



**UNIVERSIDAD DE GUAYAQUIL
FACULTAD DE INGENIERÍA INDUSTRIAL
DEPARTAMENTO ACADÉMICO DE GRADUACIÓN**

**TRABAJO DE TITULACIÓN
PREVIO A LA OBTENCIÓN DEL TÍTULO DE
INGENIERÍA EN TELEINFORMÁTICA**

**ÁREA
TECNOLOGÍA DE LOS ORDENADORES**

**TEMA
“DISEÑO DE PROTOCOLO DE SEGURIDAD POST-
EVENTO INFORMÁTICO BASADO EN LA NORMA
ISO/IEC-17799 PARA LA FACULTAD DE
INGENIERÍA INDUSTRIAL”**

**AUTOR
PÁRRAGA OLVERA RENÉ GREGORIO**

**DIRECTOR DEL TRABAJO
ING. TELECOM. PINOS GUERRA MARIO, MSIA**

**2018
GUAYAQUIL – ECUADOR**

DECLARACIÓN DE AUDITORÍA

“La responsabilidad del contenido de este trabajo de titulación, me corresponden exclusivamente; y el patrimonio intelectual del mismo a la Facultad de Ingeniería Industrial de la Universidad de Guayaquil”

Párraga Olvera René Gregorio

C.I. No. 1311219297

AGREDECIMIENTO

A Dios que me dio la sabiduría, la fortaleza, la salud, la perseverancia para terminar este proyecto.

A mis padres, quienes me han dado su amor, sus esfuerzos, su trabajo y que me han enseñado a luchar cada día para alcanzar mis metas.

A mi hermana por estar pendiente cada día de mí y de mi salud.

A mi pareja por darme esa fortaleza de seguir adelante cada día sin importar los obstáculos que se presente y superarlos.

A mi tutor, Ing. Mario Pinos, gracias a su ayuda y sus conocimientos he podido terminar este proyecto.

ÍNDICE GENERAL

N°	Descripción	Pág.
	Introducción	1

CAPÍTULO I EL PROBLEMA

N°	Descripción	Pág.
1.1	Introducción	2
1.2	Planteamiento del Problema	3
1.3	Objetivo de la Investigación.	4
1.4	Justificación.	4
1.5	Objetivos generales.	5
1.5.1	Objetivos específicos.	5
1.6	Delimitación del problema	6

CAPÍTULO II MARCO TEÓRICO

N°	Descripción	Pág.
2	Antecedentes del Estudio	8
2.1	Importancia de la Seguridad Informática	8
2.2	Fundamentación Teórica	9
2.2.1	Resumen de la ISO/IEC-17799	9
2.3	Seguridad de la información	11
2.3.1	Seguridad Organizacional	12
2.3.2	Seguridad Lógica	12
2.3.3	Seguridad Legal	12
2.3.4	Seguridad Física	12
2.4	Análisis de Riesgos	13

N°	Descripción	Pág.
2.4.1	Definición del Riesgo	13
2.4.2	Riesgos de Seguridad Digital	15
2.4.3	Riesgos de Privacidad	17
2.4.4	Factores de Riesgos	17
2.5	Amenazas a la Seguridad de la información	18
2.5.1	Tipos de Amenazas	19
2.5.2	Cómo Actuar Frente una Amenaza	19
2.6	Los Activos de una Organización	22
2.6.1	Riesgos para los Activos de la Seguridad de la Información	24
2.7	Política de Seguridad de la información	25
2.7.1	Política para Uso de Dispositivos Móviles.	27
2.8	Política para uso de Conexiones Remotas	27
2.9	Políticas de Seguridad de los Recursos Humanos	27
2.9.1	Políticas Antes de Asumir el Empleo	27
2.9.2	Políticas Durante la Ejecución del Empleo	28
2.9.3	Política de Terminación de Cambio de Empleo	28
2.10	Políticas de Gestión de Activos de Información	28
2.10.1	Política de Responsabilidad por los Activos.	28
2.10.2	Política de Clasificación y Etiquetado de la Información	29
2.10.3	Política de Manejo de Medios	29
2.11	Política de Control de Acceso	29
2.11.1	Política de Acceso a Redes y Recursos de Red	29
2.11.2	Política de Responsabilidades de Acceso de los Usuarios	30
2.12	Política de Criptografía	30
2.12.1	Política de Controles Criptográficos	30

N°	Descripción	Pág.
2.12.2	Política de Áreas Seguras	30
2.12.3	Políticas de Seguridad de las Operaciones	31
2.12.4	Política de Protección contra Código Maliciosos	31
2.12.5	Política de Copias de Respaldo de la Información	31
2.13	Políticas de Seguridad de las Comunicaciones	31
2.13.1	Política de Gestión de la Seguridad de las Redes	31
2.13.2	Política de Uso del Correo Electrónico Institucional	32
2.13.3	Política de Uso Adecuado de Internet	32
2.14	Política de Destrucción de Datos	32
2.15	Política de Administración de los Firewalls	32
2.16	Protocolos de seguridad de la Información	32
2.17	Ingeniería Social	33
2.17.1	Formas de Ataque de la Ingeniería Social	35
2.17.2	Como defenderse con la Ingeniería Social	36
2.18	Antecedentes Legales	37
2.18.1	Delitos contra la Seguridad de los activos de los sistemas de información y comunicación dentro de la Organización	37

CAPÍTULO III METODOLOGÍA

N°	Descripción	Pág.
3.1	Diseño de la Investigación	40

N°	Descripción	Pág.
3.1.1	Modalidad de la Investigación	40
3.2	Justificación de elección de Métodos	40
3.3	Procedimientos de la Investigación	42
3.4	Población y Muestra	43
3.5	Delimitación de la Población	43
3.6	Técnicas e instrumentos	43
3.7	Tipo de Muestra	44
3.7.1	Tamaño de la Muestra	44
3.7.2	Calculo del Tamaño de la muestra desconociendo el tamaño de la población.	45
3.8	Proceso de selección	45
3.9	Viabilidad del estudio	46
3.10	Alcances y limitaciones del proyecto	47
3.11	Análisis de los activos	47
3.12	Valoración de la Activos	51
3.13	Identificación y Valoración de las Amenazas	53
3.14	Importancia de la implementación de un protocolo de seguridad Post-evento informático en la Facultad de Ingeniería Industrial	64

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

N°	Descripción	Pág.
4.1	Título de la Propuesta	66
4.2	Objetivos de la propuesta	66
4.2.1	Objetivo General	66
4.2.2	Objetivos específicos.	66

N°	Descripción	Pág.
4.3	Elaboración de la propuesta	67
4.3.1	Análisis de las posibles fallas de seguridad en la Facultad de Ingeniería Industrial	67
4.4	Vulnerabilidades encontradas	67
4.5	Protocolos de seguridad de la información	68
4.5.1	Introducción	68
4.5.2	Alcance	69
4.5.3	Compromiso de la dirección	69
4.5.4	Actualización	70
4.5.5	Lineamientos de políticas de seguridad	70
4.6	Políticas de seguridad de la información	71
4.6.1	Políticas de la Organización de la Seguridad de la Información	71
4.6.2	Políticas de Seguridad de los Recursos Humanos	76
4.6.3	Políticas de Gestión de Activos de Información	78
4.6.4	Política de Control de Acceso	80
4.6.5	Políticas de Criptografía	83
4.6.6	Políticas de Seguridad de las Operaciones	86
4.6.7	Políticas de seguridad de las comunicaciones	88
4.6.8	Políticas de Gestión de Incidentes de Seguridad de la Información	90
4.6.9	Política de administración de Servidores	
4.6.10	Sanciones	
4.7	Conclusiones	92
4.8	Recomendaciones	93
	ANEXO	95
	BIBLIOGRAFÍA	116

