALBERTO

Cédula: 0107428492

RESUMEN

La presente tesis realiza el análisis y la evaluación de activos de información de una empresa, basándose en la Metodología Octave-S diseñada para PYMES y que cuenten con 100 empleados o menos. Así mismo hace énfasis en la necesidad de contar con un plan de buenas prácticas como medida para alcanzar los objetivos establecidos y resguardar su información para evitar pérdidas económicas.

Esta metodología fue empleada para mostrar que en la empresa existen activos de información bastante vulnerable desde el hardware, hasta el software y que se debe tomar decisiones para su seguridad en cada departamento que maneje la información valiosa para la empresa.

El documento presentado, nos plantea la problemática, la justificación, el objetivo general y los objetivos específicos. El primer capítulo presenta el marco teórico para orientarnos hacia el trabajo que se realizara y en que se basó para hacerlo. El segundo capítulo permite conocer acerca de la Metodología Octave-S que fue utilizada para el análisis de riesgos dentro de la Industria Referee. El capítulo tres nos sitúa en el estado actual de la empresa, desarrollando así la Metodología Octave-S implementada para el estudio de las vulnerabilidades de la empresa, mediante cuadros y tablas que exponen porcentajes de las seguridades de la información. En el cuarto capítulo, basándose en los resultados obtenidos mediante el análisis anterior, se desarrolló un Plan De Buenas Prácticas que servirá de apoyo dentro la empresa para mantener seguros sus datos.

Se realiza de la misma manera una proforma para que la empresa se oriente en precios y las necesidades dentro de sus áreas de trabajo, para implementar las soluciones. Se redactan las conclusiones de la tesis desarrollada y se enuncian las recomendaciones finales.

ABSTRACT

This thesis carries out the analysis and evaluation of information assets of a company, based on the Octave-S Methodology designed for PYMES and with 100 employees or less. It also emphasizes the need for a good practice plan as a measure to achieve the established objectives and safeguard your information to avoid economic losses.

This methodology was used to show that in the company there are quite vulnerable information assets from the hardware, to the software and that decisions must be made for your security in each department that handles the valuable information for the company.

The document presented, presents the problem, the justification, the general objective and the specific objectives. The first chapter presents the theoretical framework to guide us towards the work that will be done and on which it was based to do it. The second chapter allows to know about the Octave-S Methodology that was used for risk analysis within the Referee Industry. Chapter three puts us in the current state of the company, thus developing the Octave-S Methodology implemented for the study of the vulnerabilities of the company, through tables and tables that show percentages of information security. In the fourth chapter, based on the results obtained through the previous analysis, a Good Practices Plan was developed that will support the company to keep their data safe.

A proforma is carried out in the same way for the company to focus on prices and needs within its work areas, to implement the solutions. The conclusions of the thesis developed are written and the final recommendations are stated.

PALABRAS CLAVES

Octave-S

PYMES

Hardware

Software

Vulnerabilidades

Activos de Información

C.I.D (Confidencialidad, Integridad, Disponibilidad)

KEYWORDS

Octave-S

PYMES

Hardware

Software

Vulnerabilities

Information Assets

C.I.A (Confidentiality, Integrity, Availability)

AGRADECIMIENTOS

Agradezco primeramente a Dios por la vida y por sembrar en mi corazón la vocación de estudio, permitiéndome alcanzar una meta más en mi vida; igual forma a mis padres y hermanos por ser los pilares fundamentales de apoyo y amor incondicional; al Instituto Sudamericano y a mis maestros que me abrieron las puertas y transmitieron su conocimiento para alcanzar mis objetivos planteados; y finalmente a mis amigos que estuvieron conmigo en las buenas y en las malas durante todo este proceso educativo.

Ángel Alberto Alvarado Alvarado

DEDICATORIA

Siempre ha sido mi inspiración, mi motivación y sobretodo mi fortaleza, a pesar de las grandes bendiciones que Dios me ha brindado; tu eres la mejor de ellas, a pesar de los problemas y las circunstancias que la vida te puso, siempre estuviste luchando como una gran guerrera; aunque pasaste años sola nunca miraste hacia abajo, con tu sonrisa y tus fuerzas motivabas mi día a día; sacabas fuerzas donde creía que ya era imposible ponerse de pie, pero tú estabas ahí llena de vida y esperanza, siempre serás mi guerrera y por la que la vida diera; te amo mamá “Luz”.

Ángel Alberto Alvarado Alvarado

AGRADECIMIENTOS

Le doy gracias a Dios y la Virgen que me permitieron llegar hasta este punto en mi vida, donde junto a mis padres Segundo y Fanny me han guiado por el camino correcto, a mis hermanos que han sido el pilar fundamental en donde me he apoyado este tiempo. Al Instituto Tecnológico Sudamericano que han generado en mí el conocimiento durante mi carrera, a nuestro tutor Mg. Galo Hurtado quien nos guío para el desarrollo de nuestra tesis, a mis compañeros, y a mis amigos quienes me apoyaron para llegar a este fin.

Cinthya Silvana Quintuña Mora

DEDICATORIA

Este logro se lo dedico a mis padres, que a pesar de lo difícil que ha sido mi camino nunca han soltado mi mano y han caminado a mi lado sin dejarme caer. A mis hermanos que con su alegría y amor me han hecho saber que siempre contaré con ellos en cualquier dificultad. Para mis ángeles en el cielo Joaquín, Julio y Guillermo que han cuidado de mí. A mis amigos Anita, Gabriela, Bryan y Andrés que con sus consejos me he levantado a seguir con ánimo y fuerza.

Cinthya Silvana Quintuña Mora

Índice

INTRODUCCION 16
OBJETIVOS 17
OBJETIVO GENERAL: 17
OBJETIVOS ESPECIFICOS 17
PROBLEMÁTICA 18
JUSTIFICACION 19
CAPITULO 1: SEGURIDADES 20
1.1. SEGURIDAD DE LA INFORMACION 20
1.1.1. Definición 20
1.1.2. Aspectos importantes en la seguridad informática 20
1.1.3. Seguridad Interna 20
1.1.4. Seguridad Física 21
1.1.5. Seguridad Lógica 22
1.2. NATURALEZA DE LAS AMENAZAS DE LA SEGURIDAD DE LA INFORMACIÓN. 22
1.3. TIPOS DE ATAQUES INFORMATICOS 22
1.3.1. CIBERSEGURIDAD CON DELOITTE 23
1.3.2. ATAQUES A EMPRESAS EN ECUADOR 24
1.4. ESTRUCTURA DE LA RED 24
1.4.1. ELEMENTOS DE UNA RED 25
1.4.1.1. MODELO OSI 25
1.5. VULNERABILIDADES EN SISTEMAS DE INFORMACION 26
1.5.1. FACTOR HUMANO 26
1.6. HERRAMIENTAS PARA ANALISIS DE VULNERABILIDADES Y RIESGOS 27
1.6.1. METODOLOGIAS A UTILIZAR EN EL TEST DE PENETRACION 27
1.6.1.1. ISSAF 27
1.6.1.2. OTP (OWASP Testing Project) 27
1.6.1.3. OSSTMM 29
1.6.2. HERRAMIENTAS PARA EL ANALISIS DE RIESGOS EN LA RED 29
1.6.2.1. MAGERIT 29
1.6.2.2. OCTAVE 30
1.7. TABLA COMPARATIVA DE LAS METODOLOGÍAS 31
CAPITULO 2: 32
METODOLOGIA DE ANALISIS DE RIESGOS OCTAVE-S 32
CAPITULO 3 34

SITUACION ACTUAL DE LA EMPRESA 34
3.1. DESARROLLO DE LA METODOLOGÍA OCTAVE-S 36
3.1.1. FASE 1: CONSTRUIR PERFILES DE AMENAZA BASADA EN ACTIVOS 37
3.1.2. PROCESO S1: IDENTIFICAR LA INFORMACIÓN ORGANIZACIONAL 38
3.1.2.1. ACTIVIDAD S1.1: ESTABLECER LOS CRITERIOS DE EVALUACIÓN 38
3.1.2.2. ESTADO DE LA EMPRESA CON LOS CRITERIOS DE EVALUACIÓN 47
3.1.2.3. ACTIVIDAD S1.2: IDENTIFICAR ACTIVOS 50
3.1.2.4. ACTIVIDAD S1.3: EVALUAR LAS PRÁCTICAS DE SEGURIDAD 51
3.1.3. PROCESO S2: CREAR PERFILES DE AMENAZA 53
3.1.3.1. ACTIVIDAD S2.1: SELECCIONAR ACTIVOS CRÍTICOS 54
3.1.3.2. ACTIVIDAD S2.2: IDENTIFICAR REQUERIMIENTOS DE SEGURIDAD 55
3.1.3.3. ACTIVIDAD S2.3: IDENTIFICAR AMENAZAS A LOS ACTIVOS 56
3.1.4. FASE 2: IDENTIFICAR VULNERABILIDADES EN LA INFRAESTRUCTURA 57
3.1.5. PROCESO S3: EXAMINAR LA INFRAESTRUCTURA COMPUTACIONAL CON LOS ACTIVOS 58
3.1.5.1. ACTIVIDAD S3.1: EXAMINAR RUTAS DE ACCESO 58
3.1.5.2. ACTIVIDAD S3.2: ANALIZAR PROCESOS RELACIONADOS CON LA TECNOLOGÍA 59
3.1.6. FASE 3: DESARROLLO DE PLANES Y ESTRATEGIAS DE SEGURIDAD 60
3.1.7. PROCESO S4: IDENTIFICAR Y ANALIZAR LOS RIESGOS 61
3.1.7.1. ACTIVIDAD S4.1: EVALUAR EL IMPACTO DE LAS AMENAZAS 61
3.1.7.2. ACTIVIDAD S4.2: ESTABLECER CRITERIOS DE EVALUACIÓN PROBABILÍSTICA 61
3.1.7.3. ACTIVIDAD S4.3: EVALUAR PROBABILIDADES DE AMENAZAS 62
3.1.8. PROCESO S5: DESARROLLAR ESTRATEGIAS DE PROTECCIÓN Y PLANES DE MITIGACIÓN 63
3.1.8.1. ACTIVIDAD S5.1: DESCRIBIR LAS ESTRATEGIAS DE PROTECCIÓN ACTUALES 64
3.1.8.2. ACTIVIDAD S5.2: SELECCIONAR APROXIMIDADES DE MITIGACIÓN 65
3.1.8.3. ACTIVIDAD S5.3: DESARROLLAR PLANES DE MITIGACIÓN DE RIESGOS 66
3.1.8.4. ACTIVIDAD S5.4: IDENTIFICAR CAMBIOS EN LAS EXTRATEGIAS DE PROTECCIÓN 67
3.1.8.5. ACTIVIDAD S5.5: IDENTIFICAR LOS SIGUIENTES PASOS 67
CAPITULO 4 69
APLICACION DEL PLAN DE BUENAS PRÁCTICAS 69
PLAN DE BUENAS PRACTICAS EN EL MANEJO DE SEGURIDAD DE LA INFORMACION 69
INTRODUCCION 69
POLITICAS DE SEGURIDAD DE LA INFORMACION 70
MANEJO APROPIADO DE CONTRASEÑAS 70
MANEJO APROPIADO DEL ANTIVIRUS 71
MANEJO DE CUENTAS DEL SISTEMA 71

MANEJO DE ACCESO A INTERNET 71
MANEJO DE CORREO ELECTRONICO 72
MANEJO DE REDES SOCIALES 72
MANEJO DE SOFTWARE (SISTEMA, PAGINA WEB, S.O, SERVIDOR) 73
CRONOGRAMA 75
CONCLUSIONES 76
RECOMENDACIONES 77
BIBLIOGRAFÍA 78

Índice de Figuras

Figura 1 Diseño de Fábrica y Almacenes Referee 18
Figura 2 Modelo OSI 25
Figura 3 Fases de Evaluación OCTAVE-S 33
Figura 4 Red de la Fábrica de la Industria Referee 34
Figura 5 Red de Almacén 1 de la Industria Referee 34
Figura 6 Red de Almacén 2 de la Industria Referee 35
Figura 7 Red Consolidada de la Industria Referee 35
Figura 8 Fases de Desarrollo de OCTAVE-S **Fuente:** (Autores, 2019) 36
Figura 9 Valoración de Criterios 38
Figura 10 Proceso de Ventas 39
Figura 11 Proceso de Pedidos 40
Figura 12 Procesos de Ventas Web 41
Figura 13 Procesos de Diseño de Pedido 42
Figura 14 Proceso de Diseño Colección 43
Figura 15 Procesos de Producción y Pedido 44
Figura 16 Procesos de Bodega 45
Figura 17 Procesos de Finanzas 46
Figura 18 Proceso de Gerencia 47
Figura 19 Cuadro Estadístico de Impacto 49
Figura 20 Cuadro Estadístico de Prácticas de Seguridad 53
Figura 21 Cuadro Estadístico de Amenazas 63
Figura 22 Cronograma de actividades para el desarrollo del Proyecto de Tesis 75

Índice de Tablas

Tabla 1 Naturaleza de Amenazas de la Seguridad de Información 22
Tabla 2 Porcentaje de Aplicación de Seguridades en Empresas 24
Tabla 3 Proceso OTP para Seguridad de Aplicaciones Web 28
Tabla 4 Fases de Evaluación de Riesgos de Octave 30
Tabla 5 Tabla Comparativa de Metodologías 31
Tabla 6 Registro de Equipo de Análisis 37
Tabla 7 Tabla de procesos, actividades y pasos de Fase 1 de OCTAVE-S 37
Tabla 8 Criterios de Evaluación en referencia a Ventas 39
Tabla 9 Criterios de Evaluación en referencia al proceso de Pedidos 40
Tabla 10 Criterios de Evaluación en referencia al área de Ventas Web 41
Tabla 11 Criterios de Evaluación en referencia al área de Diseño 42
Tabla 12 Criterios de Evaluación en Referencia al área de Diseño 43
Tabla 13 Criterios de Evaluación en referencia al área de Producción 44
Tabla 14 Criterios de Evaluación en referencia al área de Bodega 45
Tabla 15 Criterios de Evaluación en referencia al área de Finanzas 46
Tabla 16 Criterios de Evaluación en referencia al área de Gerencia 47
Tabla 17 Estado Actual Departamentos y Activos **Fuente:** (Autores, 2019) 48
Tabla 18 Criterios de Evaluación en referencia al estado actual de la empresa 49
Tabla 19 Tabla de Activos de la Empresa 50
Tabla 20 Tablas de Prácticas de Evaluación de la Organización **Fuente:** (Autores, 2019) 53
Tabla 21 Tabla de Activos Críticos de la Organización 54
Tabla 22 Tablas de Requerimiento de seguridad 55
Tabla 23 Tabla de Amenazas de Activos 56
Tabla 24 Tabla de procesos, actividades y pasos de la Fase 2 de OCTAVE-S 57
Tabla 25 Tablas de Rutas de Acceso 58
Tabla 26 Tabla de Procesos Relacionados con la Tecnología 59
Tabla 27 Tabla de procesos, actividades y pasos de la Fase 3 de OCTAVE-S **Fuente** (Autores, 2019) 60
Tabla 28 Tabla de Valoración de Criterios de Evaluación 62
Tabla 29 Criterios de Evaluación en referencia al estado actual de la empresa 63
Tabla 30 Prácticas de Seguridad 64
Tabla 31 Prácticas de Seguridad de la Organización 65
Tabla 32 Prácticas de Seguridad para la Organización 66
Tabla 33 Clasificación de Caracteres para Contraseñas 70
Tabla 34 Criterios de Evaluación Sin Implementación 73
Tabla 35 Criterios de Evaluación con Capacitación 74
Tabla 36 Criterios de Evaluación con Implementación de Plan de Buenas Prácticas 74
Tabla 37 Proforma 1 Desarrollo y Capacitación 83
Tabla 38 Proforma 2 Desarrollo, Capacitación e Implementación Plan de Buenas Prácticas 84

INTRODUCCION

La presente investigación se refiere al Estudio de la Vulnerabilidades y Seguridades de la Red de la Industria Referee CIA. LTDA. en donde mediante la implementación de la Metodología Octave-S se llegó a conocer los riesgos a los que la empresa está expuesta tanto en sus sistemas como en su infraestructura por la no inversión en seguridad de la información

La característica principal de este tipo de análisis es que nos permite conocer mediante rangos de porcentajes, cuan expuesta se encuentra la información de la empresa debido al no conocimiento de la importancia de resguardar los activos de información.

De la misma manera los daños que ocasionarían si se llegan a materializar, puesto que se realiza el estudio de las actividades que realiza cada uno de los departamentos de la empresa. Se da a conocer el tipo de amenazas a los que los departamentos estudiados pueden ser expuestos.

Para analizar esta problemática es necesario mencionar las causas que lo provocan. Una de ellas es la no inversión en seguridad en la red de la empresa, puesto que no demuestra una problemática para los ojos de los usuarios. Se entiende por no inversión a que no se desea realizar gastos económicos para la aplicación de algún activo que represente la capacidad de obtener ganancias o pérdidas en un futuro.

De esta manera, se realiza el balance de las amenazas que para su solución. Finalmente se desarrolla un plan de buenas prácticas para los usuarios de los equipos, sistemas e información de la empresa, generando un costo aproximado de la implementación interna del proyecto.

OBJETIVOS

OBJETIVO GENERAL:

Analizar las vulnerabilidades y seguridades de la red LAN de la Industria Referee Cía. Ltda., aplicando la metodología OCTAVE para identificar las amenazas, probabilidad de materialización y el impacto hacia los activos de la red

OBJETIVOS ESPECIFICOS

- Valorar las amenazas que pueden surgir en la red de la Industria Referee
- Determinar el grado de exposición a riesgos con un levantamiento de activos vulnerables de la red.
- Evaluar los riegos que se generan en la red de la Industria Referee
- Generar un plan de buenas prácticas para mitigar posibles riesgos y reducir la probabilidad de que se materialice, previniendo desde el interior de la organización.

PROBLEMÁTICA

La Industria Referee Cía. Ltda. cuenta con una fábrica y dos almacenes ubicados en la ciudad de Cuenca en la provincia del Azuay, los cuales se encuentran muy bien distribuidos en puntos clave en la misma ciudad. La Industria Referee Cía. Ltda. está conectada entre departamentos, por medio de una red que comunica a los empleados y que se encuentra ubicada en la fábrica y almacenes contando con 14 Pc en su totalidad, de esta manera debido a la distancia existente en los diferentes departamentos de la Industria Referee, se presenta un problema en la velocidad de la transmisión de información en la red de la empresa, así mismo como peligros a los que se encuentra expuesta y la posible vulneración en su información por no contar con las seguridades requeridas.