ÍNDICE DE TABLAS

N°	Descripción	Pág.
1	Tabla de los factores de riesgos que afectan la seguridad de la información	18
2	Laboratorios de la Facultad de Ingeniería Industrial	47
3	Identificación de los activos de la Facultad de Ingeniería Industrial	50
4	Tabla de escala de valoración de los activos mediante calificación	51
5	Valoración de los activos de la Facultad de Ingeniería Industrial de acuerdo con su escala de gravedad	52
6	Tabla de probabilidad de frecuencia en que ocurren la amenazas	53
7	Tabla porcentual del nivel de frecuencias de las amenazas	53
8	Tabla de análisis de amenazas de los activos de información	54
9	Nivel de riesgo totalizado de acuerdo con su nivel de amenaza	64
10	Nivel de riesgo de las vulnerabilidades encontradas en la Facultad de Ingeniería Industrial	69
11	Nivel de conocimiento de sus funciones laborables	96
12	Nivel de conocimiento que hay políticas de seguridad de la Facultad de Ingeniería Industrial	97

N°	Descripción	Pág.
13	Nivel de conocimiento de las políticas de seguridad de la Facultad de Ingeniería Industrial	98
14	Nivel de capacitación de las políticas de seguridad de información la Facultad de Ingeniería Industrial	99
15	Manejo de activos informáticos la Facultad de Ingeniería Industrial	100
16	Nivel de acceso de los usuarios a internet desde computador o laptop en la Facultad de Ingeniería Industrial	101
17	Almacena información confidencial en su computador de la Facultad de Ingeniería Industrial	102
18	Comparte esta información sin cifrarla por algún medio informático	103
19	Se realiza copias de seguridad de la información en el computador de la Facultad de Ingeniería Industrial	104
20	Tiene cuenta de correo electrónico institucional Facultad de Ingeniería Industrial	105
21	Conoce la clave de su correo electrónico institucional Facultad de Ingeniería Industrial de la Universidad de Guayaquil	106
22	Cuenta con clave de acceso a su computador de trabajo en la Facultad de Ingeniería Industrial	107

N°	Descripción	Pág.
23	Cambia periódicamente las claves de acceso a su computador de trabajo o correo en la Facultad de Ingeniería Industrial	108
24	Cuenta con un comité de seguridad de la información en la Facultad de Ingeniería Industrial	109
25	Se realizan evaluaciones de seguridad por entidades públicas o privadas en la Facultad de Ingeniería Industrial	111
26	Se encuentra preparado por incidentes que sucedan en los sistemas de información en la Facultad de Ingeniería Industrial	112

ÍNDICE DE FIGURAS

N°	Descripción	Pág.
1	Fórmula del riesgo de la seguridad de la información	14
2	Cuadro de riesgo de seguridad y privacidad de la información	14
3	Principales factores que causan una pérdida de información.	18
4	Principales Amenazas en la Seguridad de Información	20
5	Metodología de un sistema de seguridad	22
6	Nivel de riesgo en los activos de información dentro de la organización	24

N°	Descripción	Pág.
7	Define el proceso del sistema de gestión seguridad de la información	26
8	Ingeniería social en los usuarios para seguridad dentro de la organización	34
9	Técnicas de ingeniería social	36
10	Demostración de la cadena de seguridad	37
11	Fórmula para calcular el tamaño de la muestra	45
12	Numero de computadoras en el área administrativa	48
13	Estructura de la red de la Facultad de Ingeniería Industrial	49

ÍNDICE DE GRÁFICOS

N°	Descripción	Pág.
1	Resultado de nivel de conocimiento de sus funciones laborables	96
2	Resultado de nivel de conocimiento que hay políticas de seguridad de la Facultad de Ingeniería Industrial	97
3	Resultado de nivel de conocimiento de las políticas de seguridad de la Facultad de Ingeniería Industrial	98

N°	Descripción	Pág.
4	Resultado de nivel de capacitación de las políticas de seguridad información de la Facultad de Ingeniería Industrial	99
5	Resultado del manejo de activos informáticos de la Facultad de Ingeniería Industrial	100
6	Resultado nivel de acceso de los usuarios a internet desde computador o laptop de la Facultad de Ingeniería Industrial	101
7	Resultado de almacena información confidencial en su computador de la Facultad de Ingeniería Industrial	102
8	Resultado de comparte información sin cifrarla por algún medio informático	103
9	Resultado se realiza copias de seguridad de la información en el computador de la Facultad de Ingeniería Industrial	104
10	Resultado debe tener cuenta de correo electrónico institucional Facultad de Ingeniería Industrial	105
11	Resultado de conocer la clave de su correo electrónico institucional Facultad de Ingeniería Industrial de la Universidad de Guayaquil	106
12	Resultado de cuenta con clave de acceso a su computador de trabajo en la Facultad de Ingeniería Industrial	107
13	Resultado de cambia periódicamente las claves de acceso a su computador de trabajo o correo en la Facultad de Ingeniería Industrial	108

N°	Descripción	Pág.
14	Resultado de cuenta con un comité de seguridad de la información en la Facultad de Ingeniería Industrial	109
15	Resultado de se realizan evaluaciones de seguridad por entidades públicas o privadas en la Facultad de Ingeniería Industrial	111
16	Resultado de encuentra preparado por incidentes que sucedan en los sistemas de información en la Facultad de Ingeniería Industrial	112

ÍNDICE DE ANEXOS

N°	Descripción	Pág.
1	Encuestas realizadas al personal administrativo y profesores de las distintas carreras de la Facultad de Ingeniería Industrial de la Universidad estatal de Guayaquil	96
2	Pruebas de las políticas de seguridad de la información para los empleados de la Facultad de Ingeniería Industrial	113
3	Formato de reporte de incidentes de la seguridad de la información	114
4	Formato de ingreso y eliminación de usuarios	115

AUTOR: PÁRRAGA OLVERA RENÉ GREGORIO
**TÍTULO: DISEÑO DE UN PROTOCOLO DE SEGURIDAD POST-
 EVENTO INFORMÁTICO BASADO EN LA NORMA ISO/IEC-
 17799 PARA LA FACULTAD DE INGENIERÍA INDUSTRIAL**
DIRECTOR: ING. TELEC. PINOS GUERRA MARIO, MSIA.

RESUMEN

La presente investigación está basada en cómo actuar en diferentes post-eventos informáticos que se haya generado en la facultad de ingeniería industrial, es decir, las vulnerabilidades que se encuentren en los sistemas operativos, aplicaciones, base de datos, software que se utilicen dentro la institución y el hardware que puedan ocasionar la perdida de información o alterar las bases datos, por lo tanto, todos los equipos que se encuentren dentro de la infraestructura, es decir, servidores y computadoras en áreas administrativas deben tener vigente los antivirus y todas las firmas actualizadas al día, por la tanto, este proyecto muestra el diseño del protocolo basado en la norma ISO/IEC-17799 que permita generar buenas prácticas en la seguridad de la información por lo que se mantiene la base de datos seguras. La seguridad informática y de información es la disciplina que se encarga de implementar los procedimientos, normas, técnicas y métodos que se designa para conseguir que el sistema de información sea confiable y seguro. Este protocolo se realizó como proyecto de tesis por lo que es un activo importante que debe poseer una organización este protocolo de seguridad aseguran tanto la parte física (hardware) y la lógica (software) y las mantiene protegidas basándose de los protocolos de seguridad de la información propuestos en este proyecto.

PALABRAS CLAVES: Información, Datos, Seguridad, Sistemas, Protocolo.

Párraga Olvera René Gregorio Ing. Telecomunicaciones Pinos Guerra Mario, MSIA

C.C 1311219297 Director del trabajo

AUTHOR: PARRAGA OLVERA RENE GREGORIO
TOPIC: SECURITY PROTOCOL POST- EVENT INFORMATIC
DESIGN FOR THE INDUSTRIAL ENGINEERING
FACULTY BASED ON THE ISO/IEC-17799 PROTOCOL
DIRECTOR: TE PINOS GUERRA MARIO, SIAM

ABSTRACT

This research is based on how to proceed in different computer post-events that have been generated in the Industrial Engineering faculty of the University of Guayaquil, that means how to find all the vulnerabilities that can be detected on the operative systems, applications, database, the software that is used in the institution and also the hardware that may cause the loss of information or alter them, therefore all the equipment that is inside the infrastructure, that means: servers and computers in administrative department that have the antivirus licenses and other signatures must have been updated. This project shows the design of the protocol based on the ISO / IEC-17799 standard that allows to generate good practices in information security, which is why the secure database is maintained. Computer and information security is the discipline that is responsible for implementing procedures, standards, techniques and methods that are designed to make the information system reliable and safe. This protocol was made as a thesis project so it is an important asset that an organization must have; this security protocol ensure both the physical (hardware) and logic (software), and keeps them protected based on the security protocol of information that is proposed in this project.