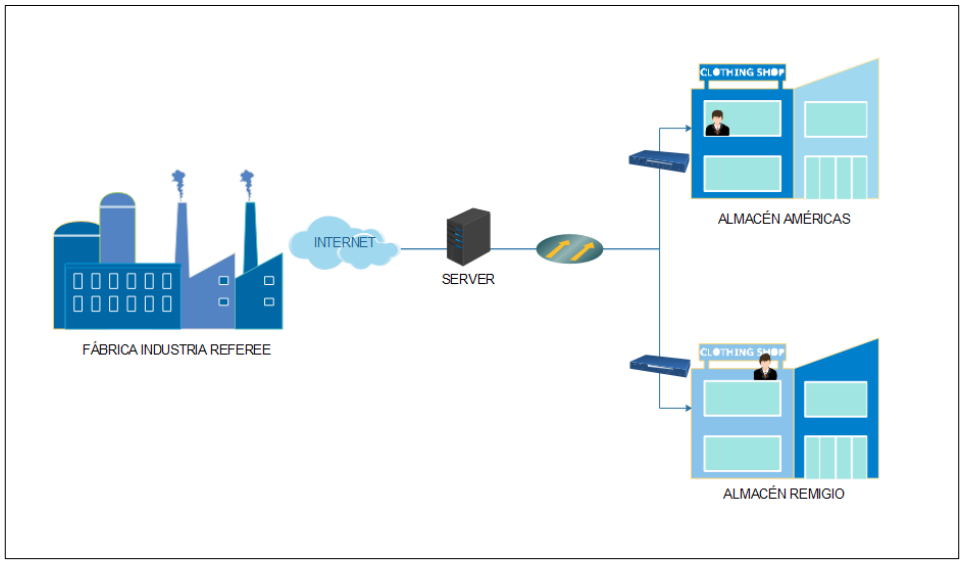


Figura 1 Diseño de Fábrica y Almacenes Referee
Fuente: (Autores, 2019)

Representación de la comunicación del Internet y de la red de la Industria Referee Cía. Ltda. para el acceso de la información en los almacenes ubicados en la ciudad de Cuenca

JUSTIFICACION

Las seguridades en la red se convierten en necesidades cada vez más requeridas por las organizaciones actuales, que desean proteger la información de su empresa y así evitar generar pérdidas económicas. Contrariamente de que la seguridad de la información es un tema bastante relevante en una organización para evitar pérdidas, en la actualidad, en la ciudad de Cuenca no se establece como una prioridad aplicar la seguridad en su sistema de trabajo, ya que muchas de las empresas no deciden invertir en la seguridad de su información y no se le da la importancia necesaria.

La presente investigación se realiza con el propósito de brindar seguridad a las vulnerabilidades de la red de las organizaciones, e incluir más empresas a las que brindar mencionado servicio, pero enfocándonos en la Industria Referee Cía. Ltda. su red interna de trabajo y de proporcionar las soluciones de seguridad necesarias, utilizando la metodología Octave-S.

Octave-S es un proceso más reducido, es una metodología que fue desarrollada para ser implementada en organizaciones con menos o hasta de 100 empleados. El objetivo es facilitar la evaluación de riesgos en una organización, y que, mediante el análisis de vulnerabilidades realizadas en la empresa, ofrecer la implementación de las seguridades requeridas en la red de la Industria Referee para el buen manejo de la información en la empresa.

CAPITULO 1: SEGURIDADES

1.1. SEGURIDAD DE LA INFORMACION

1.1.1. Definición

En el estudio realizado por (Oficina Nacional de Gobierno Electrónico e Informática del Perú, 2018), define a la seguridad de la información como un conjunto o como la agrupación de medidas preventivas y que producen reacciones de las organizaciones debido a que nos permite resguardar y proteger la información buscando mantener la C.I.D de la organización.

1.1.2. Aspectos importantes en la seguridad informática

Se debe considerar que existen algunas características importantes al momento de realizar un análisis de vulnerabilidades en una red y es la C.I.D

- *Confidencialidad:* su trabajo es el mantener los datos requeridos de los usuarios facultados, de esta manera se permite asegurar que los mismos individuos autorizados sean quienes accedan a la información de la empresa de manera segura para su manipulación.
- *Integridad:* su fin es la correctitud y completitud de la información que está almacenada ya que se debe garantizar que no se realicen cambios, que no se generen pérdidas y que los datos sean consistentes.
- *Disponibilidad:* implica que la información debe ser accesible para los usuarios que son autorizados en el tiempo establecido y cumplirlo en ese rango para su paso hacia la información.

1.1.3. Seguridad Interna

La seguridad interna, surge como la necesidad de establecer en una organización protecciones a nivel de la red local, para resguardar la información de acciones voluntarias o no voluntarias de los mismos usuarios o de un tercero.

La facultad de (Ingenieria de Sistemas y Automatica ; Universidad de Oviedo, 2017) recalcó que los ataques a la seguridad de la información pueden realizarse por los mismos empleados de la empresa, también por intrusos que acceden a la red de manera indebida. Al ocasionarse uno de estos dos últimos, por lo general se crea una

suplantación de usuarios legítimos de la red, ingresan por algún error de programación o algún problema de seguridad de la red. Para evitar estos inconvenientes se pueden implantar técnicas como:

- *Compartamentalización*: Los repetidores y conmutadores consiguen que el tráfico de tramas de unas zonas de la red no pueda ser visto por los sistemas conectados en otras zonas.
- *Monitorización:* Es uno de los procesos para prevenir un ataque, la red puede ser monitoreada por aplicaciones que aferrarán paquetes que se encuentran circulando a través de una red informática instalado en un sistema de la red.
- *Seguridad en Servidores:* Al instalarse algún servicio en una máquina o en un servidor, se tiende a considerar que requiere de seguridad para todos los servicios que puedan ser accedidos de máquinas propias de red o servicios ofrecidos a otras redes.

1.1.4. Seguridad Física

La seguridad física mediante el concepto de (Aguilera, 2017), dispone que es la protección del ambiente externo en donde permanece la información relevante que se mantiene resguardada para ser protegida, colocar a consideración que la información corresponde, en la mayoría de los casos a hardware, software, e instalaciones en los que se protege el activo de información.

Según (Alegre & Cervigón, Seguridad Informática Ed.11, 2017), las amenazas pueden presentarse de manera accidental o voluntaria por parte del humano, o a la misma vez ser causada por desastres naturales.

- *Accidentales:* son las amenazas que se realizan sin tener el conocimiento que sucederán como un olvido de clave, un borrado accidental, etc.
- *Voluntarios:* suceden al momento en que la persona es consciente de que se puede generar un daño o perdida de información, como el robo de las contraseñas, borrado de información, robo de datos, etc.
- *Naturales:* son amenazas que en la mayoría de los casos se presentan al existir fenómenos naturales que no se pueden controlar, como deslave, un incendio, una inundación, etc.

1.1.5. Seguridad Lógica

La seguridad lógica es la que se encargará de asegurar el software de un sistema informático, esto significa los programas y datos en un hardware. Para (Alegre & Cervigón, Seguridad Informática Ed.11, 2017), la seguridad informática es la encargada del control de accesos a un sistema informático y que igualmente se acceda correctamente y por personas autorizadas usando la web, VPN, conexiones remotas, etc.

1.2. NATURALEZA DE LAS AMENAZAS DE LA SEGURIDAD DE LA INFORMACIÓN.

La asociación de amenazas que se presentan teniendo en cuenta el factor de seguridad que se verían comprometidas son:

Tabla 1 Naturaleza de Amenazas de la Seguridad de Información
Fuente: *(Autores, 2019)*

AMENAZA	DESCRIPCION
Intercepción	Se identifica como el acceso no autorizado por terceras personas
Modificación	Acceso no autorizado que genera cambios en la información.
Interrupción	Genera que la información enviada se pierda, no esté disponible
Fabricación	Se consigue generar información idéntica a la original pero con modificaciones en su contenido.

Da a conocer las distintas naturalezas de amenazas en un sistema y cuál es el objetivo que realizarían en el software cada una de ellas para generar daños en el mismo.

1.3. TIPOS DE ATAQUES INFORMATICOS

Para (ACISSI, 2018) los ataques informáticos siguen un esquema que le permiten el éxito al momento de la intrusión en un sistema. Un ataque informático consiste en el aprovechar una debilidad o falla en el software, hardware, e incluso a quienes son los que forman parte de un entorno informático.

- *Ataques Pasivos:* son ataques que monitorean la transmisión de datos.

- *Ataques Activos:* su objetivo es la creación de un flujo de datos falsos o la modificación de los mismos datos.

1.3.1. CIBERSEGURIDAD CON DELOITTE

(Deloitte, 2018) realizó una encuesta sobre las Tendencias de Ciber Riegos y Seguridad de la Información en Ecuador. La firma Deloitte en su estudio logra mostrar a las organizaciones en Ecuador introducidas en el desarrollo notorio de negocios digitales, que están más expuestos a las amenazas, así se identificó las principales tendencias de ciber riesgos y seguridad de la información.

Se efectuó un estudio detallado de las industrias y sectores de varios servicios dados en Ecuador, mediante un proceso de recopilación de información dado en un cuestionario de 41 preguntas centradas en las prácticas de Ciberseguridad que fue dirigido a ejecutivos a cargo de la gestión de ciber riesgos y seguridad de la información

Por los datos recopilados por la firma Deloitte en 2018, entre los ataques que pueden afectar la información interna de las organizaciones, y se encuentran los producidos por personas internas o externas de la organización como son los siguientes:

- Vulnerabilidad en el software
- Infección por malware
- Fuga de información
- Ingeniería social

Según (Deloitte, 2018) la tendencia que fue obtenida es de que 4 de cada 10 de las organizaciones han sufrido un incidente de ciberseguridad en los últimos 24 meses, basados en un estudio del año 2018, la principal barrera en el año 2019 que enfrentan las organizaciones es la falta de presupuesto y recursos suficientes para la gestión en seguridad. También nos muestran el resultado de como 1 de cada 10 organizaciones cuentan con una correcta seguridad para dar recursos y administrar las iniciativas de ciberseguridad, contando con una alineación muy estratégica, y 5 de cada 10 organizaciones se han visto preocupadas en brindar una correcta concientización en ciberseguridad a los empleados, pero de igual manera las personas siguen siendo la parte más vulnerable en el proceso de protección de la información empresarial

1.3.2. ATAQUES A EMPRESAS EN ECUADOR

Según el estudio realizado en los últimos años en Ecuador, se demuestra que los ataques informáticos realizados a micro, pequeñas, medianas y grandes empresas ha ido en aumento, pues no se cuenta con un control en la seguridad adecuada de navegación en su red y desde el ISP correspondiente.

Mediante en la investigación de (MINTEL (Ministerio de Telecomunicaciones y Sociedad de la Información), 2018) del Libro Blanco de la Seguridad de la Información y Comunicación en Ecuador, las empresas amparan las tecnologías de una manera creciente. Con el propósito de medir el grado de acogimiento de tecnologías. El INEC (Instituto Nacional de Estadísticas y Censos) realizó una encuesta a los diferentes sectores productivos como los de manufactura, minería, comercio y servicios donde en su totalidad se evaluó a 3245 empresas, para así obtener los siguientes resultados: el 39% responde que: utilizó TIC en control de pedidos, 41% lo hizo en gestión de recursos humanos y en un 48% en su gestión financiera con apoyo de las TIC. El 99,6% tiene acceso a Internet y un 90% de todas las empresas, usó correo electrónico, quedando demostrado con las cifras resultantes la necesidad de inversión y uso de un departamento de TIC como un sustento en sus negocios para prepararse para un Transformación Digital.

Tabla 2 Porcentaje de Aplicación de Seguridades en Empresas
Fuente: *(Autores, 2019)*

AÑO	MICROEMPRESA	PEQUEÑA	MEDIANA	GRANDE
2012-2016	3543	4325	845	277
	39,41%	48,11%	9,4%	3,08%

Estudio realizado por la firma Deloitte en Ecuador para los resultados de análisis de PYMES que aplicaron seguridad en su información de software con TIC.

1.4. ESTRUCTURA DE LA RED

Al realizar el estudio de la red en la Industria Referee se percató que su red interna LAN, genera una WAN que permite trabajar entre distintas edificaciones que la constituyen. Una red WAN se encuentran formada por interconexiones de otras redes en un área geográfica grande, empleando sistemas de telecomunicaciones por compañías externas

1.4.1. ELEMENTOS DE UNA RED

En los componentes de una red podremos diferenciar desde equipos de red y una subdivisión en equipos que se interconectan a un fragmento de las mismas, y de igual forma cableados y conectores.

1.4.1.1. MODELO OSI

El modelo OSI fue desarrollado por la ISO en 1984 (Tolosa, 2017). El estándar perseguía la meta de interconectar sistemas de procedencia distinta, que divide la complejidad de la comunicación en 7 capas que poseen un orden jerárquico.

Para (Castillo J. A., 2018) cada una de las 7 capas poseen sus funciones propias para alcanzar la intercomunicación de protocolos distintos. Así un modelo OSI puntualiza la funcionalidad para conseguir un estándar. Los niveles que integran un modelo OSI son:

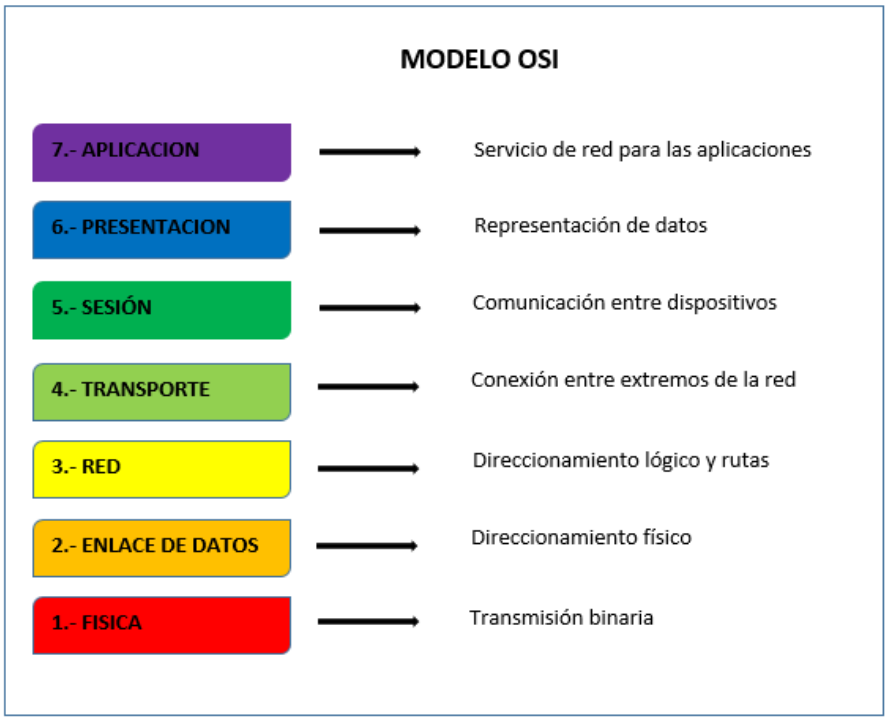


Figura 2 Modelo OSI
Fuente: (Autores, 2019)

Se trata de un modelo de referencia para los protocolos de red, su objetivo es la interconexión de redes en un modelo conformado por 7 capas o niveles de abstracción.

1.5. VULNERABILIDADES EN SISTEMAS DE INFORMACION

El objetivo de identificar las vulnerabilidades en sistemas de información es el poder educar a las organizaciones que hacen uso de las seguridades, para así de esta manera prevenir daños en sus sistemas o que los mismas sean vulnerados por medio de su red.

Para (Hernández & Mejia, 2017) entre los ataques más conocidos se encuentran

- *Inyección:* ocurren al momento en que los datos no confidenciales son enviados a un receptor como segmento de un comando o consulta, ya que trata de acceder a datos no autorizados con comandos perversos y así engañando al intérprete.
- *Secuencia de Comandos en Sitios Cruzados:* suceden cuando en una aplicación se toma datos no confidenciales, y se los transfiere a un navegador web sin una validación y codificación apropiada.
- *Configuración de Seguridad Incorrecta:* una buena seguridad requiere tener definidas e implementadas configuraciones seguras para la aplicación, servidores, base de datos y plataformas, y estas configuraciones deben encontrarse definidas, implementadas y mantenidas.
- *Exposición de datos sensibles:* los datos sensibles merecen métodos de protección adicional como es el cifrado de datos, pues en la mayoría de aplicaciones web no se protege de manera adecuada números de tarjetas de crédito o credenciales que son datos muy sensibles.
- *Falsificación de Petición en Sitios Cruzados:* al presentarse un ataque de este tipo exige a la víctima autenticada en un navegador que pueda enviar una petición HTTP falsa, en esta petición debe incluir la sesión de usuario y otra información de autenticación contenida automáticamente.

1.5.1. FACTOR HUMANO

El factor humano se presenta como uno de los pilares más importantes y valioso internamente en cualquier organización, pero al estar tan vinculado con todos los procesos, con los medios y los dispositivos de la empresa se convierten en un actor muy necesario. Sin duda al tener el conocimiento absoluto o mayor de la información de la empresa, este actor puede causar un gran impacto negativo, provocando u ocasionando daños o perjuicios, ya sea por la pérdida de la misma información, mal uso de sistemas, poca cultura de seguridad, etc.

Según (Echeverry, María, Sánchez, & Andrea, 2016) dice que: “Se recomienda que los usuarios finales tengan políticas diferentes, ya que son usuarios normales con una formación tecnológica distinta y representan el eslabón más débil de la cadena de seguridad”. Los usuarios son los más vulnerables, al ser interceptados es robada su información puesto que, al ser atacados inconscientemente a través de ingeniería social, que se basa en preguntas de una conversación normal se puede obtener información valiosa de la empresa.