Keywords: Information, data, security, systems, protocol.

Párraga Olvera René Gregorio

I.C 1311219297

T E Pinos Guerra Mario, SIAM

Director of work

INTRODUCCIÓN

La presente investigación tiene como objetivo principal establecer un protocolo post-evento informático de las inseguridades eventuales existentes en la Facultad de Ingeniería Industrial en la Universidad de Guayaquil. Que se puedan dar soluciones a los problemas o sucesos que se generen dentro de la Facultad.

Esta investigación esta constituida por tres capítulos que se detallaran a continuación:

Primer capítulo: Abarca la problemática existente en la seguridad informática y la realización de un protocolo post-evento de la Facultad de Ingeniería Industrial en la Universidad de Guayaquil, justificativos de la investigación, objetivos a alcanzar. Además, contiene fundamentos legales, teóricos, históricos que se justificara en esta investigación.

Segundo capítulo: Se especificará la metodología que se va a implementar y contiene el proceso de la información que se ira recolectando con las investigaciones a realizar sobres guías, folletos de protocolos de seguridad informática.

Tercer y cuarto capítulo: Se ejecutará un análisis de la seguridad implementada, y se identificara los puntos importantes que se deben considerar para establecer las buenas prácticas en la gestión de la seguridad y diseñar un protocolo post-evento informático basado en la norma ISO/IEC-17799.

CAPÍTULO I

EL PROBLEMA

1.1 Introducción.

La presente investigación se refiere al tema de un Diseño de protocolo de seguridad Post- Evento Informático basado en la norma ISO/IEC-17799 por el motivo que la información es la clave en que las organizaciones funcionen porque sin ella las empresas dejarían de funcionar solo con realizar actividades informáticas para saber que una empresa necesita de seguridad dentro de ella.

Los procedimientos, políticas y estándares de seguridad forman un conjunto de normas que una organización debe seguir para asegurar cada uno de sus sistemas y que no tenga una libre salida de información en cada uno de los departamentos, por lo tanto, las instituciones deben de tener intereses en las necesidades de seguridad para la protección y restauración de los sistemas y así administrar todos los recursos dentro de la institución.

Mientras evoluciona la tecnología, confronta a los diferentes tipos de inseguridades que van evolucionando y desarrollando junto con este avance, por lo tanto, se puede implementar a través de la norma ISO/IEC-17799 un protocolo post-evento y ejecutar los

procedimientos de seguridad informática vigentes en caso de quebrantar la seguridad establecida.(Gabriel, 2015)

1.2 Planteamiento del problema

En la actualidad diferentes tipos de entidades se enfrentan a muchos riesgos e inseguridades procedentes de diferentes factores. Se puede indicar que los elementos informáticos contienen información son de gran importancia para una organización, y se encuentran asociados a los riesgos y amenazas que explotan una amplia tipología de vulnerabilidades en Facultad de Ingeniería Industrial.

En este diseño se desarrollará un análisis para la propuesta de un protocolo de seguridad post-evento informático basado en la norma ISO/IEC-17799, ayudara a fortalecer las debilidades en el desarrollo de los pasos a seguir en la perdida de información y lo punto que se deben a considerar de suma importancia al momento de restablecer la información en sistema o base de datos que se esté utilizando.

La seguridad de estos activos de la información con lleva a realizar una correcta gestión de los diferentes factores como son: la capacidad, la elaboración de un plan de contingencias frente a los incidentes, el análisis de los riesgos, las competencias, el grado de participación del departamento directivo, las inversiones en la seguridad y el grado de implementación de las nuevas tecnologías.

La infraestructura computacional de la Facultad de Ingeniería Industrial es una parte fundamental para el almacenamiento y

gestión de la información en esta área es de suma importancia estar en constante revisión de los equipos para que estén funcionando correctamente y anticiparse a los diferentes tipos de casos que se puedan presentar como robos de información, fallas de equipos, incendios en el establecimiento, desastres naturales, fallas en el suministro eléctrico o cualquier otro factor que atente contra la seguridad de información y pueda ser afectada.

1.3 Objetivo de la Investigación.

El modelo de esta investigación es de crear protocolos de seguridad post-evento informático basado al estándar de seguridad de la norma ISO/IEC-17799 que garantice la integridad de la información de los datos durante el ciclo de transferencia que se esté utilizando dentro de la Facultad de Ingeniería Industrial.

Es de gran importancia saber cómo reaccionar a los diferentes eventos que hoy en día se presentan en la seguridad informática dentro de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil ubicado en la Av. Las Aguas, y utilizar los protocolos de seguridad que se desean implementar por medio de la ISO/IEC-17799 y se podrán realizar las conclusiones y recomendaciones que puedan fortalecer los protocolos de seguridad.

1.4 Justificación.

La importancia del estudio de un diseño de un protocolo de seguridad post-evento informático basado en la norma ISO/IEC-17799 brindará como resultado la preservación de confidencialidad, integridad y disponibilidad de la información y a la vez reaccionar a los diferentes eventos de seguridad de la información que se aparezcan se identifica el estado de un sistema, servicio o red indicando una posible falla o amenazas en la política de seguridad

dentro de la Facultad de Ingeniería Industrial que pueda ser relevante para su seguridad.

La justificación de este tema de investigación surge a los incidentes de seguridad de información que es indicado por una eventualidad o una serie de sucesos inesperados en la seguridad de la información en la Facultad Ingeniería Industrial que tiene una probabilidad significativa en las operaciones de los sistemas informáticos, por ello es el diseño del protocolo de seguridad de información basado en la norma ISO/IEC-17799.

1.5 Objetivos general.

Diseñar un protocolo de seguridad post-evento informático basado en la norma ISO/IEC-17799 en la Facultad de Ingeniería Industrial, ya que la norma está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información con un enfoque de nuevas técnicas de seguridad.

1.5.1 Objetivos específicos.

1. Analizar las Metodologías de Seguridad Implementadas en la Facultad de Ingeniería Industrial.
2. Identificar los puntos importantes que se deben considerar para establecer las buenas prácticas en la gestión de la seguridad de la información en la Facultad de Ingeniería Industrial.
3. Diseñar un protocolo de seguridad post-evento informático basado en la norma ISO/IEC-17799 para que se considere como medidas correctivas en la Facultad de Ingeniería Industrial.

1.6 Delimitación del problema

Este proyecto tendrá un alcance en diseñar un protocolo post-evento tomando como guía la norma ISO/IEC-17799 y quedará como un protocolo post-evento de cómo reaccionar a todas las situaciones de inseguridad que surjan en la Facultad de Ingeniería Industrial.

CAPÍTULO II

MARCO TEÓRICO

2. Antecedentes del Estudio

2.1. Importancia de la Seguridad Informática

Para garantizar la seguridad dentro de la Facultad de Ingeniería Industrial se realizará un “DISEÑO DE PROTOCOLO DE SEGURIDAD POST-EVENTO INFORMÁTICO BASADO EN LA NORMA ISO/IEC-17799 PARA LA FACULTAD DE INGENIERÍA INDUSTRIAL”. Esta investigación lleva acabo una metodología que se va a diseñar un protocolo mediante el análisis de las amenazas existentes y crear medidas de seguridad que permitan rastrear cuales fueran las causas en la que la seguridad fue alterada.

La seguridad Informática o seguridad de tecnologías de la información es el área de protección de la infraestructura de los equipos computacionales dentro una institución que están relacionados en el contenido de la información que se está enviando o recibiendo mediante los sistemas informáticos. (institute, 2014)

Para realizar estos procedimientos es necesario que existan estándares, protocolos, métodos, reglas, herramientas y leyes que sirvan para proteger la información y mantener la seguridad informática que está comprendida en el software es decir en los archivos, bancos de información o la base datos y el hardware que son todos los equipos que se encuentren dentro de la Facultad de Ingeniería Industrial.