1.6. HERRAMIENTAS PARA ANALISIS DE VULNERABILIDADES Y RIESGOS

1.6.1. METODOLOGIAS A UTILIZAR EN EL TEST DE PENETRACION

Podemos identificarlas como las siguientes

- ISSAF
- OTP
- OSSTMM

1.6.1.1. ISSAF

El ISSAF identificado en español como el Marco de Evaluación en Sistemas de Información de Seguridad por el estudio de la (Junta de Andalucía, 2017). Permite la clasificación de la información de evaluación de seguridad en varios dominios, esta herramienta ofrece medidas que permiten mostrar en escenarios reales condiciones de evaluaciones de seguridad, ya que se encuentra orientada a cubrir procedimientos de seguridad y obtener de la misma manera un panorama de las vulnerabilidades. Cuentan con criterios de evaluación y son:

- Descripción de los criterios de evaluación
- Puntos y objetos a cubrir
- Proceso de evaluación
- Informe de resultados
- Contramedidas y recomendaciones

1.6.1.2. OTP (OWASP Testing Project)

En el estudio realizado por la (Junta de Andalucía, 2017) define que su trabajo es realizar pruebas sobre aplicaciones web, el OWASP es en sí una referencia muy habitual para los ámbitos de seguridad. El OTP en general se enfoca en testear una aplicación web mediante los siguientes puntos

- Alcance de testeo
- Principios de testeo
- Técnicas de testeo
- Explicación sobre el framework de testeo de OWASP

Teniendo en consideración que la efectividad de un programa se da con el testeo de las aplicaciones web, se deben incluir elementos a testear como son usuarios, procesos y tecnologías. Existe un proceso diseñado para evaluar la seguridad de las aplicaciones web a lo largo de su vida. El proceso está basado en 5 pasos cada uno con diferentes especificaciones que se deben tener en consideraciones para el análisis de la seguridad de las aplicaciones web.

Tabla 3 Proceso OTP para Seguridad de Aplicaciones Web
Fuente: (Autores, 2019)

PROCESO
Paso 1 Antes de Comenzado el desarrollo
Paso 1A Revisión de Políticas y Estándares
Paso 1B Desarrollo de Criterio de Medidas y Métricas
Paso 2 Durante la definición
Paso 2A Revisión de requerimiento de Seguridad
Paso 2B Diseño de Revisión de Arquitectura
Paso 2C Creación y Revisión de modelos UML
Paso 2D Creación y Revisión de modelos de Amenazas
Paso 3 Durante el desarrollo
Paso 3A Tutorías de código
Paso 3B Revisión de Código
Paso 4 Durante el deployment
Paso 4A Testeo de Penetración sobre la Aplicación
Paso 4B Testeo sobre la Administración y Configuración
Paso 5 Operación y mantenimiento
Paso 5A Revisión Operacional
Paso 5B Conducción de chequeos periódicos
Paso 5C Verificación del control de cambio

Tabla de proceso de desarrollo por pasos de la metodología de análisis de red OTP en una organización

1.6.1.3. OSSTMM

En la (Junta de Andalucía, 2017) se define como el Manual de la Metodología Abierta de Testeo de Seguridad se ha convertido en una auténtica referencia para que las organizaciones y organismos desarrollen un testeo de calidad, ordenado y eficiente de la misma forma se subdivide en los aspectos considerables de los sistemas de información y enfatizan los siguientes aspectos:

- Seguridad de la Información
- Seguridad de los Procesos
- Seguridad en las Tecnologías de Internet
- Seguridad en las Comunicaciones
- Seguridad Inalámbrica
- Seguridad Física

La serie de actividades serán identificadas en el testeo especifico por áreas, sobre las que se comprobarán los detalles de seguridad, con esta metodología aumenta la calidad del desarrollo pues se basa en un esfuerzo para convertir lo predecible QUE probar, COMO hacerlo y CUANDO ejecutarlo. La metodología OSSTMM permite identificar de manera transparente el alcance de cada una de las acciones y así evitar inconvenientes.

1.6.2. HERRAMIENTAS PARA EL ANALISIS DE RIESGOS EN LA RED

Para realizar un análisis correcto de los riegos en la red se cuenta con varias herramientas de análisis como:

- MAGERIT
- OCTAVE

1.6.2.1. MAGERIT

Es el acrónimo de Metodología de Análisis y Gestión de Riesgo de Sistemas de la Información (Hurtado, 2017). Magerit fue creada en el año de 1997, siendo una metodología de análisis y gestión de riesgos de los sistemas de información, y en la actualidad ya se encuentra en su segunda versión, Magerit se basa en algunos parámetros en los que la presente metodología trabaja como:

a) Activos
b) Amenazas

c) Vulnerabilidades
d) Impacto
e) Riesgo
f) Contingencia

Para (Hurtado, 2017) el uso de la metodología genera beneficios en cantidades elevadas, de la misma manera día a día las vulnerabilidades son altas y así de la misma manera los atacantes incrementan. Magerit focaliza su meta en el análisis de los riesgos en los Sistemas de Seguridad. MAGERIT enfoca sus objetivos en 2 fases

1. El análisis de riesgo
2. La gestión de riesgo

1.6.2.2. OCTAVE

Octave se considera para (Gómez, Pérez, Donoso, & Herrera, 2017), es una metodología auto dirigida, la cual se centra para el estudio de riesgos de una organización, que igualmente estudia la infraestructura de la información. Se desarrolla por un equipo de análisis, que inicia a partir de la identificación de los activos de información que representan valor para la empresa. OCTAVE se encuentra organizado en tres fases que se subdividen en varios procesos

Tabla 4 Fases de Evaluación de Riesgos de Octave
Fuente (Autores, 2019)

FASES	DESCRIPCION
FASE 1	**Construir perfiles de amenazas basados en activos**
Proceso 1	Identificación de la información a nivel gerencial
Proceso 2	Identificación de la información a nivel operacional
Proceso 3	Identificación de la información al usuario final
Proceso 4	Consolidación de la información y creación de perfiles de amenazas
FASE 2	**Identificar los puntos vulnerables en la infraestructura**
Proceso 5	Identificación de componentes claves
Proceso 6	Evaluación de componentes seleccionados
FASE 3	**Desarrollo de planes y estrategias de seguridad**
Proceso 7	Análisis de riesgos
Proceso 8	Desarrollar estrategias de protección

Muestra las fases de evaluación de riesgos que utiliza la metodología OCTAVE para analizar los riesgos a los que está expuesta una organización y así mismo sobre su construcción de información.

1.7. TABLA COMPARATIVA DE LAS METODOLOGÍAS

Las diversas metodologías que han sido indagadas con anterioridad, permiten realizar un análisis y acciones de investigación técnica, con el fin de brindar la información sobre la calidad del software, comprobar seguridad y vulnerabilidades de un sistema, por lo cual (Belloso, 2017) da a conocer sobre las características principales y beneficios de cada metodología:

Tabla 5 Tabla Comparativa de Metodologías
Fuente: (Autores, 2019)

	ISSAF	OTP	OSSTMM
Estándar			✓
Framework	✓	✓	
Metodología	✓	✓	✓
Comunidad Activa		✓	✓
Manual o Recurso	✓		✓
Búsqueda de Vulnerabilidades	✓	✓	✓
Escaneo de Seguridad		✓	✓
Pruebas de Penetración	✓	✓	✓
Evaluación de Seguridad	✓	✓	✓
Auditoria de Seguridad	✓		✓
Hacking Ético			✓

Tabla comparativa para reconocer los beneficios de las distintas metodologías utilizadas en test de penetración en una red

CAPITULO 2:

METODOLOGIA DE ANALISIS DE RIESGOS OCTAVE-S

OCTAVE-S fue escogida para realizar un estudio comparativo porque:

Acude al personal de la organización y/o empresa ya que son ellos los que conocen con exactitud dónde encontrar de manera ágil los puntos más críticos, para así reducir costes de implementación de la mencionada metodología

OCTAVE-S se estructura en 3 fases:

- Fase Uno: Construir perfiles de amenaza basada en activos
- Fase Dos: Identificar vulnerabilidades de la infraestructura
- Fase Tres: Desarrollo de planes y estrategias de seguridad

La metodología Octave-S evalúa riesgos de seguridad de información para así plantear planes de mitigación dentro de la misma empresa. Esta metodología se centra en el diario trabajo de las organizaciones. Al equilibrar distintas unidades empresariales se puede de tal manera tomar decisiones de protección de información.

Para realizar el análisis se procede a conformar un grupo integrado por distintas personas de las áreas del negocio, que tengan el mayor conocimiento de las operaciones que se realizan dentro de la empresa.

Para empezar con el desarrollo de esta metodología el equipo de análisis procede a estudiar cada activo de información que se relevante para la empresa, es decir garantizar la prolongación de la operación.

Al finalizarse el análisis de los activos de información importantes se da una preferencia a dichos activos y de tal forma conocer cuál de ellos se identifican en los más críticos, sus vulnerabilidades y amenazas en su seguridad

Como resultado se realizará un plan de mitigación o plan de buenas prácticas, que se enfocará en un mejoramiento organizacional y en los sistemas que se utilizará dentro de la empresa para así poder minimizar el riesgo en los activos de información ya antes analizados

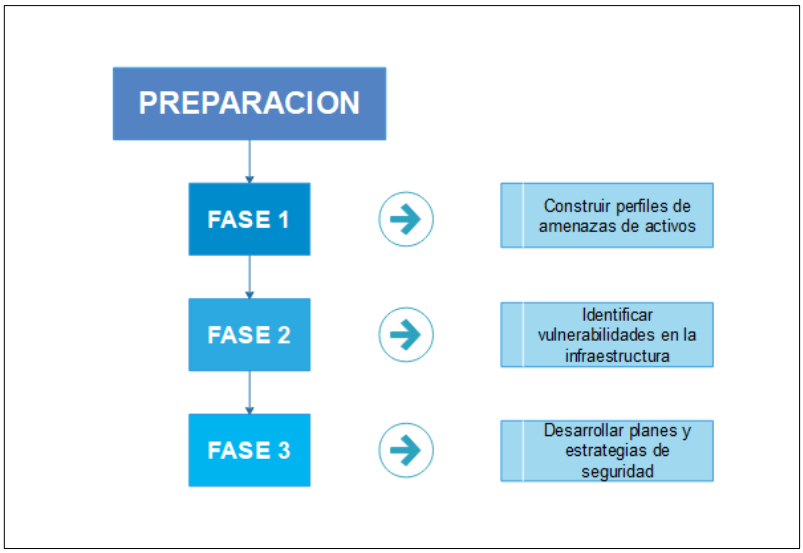


Figura 3 Fases de Evaluación OCTAVE-S
Fuente (Autores, 2019)

Representación de las tres fases utilizadas para el análisis de riesgos basándose en la metodología OCTAVE-S

CAPITULO 3

SITUACION ACTUAL DE LA EMPRESA

Actualmente la Industria Referee Cía. Ltda. Cuenta con un diseño de red como se demostrarán en las figuras 2, 3, 4 y 5, en donde constan equipos de gestión de la red y elementos que la constituyen.

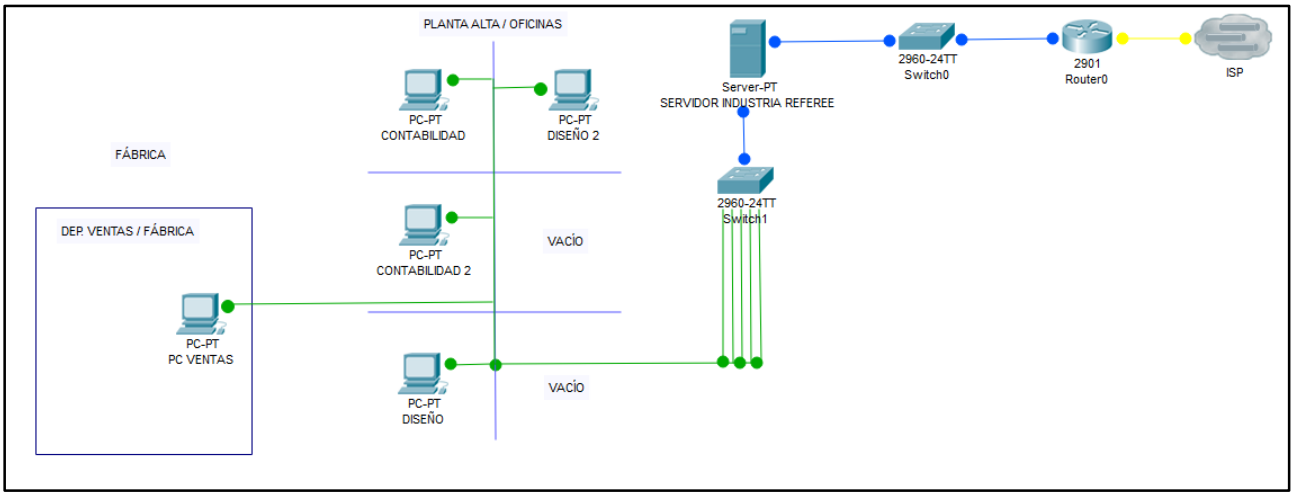


Figura 4 Red de la Fábrica de la Industria Referee
Fuente: (Autores, 2019)

Diseño de red de la fábrica de la Industria Referee, que nos muestra la manera en que esta compuestos los diferentes departamentos para el funcionamiento de la red en la organización.

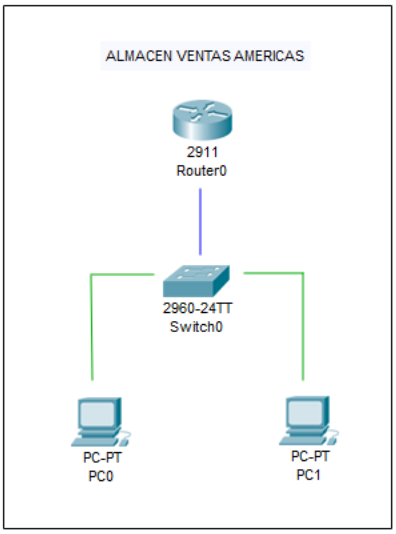


Figura 5 Red de Almacén 1 de la Industria Referee
Fuente: (Autores, 2019)

Red LAN del almacén 1 de las Américas que muestra el funcionamiento del departamento de ventas.

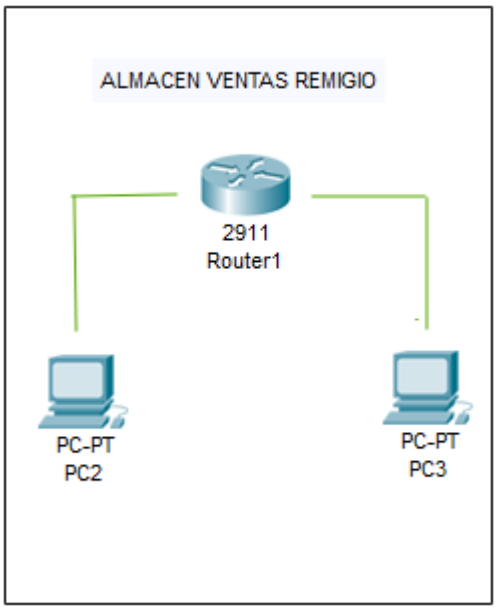


Figura 6 Red de Almacén 2 de la Industria Referee
Fuente: (Autores, 2019)

Red LAN del almacén 2 de la Remigio que muestra el funcionamiento del departamento de ventas.

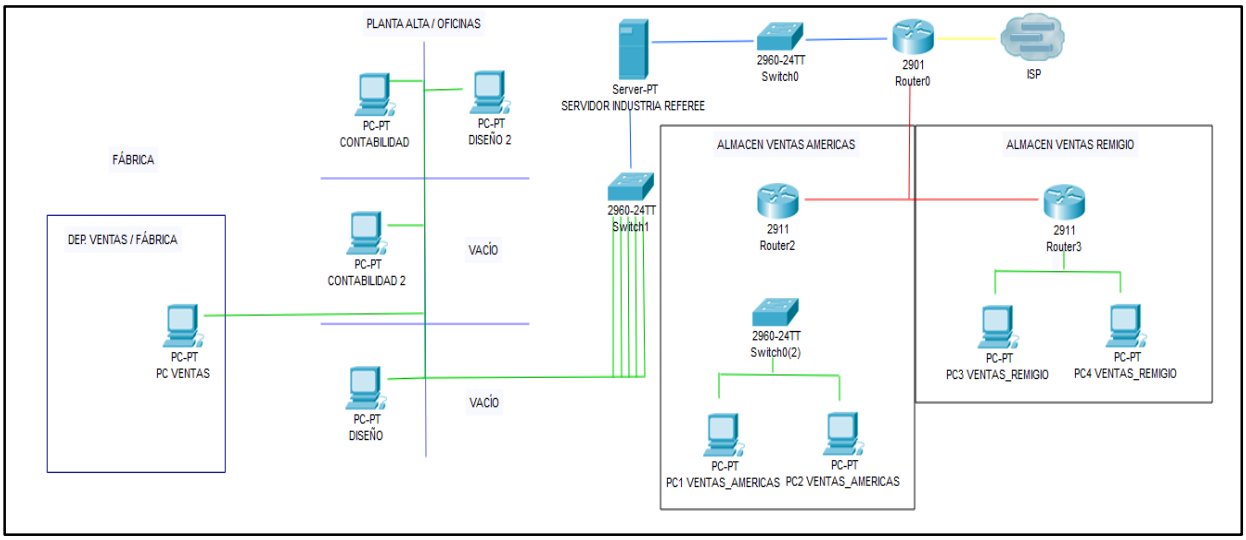


Figura 7 Red Consolidada de la Industria Referee
Fuente: (Autores, 2019)

Se presenta la Red de la Industria Referee consolidada entre una Red WAN que podrán interconectar diferentes edificaciones con el propósito de mantenerse en contacto por una red de trabajo.

3.1. DESARROLLO DE LA METODOLOGÍA OCTAVE-S

Para (López & Vásquez , 2017) el desarrollo de la metodología debe empezar con la identificación de los activos, sean estos tanto tangibles o intangibles y que para la organización forman parte de la actividad del día a día. Posteriormente, identificado estos activos proceder a identificar las vulnerabilidades, probabilidades, mediciones de riegos y concluir con el cálculo de riesgo para la organización

OCTAVE-S consta de 3 fases:

- Fase Uno: Construir perfiles de amenazas basada en activos.
- Fase Dos: Identificar vulnerabilidades de la infraestructura.
- Fase Tres: Desarrollo de planes y estrategias de seguridad.