El concepto de seguridad de la información no debe ser confundido con el de “seguridad informática”, ya que este último solo se encarga de la seguridad en el medio informático, pero la información puede encontrarse en diferentes medios o formas, y no solo en medios informáticos. (institute, 2014)

Por lo tanto, la información es lo más importante dentro de una organización, deben existir diferentes tipos de técnicas que resguarden y aseguren la información mediante la seguridad lógica es decir aplicando obstáculos y procedimientos que solo se permita acceder al personal autorizado en cada área dentro de la Facultad de Ingeniería Industrial.

Ecuador es un país vulnerable con respecto a ataques cibernéticos en el año 2017 las mafias liberaron un virus con el nombre WannaCry, las primeras alertas se encendieron cuando los sensores de los sistemas informáticos empezaron a detectar las amenazas afectando a estas ciudades como Quito, Guayaquil y Manta. Esto significaba que el virus WannaCry que estaba en la red intento penetrar las cuentas personales y corporativas, para apoderarse de los equipos y de la información que existente en las empresas. (Medina, 2017)

Las empresas de seguridad cibernética indicaron que unas 27 empresas y 15000 personas fueron amenazadas y afectadas por el virus WannaCry, porque las pantallas de las computadoras se visualizaban con un aviso de color rojo con cronómetro. Este dialogo indicaba que los documentos habían sido robados por las ciber mafias y exigían dinero para recuperar los documentos por valores de USD 700 y 300. Las empresas que fueron atacadas en Ecuador fueron organizaciones tales como supermercados, la banca y telefónicas. Las ciber mafias tienen como objetivo de apoderarse de la información o base de datos para luego

venderlas en el mercado ilegal, pero esto no garantiza que devuelvan información obtenida ilegalmente. (Medina, 2017)

2.2 Fundamentación Teórica

2.2.1 Resumen de la ISO/IEC-17799

Se define como una guía protocolar en la implementación del sistema de administración de la seguridad de la información. En general proporciona las pautas para la implementación basada en la sugerencia que deben ser consideradas por una organización o empresa para construir un programa comprensivo de gestión de seguridad de la información. (Elcas21, 2015)

Está orientada en los siguientes principios:

- 1. Confidencialidad:** Se asegura que solo el personal o usuarios estén autorizados en acceder a la información.
- 2. Integridad:** Garantiza que la información no será alterada, eliminada o destruida por entidades no autorizadas; preservando exactitud y completitud de esta.
- 3. Disponibilidad:** Cerciorar que los usuarios autorizados tendrán acceso a la información cuando lo requieran y sus medios asociados. (Elcas21, 2015)

La norma ISO/IEC-17799 establece diez dominios que representan por completo la Gestión de la Seguridad de la Información.

- 1. Políticas de Seguridad:** El estándar define como obligatorias las políticas de seguridad dentro de una organización y

procedimientos que se realicen dentro de esta y la revisión del equipo o comité de Seguridad.

2. Aspectos Organizativos: Fomenta el marco formal en la seguridad de la Organización debe estar integrada.

3. Clasificación y controlar personal: Es el análisis de los riesgos tanto interno como externo y como deben ser administrados y controlados, esto deber ser de acuerdo con su nivel de confidencialidad dentro de la organización.

4. Seguridad ligada al personal: Su objetivo es contar con los elementos necesarios para mitigar el riesgo inherente a la interacción humana, se refiere a establecer responsabilidades a todo personal en materia de la seguridad de la información dentro la organización.

5. Seguridad física y del entorno: Se identifica el contorno dentro de la organización para definir los controles de manejo de equipos, transferencias de información y control al acceso a los diferentes departamentos bajo la seguridad establecidas.

6. Gestión de comunicaciones y Operaciones: Son los procedimientos de la operación de la infraestructura de la organización y los controles de seguridad documentados.

7. Control de Acceso: Permitan monitorear el acceso a la información es decir la administración usuarios y la definición de cada uno la responsabilidades o perfiles de seguridad de esta.

8. Desarrollo y Mantenimiento de sistemas: La organización debe disponer diferentes procedimientos que garanticen la calidad y seguridad de la información y de los sistemas en que se manejan.

9. Gestión de continuidad del negocio: Las Interrupciones de las actividades comerciales y proteger las fallas importantes o desastres en el sistema de información y asegurar su recuperación oportuna. (Elcas21, 2015)

10.Cumplimiento de los requerimientos Legales: Evitar las violaciones a cualquier ley y cualquier requerimiento de seguridad de la información de la organización.

2.3 Seguridad de la información

La seguridad de la Información consiste en asegurar que los recursos del sistema de información de una empresa u organización se utilicen de la forma que haya sido establecida, y así como controlar la modificación que solo sea posible por parte de las personas autorizadas para tal fin y por supuesto, siempre dentro de los límites de la autorización. (PMG, 2015)

Mientras tanto la seguridad de la información va creciendo en estos últimos años, y además ha tenido cambios considerables. Se ha convertido en una profesión realmente conocida mundialmente porque en esta área se van incrementado las especializaciones que se pueden integrar al realizar una auditoría, como los siguientes puntos que se deben considerar:

- Planificación de la continuidad del negocio
- Ciencia Forense Digital (Software y Hardware)

- Administración de los Sistemas de Seguridad

2.3.1 Seguridad Organizacional

Este tipo de seguridad se debe sustentar dentro de la organización o institución, es decir se está tomando en cuenta los servicios y contrataciones externas en la infraestructura de la seguridad, evidenciando las responsabilidades y actividades antes las situaciones irregulares dentro de la seguridad de la información.

2.3.2 Seguridad Lógica

Este tipo de seguridad está integrada en los procedimientos que permiten visualizar el acceso a los activos de la información de la organización, es decir los procedimientos en la administración de usuarios, responsabilidades, perfiles de seguridad, control de ingreso a las aplicaciones y documentos que se almacena dentro del sistema, que son los cambios irregulares dentro de los equipos y los sistemas de información.

2.3.3 Seguridad Legal

Este tipo de seguridad incluye que todos los integrantes dentro de la organización y los usuarios dentro de la red de la organización deben cumplir con las normas internas como políticas y manuales de procedimientos en la seguridad de la información, en cuantos los recursos humanos se aplicaran sanciones en la salida de información indebida de acuerdo con la legislación del país.

2.3.4 Seguridad Física

Esta seguridad está relacionada en que deben de cumplir las políticas establecidas, como control de manejos de equipos, envío de

información de los diferentes puntos y el control al acceso de las diferentes áreas de la organización por las importancias de sus activos.

2.4 Análisis de Riesgos

Lo más importante de una Organización o Institución es la información que maneja cada uno de los departamentos, por lo que tienen que existir técnicas que se establezcan y la mantengan segura, ya que con la seguridad física que contienen los equipos no es suficiente para guardar dicha información dentro de la Institución.

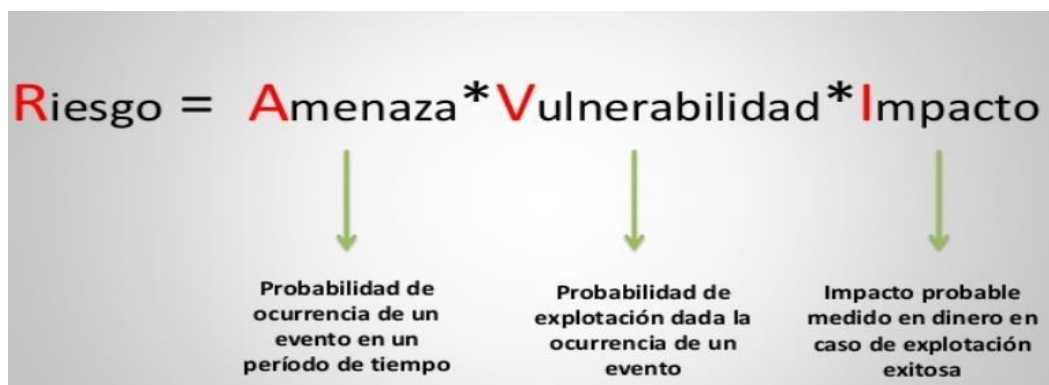
La Información puede ser asegurada como seguridad lógica, es decir que se apliquen diferentes tipos de obstáculos o barreras y procedimientos que resguarden el acceso a toda la información y poner filtros a todas las personas no autorizadas al momento de ingresar al sistema y a la información.

2.4.1 Definición del Riesgo

De acuerdo con la norma ISO/IEC-17799, se define el riesgo como la posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un dispositivo informático que este almacenando información debido a los eventos o consecuencias que se desarrollan dentro de la organización. (informacio, 2016)

La amenaza es un componente de riesgo, y se puede considerar de la siguiente forma: Un agente de amenazas, ya sea humano o no humano, toma como acción de identificar y explotar la debilidad que da lugar a un resultado inesperado y no deseado como la modificación o divulgación de la información y a su acceso dentro de la organización. (Target, 2016)

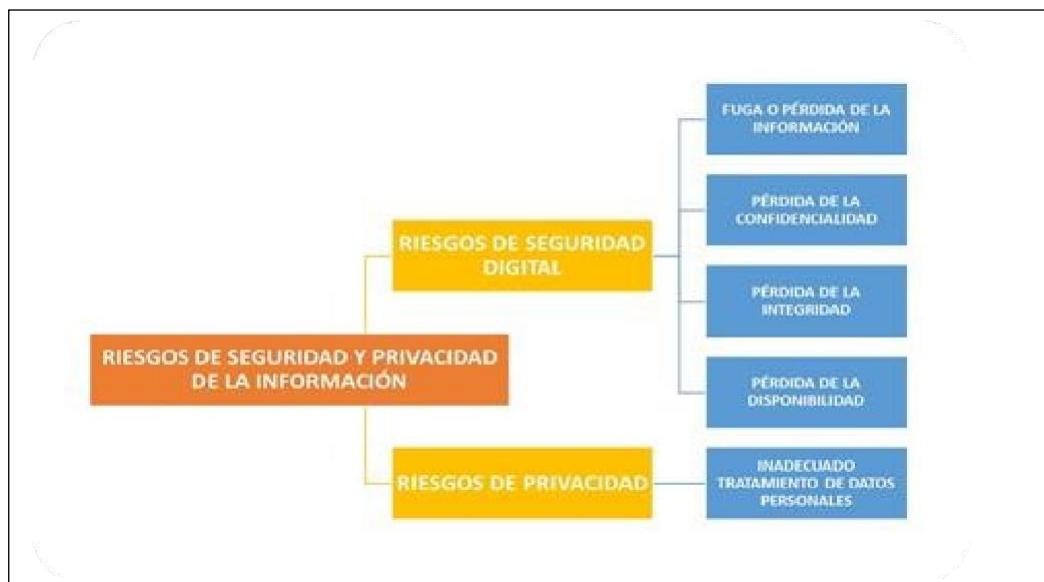
FIGURA N°1
FORMULA DEL RIESGO DE LA SEGURIDAD DE LA INFORMACIÓN



Fuente: Estado del arte de la seguridad de la Información
 Realizado por: Xnativa technology S.A

Para el desarrollo de esta metodología para identificación, gestión y tratamientos de los riesgos de la seguridad y privacidad de información se realizó la siguiente demostración que emplea los diferentes riesgos de forma de digital o privacidad.

FIGURA N°2
CUADRO DE RIESGO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



Fuente: Guía metodológica de análisis de riesgos de seguridad y privacidad de la información.
 Realizado por: Profesional Oficina de Tecnologías de la Información.

2.4.2 Riesgos de Seguridad Digital

La seguridad digital es comprender que el internet como un escenario real cada momento que se manipula un dispositivo informático es decir en la calle, oficina o en el hogar en donde se utilizan en situaciones reales. Se debe tener en consideración situaciones de riesgos al manipular los diferentes dispositivos como, por ejemplo, al extraviar información laboral al dañarse la computadora, el acceso a personas a otras cuentas es decir las redes sociales o también las transacciones bancarias que se realizan en el celular y se mantienen las cuentas registradas en el teléfono, y entre otras formas que se puedan encontrar los riesgos de seguridad digital de la información. En dichos riesgos se encuentran los siguientes puntos:

a. Pérdida o Fuga de la Información: Se denomina perdida o fuga de información al suceso de entregar información a una persona desconocida que no forma parte de la organización, la información tiene un nivel de importancia muy alto que solo debe ser manejado de manera confidencial y estar disponible para los usuarios de la misma organización. Se trata de un incidente que puede ser tanto interno como externo, y a la vez intencional. (bortnik, 2010)

b. Pérdida de Confidencialidad: Los sucesos o abuso a la propiedad de la información que evita la difusión a usuarios, entidades o procesos no autorizados dentro de una organización.

c. Pérdida de la Integridad: La información debe ser consistente, fiable y completa, pero puede suceder que en su ciclo de vida algo le afecte, puede ser de una forma voluntaria o

involuntaria, y esto provoque consecuencias y problemas en la calidad de datos. (Datos, 2013)

La pérdida de la integridad de la información puede ser las tres principales:

- Los datos no están estructurados
 - La introducción manual de datos
 - Los ataques directos a los datos o su modificación intencional.
- (Datos, 2013)

1. Los datos no estructurados: En muchas empresas es habitual que realicen actividades con diferentes tipos de formatos de hojas cálculo para manejar la base de datos, por lo consiguiente estos formatos no se encuentran estructurados y no permiten almacenar información o datos sin ningún control.

2. La introducción manual de datos: Es cuando los sistemas de base de datos que se denominan que son seguros y confiables, la única forma en que estos sistemas puedan ocurrir errores y que no puedan ser confiables, es por el error humano.

3. Ataques a la Integridad de los datos: Son aquellos procesos como la modificación intencional de los datos que perjudican y afectan a la seguridad de la información y los datos existen dentro de la organización. Estos ataques o cambios de la base de datos generados en la organización son un 80% dentro de la misma.

d. Pérdida de la Disponibilidad: Es la pérdida de la capacidad o habilidad de la información en que se puede encontrar a la orden de los diferentes accesos a ella como personas o usuarios, procesos o aplicaciones que dependan a la información solicitada.

2.4.3 Riesgos de Privacidad

Los riesgos afectan a todas las personas cuya información es manipulada y que se reconoce como la posible violación de sus derechos, la pérdida de información necesaria o el daño causado por un utilización ilícita o fraudulenta de la misma que este dentro de la organización. (Datos, 2013)

a. Inadecuado Tratamiento de los Datos Personales:

Utilización de la información que reconoce a las personas, lo que se indicara como violación a los derechos constitucionales.

2.4.4 Factores de Riesgos

Son aquellos factores que pueden afectar en la confidencialidad, la integridad de la información dentro de una organización. Por lo tanto, la pérdida de datos tiende a estar relacionado a nuestro trabajo del día a día y en la forma que almacenamos y manejamos la información.

Los factores que se encuentran identificados como riesgos dentro una organización son las siguientes.

TABLA N°1

**TABLA DE LOS FACTORES DE RIESGOS QUE AFECTAN LA
SEGURIDAD DE LA INFORMACIÓN**

Factor de Riesgo	Descripción
Personas	Personal de la organización que se encuentra relacionado con la ejecución del proceso de forma directa o indirecta.

Factor de Riesgo	Descripción
Procesos	Conjunto interrelacionado entre sí de actividades y tareas necesarias para llevar a cabo el proceso.
Tecnología	Conjunto de herramientas tecnológicas que intervienen de manera directa o indirecta en la ejecución del proceso.
Infraestructura	Conjunto de recursos físicos que apoyan el funcionamiento de la organización y de manera específica el proceso.
Factores Externos	Condiciones generadas por agentes externos, las cuales no son controlables por la empresa y que afectan de manera directa o indirecta el proceso.

Fuente: Guía metodológica de análisis de riesgos de seguridad y privacidad de la información.
Realizado por: Profesional Oficina de Tecnologías de la Información

En el siguiente grafico muestra los principales factores que causan una pérdida de información.

FIGURA N°3
PRINCIPALES FACTORES QUE CAUSAN UNA PÉRDIDA DE INFORMACIÓN.



Fuente: Recovery Labs
Realizado por: Recovery Labs

2.5 Amenazas a la Seguridad de la información

Se puede definir como amenaza a todo elemento o acción capaz de atentar con la seguridad de la información. Las amenazas surgen a partir

de la existencia de vulnerabilidades, es decir que una amenaza solo puede existir si existe una vulnerabilidad que pueda ser aprovechada y realizar diferentes acciones que puedan dañar la integridad de la información. (lujan, s.f.)