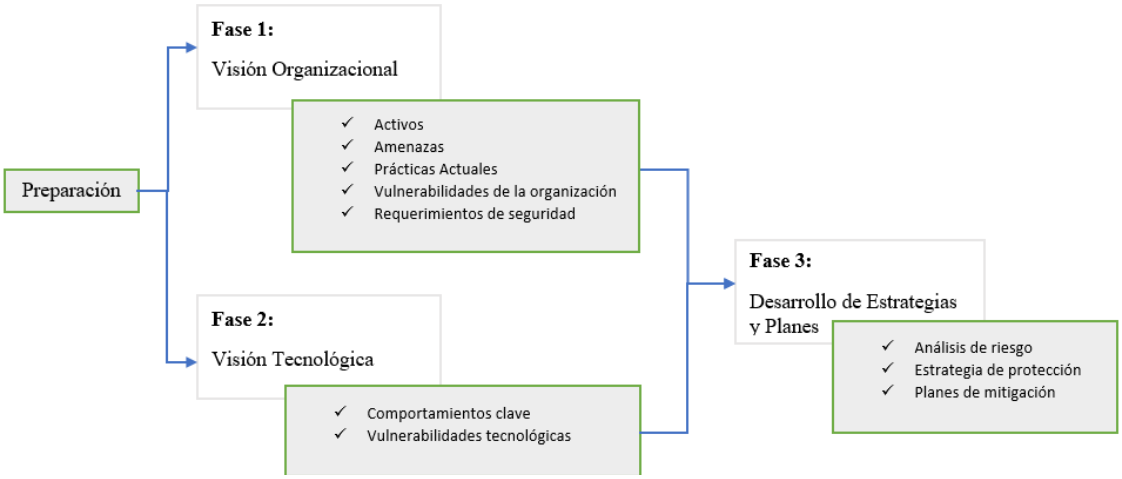


Figura 8 Fases de Desarrollo de OCTAVE-S
Fuente: (Autores, 2019)

Indica las fases para el desarrollo de la metodología OCTAVE, con sus respectivos subprocesos que debe contener cada fase, y de igual forma la manera en cómo trabaja cada fase para generar una mitigación de riesgos para la organización.

Para empezar con la primera fase de la metodología es necesario una fase inicial de preparación donde se establecerá el "equipo de análisis", en donde los involucrados en la actividad serán quienes tengan el conocimiento suficiente acerca de activos, departamentos y funciones de la organización. En algunos casos las personas pueden ser también externas de la organización:

Tabla 6 Registro de Equipo de Análisis
Fuente: (Autores, 2019)

N°	Nombre Miembro	Función en la Evaluación
1	Eulalia Maldonado	Gerente de Referee
2	Rosa Manjarres	Departamento de Ventas
3	Diana Cabrera	Patronaje

Da a conocer las personas o miembros de la organización quienes estarán en el proceso de análisis, para obtener mediante su colaboración información sobre los activos críticos, las actividades que realizan y que comparten con otros procesos; ellos son escogidos por el diverso conocimiento absoluto que poseen en relación con la organización.

Con el equipo de análisis conformado, da a conocer la forma tanto organizacional, operativa y de empleados de la organización, que brinda la información sobre los activos que cada uno considera relevante y necesario para la organización, como de igual forma induciendo sobre los aspectos negativos que pueden para la empresa.

3.1.1. FASE 1: CONSTRUIR PERFILES DE AMENAZA BASADA EN ACTIVOS

En la siguiente tabla se demuestra los diversos procedimientos, actividades y pasos que debe seguirse para completar la fase 1 de OCTAVE-S:

Tabla 7 Tabla de procesos, actividades y pasos de Fase 1 de OCTAVE-S
Fuente: (Autores, 2019)

Fase 1	Proceso	Actividad	Pasos
Fase 1: Construir perfiles de amenazas basada en activos	Proceso S1: Identificar la información organizacional	S1.1: Establecer criterios de evaluación	1
		S1.2: Identificar activos	2
		S1.3: Evaluar prácticas de seguridad	3
	Proceso S2: Crear perfiles de amenaza	S2.1: Seleccionar activos críticos	4
		S2.2: Identificar requerimientos de seguridad	5
		S2.3: Identificar amenazas a los activos	6

Muestra con respecto a la fase 1 de OCTAVE- los diversos procesos, actividades y pasos, que se deben llevar a cabo para realizar un levantamiento de activos correcto, de igual forma indica

las evaluaciones a realizar, siguiendo los pasos respectivos para obtener efectividad en los procesos a realizar.

3.1.2. PROCESO S1: IDENTIFICAR LA INFORMACIÓN ORGANIZACIONAL

3.1.2.1.ACTIVIDAD S1.1: ESTABLECER LOS CRITERIOS DE EVALUACIÓN

Lo relevante es identificar o definir los rangos de impacto en el caso es: bajo, básico, medio, alto y muy alto; que pueden sufrir los diversos activos de la organización, según (Alberts, Dorofee, Stevens, & Woody, OCTAVE- Implementation Guide, 2017) propone en las áreas:

- Ventas
- Ventas Web
- Diseño
- Producción
- Bodega
- Financiero
- Gerencia

Valoración de Críterios			
Nombre	**Número**	**Descripción**	**Porcentaje**
Bajo	1	La organización contiene seguridad máxima e integra y cumple las prácticas de seguridad.	0%
Básico	2	La organización tiene ciertos fallos, pero faciles de corregir y cumple casi todas las prácticas de seguridad.	25%
Medio	3	La organización tiene problemas, pero para la solución necesita ayuda y cumple hasta cierto punto las prácticas de seguridad.	50%
Alto	4	La organización necesita ayuda urgente, tiene perdidas ecomicas y materiales, tiene pocas prácticas de seguridad.	75%
Muy Alto	5	La organización se encuentra en la ruina provocando su quiebra y no cumple con las prácticas de seguridad.	100%

Figura 9 Valoración de Criterios
Fuente: (Autores, 2019)

Indica los niveles por los que se les puede clasificar según el nivel de seguridad de los activos en relación a los áreas o departamentos de la organización, da a conocer sobre los daños que puede ocasionar con la descripción de forma global y el porcentaje de afectación respectivo.

Para lo cual se puede llegar a conocer mediante rangos mostrados a continuación de las diferentes áreas:

Tabla 8 Criterios de Evaluación en referencia a Ventas
Fuente: (Autores, 2019)

Ventas					
Tipo de Impacto	**Bajo (1)**	**Básico (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Ventas	La ventas de la organización se realizan de una forma segura, y no hay inconvenientes en el proceso.	Las ventas tienen problemas leves, pero fáciles de solucionar.	Las ventas de la organización está en problemas y necesita de ayuda externa, inclusive necesita de un gasto económico.	Las ventas de la organización está colapsada, lo cual provoca numerosas pérdidas económicas.	Las ventas provocan ruina y quiebra a la organización.

Tabla que da a conocer sobre los criterios que evaluación para el tema de ventas de la organización mediante los rangos de bajo, básico, medio, alto y muy alto, para la determinación de la situación de la organización en relación a dicha área.

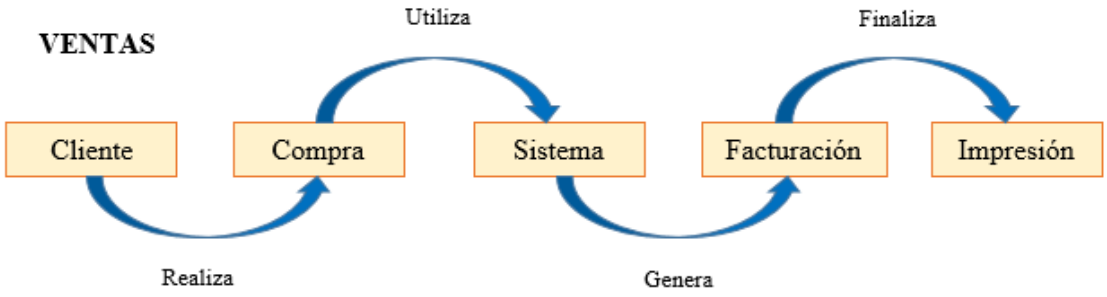


Figura 10 Proceso de Ventas
Fuente: (Autores, 2019)

Indica los procesos en los que la organización realiza las ventas, empezando con la compra del cliente, posterior a la verificación en el sistema, comprobado la existencia se generado la facturación de los productos y finalización con la impresión del a factura.

Tabla 9 Criterios de Evaluación en referencia al proceso de Pedidos
Fuente: (Autores, 2019)

Pedidos					
Tipo de Impacto	**Bajo (1)**	**Básico (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Pedidos	La organización realiza los pedidos de forma íntegra, la ocasión de problemas es casi nula.	La organización presenta problemas leves y son fácil de solucionar.	La organización tiene conflictos con los pedidos, generando inconvenientes tanto económicos y necesita ayuda externa.	La organización genera pedidos inexistentes o falsos, provoca pérdidas económicas y perdida de reputación por partes de sus clientes.	Los pedidos provocan ruina y quiebra a la organización.

Tabla que da a conocer sobre los criterios que evaluación para el tema del área de pedidos de la organización mediante los rangos de bajo, básico, medio, alto y muy alto, para la determinación de la situación de la organización en relación a dicha área.

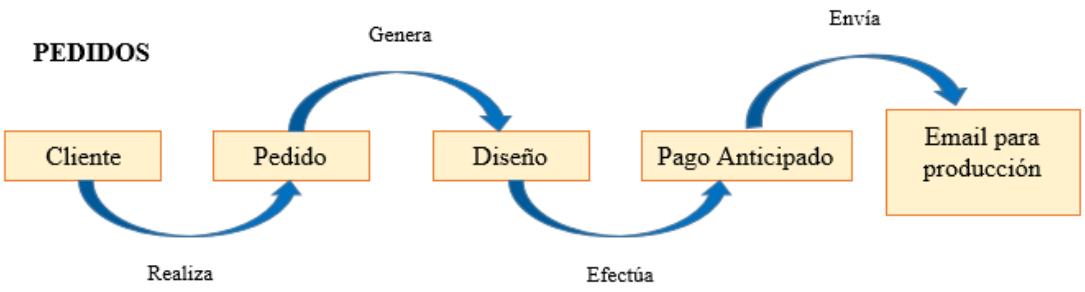


Figura 11 Proceso de Pedidos
Fuente: (Autores, 2019)

Indica los procesos en los que la organización realiza la actividad de pedidos, empezando con el pedido del cliente, posterior a la generación del diseño, se realiza el pago por anticipado del diseño para ser enviado a producción mediante correo electrónico.

Tabla 10 Criterios de Evaluación en referencia al área de Ventas Web
Fuente: (Autores, 2019)

Ventas Web					
Tipo de Impacto	**Bajo (1)**	**Básico (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Ventas Web	La organización da confianza a sus clientes al desarrollo de transacciones, las cuales se realizan de forma segura e integra.	La organización presenta problemas leves y son fácil de solucionar.	La organización no tiene cifrados correctos, provoca fallas en las transacciones y caídas del sistema, necesita ayuda externa.	La organización no tiene seguridades, provoca pérdidas económicas y problemas legales con instituciones bancarias.	Las ventas web provocan ruina y quiebra a la organización.

Tabla que da a conocer sobre los criterios que evaluación para el tema del área de ventas web de la organización mediante los rangos de bajo, básico, medio, alto y muy alto, para la determinación de la situación de la organización en relación a dicha área.

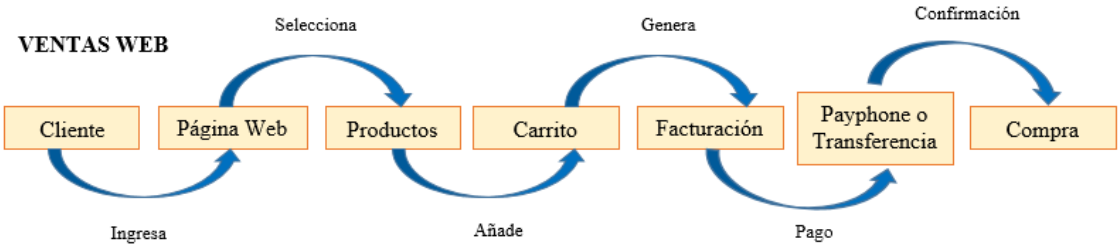


Figura 12 Procesos de Ventas Web
Fuente: (Autores, 2019)

Indica los procesos en los que la organización realiza la actividad de ventas web, empezando con el ingreso, posterior a la selección de productos, se realiza la facturación y el pago por payphone o transferencia

Tabla 11 Criterios de Evaluación en referencia al área de Diseño
Fuente: (Autores, 2019)

Diseño Pedido					
Tipo de Impacto	**Bajo (1)**	**Básico (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Diseño Pedido	La organización desarrolla sus diseños de acuerdo a la orden de pedidos, no sufre ningún tipo de alteraciones.	La organización presenta problemas y son fáciles de solucionar.	La organización desarrolla sus diseños pero con ciertos problemas que pueden causar interrupciones a nivel económico y laboral.	La organización no desarrolla sus diseños de manera controlada y de forma correcta en relación a sus pedidos, causa pérdidas económicas.	Los diseños provocan ruina y quiebra a la organización.

Tabla que da a conocer sobre los criterios que evaluación para el tema del área de diseño pedido de la organización mediante los rangos de bajo, básico, medio, alto y muy alto, para la determinación de la situación de la organización en relación a dicha área.

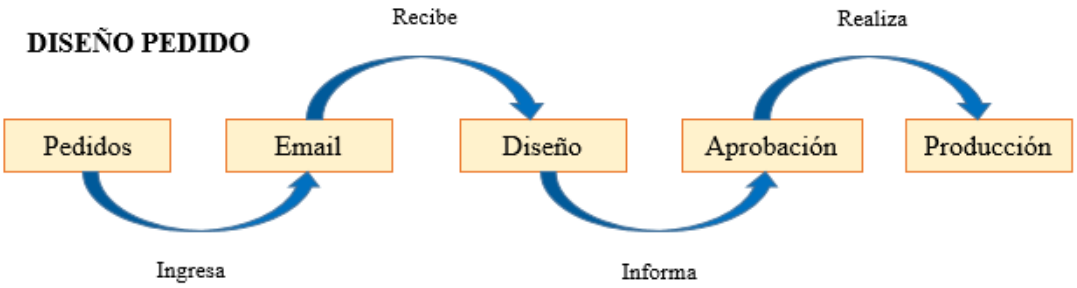


Figura 13 Procesos de Diseño de Pedido
Fuente: (Autores, 2019)

Indica los procesos en los que la organización realiza la actividad de diseño pedido, empezando con el ingreso del pedido mediante un email, posterior se obtiene el diseño para realizar una consulta de la aprobación y finaliza con la producción del diseño.

Tabla 12 Criterios de Evaluación en Referencia al área de Diseño
Fuente: (Autores, 2019)

Diseño Colección					
Tipo de Impacto	**Bajo (1)**	**Básico (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Diseño Colección	La organización desarrolla sus diseños de acuerdo a pedidos de forma correcta e integra.	La organización tiene problemas leves y son fáciles de solucionar.	La organización desarrolla sus diseños pero en casos ocurren problemas del sistema que provocan gastos económicos.	La organización no desarrolla sus diseños a cabalidad con sus pedidos, ocasiona pérdidas numerosas de dinero y materias primas.	Los diseños provocan ruina y quiebra a la organización.

Tabla que da a conocer sobre los criterios que evaluación para el tema del área de diseño colección de la organización mediante los rangos de bajo, básico, medio, alto y muy alto, para la determinación de la situación de la organización en relación a dicha área.

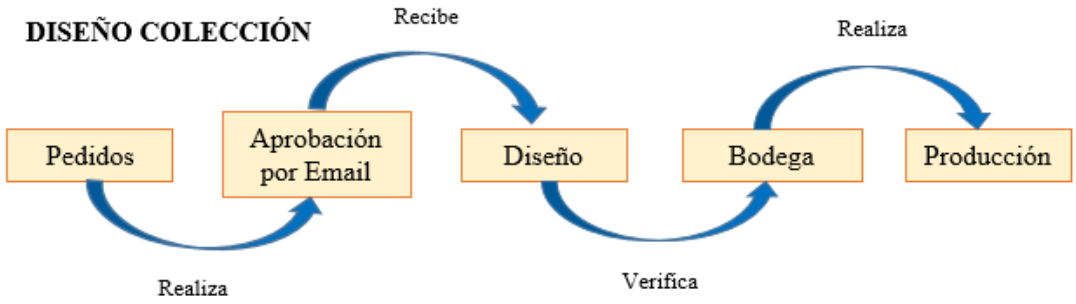


Figura 14 Proceso de Diseño Colección
Fuente: (Autores, 2019)

Indica los procesos en los que la organización realiza la actividad de diseño colección, empezando con el ingreso del, posterior se recibe el diseño, luego se verifica el material y finalmente se realiza la producción del diseño.

Tabla 13 Criterios de Evaluación en referencia al área de Producción
Fuente: (Autores, 2019)

Producción Diseño y Colección					
Tipo de Impacto	**Bajo (1)**	**Básico (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Producción	La organización concreta sus pedidos con la materia prima necesaria y a medida de los pedidos.	La organización tiene problemas leves y son fáciles de solucionar.	La organización tiene problemas en los sistemas, provoca falta de materias primas y reducciones de dinero.	La organización no cuenta con un control de producción exacto, provoca problemas de producción y fuertes gastos económicos.	La producción provoca ruina y quiebra a la organización.

Tabla que da a conocer sobre los criterios que evaluación para el tema del área de producción diseño y colección de la organización mediante los rangos de bajo, básico, medio, alto y muy alto, para la determinación de la situación de la organización en relación a dicha área.

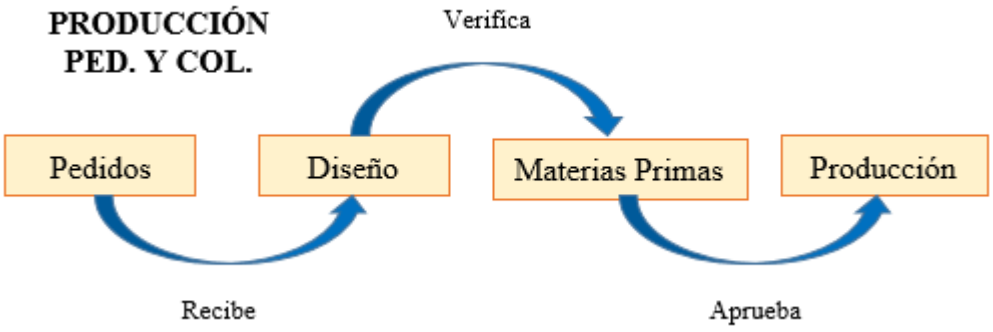


Figura 15 Procesos de Producción y Pedido
Fuente: (Autores, 2019)

Indica los procesos en los que la organización realiza la actividad de producción pedido y colección, empezando con el ingreso del pedido para la obtención del diseño, posterior se verifica la materia prima para el desarrollo, aprobado se procede a la producción del pedido.

Tabla 14 Criterios de Evaluación en referencia al área de Bodega
Fuente: (Autores, 2019)

Bodega					
Tipo de Impacto	**Bajo (1)**	**Básico (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Bodega	La organización siempre cuenta con material disponible para la producción.	La organización tiene problemas leves de material y son fáciles de solucionar.	La organización tiene problemas en la bodega, retrasa a la producción.	La organización no tiene control de material, genera pérdidas en pedidos, reputación y perdidas económicas.	La organización no tiene control de bodega, no existe material disponible, no genera economía.