Diversas situaciones, tales como el incremento y el perfeccionamiento de las técnicas, la falta de capacitación y concientización a los usuarios en el uso de la tecnología, y sobre todo la creciente rentabilidad de los ataques, han provocado en los últimos años el aumento de amenazas intencionales. (lujan, s.f.)

2.5.1 Tipos de Amenazas

Las amenazas pueden clasificarse de la siguiente forma:

1. Intencionales, es en el caso que se intenta producir un daño dentro de la organización. Por ejemplo, robo de la información aplicando daños en el sistema, la liberación de virus o códigos maliciosos.

2. No Intencionales, es donde se producen acciones u omisiones de acciones que, si bien no buscan explotar una vulnerabilidad, ponen en riesgo la información que se maneja dentro de la organización y pueden producir daños de esta. Por ejemplo, las amenazas relacionadas con fenómenos naturales. (lujan, s.f.)

2.5.2 Cómo Actuar Frente una Amenaza

La presencia de una amenaza es una advertencia que pueden ocurrir daños al activo de la información, por lo tanto, es un indicador que

un daño que esta produciendo o fue producido por ese hecho es importante de reportar un incidente de seguridad de la información. (Iujan, s.f.)

En la siguiente figura cuatro demuestra la principales Amenazas de la información

FIGURA N°4
Principales Amenazas en la Seguridad de Información

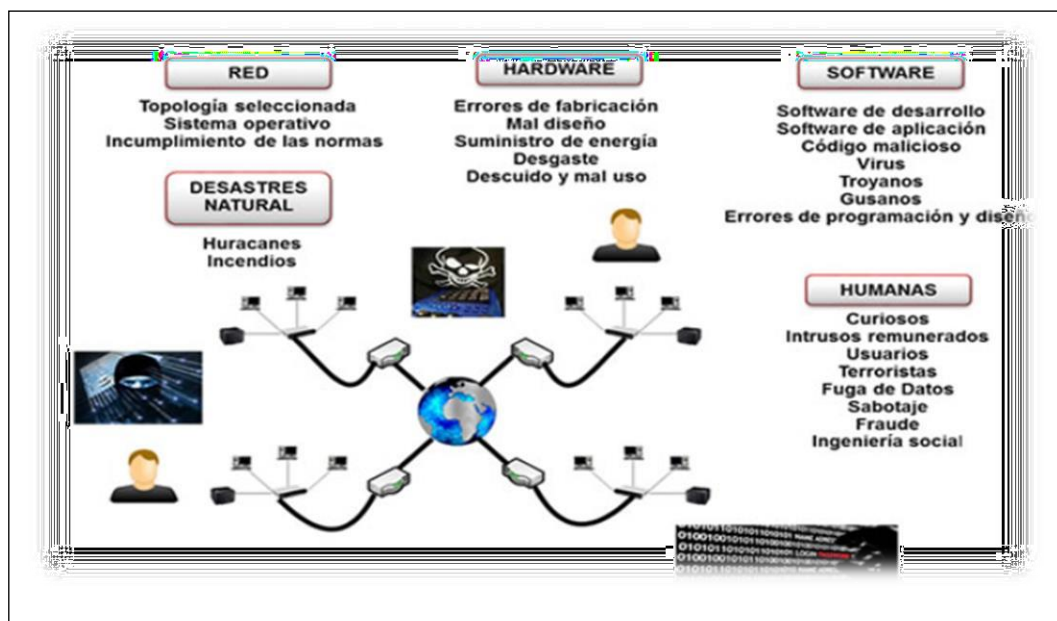


Figura: Principales Amenazas
Fuente: <https://manred.es/seguridad/>

Catástrofes Naturales: Estos tipos de amenazas se realizan o provocan en la interrupción de los servicios que se está proporcionando y que afectan directamente a la disponibilidad de la información, por ejemplo, las inundaciones, terremotos, tornados entre otros.

Amenazas Físicas: Este tipo de amenazas se refiere a las fallas de los dispositivos, accidentes que son eventos provocados de manera involuntaria por descuidos o desconocimientos de los

usuarios, a esto da como resultado a robos, daños en los equipos informáticos o sabotajes.

Fraude Informático: Es debido a la falsedad de los productos que se ofrecen en la red de los diferentes servicios o promociones que no existente.

Intrusiones: El acceso no permitido a los sistemas de comunicaciones o a los servidores con la finalidad de perjudicar la imagen de la Organización y obtener beneficios económicos ilegales.

Errores Humanos: Esto es resultado de las acciones humanas como obtener contraseñas fácilmente o vulnerables, al igual como configuraciones incompletas de los dispositivos o interrupción de los servicios establecidos.

Software Ilegal: Las consecuencias de copiar softwares ilegales están expuestos a las vulnerabilidades en los sistemas informáticos, ya que este software no cuenta con actualizaciones que se disponen de sus desarrolladores y al adquirir estos softwares pueden contener amenazas como los códigos maliciosos.

Código Maliciosos: Estos programas o partes de programas pueden ocasionar diferentes problemas en el sistema informático, como son los gusanos, troyanos, virus o puertas traseras que se activan en los sistemas.

Fallos Electrónicos: En este tipo de fallas en el sistema informático puede ser afectado por los apagones en el suministro eléctrico o por los lógicos errores que estén dentro del dispositivo es

decir por fallas de ensamblaje y del dispositivo porque no es perfecto.

FIGURA N°5
METODOLOGÍA DE UN SISTEMA DE SEGURIDAD



Figura: Metodología de un sistema de Seguridad

Fuente: http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid

2.6 Los Activos de una Organización

Las organizaciones tienen información o datos que si deben preservar al frente de tantas amenazas y riesgos para asegurar el correcto uso de la información dentro de la organización. Este tipo de datos son necesarios para las instituciones o empresas es lo que se designa como Activo de la Seguridad de la Información.

Se denomina Activo aquello que tiene valor dentro de la Institución ó Organización y por lo tanto se debe proteger la información que esta contiene o manipula dentro de la organización. (Ecuador, 2018)

Los activos de información están divididos en diferentes grupos según su naturaleza:

- 1.- Están los servicios se refiere a los procesos que se realizan dentro de la Institución tanto al interior como al exterior.
- 2.- Los datos es información que se manejan dentro de la institución u organización.
- 3.- Esta formado por todas las aplicaciones de software.
- 4.-Esta formado por todos los equipos Informáticos dentro de la Organización.
- 5.- Esta formado por el personal tanto interno como externo por lo que es el activo principal.
- 6.- Esta conformada en las redes de comunicaciones es decir redes propias o subcontratadas en la organización.
- 7.-Esta conformado por las configuraciones en los soportes de la información, que permitan almacenar la información por largos períodos de tiempo.
- 8.- Esta conformado por el equipamiento auxiliar que realiza soporte en los sistemas de información tales equipos climatización, aire acondicionado o trituradora de papeles.
- 9.-Esta se indica a las instalaciones en donde se encuentran ubicadas los sistemas de información.

Para preservar los activos de la información es necesario identificarlos y conocer cuáles son dentro de la institución ó organización.