La posterior tabla que da a conocer sobre los criterios que evaluación para el tema del área de bodega de la organización mediante los rangos de bajo, básico, medio, alto y muy alto, para la determinación de la situación de la organización en relación a dicha área.

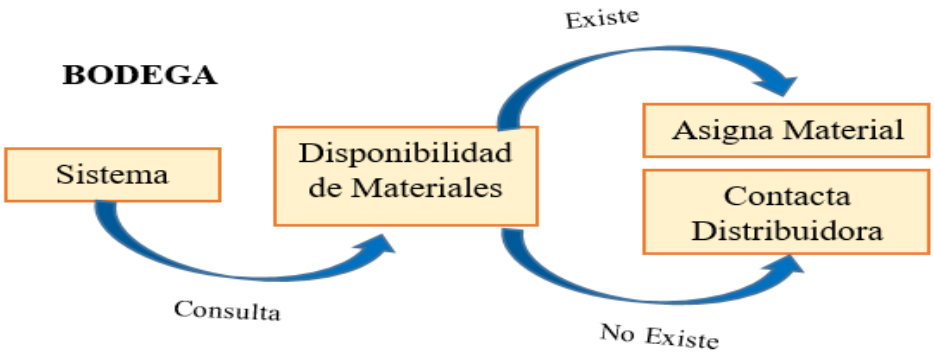


Figura 16 Procesos de Bodega
Fuente: (Autores, 2019)

Indica los procesos en los que la organización realiza la actividad por parte de bodega, empezando con una consulta en el sistema, el cual se encarga de revisar si existe o no material disponible, en el caso de que exista o no el material

Tabla 15 Criterios de Evaluación en referencia al área de Finanzas
Fuente: (Autores, 2019)

Financiera					
Tipo de Impacto	**Bajo (1)**	**Básico (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Financiera	La organización siempre tiene sus balances cuadrados y estables.	La organización tiene problemas en las finanzas, pero no ocasiona conflictos.	La organización tiene problemas en las finanzas, provoca pérdidas económicas.	La organización no tiene control de finanzas, provoca conflictos económicos para la empresa, clientes y distribuidores.	La organización no tiene control de finanzas, provoca ruina y quiebra.

La posterior tabla da a conocer sobre los criterios que evaluación para el tema del área de finanzas de la organización mediante los rangos de bajo, básico, medio, alto y muy alto, para la determinación de la situación de la organización en relación a dicha área.

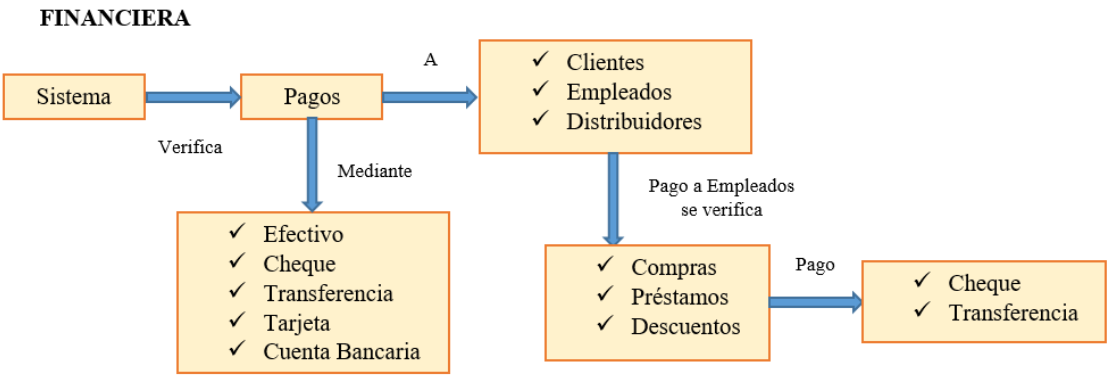


Figura 17 Procesos de Finanzas
Fuente: (Autores, 2019)

Indica los procesos en los que la organización realiza la actividad de finanzas, empezando con una verificación en el sistema sobre los pagos realizados a los clientes, empleados y distribuidores, estos pagos que pueden ser realizados en diferentes formas, y para el pago a empleados se revisa que no exista compras, préstamos o deudas para realizar los respectivos pagos.

Tabla 16 Criterios de Evaluación en referencia al área de Gerencia
Fuente: (Autores, 2019)

Gerencia					
Tipo de Impacto	**Bajo (1)**	**Básico (2)**	**Medio (3)**	**Alto (4)**	**Muy Alto (5)**
Gerencia	La organización siempre tiene absoluto control de los departamentos.	La organización tiene problemas leves de control a los departamentos.	La organización tiene problemas en el funcionamiento de sus departamentos.	La organización no tiene control de los departamentos, provoca conflictos económicos	La organización no tiene control de los departamentos, provoca ruina y quiebra.

La posterior tabla da a conocer de los criterios que evaluación para el tema del área de gerencia de la organización mediante los rangos de bajo, básico, medio, alto y muy alto

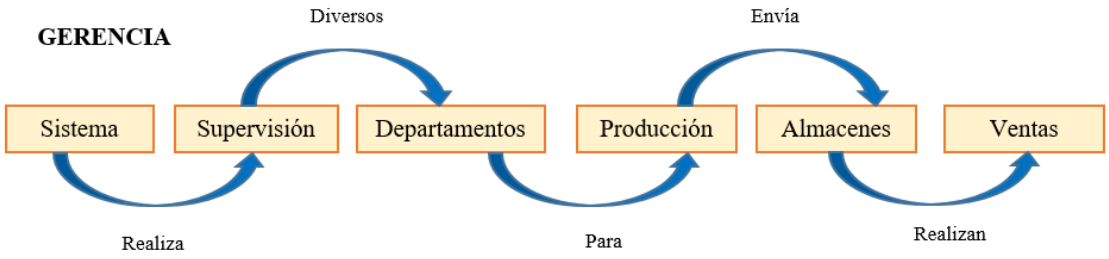


Figura 18 Proceso de Gerencia
Fuente: (Autores, 2019)

3.1.2.2. ESTADO DE LA EMPRESA CON LOS CRITERIOS DE EVALUACIÓN

Estado de la situación actual de los respectivos departamentos y los activos de la empresa presentados para ser evaluados a continuación:

Basándose en el análisis realizado dentro de la Industria Referee se procede a la evaluación de los activos de información, su cantidad, como se los identifica, el tipo de seguridad al que están expuestos, sus requisitos como sus políticas de seguridad, basándonos en un criterio de evaluación numerados del 1 al 5, su resultado total y en porcentaje de cada departamento que conforma toda la empresa para así generar la evaluación que es requerida

Tabla 17 Estado Actual Departamentos y Activos

Fuente: (Autores, 2019)

Estado Actual de los Departamentos y Activos															
Departamento	**Activo**		**Seguridad**		**Respaldos**	**Políticas de Seguridad**	**Criterio**					**Resultado**		
	Cantidad	**Nombre**	**Fisica**	**Lógica**			**1**	**2**	**3**	**4**	**5**	**Total**	**Porcentaje**	**%**
Ventas														
Americas	2	PC	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Impresora	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada			3					
	1	Router	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada				4				
	1	Programa	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Base de Datos	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Switch	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada				4				
							0	0	12	8	0	20	66,67	%
Remigio	2	PC	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Impresora	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada			3					
	1	Router	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada				4				
	1	Base de Datos	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Programa	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
							0	0	12	4	0	16	64,00	%
Fábrica	1	PC	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Impresora	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada			3					
	1	Programa	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Base de Datos	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Switch	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada				4				
							0	0	12	4	0	16	64,00	%
Ventas Web														
	1	Página Web	Ninguna Protección	Ninguna Seguridad Implementada	No existe ningún tipo de respaldo	Ninguna Implementada					4			
							0	0	0	0	4	4	80,00	%
Diseño														
	1	PC	Ninguna Protección	Acceso de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Base de Datos	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Programa	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
							0	0	9	0	0	9	60,00	%
Producción														
	2	PC	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	2	Impresoras	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada			3					
	1	Teléfono IP	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada		2						
	1	Switch	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada				4				
							0	2	6	4	0	12	60,00	%
Bodega														
	1	PC	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Programa	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Teléfono IP	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada		2						
	1	Base de Datos	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Inventarios	Ninguna Protección	Ninguna Seguridad Implementada	No existe ningún tipo de respaldo	Ninguna Implementada		2						
	1	Switch	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada				4				
							0	4	9	4	0	17	56,67	%
Financiera														
	2	PC	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Impresora	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada			3					
	1	Programa	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Teléfono IP	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada		2						
	1	Base de Datos	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Switch	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada				4				
							0	2	12	4	0	18	60,00	%
Gerencia														
	1	PC	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Switch	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada				4				
	1	Router	Ninguna Protección	Ninguna Seguridad Implementada	Innecesario	Ninguna Implementada				4				
	1	Servidor	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
	1	Base de Datos	Ninguna Protección	Inicio de Sesión de Usuario y Clave	Innecesario	Ninguna Implementada			3					
	1	Programa	Ninguna Protección	Inicio de Sesión de Usuario y Clave	No existe ningún tipo de respaldo	Ninguna Implementada			3					
							0	0	12	8	0	20	66,67	%

Tabla que da a conocer sobre la información de los activos que cada departamento posee.

Con los criterios de evaluación detallados anteriormente se determinó lo siguiente con la información obtenida de las áreas de la empresa:

Tabla 18 Criterios de Evaluación en referencia al estado actual de la empresa
Fuente: (Autores, 2019)

Críterios de Evaluación			
Área o Departamento	**Valoración**	**Porcentaje**	
Ventas	Medio	50	%
Ventas Web	Alto	75	%
Diseño	Medio	50	%
Producción	Medio	50	%
Bodega	Medio	50	%
Financiero	Medio	50	%
Gerencia	Medio	50	%
Total		62,50	%

Da a conocer en relación a los criterios de evaluación de forma general el estado actual en el que la organización se encuentra, con relación a los tipos de áreas que maneja.

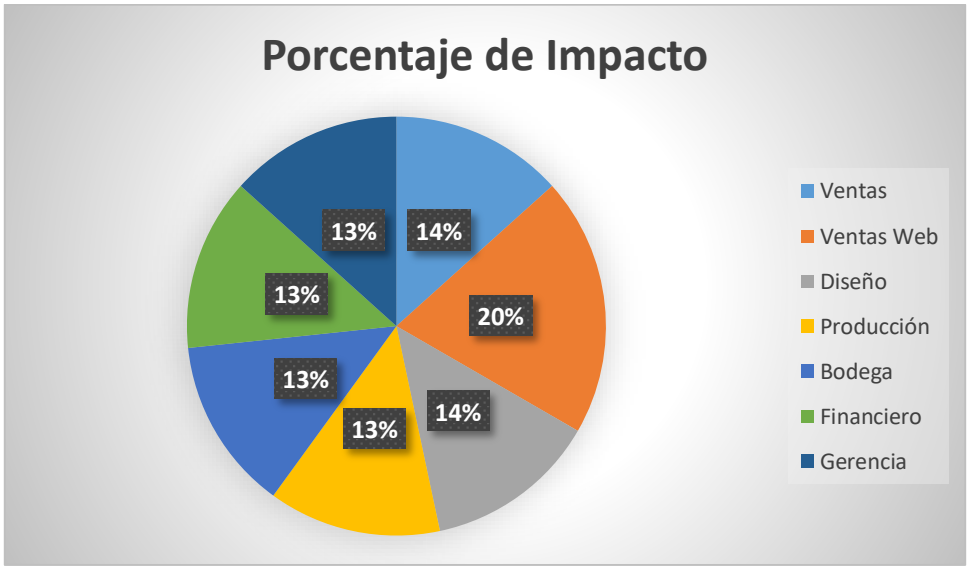


Figura 19 Cuadro Estadístico de Impacto
Fuente: (Autores, 2019)

Indica los porcentajes del impacto que sufre cada una de las áreas de la organización, muestra la situación por medio de valores para la determinación del valor del impacto que sufre cada área por no tener una seguridad apropiada.

3.1.2.3.ACTIVIDAD S1.2: IDENTIFICAR ACTIVOS

Con el equipo de análisis y definido ya los rangos de valoración de impacto, se procede al paso de identificar los activos críticos para a organización, entre los que pueden estar sistemas, aplicaciones, información y personas, a continuación, se presenta los activos que posee la organización:

Tabla 19 Tabla de Activos de la Empresa
Fuente: (Autores, 2019)

Nombre del Activo	Tipo de Activo	Descripción
Base de Datos	Información	Utilizado para gestionar la información, dependiendo de cada área de la organización.
Servidor	Físico/Información	Encargado de proveer servicios a los equipos cliente quienes realizan peticiones.
Máquina de Ventas	Físico	PC utilizada para el área de ventas de la organización.
Máquina de Bodega	Físico	PC utilizada para el área de bodega de la organización.
Máquina de Cortes	Físico	PC utilizada para el área de cortes de la organización.
Máquina de Contabilidad	Físico	PC utilizada para el área de contabilidad de la organización.
Impresoras	Físico	Utilizado para realizar impresiones de información de facturas, pedidos, etc.
Inventarios	Información	Utilizado para llevar el control de unidades tanto de productos finales y materias primas.
Página Web	Aplicación	Aplicación en la cual se difunde información y productos que la organización ofrece.
Programa	Sistema	Software diseñado para cada una de las áreas de la organización.
Router	Físico	Utilizado para interconectar los equipos dentro de la red y direccionamiento de paquetes.
Switch	Físico	Encargado para resolver problemas de rendimiento de la red y distribución de paquetes.

Tabla que representa los diversos activos que se considera con relación al grupo de análisis son relevantes internamente en la organización.

3.1.2.4.ACTIVIDAD S1.3: EVALUAR LAS PRÁCTICAS DE SEGURIDAD

En la actividad se comprobará que prácticas de seguridad son aplicadas en la empresa, de igual forma lo que la empresa realiza correctamente y lo que le falta es decir las vulnerabilidades, para lo cual OCTAVE-S propone 15 practicas:

1. Concientización y Formación en Seguridad: No divulgar información sensible a terceros, capacidad para manejar hardware y software, reportar incidentes y cursos de capacitación de seguridad de la información.
2. Estrategia de Seguridad.
3. Gestión de Seguridad: Dar soluciones a problemas de seguridad que se presenten en cada una de las áreas de trabajo.
4. Políticas y Regulaciones de Seguridad: Tener procedimientos que se deben realizar cuando se presenta algún incidente de seguridad de la información, con ello soluciones dichos incidentes.
5. Gestión de Seguridad Colaborativa: Tener políticas y procedimientos para proteger la información cuando se trabaja con organizaciones externas y a su vez estas organizaciones cumplan con sus necesidades y requerimientos.
6. Planes de Contingencia/Recuperación de Desastres: Tales como:
    - Seguridad del a instalación.
    - Disponibilidad de recursos hardware y software.
    - Políticas y procedimientos de respaldo de información.
    - Recuperación de información.
7. Control de Acceso Físico: determinar los mejores controles de seguridad física para proteger los activos de la organización, tales como:
    - Accesos restringidos a las áreas donde existe activos de información.
    - Proteger los computadores con claves personales.
    - Cámaras de circuito cerrado.
    - Utilización de sistemas biométricos para el control de acceso.
8. Monitoreo y Auditoria de Seguridad Física: Asegurar que todos los equipos, dispositivos e información estén asegurados, saber quién es el responsable y manteniendo un monitoreo constante de cada uno de ellos.
9. Gestión de Sistemas y Redes: Poseer herramientas para gestionar la seguridad y almacenamiento de datos.

10. Monitoreo y Auditoria de Seguridad de TI: Para realizar un correcto procedimiento de monitoreo y auditoria de los sistemas, de la red y la información, es necesario poseer herramientas que ayuden al desarrollo del mismo, al igual se debe contar con políticas documentadas.
11. Autenticación y Autorización: Se debe implementar mecanismo de control de acceso a los usuarios que accedan a los activos de información, sin olvidar de la respectiva autorización otorgada por su jefe inmediato, o al personal encargado de dicho activo de información.
12. Gestión de Vulnerabilidades: Documentar procedimientos y políticas de cómo desarrollar un análisis y gestión de vulnerabilidades de los sistemas.
13. Encriptación: Hace referencia a una manera de proteger la información de gran importancia de la organización contra ataques informáticos.
14. Diseño y Arquitectura de Seguridad: Poseer documentación del diseño de la red informática, con ello se puede tomar acciones y crear planes de seguridad.
15. Gestión de Incidentes: Documentación para saber cómo reaccionar en caso de surgir algún incidente, además guías de realizar respaldos de información y recuperación de datos.

Para determinación del estado de la organización se utiliza un estado de bajo, medio y alto para cada practica de seguridad:

Bajo (1): Hace referencia a que la organización cumple correctamente con las prácticas de seguridad.

Básico (2): La organización cumple con casi la mayoría de las prácticas de seguridad, las faltantes son leves.

Medio (3): La organización cumple hasta cierto punto las prácticas de seguridad con espacio a mejora.

Alto (4): La organización tiene pocas prácticas de seguridad que resultan conflicto para el desenvolvimiento de la empresa.

Muy Alto (5): La organización no cumple con las prácticas de seguridad

Tabla 20 Tablas de Prácticas de Evaluación de la Organización
Fuente: (Autores, 2019)

Prácticas de Seguridad								
Práctica	**Valoración**					**Resultado**	**Porcentaje**	
	1	**2**	**3**	**4**	**5**			
Concientización y Formación en Seguridad				4		Alto	75	%
Estrategia de Seguridad				4		Alto	75	%
Gestión de Seguridad				4		Alto	75	%
Políticas y Regulaciones de Seguridad				4		Alto	75	%
Gestión de Seguridad Colaborativa					5	Muy Alto	100	%
Planes de Contingencia/Recuperación de Desastres				4		Alto	75	%
Control de Acceso Físico			3			Medio	50	%
Monitoreo y Auditoria de Seguridad Física			3			Medio	50	%
Gestión de Sistemas y Redes			3			Medio	50	%
Monitoreo y Auditoria de Seguridad de TI				4		Alto	75	%
Autenticación y Autorización		2				Básico	25	%
Gestión de Vulnerabilidades				4		Alto	75	%
Encriptación			3			Medio	50	%
Diseño y Arquitectura de Seguridad			3			Medio	50	%
Gestión de Incidentes				4		Alto	75	%
Total							65,00	%

Da en un rango de semáforo el cual indica por medio de colores sobre la situación en la que la organización.

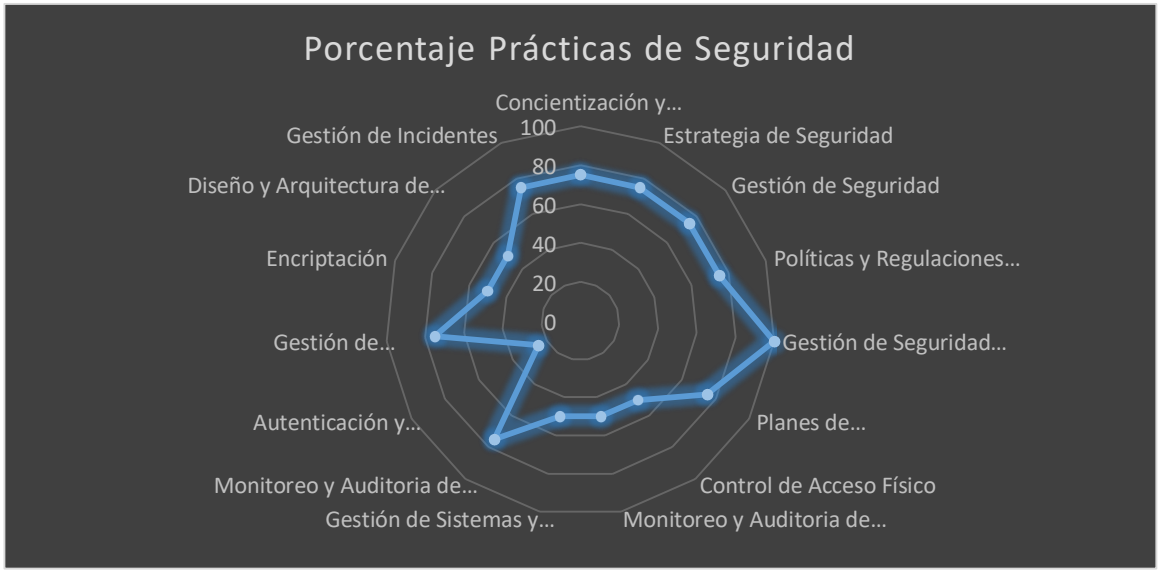


Figura 20 Cuadro Estadístico de Prácticas de Seguridad

Fuente: (Autores, 2019)

3.1.3. PROCESO S2: CREAR PERFILES DE AMENAZA

En este proceso con la identificación de los activos de la organización, se procede con la identificación de los activos más críticos, para poder definir los requerimientos de seguridad y finalmente determinar las amenazas que se presenten en contra de los activos.

3.1.3.1. ACTIVIDAD S2.1: SELECCIONAR ACTIVOS CRÍTICOS

En la actividad se seleccionará entre 3 a 5 activos más críticos, sus respectivos nombres, razón por la cual se considere un activo crítico, las personas quienes usan y los que están a cargo del respectivo activo, y otros activos que puedan estar relacionados.

Tabla 21 Tabla de Activos Críticos de la Organización
Fuente: (Autores, 2019)

Activo Crítico	Razón	Utilizan	Encargado	Otros Activos
Servidor	Es el que brinda todos los servicios a las diversas peticiones de sus Pc cliente, lo cual no puede faltar.	Empleados	TIC	Base de Datos Página Web Programa
Base de Datos	Es el encargado de gestionar toda la información de la organización, sin una BD no permitiría obtener información de la empresa.	Empleados	Ventas Bodega	Página Web Servidor Programa
Página Web	Mediante la cual se da a conocer a la organización, así como gana fama con mala difusión podría ocasionar mala reputación a la empresa.	Empleados	Ventas	Servidor
Programa	Es el que utiliza la organización para poder realizar sus actividades.	Empleados	Ventas Diseño Financiero Bodega	Servidor Base de Datos

Da a conocer sobre los activos más críticos que la organización posee, como igual forma la razón por la cual es considera un activo crítico, la persona que utiliza y el encargado del activo, y su relación con otros posibles activos.

3.1.3.2. ACTIVIDAD S2.2: IDENTIFICAR REQUERIMIENTOS DE SEGURIDAD

En el siguiente paso se procede a la identificación de requerimientos de seguridad para cada activo crítico, para lo cual OCTAVE-S propone los siguientes requerimientos de seguridad:

- **Confidencialidad:** La información sea utilizada solo por personas autorizadas.
- **Integridad:** Garantiza que la información puede ser manipula o modificada solo por personas autorizadas.
- **Disponibilidad:** La información estará disponible a todo momento, es decir cuando el personal la necesite. A continuación, se presenta los requerimientos de seguridad

Tabla 22 Tablas de Requerimiento de seguridad
Fuente: (Autores, 2019)

Activo Crítico	Requerimiento de Seguridad	Requerimiento más Importante	Justificación
Servidor	Disponibilidad Integridad Confidencialidad	Disponibilidad	Lo primordial para la organización es tener su servidor disponible a todo momento, para las peticiones que realizan sus clientes.
Base de Datos	Disponibilidad Integridad Confidencialidad	Integridad	Mantener la información de la organización de forma íntegra es lo más importante, por motivo que maneja información de producción, clientes y otros.
Página Web	Disponibilidad Integridad Confidencialidad	Disponibilidad	Para la organización lo relevante en la página es tenerla disponible 24/7, por motivo que es un parte de las cuales los clientes conocen los productos y realizan compras.
Programa	Disponibilidad Integridad Confidencialidad	Disponibilidad	Lo importante para la organización es poder mantener su programa siempre en funcionamiento, para desarrollo de las diversas actividades que desarrolla la empresa.

Da a conocer sobre los requerimientos de seguridad que son necesarios en cada uno de los activos críticos, y cuál de ellos es el más importante para conveniencia de la organización.

3.1.3.3. ACTIVIDAD S2.3: IDENTIFICAR AMENAZAS A LOS ACTIVOS

En este paso se desarrolla el árbol de la amenaza de los activos críticos, para OCTAVE-S utiliza las categorías de amenazas:

1. Actores humanos usando acceso a la red.
2. Actores humanos usando acceso físico.
3. Problemas del sistema.

Otro punto relevante y a tomar en cuenta para determinar las amenazas de los activos es tomar en cuenta las combinaciones siguientes:

- Internos actúan por accidente.
- Internos actúan deliberadamente.
- Externos actúan por incidente.
- Externos actúan deliberadamente.

Para lo cual se da a conocer las amenazas para los activos, que pueden surgir en la organización ya sea por actores internos o externos, detallados a continuación:

Tabla 23 Tabla de Amenazas de Activos
Fuente: (Autores, 2019)

Amenaza	Activo	Acceso	Actor	Motivo	Resultado
Denegación de Servicio (DoS)	Página Web	Red	Externo	Premeditado	Interrupción
Virus Informático	Página Web	Red	Externo	Premeditado	Modificación
Espionaje	Página Web	Red	Externo	Premeditado	Intercepción
Divulgación de Información	Página Web	Físico	Interno	Premeditado	Intercepción
Uso incorrecto	Base de Datos	Red	Interno	Accidental	Modificación
Virus Informático	Base de Datos	Red	Externo	Premeditado	Modificación

Alteración de Información	Base de Datos	Red	Externo	Premeditado	Fabricación
Uso no Autorizado	Base de Datos	Red	Interno	Premeditado	Intercepción
Denegación de Servicio (DoS)	Servidor	Red	Externo	Premeditado	Interrupción
Uso no Autorizado	Servidor	Red	Interno	Accidental	Intercepción
Robo de Información	Programa	Red	Interno	Premeditado	Intercepción
Alteración de Información	Programa	Red	Interno	Accidental	Modificación
Uso incorrecto	Programa	Red	Interno	Accidental	Modificación
Suplantación de Identidad	Programa	Red	Externo	Premeditado	Intercepción
Ataque de Fuerza Bruta	Programa	Red	Externo	Premeditado	Intercepción

Da a conocer sobre las posibles amenazas que pueden surgen en la organización, de igual forma se identifica el acceso, el autor, el motivo y el resultado que puede provocar la amenaza en relación a los activos críticos de la empresa.

3.1.4. FASE 2: IDENTIFICAR VULNERABILIDADES EN LA INFRAESTRUCTURA

En la siguiente tabla se demuestra los diversos procedimientos, actividades y pasos que debe seguirse para completar la fase 2 de OCTAVE-S:

Tabla 24 Tabla de procesos, actividades y pasos de la Fase 2 de OCTAVE-S
Fuente: (Autores, 2019)

Fase 2	Proceso	Actividad	Pasos
Fase 2: Identificar las Vulnerabilidades de la Infraestructura	Proceso S3: Examinar la infraestructura computacional en relación con los activos críticos	S3.1: Examinar rutas de acceso	7
		S3.2: Analizar procesos relacionados con la tecnología	8

Muestra con respecto a la fase 2 de OCTAVE- los diversos procesos, actividades y pasos, que se deben llevar a cabo para identificar vulnerabilidades de la infraestructura,

3.1.5. PROCESO S3: EXAMINAR LA INFRAESTRUCTURA COMPUTACIONAL CON LOS ACTIVOS

3.1.5.1.ACTIVIDAD S3.1: EXAMINAR RUTAS DE ACCESO

En la actividad se realiza principalmente la determinación de cuál es el sistema que este más estrechamente ligado a cada activo crítico, para identificar así el sistema de interés, por tal motivo se examina cuáles son las rutas de acceso de la información, posterior determinar las maneras en las que se pueden realizar la transmisión o extracción de la información del sistema, finalmente analizar que componentes son usados y la forma en la que se respalda la información del sistema.

Tabla 25 Tablas de Rutas de Acceso
Fuente: (Autores, 2019)

Activo	Sistema	Ruta de Acceso	Componentes	Transmisión	Respaldos
Servidor	Windows Server	La PC solicita algún servicio, este petición pasa a un switch y posterior llega al servidor.	Router Cable PC's	Solo pueden ingresar al servidor las PC's que se encuentren en red.	Cuenta con un cuarto frio alejado de la empresa.
Base de Datos	MySQL	La PC solicita información de la BD, llega a un switch y es enviado a la BD.	PC's Router Servidor	El personal interno no puede ingresar desde el exterior.	Realiza un backup cada mes.
Página Web	Html	La PC ingresa a la dirección web, esta es solicita al servidor, y finalmente enviada al servidor web.	Servidor PC	No se puede acceder a la administración sin las credenciales.	Tiene la estructura inicial de la página.
Programa	Abago	La PC solicita uso del programa, este pasa al switch, llega al servidor la petición.	PC's Router Repetidor Servidor	Solo pueden ingresar las maquinas en red y las que tengas instaladas el programa.	Cuenta con la versión 1 del programa.

Muestra las rutas de acceso sobre las cuales están involucrados cada uno de los activos, detallando el sistema que utiliza, la ruta para llegar al sistema, los componentes de red que utiliza el sistema, la transmisión o forma de cómo se podría extraer la información del sistema y si cada sistema cuenta con un respaldo.

3.1.5.2. ACTIVIDAD S3.2: ANALIZAR PROCESOS RELACIONADOS CON LA TECNOLOGÍA

Para culminar con la fase 2 de OCTAVE-S, es necesario determinar la clase de los componentes que están vinculados o forman parte de los activos críticos analizados anteriormente, para asignar la responsabilidad a alguna persona de la organización sobre los componentes de la red y finalmente estimar un grado de seguridad sobre los diversos procesos de configuración y mantenimiento de los componentes de la red.

Tabla 26 Tabla de Procesos Relacionados con la Tecnología
Fuente: (Autores, 2019)

Clase	Relación con los Activos	Responsabilidad	Grado de Seguridad
Servidores	Servidor	Encargado de Sistemas	No toma en cuenta la seguridad, no realiza mantenimientos periódicos.
Switch	Servidor Programa	Encargado de Sistemas	No son verificados en ningunos casos, seguridad baja.
Estaciones de Trabajo	Servidor Programa Base de Datos	Encargado de Sistemas	Se hace mantenimientos a largos plazos, no hace cuenta la seguridad.
Repetidores	Programa Base de Datos	Encargado de Sistemas	No se le realiza mantenimiento consecutivo
Cables	Servidor Base de Datos Programa	Encargado de Sistemas	No existe mantenimiento, poca seguridad.
Tarjetas de Red	Programa Base de Datos	Encargado de Sistemas	El realizado con mantenimientos iguales a las estaciones de trabajo.
Software	Programa	Encargado de Sistemas	No se realiza configuraciones y mantenimientos en periodos cortos.

La tabla muestra los procesos de la organización que están relacionados con la tecnología, para lo cual se establece las clases de componentes de la red, la relación respectiva con los activos críticos, y la responsabilidad de la persona sobre estos componentes y el grado de seguridad que la empresa está actualmente tomando en cuenta.

3.1.6. FASE 3: DESARROLLO DE PLANES Y ESTRATEGIAS DE SEGURIDAD

En la siguiente tabla se demuestra los diversos procedimientos, actividades y pasos que debe seguirse para completar la fase 3 de OCTAVE-S:

Tabla 27 Tabla de procesos, actividades y pasos de la Fase 3 de OCTAVE-S
Fuente (Autores, 2019)

Fase 3	Proceso	Actividad	Pasos
Fase 3: Desarrollo de estrategias y planes de seguridad	Fase S4: Identificar y analizar los riesgos	S4.1: Evaluar el impacto de las amenazas	9
		S4.2: Establecer criterios de evaluación probabilística	10
		S4.3: Evaluar probabilidades de amenazas	11
	Fase S5: Desarrollar estrategias de protección y planes de mitigación	S5.1: Describir las estrategias de protección actuales	12
		S5.2: Seleccionar aproximaciones de mitigación	13
		S5.3: Desarrollar planes de mitigación de riesgos	14
		S5.4: Identificar cambios en las estrategias de protección	15
		S5.5: Identificar los siguientes pasos	16

Muestra con respecto a la fase 3 de OCTAVE-S los diversos procesos, actividades y pasos, para generar ciertas estrategias y planes de seguridad, para lo cual las actividades permiten llegar a la conclusión del siguiente proceso realizando evaluaciones de amenazas, probabilidades y finalmente desarrollar estrategias y planes de mitigación en base a las protecciones actuales de la organización.

3.1.7. PROCESO S4: IDENTIFICAR Y ANALIZAR LOS RIESGOS

En el siguiente proceso se enfoca en la evaluación de impacto y la probabilidad que tienen las diversas amenazas encontradas en relación de los activos críticos, de igual forma los criterios de evaluación de la probabilidad, por tal motivo se debe desarrollar las siguientes actividades descritas a continuación:

3.1.7.1. ACTIVIDAD S4.1: EVALUAR EL IMPACTO DE LAS AMENAZAS

En la posterior actividad se evaluará el impacto que tiene cada uno de los activos críticos, identificados en las diferentes áreas o departamentos de la organización, los cuales son:

- Ventas
- Ventas Web
- Diseño Pedido
- Producción
- Bodega
- Financiero
- Gerencia

3.1.7.2.ACTIVIDAD S4.2: ESTABLECER CRITERIOS DE EVALUACIÓN PROBABILÍSTICA

Para determinar los criterios probabilísticos de las posibles amenazas que la organización puede tener, se utiliza los criterios de bajo, básico, medio, alto y muy alto; lo cual permite determinar la situación de la empresa en relación a las amenazas, por lo que se detalla a continuación los criterios de evaluación:

Tabla 28 Tabla de Valoración de Criterios de Evaluación
Fuente: (Autores, 2019)

Valoración de Críterios			
Nombre	**Número**	**Descripción**	**Porcentaje**
Bajo	1	La organización en el transcurso de activida no ha tenido ninguna amenaza.	0%
Básico	2	La organización tiene pocas amenazas, pero no han provocado algún perjuicio o daño.	25%
Medio	3	La organización tiene amenazas, que se necesita ayuda para resolverlas y provoca conflictos a la empresa.	50%
Alto	4	La organización tiene amenazas repetitivas, que provocan pérdidas y problemas a las actividades diarias.	75%
Muy Alto	5	La organización no tiene ninguna protección, las amenazas son ocasionadas con facilidad y provoca perdidas económicas y materiales.	100%

Muestra una valoración sobre los criterios de evaluación que van a ser determinados para obtener un porcentaje de que suceda la amenaza

3.1.7.3. ACTIVIDAD S4.3: EVALUAR PROBABILIDADES DE AMENAZAS

Con la tabla de valoración de criterios de evaluación, se podrá asignar un valor de probabilidad para cada amenaza, el cual es detallado a continuación:

Tabla 29 Criterios de Evaluación en referencia al estado actual de la empresa

Críterios de Evaluación								
Amenaza	**Valoración**					**Resultado**		
	1	**2**	**3**	**4**	**5**		**Porcentaje**	
Denegación de Servicio (DoS)		2				Básico	25	%
Espionaje			3			Medio	50	%
Divulgación de Información				4		Alto	75	%
Virus Informático		2				Básico	25	%
Alteración de Información			3			Medio	50	%
Uso no Autorizado			3			Medio	50	%
Robo de Información				4		Alto	75	%
Suplantación de Identidad		2				Básico	25	%
Uso Incorrecto			3			Medio	50	%
Ataque de Fuerza Bruta		2				Básico	25	%
Total							75,00	%

Fuente: (Autores, 2019)

Indica o da a conocer sobre los criterios de evaluación sobre algunas amenazas que la organización se encuentra, indica el nivel tanto bajo, básico, medio, alto y muy alto.