FIGURA N°6

NIVEL DE RIESGO EN LOS ACTIVOS DE INFORMACIÓN DENTRO DE LA ORGANIZACIÓN

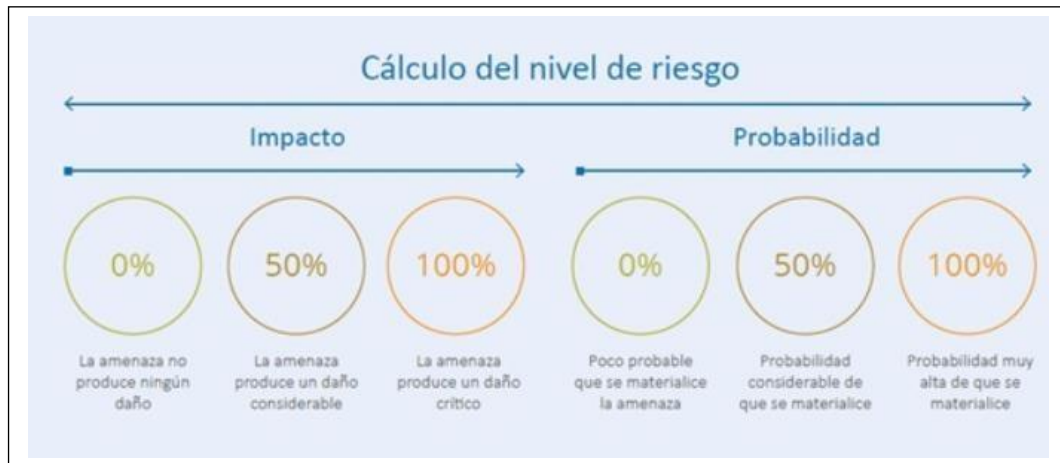


Figura: Nivel de riesgo en los Activos de la Información

Fuente: <http://www.policiaecuador.gob.ec/wp-content/uploads/2018/03/riesgos.jpg>

2.6.1 Riesgos para los Activos de la Seguridad de la Información

El riesgo de los activos se realiza un cálculo dependiendo de las distintas metodologías y identificando las amenazas, vulnerabilidades y amenazas, para realizar la debida valoración adecuada y el análisis de la seguridad por lo tanto cada formula se utiliza de forma distinta para evaluar el nivel de riesgos que se encuentran en los activos de información de la organización. (Ecuador, 2018)

Se realiza una formula simple de dos parámetros fundamentales:

- 1.- Probabilidad de que un peligro se represente, utilizando debilidades existentes de un activo o un grupo de activos, realizando

daños y pérdidas en los sistemas informáticos dentro de la institución.

2.- El impacto dentro de la organización es el resultado de la visualización de los peligros existentes que muestren las debilidades o la credibilidad de las instituciones. (Ecuador, 2018)

2.7 Política de Seguridad de la información

La información es un recurso que tiene un gran valor para la organización y por consiguiente debe ser debidamente protegida. Proporcionar a la gerencia la dirección y soporte para la seguridad de la información en concordancia con los requerimientos comerciales y las leyes y regulaciones relevantes. El establecimiento debe realizar un seguimiento de mejora continua y la aplicación de las políticas de seguridad que garanticen una protección a los diferentes tipos de amenazas existentes. (Caldas, 2017)

La definición de roles y responsabilidades depende de las políticas de la seguridad información dentro de una organización. Cada entidad posee necesidades diferentes, una estructura organizacional diferente, procesos diferentes, condiciones tecnológicas diferentes. (Central, 2017)

Responsabilidades de áreas:

1.- Alta Dirección aprueba cada una de las responsabilidades en la seguridad de la información en el nivel operativo y directivo.

2.- Comité de Seguridad debe revisar, constantemente las políticas de seguridad de la información, análisis de riesgo de seguridad dentro de la organización.

3.-Profesional de Seguridad de la Información debe gestionar los lineamientos de la seguridad de información dentro de la organización como los controles técnicos, físicos y administrativos, derivados de los riesgos en los análisis realizados en la organización.

FIGURA N°7
DEFINE EL PROCESO DEL SISTEMA DE GESTIÓN SEGURIDAD DE LA INFORMACIÓN

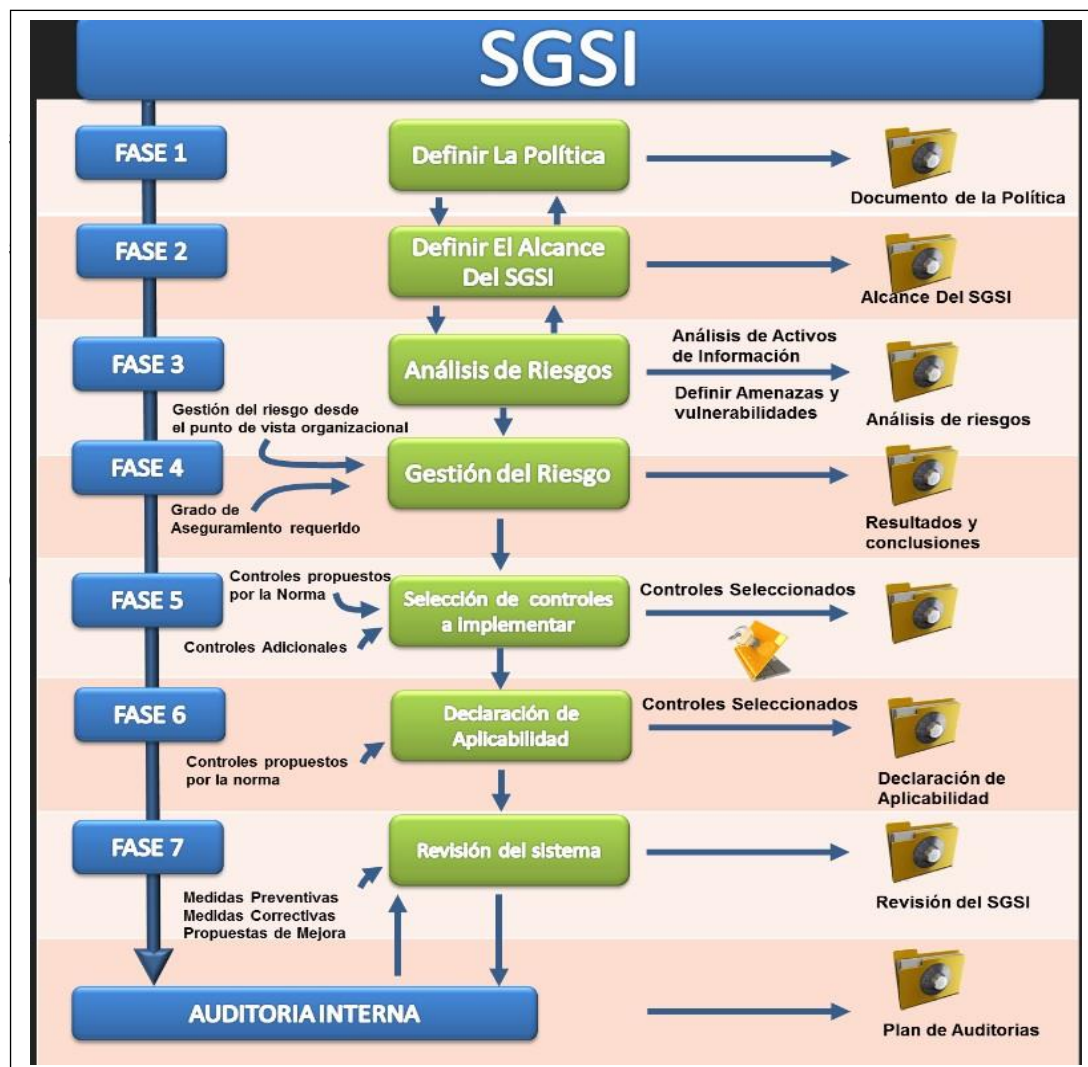


Figura: Definir el Diseño de la Seguridad del Sistema Información
Fuente: <http://www.normas-iso.com/iso-27001/>.

2.7.1 Política para Uso de Dispositivos Móviles.

El objetivo del uso dispositivos móviles es de aplicar las condiciones para la utilización de los dispositivos móviles de las organizaciones y personales tales como teléfonos inteligentes tablets en otros, que hagan uso de los servicios dentro de la Organización. Esta política será aplicada en los departamentos de informática y Comunicaciones que utilicen los diferentes dispositivos móviles que accedan a los servicios ofrecidos dentro de la Organización. (Central, 2017)

2.8 Política para uso de Conexiones Remotas

El Objetivo es de garantizar los métodos de conexión remota, dentro de las redes LAN de la Facultad de Ingeniería Industrial y así garantizar que todos los niveles sean óptimos en seguridad mientras se ejecutan las actividades remotas dentro de la Institución.

La política para el Uso de conexiones remotas será aplicada en el departamento de Informática de la institución y comunicaciones, profesional de seguridad de la Información y partes interesadas de la Facultad de Ingeniería Industrial, que utilicen los servicios de las conexiones remotas en sus diferentes actividades en el envío de la información.