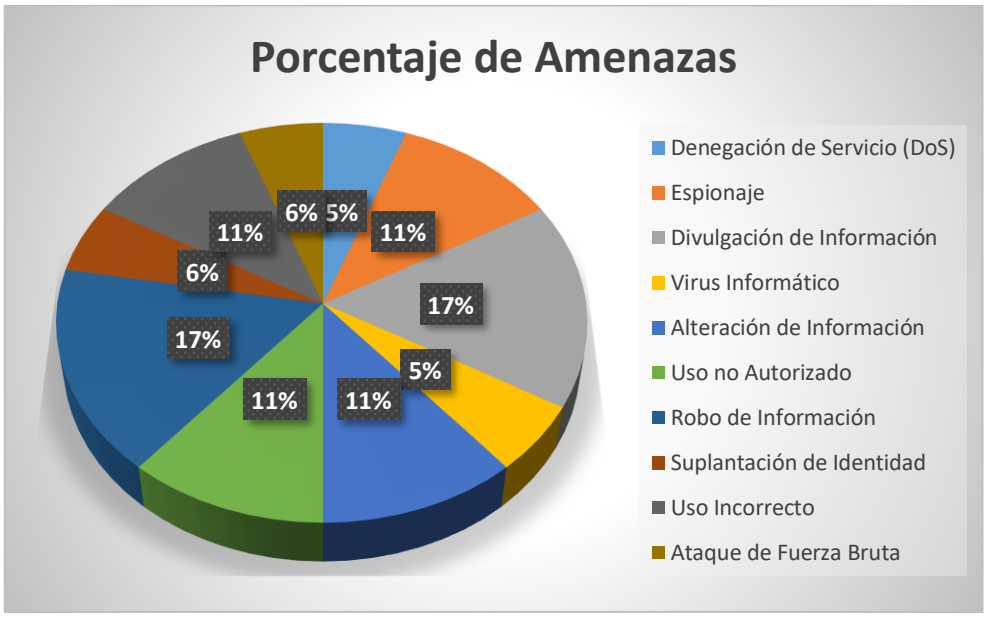


Figura 21 Cuadro Estadístico de Amenazas
Fuente: (Autores, 2019)

3.1.8. PROCESO S5: DESARROLLAR ESTRATEGIAS DE PROTECCIÓN Y PLANES DE MITIGACIÓN

En este proceso basados en los resultados obtenidos por la evaluación de la metodología OCTAVE-S, se planteará estrategias de protección y planes de mitigación para evitar que las amenazas puedan producirse de manera eficiente, provocando problemas para la organización.

3.1.8.1. ACTIVIDAD S5.1: DESCRIBIR LAS ESTRATEGIAS DE PROTECCIÓN ACTUALES

En esta actividad se procede a describir en relación a las prácticas de seguridad que son establecidas por OCTAVE-S, para determinar la protección actual sobre las diversas amenazas que fueron establecidas o descritas anteriormente, en este punto las se divide las 15 prácticas de seguridad en 2 áreas principales:

Tabla 30 Prácticas de Seguridad
Fuente (Autores, 2019)

Área de Práctica de Seguridad Estratégica	**Área de Práctica de Seguridad Operacional**
Concientización y Formación en Seguridad	Control de Acceso Físico
Estrategia de Seguridad	Monitoreo y Auditoria de Seguridad Física
Gestión de Seguridad	Gestión de Sistemas y Redes
Políticas y Regulaciones de Seguridad	Monitoreo y Auditoria de Seguridad de TI
Gestión de Seguridad Colaborativa	Autenticación y Autorización
Planes de Contingencia/Recuperación de Desastres	Gestión de Vulnerabilidades
	Encriptación
	Diseño y Arquitectura de Seguridad
	Gestión de Incidentes

La tabla muestra la información de la practicas de seguridad que OCTAVE-S propone, pero esta vez dividida en las 2 áreas que son estratégica y operacional, la cual permite dar a conocer como está la situación actual de las estrategias de seguridad ante las diversas amenazas de la organización.

En la siguiente tabla muestra la situación actual de la organización:

Tabla 31 Prácticas de Seguridad de la Organización
Fuente (Autores, 2019)

Prácticas de Seguridad			
Práctica Estratégica	**Situación Actual**	**Práctica Operacional**	**Situción Actual**
Concientización y Formación en Seguridad	La organización no realiza charlas u capacitaciones a los empleados para generar concientización sobre no divulgar información sensible a terceros.	Control de Acceso Físico	La organización no cuenta con seguridades físicas adecuadas, como cámaras, en algunas computadoras no cuenta con claves, no contiene biométricos de acceso.
Estrategia de Seguridad	En ningún momento la organización genera alguna estrategia de seguridad que premita brindar seguridad ante las amenazas que pueden surgir en la empresa.	Monitoreo y Auditoria de Seguridad Física	En este punto solo existe una persona a cargo el cuál es el único que debe verificar el mantenmientos; pero en este caso no se lo realiza periodicamente.
Gestión de Seguridad	Al momento de que exista algun problema o amenaza la organización no gestiona los problemas para evitar futuras amenazas.	Gestión de Sistemas y Redes	La organización no cuenta con herramientas o software que permitan mantener gestionar seguridad y el respectivo almacenamiento de datos.
Políticas y Regulaciones de Seguridad	Las organización no cuenta con politicas que permitan a la empresa seguir ciertos procedimientos ante algún incidente o amenaza.	Monitoreo y Auditoria de Seguridad de TI	En este caso igual no existe un sistema que permita monitorear sistemas, red, ni la información; e igual no cuenta con políticas documentadas.
Gestión de Seguridad Colaborativa	La organización no cuenta con políticas de empresas externas, ni con empresas extersas quienes puedan ayudar al control de amenazas.	Autenticación y Autorización	En algunos equipos si se lleva el control de acceso que el jefe otorga a usuarios autorizados, pero en otros equipos no existe control, lo cual provoca usos no autorizados.
Planes de Contingencia/Recuperación de Desastres	La organización no cuenta con planes de contingencia, ni recuperación de desastres, lo cual la vuelve muy vulnerable a que las amenazas provoquen fallas irreparables.	Gestión de Vulnerabilidades	No existe ninguna documentación dentro de la empresa que permita llevar un control y como proceder antes vulnerabilidades que puedan tener los sistemas.
		Encriptación	No cuentan con encriptaciones que eviten ante posibles ataques informáticos, lo cual es una manera fácil de que una amenaza se materialice.
		Diseño y Arquitectura de Seguridad	Algo primordial que la organización debe poseer es la estrucutura de la red, la cual no la posee, en caso de alguna amenaza no se podra tomar acciones.
		Gestión de Incidentes	En algún incidente la organización no tiene conocimientos o planes para poder realizar respaldos o recuperación de información.

Da a conocer sobre la situación actual que la organización se encuentra en relación a las prácticas de seguridad establecidas en las dos áreas, el cual indica sus estrategias de protección

3.1.8.2.ACTIVIDAD S5.2: SELECCIONAR APROXIMIDADES DE MITIGACIÓN

En esta actividad se procede a la selección sobre las prácticas de seguridad a las cuales se va a implementar actividades de mitigación, las que necesitan una mitigación urgente y sobre todo ayude a evitar que las amenazas se materialicen.

Para lo cual se seleccionaron las más importantes para la organización que son:

- ✓ Concientización y Formación en Seguridad: Para mitigar las amenazas en relación a esta práctica se
- ✓ Políticas y Regulaciones de Seguridad.
- ✓ Planes de Contingencia / Recuperación de Desastres.
- ✓ Control de Acceso Físico.

- ✓ Gestión de Sistemas y Redes.
- ✓ Autenticación y Autorización.
- ✓ Encriptación.
- ✓ Diseño y Arquitectura de Seguridad.
- ✓ Gestión de Incidentes.

3.1.8.3.ACTIVIDAD S5.3: DESARROLLAR PLANES DE MITIGACIÓN DE RIESGOS

En la siguiente actividad se plantea los planes de mitigación para contrarrestar las posibles amenazas que pueden surgir en la organización, los cuales son detallados a continuación:

Tabla 32 Prácticas de Seguridad para la Organización
Fuente: (Autores, 2019)

Planes de Mitigación			
Práctica Estratégica	**Actividad de Mitigación**	**Práctica Operacional**	**Situción Actual**
Concientización y Formación en Seguridad	Dar capacitación a los empleados de la empresa, sobre divulgación de información, conocimiento para manejo de software y hardware.	Control de Acceso Físico	Implementar cámaras de seguridad, accesos biométricos para ingreso de personal y control de ingreso y salida de personas.
Estrategia de Seguridad	En ningún momento la organización genera alguna estrategia de seguridad que premita brindar seguridad ante las amenazas que pueden surgir en la empresa.	Monitoreo y Auditoria de Seguridad Física	Usar un programa que permita llevar el monitoreo o control de ingresos al menos guardar por un mes.
Gestión de Seguridad	Poseer un control de seguridad documentado que permita evitar exista una amenaza.	Gestión de Sistemas y Redes	Obtener programas que permitan mantener un respaldo de información en caso de algun incidente, como respaldos en la nube.
Políticas y Regulaciones de Seguridad	Implementar políticas de seguridad para brindar seguridad dentro de la organización.	Monitoreo y Auditoria de Seguridad de TI	Obtener un programa que permita hacer un análisis durante ciertos periodos para anticipar cualquier amenaza que pueda persentar .
Gestión de Seguridad Colaborativa	Contratar al menos una organización que se encargue de la amenaza en caso de no poder resolver por la misma compañía.	Autenticación y Autorización	Para cada uso o manipulación de sistemas, gestionar que el ingreso sea con la autenticación y cambio periódica de claves.
Planes de Contingencia/Recuperación de Desastres	Generar backups tanto de los sistemas, información primordial de la empresa y cualquier otro dato importante para la organización.	Gestión de Vulnerabilidades	Mantener una documentación que permita saber como actuar de manera correcta ante alguna vulnerbilidad del sistema.
		Encriptación	Algún código que permita que la información sea receptada por terceros.
		Diseño y Arquitectura de Seguridad	Desarrollar la estructura de la red, con todos sus componentes, conexiones, equipos y demás activos para conocer la estructura total en caso de amenaza.
		Gestión de Incidentes	Tener documentado todos los incidentes para en repetición saber como afrontarlo de forma rápida y segura.

Presenta las estrategias de mitigación que se debe realizar para brindar seguridad a los activos de información relevantes de la organización, en donde se demuestra en relación a las prácticas de seguridad que OCTAVE-S tiene planteado, así permite que la empresa este seguro ante cualquier amenaza.

3.1.8.4.ACTIVIDAD S5.4: IDENTIFICAR CAMBIOS EN LAS EXTRATEGIAS DE PROTECCIÓN

En esta actividad se da a conocer sobre cambios en las estrategias de protección para las respectivas áreas de prácticas se seguridad.

La organización no posee con muchas de las practicas implementadas las cuales son necesarios cambios y mejoras para aplicar estas prácticas como son:

- ✓ Implementar software para control de acceso, seguridades y sistemas.
- ✓ Mejorar de capacitaciones para empleados.
- ✓ Cambio y asignación de responsables para las áreas.
- ✓ Generar backups de sistema, información y datos.

En este punto no surgen muchos cambios, por motivo que la organización no cuenta con prácticas, se tiene que realizar implementaciones totales.

3.1.8.5.ACTIVIDAD S5.5: IDENTIFICAR LOS SIGUIENTES PASOS

En este último punto se determina las actividades que pueden generar ayuda para facilitar la implementación de los resultados obtenidos, es decir toma de decisiones.

Por lo cual OCTAVE-S propone:

- ✓ Relación de las Evaluaciones Posteriores: En este caso surge que la empresa tenga evaluaciones periódicas sobre las seguridades, amenazas o conflictos que surgen en la organización.
- ✓ Monitoreo de la Implementación del Plan: Tener un control o supervisión si el plan se está llevando a cabo como lo establecido.
- ✓ Aplicación de las Actividades de Mitigación: Que las actividades desarrollar para generar la mitigación de amenazas sean realizadas a cabalidad y con los respectivos procesos determinados.

- ✓ El apoyo por parte de los Altos Funcionarios: Al surgir cualquier problema o conflicto dentro de la organización se tenga el apoyo inmediato de autoridades superiores para solución de los inconvenientes.

CAPITULO 4

APLICACION DEL PLAN DE BUENAS PRÁCTICAS

El desarrollo de un plan de buenas prácticas se realiza con el objetivo de ayudar a la gestión dentro de la empresa, para el buen manejo de su seguridad en hardware y en software, y que de esta manera la empresa pueda evitar pérdidas económicas que involucre su información relevante.

PLAN DE BUENAS PRACTICAS EN EL MANEJO DE SEGURIDAD DE LA INFORMACION.

INTRODUCCION

La información elaborada y manejada dentro de la Industria Referee CIA. LTDA. es establecida como un activo vulnerable, así mismo otros bienes de la organización, puesto que la mayoría de los activos tienen gran valor para la empresa. El plan de buenas prácticas que se mostrará a continuación, pretende educar a los usuarios de la empresa, un manejo correcto para evitar pérdidas de la información tanto, en el sistema manejado internamente, la información enviada a clientes, los productos, los diseños, la página web y los pagos mediante PayPal.

Por esta razón es importante proteger esta información, ya que es la forma más ágil de identificar los procesos y los activos que contienen esta información y como depende de la misma. Así entonces consideramos activos de información a los siguientes elementos:

- **La información** propia de la misma empresa y presentada en variados formatos (papel, digital, texto, imagen, audio, video, etc.)
- **Los equipos/sistemas/estructura** que lleva esta información.
- **Las personas** que utilizan la información, los sistemas y que tienen conocimiento de los procesos que se desarrollan dentro de la empresa.

A continuación, se detallará algunas buenas prácticas que pueden ser aplicadas por los empleados de la Industria Referee CIA. LTDA. para resguardar la información y los sistemas respectivamente.

POLITICAS DE SEGURIDAD DE LA INFORMACION

- El software utilizado por la Industria Referee CIA. LTDA. son de uso interno y solamente para ser utilizado en tareas del servicio que ofrece la empresa.
- La información generada por el personal de la Industria Referee CIA. LTDA. no debe ser entregada ni reproducirse total o parcialmente a personas ajenas que no sean parte del proceso de producción, ni administrativo correspondiente.
- El correo electrónico e internet son de uso exclusivo para la realización de trabajo de la Industria Referee CIA. LTDA. quedando así limitado el uso para otros fines.
- Se prohíbe la descarga de archivos y documentos, transmisión o almacenamiento que se consideran pornográfico, difamatorio, racista, videos, música, o que, de la misma forma atente contra las buenas costumbres o principios de los empleados y empleadores, con excepción de que el trabajo lo merezca.
- Será declarado responsable al usuario que de mal uso del equipo computacional de la empresa durante su trabajo.

MANEJO APROPIADO DE CONTRASEÑAS

- No guardar las contraseñas en ningún tipo de papel, agenda, etc.
- Cambiar periódicamente las contraseñas
- No utilizar la opción de almacenamiento de contraseñas que ofrece Internet.
- No compartir las contraseñas con otros usuarios.
- No utilizar contraseñas con números de teléfono, números de cédulas, nombres de familiares, nombre propio, etc.
- No utilizar contraseñas con variables (referee1, referee2, referee3, etc.)
- Las contraseñas deben cumplir con un nivel de dificultad que incluya el uso de diferentes caracteres

Tabla 33 Clasificación de Caracteres para Contraseñas
Fuente (Autores, 2019)

CATEGORIA DE CARACTERES	EJEMPLOS
Letras mayúsculas	A, B, C
Letras minúsculas	a, b, c
Números	0, 1, 2, 3, 4, 5, 6, 7, 8, 9
Símbolos del teclado (caracteres que no se definen como números o letras).	`? ¿¡‘= / () & % $ · @ # | ª ¨ {} ^ * + _: [ ]

La tabla muestra la clasificación de caracteres

MANEJO APROPIADO DEL ANTIVIRUS

La Industria Referee CIA. LTDA. ha determinado la utilización del producto NOD32 Antivirus en las estaciones de trabajo para proteger el correcto funcionamiento de los equipos a utilizar.

- La detección y el sistema de actualizaciones es diario y automático a nivel central.
- Comunicar cualquier infección de virus que NOD32 Antivirus no haya detectado.
- Los empleados que utilicen los equipos de la empresa no podrán bajo ningún servicio, desinstalar el producto de control de virus existente.
- Los dispositivos de almacenamiento extraíbles, deben ser analizados antes de ser utilizados.

MANEJO DE CUENTAS DEL SISTEMA

- La cuenta que desee ser modificada debe ser solicitada a través de los administradores de los sistemas (Sistema ABAGO, Página Web, Correo Electrónico).
- El procedimiento de creación de usuarios y cuentas debe ser conducido a través de la solicitud correspondiente.
- Cuenta de ABAGO: esta cuenta corresponde a la que utilizara cada usuario para realizar facturación, inventarios, etc.
- Cuenta de correo electrónico: la cuenta de correo electrónico se debe solicitar al departamento encargado de la emisión de usuarios.

La eliminación de cuentas de los usuarios que han abandonado la Industria Referee CIA. LTDA. debe ser inmediata al término del contrato, así se evitará el colapso de usuarios dentro del sistema, para un ingreso más ágil y para el control de los usuarios.

MANEJO DE ACCESO A INTERNET

El acceso a Internet se encontrará protegido por medio de filtros que reducirán sitios peligrosos con código malicioso o que se encuentren ajenos al servicio, de tal manera aumenta la velocidad de acceso a los sitios necesarios y disminuye el riego de virus. Se solicita entonces a los empleados con acceso a internet

- No navegar en sitios no confiables
- Queda prohibido el uso de sitios de radios online
- Queda prohibido el intercambio de archivos mediante plataformas no confiables
- Queda prohibido el uso de Internet para actividades ilícitas

- Se prohíbe a los empleados que utilicen Internet para el acceso a sitios o páginas con contenido amenazador, pornográfico, racista, sexista o cualquier otro que degrade la calidad del ser humano.
- No compartir claves para el ingreso a sitios que lo requiera como bancos, correo empresarial, página web, etc.
- No permitir que el navegador utilizado por los empleados recuerde la contraseña automáticamente.
- Queda prohibido el participar en juegos de entretenimiento en línea.
- El archivo que sea recibido o que se descargue de Internet debe ser analizado por el antivirus para asegurar que no ingrese malware a los equipos.

MANEJO DE CORREO ELECTRONICO

El manejo de correo empresarial cuenta por configuración propia del sistema de filtros para identificar y bloquear correos no deseados (Spam o Virus)

- El correo electrónico será de uso exclusivo para las áreas que necesiten comunicación en el desarrollo del trabajo dentro de la Industria Referee CIA. LTDA.
- Queda prohibido el uso del correo electrónico con fines personales, para envío, transferencia o almacenamiento de información de carácter pornográfico, difamatorio, racista, música, videos, o que atente contra las buenas costumbres o principios.
- Se debe cambiar la contraseña periódicamente que incluya letras, números y caracteres
- No ingresar a links sospechosos llegados por correos electrónicos de dudosa procedencia (bancos, tiendas, etc.)
- No completar datos personales en correos electrónicos sospechosos.
- Eliminar correo no deseado o Spam
- No se permitirá el envío de correos que superen los 5MB

MANEJO DE REDES SOCIALES

La Industria Referee CIA. LTDA. tiene cuentas en variadas redes sociales las cuales permiten dar a conocer el trabajo que se realiza en la empresa y publicitarlas, la empresa cuenta con personal asignado para el manejo de estas redes sociales.

- Queda prohibido la utilización de redes sociales de la Industria Referee CIA. LTDA. con fines personales o que no estén orientadas a el trabajo de la empresa.

- No se permitirá postear fotos, publicaciones, artículos o cualquier otro, que atenten contra la integridad de las personas.
- Se deberá postear información o publicaciones orientadas al tipo de servicio que se da en la Industria Referee CIA. LTDA.
- Cualquier foto subida, comentario, publicación o artículo en Facebook, Twitter, Instagram o en alguna red social es responsabilidad exclusiva de quien la emite.

MANEJO DE SOFTWARE (SISTEMA, PAGINA WEB, S.O, SERVIDOR)

- Queda prohibida la total instalación de programas que no sean de necesidad para la empresa y que no cumpla con las instrucciones requeridas en los equipos de la Industria Referee CIA. LTDA.
- Los usuarios no deben instalar, ni descargar aplicaciones que podrían provocar alguna vulnerabilidad interna en los equipos de la empresa.
- El servidor y sistemas operativos de los distintos equipos de la Industria Referee CIA. LTDA. deben contar con la licencia original.
- Los antivirus deben contar con las licencias de originalidad, ser actualizados y renovados antes de que se cumpla el periodo de uso.

Mediante el análisis realizado y con el plan de buenas prácticas diseñado se obtuvo los resultados:

Tabla 34 Criterios de Evaluación Sin Implementación
Fuente (Autores, 2019)

Criterios de Evaluación								
Amenaza	**Valoración**					**Resultado**		
	1	**2**	**3**	**4**	**5**		**Porcentaje**	
Denegación de Servicio (DoS)		2				Básico	25	%
Espionaje			3			Medio	50	%
Divulgación de Información				4		Alto	75	%
Virus Informático		2				Básico	25	%
Alteración de Información			3			Medio	50	%
Uso no Autorizado			3			Medio	50	%
Robo de Información				4		Alto	75	%
Suplantación de Identidad		2				Básico	25	%
Uso Incorrecto			3			Medio	50	%
Ataque de Fuerza Bruta		2				Básico	25	%
Total							75,00	%

Resultados obtenidos del análisis mediante Octave-S para la Industria Referee que muestra amenazas, su valoración y el resultado con el que afecta a la empresa, de la misma manera el porcentaje que esta tabla de análisis representa.

Tabla 35 Criterios de Evaluación con Capacitación
Fuente (Autores, 2019)

Críterios de Evaluación/ Implementado Capacitación								
Amenaza	**Valoración**					**Resultado**		
	1	**2**	**3**	**4**	**5**		**Porcentaje**	
Denegación de Servicio (DoS)		2				Básico	25	%
Espionaje			3			Medio	50	%
Divulgación de Información			3			Medio	50	%
Virus Informático		2				Básico	25	%
Alteración de Información		2				Básico	25	%
Uso no Autorizado		2				Básico	25	%
Robo de Información			3			Medio	50	%
Suplantación de Identidad		2				Básico	25	%
Uso Incorrecto		2				Básico	25	%
Ataque de Fuerza Bruta		2				Básico	25	%
Total							54,17	%

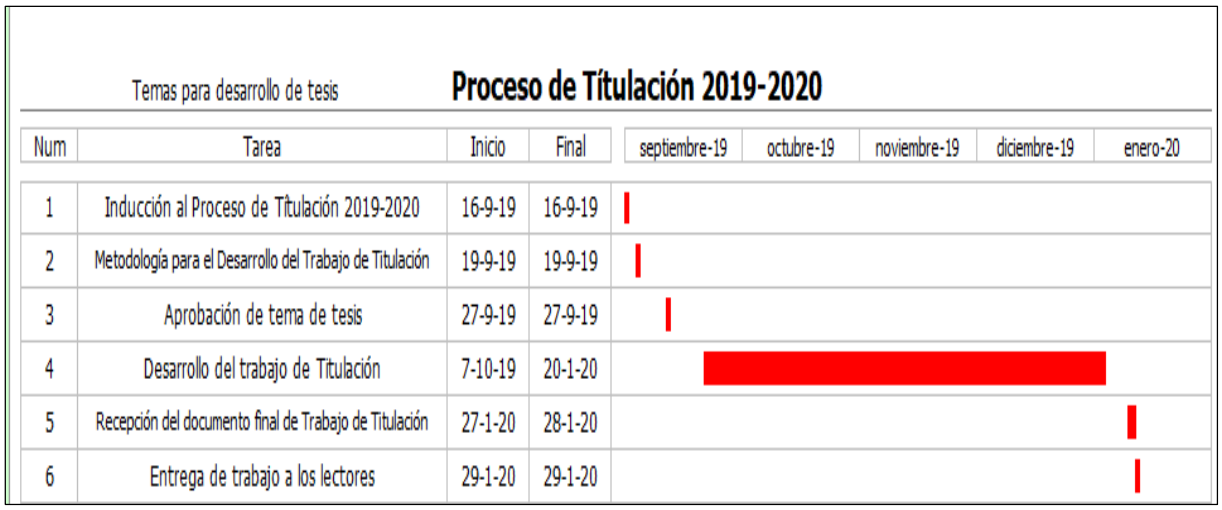
Resultados obtenidos basando el porcentaje inicial, con esta tabla que nos presenta el porcentaje de riesgos reducidos con la implementación de la capacitación a los empleados de la Industria Referee.

Tabla 36 Criterios de Evaluación con Implementación de Plan de Buenas Prácticas
Fuente (Autores,2019)

Críterios de Evaluación/ Implementado Buenas Prácticas								
Amenaza	**Valoración**					**Resultado**		
	1	**2**	**3**	**4**	**5**		**Porcentaje**	
Denegación de Servicio (DoS)		2				Básico	25	%
Espionaje		2				Básico	25	%
Divulgación de Información	1					Bajo	0	%
Virus Informático	1					Bajo	0	%
Alteración de Información	1					Bajo	0	%
Uso no Autorizado	1					Bajo	0	%
Robo de Información		2				Básico	25	%
Suplantación de Identidad		2				Básico	25	%
Uso Incorrecto	1					Bajo	0	%
Ataque de Fuerza Bruta	1					Bajo	0	%
Total							16,67	%

Resultado final de la evaluación de las amenazas en la Industria Referee con la implementación de el plan de buenas prácticas diseñado para la empresa.

CRONOGRAMA



Num	Tarea	Inicio	Final
1	Inducción al Proceso de Titulación 2019-2020	16-9-19	16-9-19
2	Metodología para el Desarrollo del Trabajo de Titulación	19-9-19	19-9-19
3	Aprobación de tema de tesis	27-9-19	27-9-19
4	Desarrollo del trabajo de Titulación	7-10-19	20-1-20
5	Recepción del documento final de Trabajo de Titulación	27-1-20	28-1-20
6	Entrega de trabajo a los lectores	29-1-20	29-1-20

Figura 22 Cronograma de actividades para el desarrollo del Proyecto de Tesis

Fuente (Autores,2019)

CONCLUSIONES

Las empresas ecuatorianas aún no consideran importante la seguridad en sus activos de información y los equipos que lo contienen. Mediante el análisis realizado a la Industria Referee CIA. LTDA. se pudo observar y de la misma forma obtener resultados lo bastante elevados para una empresa que maneja información a través de hardware, puesto que ellos no habían decidido a la implementación de seguridad en su red para evitar perdida de información y datos relevantes de la organización.

Al realizar el análisis de las vulnerabilidades y seguridades con las que contada la red de la Industria Referee CIA. LTDA. notamos la carencia de seguridad dentro de los sistemas que se manejan en la empresa. De esta manera mediante la Metodología Octave-S realizamos la valoración de amenazas que surgen en la red de la empresa puesto que la mayoría de equipos, personal y sistemas no se encuentran protegidos.

Al realizar esta valoración, procedimos a determinar el grado en el que se encontró expuesto los activos vulnerables de la red y cómo afectaría a la empresa si estos no se lograran mitigar. Para así evitar pérdidas de información mediante los riesgos que se presentaron en el análisis. Se presentaron por un análisis porcentual, la evaluación de riesgos de la empresa y sus cantidades más representativas para que generar la solución que aporte a la seguridad de la empresa

Finalmente se procedió a generar un plan de buenas prácticas para que, mediante esta guía, la empresa tenga en consideración que se debe proteger dentro de la empresa y su red. Conociendo cual será el costo de implementación y porque se lo debe implementar.

RECOMENDACIONES

Una vez que fue concluida la tesis, se considera apropiado investigar sobre otros aspectos que acojan temas relacionados con la seguridad de la información, con sus activos y se propone:

Invertir en la seguridad de la red la empresa lo que podrá evitar generar pérdidas económicas y de información, basándose en una metodología acorde a la infraestructura de la empresa, sus equipos, sus empleados, etc.

Trabajar en aplicar el plan de buenas prácticas, diseñado acorde a las necesidades de la empresa lo que permitirá mantener la seguridad de la red y disminuir las vulnerabilidades en la misma.

Analizar con detenimiento y buscar la razón del porque en la empresa se puede generar pérdidas de información, y de la misma manera si es ocasionado por sus equipos, la red o el personal que funciona internamente en la empresa.

Ampliar los estudios expuestos en esta tesis para la implementación de la seguridad de la red, y que permita a quienes lo realizaron un análisis más amplio para una salvaguarda más exitosa.

BIBLIOGRAFÍA

ACISSI. (2018). *Seguridad Informática, Hacking Ético.* Francia: Ediciones ENI.

Aguilera, P. (2017). *Seguridad Informática(Seguridad en el Entorno Físico).* Editex.

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2017). *OCTAVE- Implementation Guide.* Pittsburgh: Hanscom AFB.

Alberts, C., Dorofee, A., Stevens, J., & Woody, C. (2017). *OCTAVE- Implementation Guide.* Pittsburgh: Hanscom AFB.

Alegre, M. d., & Cervigón, A. (2017). *Seguridad Informática Ed.11.* Madrid: Parainfo.

Areitio Bertolín, J. (2017). *Seguridad de la Información. Redes, Informática y Sistemas de Información.* Madrid, España: Cengage Learning Paraninfo S.A.

Belloso, R. (2017). *Modelo de Auditoría para Servicios Telemáticos de la Universidad Simón Bolívar .* Maracaibo: Telématique Vol. 16.

Castillo, J. (s.f.).

Castillo, J. A. (2018). *Modelo OSI: que es y para que se utiliza.* Bogotá: Profesional Review.

Deloitte. (2018). *Ciberseguridad.* Quito.

Gómez, R., Pérez, D., Donoso, Y., & Herrera, A. (2017). *Metodología y gobierno de la gestión de riesgos de tecnología de la información.* Bogotá.

Hernández, L., & Mejia, J. (2017). Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. *ReCIBE*, 7-8.

Hurtado, M. (2017). *Gestión de riesgo de metolodogías OCTAVE y MAGERIT.* Girardot.

Junta de Andalucía. (Febrero de 2017). *Marco de Desarrollo de la Junta de Andalucía* . Obtenido de http://www.juntadeandalucia.es/servicios/madeja/sites/default/files/historico/1.3.0/contenido-recurso-216.html#ISSAF

López, D., & Vásquez , S. (2017). *Universidad del Azuay*. Obtenido de Respositorio Institucional: http://dspace.uazuay.edu.ec/handle/datos/5391

MINTEL (Ministerio de Telecomunicaciones y Sociedad de la Información). (2018). Libro Blanco de la Sociedad de la Información y Conocimiento. En MINTEL, *Libro Blanco de la Sociedad de la Información y Conocimiento* (págs. 46-52). Quito: Coordinación Editoral.

Oficina Nacional de Gobierno Electrónico e Informática del Perú. (2018). *Talle de Implementacióm de la Norma Iso 27001.* Lima: Oficina Nacional de Gobierno Electrónico e Informática.

Ríos, R., & Fermín, J. (2017). ANÁLISIS DE TRÁFICO DE UNA RED LOCAL UNIVERSITARIA. *Redalyc*, 17.

Tolosa, G. (2017). *Protocolos y Modelo OSI.* New Site, Alabama: Adventure Works .

GLOSARIO

Activos: son los bienes, derechos y otros recursos de los que dispone o dispondrá una empresa.

Autentificación: proceso de intento para verificar la identidad digital del remitente de una comunicación como una petición para conectarse.

Backup: es una copia de los datos originales que se realiza con el fin de disponer de un medio para recuperarlos en caso de su pérdida.

Base de Datos: es un conjunto de datos pertenecientes a un mismo contexto y almacenados sistemáticamente para su posterior uso.

Caracteres: es una unidad de información que corresponde a una unidad o símbolo, como los de un alfabeto o silabario de forma escrita de un lenguaje natural

Ciber Riesgos: son los nuevos riesgos de la era digital que involucran las nuevas tecnologías dentro de las empresas

Codificación: es la representación y la expresión de información o procesos en un lenguaje de programación

Completitud: es la propiedad meta teórica que tiene los sistemas formales cuando las formulas lógicas validas del sistema son también teoremas del sistema.

Comunidad Activa: conjunto de personas con peculiaridades idénticas en la utilización de software y hardware de características comunes.

Contingencia: suceso que puede ocurrir o no, especialmente un problema que se plantea de forma imprevista.

Contramedida: medida que se toma para anular otra, especialmente, conjunto de sistemas destinado a neutralizar los dispositivos enemigos

Correctitud: corresponde a una propiedad que distingue a un algoritmo de un procedimiento efectivo.

Encriptación: manera de codificar la información para protegerla frente a terceros, para que no pueda ser descifrado.

Framework: es un entorno de trabajo o marco de trabajo es un conjunto estandarizado de conceptos, prácticas y criterios para enfocar un tipo de problemática

Hacking: consiste en la detección de vulnerabilidades de seguridad.

Intercomunicación: es la capacidad y necesidad de transmisión reciproca de información, datos, conocimientos, experiencias, entre 2 o más personas.

ISP: es el proveedor de servicios de Internet (ISP) sus siglas en inglés, es la empresa que brinda conexión a Internet a sus clientes

Malware: hace referencia a cualquier tipo de software maligno que trata de afectar a un ordenador, teléfono celular u otro dispositivo.

Manipulación: hacer cambios o alteraciones en una cosa interesadamente para conseguir un fin determinado

Materialización: hacer real y concreto un proyecto, idea, deseo, etc.

Mitigar: atenuar o suavizar una cosa negativa, especialmente algo que afecte.

Petición: serie de palabras o escrito con que se pide una cosa

Preventivo: que previene un mal o un peligro o sirve para prevenirlo

Red LAN: son las siglas de Local Area Network, Red de Área Local. Es una red que conecta los ordenadores en un área relativamente pequeña y predeterminada

Red WAN: son las siglas de Wide Area Network, Red de Área Amplia. Se utiliza para nombrar una red de computadores que se extiende en una gran franja de territorio.

Repetidores: es un dispositivo analógico que amplifica una señal de entrada, independientemente de su naturaleza.

Router: es un dispositivo que permite interconectar computadoras que funcionan en el marco de una red

Servidor: es una aplicación en ejecución capaz de atender las peticiones de un cliente y devolverle una respuesta en concordancia.

Subprocesos: es un conjunto de actividades que tienen una secuencia lógica para cumplir un propósito.

Switch: es un dispositivo digital lógico de interconexión de equipos que opera en la capa de enlace de datos del modelo OSI

T.I: la Tecnología de la Información es la aplicación de ordenadores y equipos de telecomunicaciones para almacenar, recuperar, transmitir y manipular datos con frecuencia.

Testeo: es el proceso empleado para identificar la correctitud, completitud, seguridad y calidad en el desarrollo de un software para computadoras.

TIC: se denominan Tecnologías de la Información y Comunicación, pues permiten la adquisición, producción, almacenamiento, tratamiento, comunicación, registro y presentación de informaciones en forma de voz, imágenes y datos.

Transmisión: es la transferencia física de datos por un canal de comunicación punto a punto o punto a multipunto.

VPN: una red privada virtual, es una tecnología de red de ordenadores que permiten una extensión segura de la red de área local sobre una red pública o no controlada como Internet.

ANEXOS

Tabla 37 Proforma 1 Desarrollo y Capacitación
Fuente: (Autores,2019)

PRESUPUESTO DE DESARROLLO + CAPACITACIÓN						
Ítem		**Cantidad**	**Tiempo / Horas**	**Precio**	**Subtotal**	**Total Ítem**
A	Personal					
	Persona 1	1	170	2,08	353,60	
	Persona 2	1	170	2,08	353,60	
						707,20
B	Equipos					
	Computador	2		5,55	5,55	
						5,55
C	Servicios					
	Internet	2		100,00	100,00	
	Energía	2		35,00	35,00	
	Agua	2		25,00	25,00	
						160,00
D	Materiales					
	Copias			5,00	5,00	
	Otros varios			10,00	10,00	
						15,00
E	Formación					
	Capacitación	2	6	10,00	60,00	
						60,00
	TOTAL					**947,75**

Tabla 38 Proforma 2 Desarrollo, Capacitación e Implementación Plan de Buenas Prácticas
Fuente (Autores, 2019)

PRESUPUESTO DE DESARROLLO + PLAN DE BUENAS PRÁCTICAS						
Ítem		**Cantidad**	**Tiempo / Horas**	**Precio**	**Subtotal**	**Total Ítem**
A	Personal					
	Persona 1	1	340	2,08	707,20	
	Persona 2	1	340	2,08	707,20	
						1414,40
B	Equipos					
	Computador	2		5,55	5,55	
						5,55
C	Servicios					
	Internet	2		100,00	100,00	
	Energía	2		35,00	35,00	
	Agua	2		25,00	25,00	
						160,00
D	Materiales					
	Copias			5,00	5,00	
	Otros varios			10,00	10,00	
						15,00
E	Formación					
	Capacitación	2	6	10,00	60,00	
						60,00
F	Implementación					
	Licencia Antivirus	1		15,00	15,00	
	Firewall	3		160,00	480,00	
	Políticas de Seguridad			50,00	50,00	
	Programas	2		120,00	240,00	
	Almacenamiento en la Nube	1		150,00	150,00	
						935,00
	TOTAL					**2589,95**

BUENAS PRÁCTICAS DE SEGURIDAD INFORMÁTICA

LOS EMPLEADOS DEBEN TENER EN CUENTA LAS SIGUIENTES RECOMENDACIONES

MANEJO APROPIADO DE CONTRASEÑAS

POLITICAS DE SEGURIDAD

MANEJO APROPIADO DE ANTIVIRUS

USO CORRECTO DE CUENTAS DE USUARIO

ACCESO A INTERNET

USO ADECUADO DE CORREO EMPRESARIAL

MANEJO DE SOFTWARE DEL SISTEMA, S.O., ETC.

MANEJO APROPIADO DE REDES SOCIALES