2.9 Políticas de Seguridad de los Recursos Humanos

2.9.1 Políticas Antes de Asumir el Empleo

Para garantizar que los acuerdos y cláusulas de Confidencialidad y Aceptación de Políticas de Seguridad de la Información, se han incluidos en los contratos o cualquier otra forma de vinculación laboral, de servidores

públicos, partes interesadas y proveedores que tengo acceso a las instalaciones y al sistema informático. (Central, 2017)

2.9.2 Políticas Durante la Ejecución del Empleo

Para garantizar que todos los servidores públicos, partes interesadas y proveedores tengan acceso a las instalaciones y a los sistemas de información dentro de la institución, la responsabilidad de las instituciones es de facilitar capacitaciones de los diferentes temas de seguridad de información vigentes dentro de la institución, y disciplinar a todos los usuarios en todas las políticas de seguridad vigentes como acuerdos o cláusulas de confidencialidad y aceptación de las políticas de seguridad de la información que están dentro de la institución.

2.9.3 Política de Terminación de Cambio de Empleo

Para garantizar que todos los servidores públicos que se separen de la institución o tomen sus vacaciones, sean inhabilitados en su acceso en el sistema de control dentro de la institución para evitar la fuga de información y si el servidor público cambia de posición laboral, obtengan los privilegios adecuados que vayan de acuerdo a nueva posición laboral en el acceso de los sistemas de la institución. (Central, 2017)

2.10 Políticas de Gestión de Activos de Información

2.10.1 Política de Responsabilidad por los Activos.

Para garantizar que todos los activos de la información dentro de la institución, que posean un dueño para que garanticen la integridad, confidencialidad y disponibilidad de la información, en cada uno de los departamentos dentro de la institución. (Central, 2017)

2.10.2 Política de Clasificación y Etiquetado de la Información

Para garantizar que la información recibida sea clasificada y etiquetada adecuadamente para esto se debe proporcionar un nivel de protección de información óptima de la misma.

2.10.3 Política de Manejo de Medios

Garantizar que todos los servidores públicos, partes interesadas y proveedores, que necesiten utilizar los dispositivos o medios de almacenamiento, para que cumplan sus funciones de acuerdo con los lineamientos de las políticas de seguridad. Además, en ocasiones los usuarios guardan programas de monitoreo de redes, hackeo, entre otros que utilizan para detectar las vulnerabilidades y obtener información de ellas a su beneficio. (Central, 2017)

2.11 Política de Control de Acceso

2.11.1 Política de Acceso a Redes y Recursos de Red

Garantiza que todo servidor público, parte interesada y proveedor, tenga la necesidad de acceder a las redes de las instituciones o los recursos de la red de la institución, para que realicen una serie de lineamientos de seguridad, que contribuya en conservar la confidencialidad, integridad y la disponibilidad de la información dentro de la institución. Todos los equipos del usuario final, que se conecten o deseen conectarse a las redes de la Organización deben cumplir con los requisitos en autenticarse y realizar las tareas establecidas para los que fueron autorizados. (Central, 2017)

2.11.2 Política de Responsabilidades de Acceso de los Usuarios

Para garantizar que todos los servidores públicos, partes interesadas y proveedores, necesiten ingresar a las instalaciones, plataforma tecnológica y sistemas de información dentro de la institución, y que cada usuario se responsabilice por hacer un uso adecuado y correcto de los usuarios y de las contraseñas asignadas dentro de la red y pueden llevar acabo su trabajo. Es importante realizar la concienciación a los usuarios en tener en confidencialidad las contraseñas configuras dentro del sistema. (Central, 2017)

2.12 Política de Criptografía

2.12.1 Política de Controles Criptográficos

Garantiza que toda la información, que este etiquetada para la institución, sea guardada, transmitida y recibida de manera segura, garantizando y preservando la información y la integridad de la información llegue a su destino sin interrupciones.

2.12.2 Política de Áreas Seguras

Garantiza que todo servidor público, parte interesada, estudiante, proveedor y visitante, que utilice las instalaciones en el área de informática de la institución, proceda a ingresar y salir debe cumplir los procesos de seguridad adecuados y aceptados por la alta dirección dentro de la Institución. Por lo tanto, debe tener un sistema que permita un sistema de control de entrada y salida de los diferentes usuarios antes mencionados.

2.12.3 Políticas de Seguridad de las Operaciones

Garantiza que se realice, revise y se acepte que toda la documentación administrativa y operativa de la plataforma dentro de la Institución, que favorezca al cumplimiento de las responsabilidades operativas que están asignadas a cada usuario o servidor en departamento de informática y comunicaciones dentro de la institución.

2.12.4 Política de Protección contra Código Maliciosos

Esta política garantiza que todos los equipos informáticos dentro de la institución, y adquieran un software de antivirus, anti-spam, antimalware y antispyware deben estar debidamente instalados y configurados, para evitar la infestación de los software malicioso en la red institucional, y mantener la preservación, la integridad de la información y tener la disponibilidad de la información resguardada y custodiada. (Central, 2017)

2.12.5 Política de Copias de Respaldo de la Información

Esta política garantiza que la información que se está generando, procesando y custodiando dentro de la Institución, se encuentre respaldada, mediante copias de seguridad, que sirva para preservar la información y los dispositivos será sometidos a pruebas de recuperación de información y se verificarán el grado de integridad de los datos.

2.13 Políticas de Seguridad de las Comunicaciones

2.13.1 Política de Gestión de la Seguridad de las Redes

Esta política garantiza que el acceso a las redes de datos de la institución cuente con protocolos y controles de seguridad, que denieguen

que los usuarios, no autorizados, se conecten en equipos en las redes LAN de la institución para fines no establecidos.

2.13.2 Política de Uso del Correo Electrónico Institucional

El alcance de esta política es que todos los usuarios cuenten con una cuenta de correo institucional de la institución que cumplan las medidas de seguridad establecidas para ayudar la preservación y las buenas prácticas en su uso dentro de la institución.

2.13.3 Política de Uso Adecuado de Internet

Esta política garantiza que se utilicen adecuadamente el servicio de internet de la institución, evitando que se utilice para fines de personales o que vayan en contra de los objetivos de la Institución.

2.14 Política de Destrucción de Datos

Esta política incluye diferentes procedimientos para la destrucción segura de la información cuando se aplique, por ejemplo, en equipos que no estén funcionando o estén fuera de línea.

2.15 Política de Administración de los Firewalls

Esta Política define los procesos que permita o deniegue el ingreso al sistema, la administración y el constate monitoreo de los firewalls que se encuentren vigentes en la institución.

2.16 Protocolos de seguridad de la Información

Un protocolo de seguridad es documento donde se consignan los pasos que se deben seguir para ejecutar acciones seguras dentro de los

procesos de una organización. Se requiere que se tenga un planteamiento de todos los riesgos que puedan afectar o estar afectando a la organización estos protocolos no solo se proponen en diseñar sino en corregir un evento o ataque de carácter malicioso, que al mismo tiempo permite mejorar las acciones o procedimientos que se realizan y prevenir los riesgos. (consite, s.f.)

Los protocolos se pueden delimitar teniendo el enfoque de seguridad en los que se vaya a implementar y las diferentes necesidades de la organización. Los protocolos se implementan en base a las consecuencias de un evento o ataques que se haya generado para quebrantar la seguridad de la organización es decir protocolos de cómo reaccionar ante desastres naturales, protocolos de como ingresar a otros sitios web entre diferentes tipos de protocolos que puedan surgir a los diferentes riesgos que se presenten en la organización.

2.17 Ingeniería Social

La Ingeniería Social es el acto de manipular a las personas por medio de técnicas psicológicas y habilidades sociales para cumplir metas específicas. Están complementadas: obtener información de la organización, el acceso a los sistemas para obtener los activos de la información que pueden ser o no ser del interés de la persona que desea obtener los datos. (Mexico, 2018)

La Ingeniería Social se sustenta en sencillo principio: el usuario es el eslabón más débil dentro la organización. Dado que no hay sistema en el mundo que no dependa de un usuario, la ingeniería social es un vulnerabilidad universal e independiente de cualquier plataforma tecnológica se esté utilizando en la organización. (Mexico, 2018)

FIGURA N°8

INGENIERÍA SOCIAL EN LOS USUARIOS PARA SEGURIDAD DENTRO DE LA ORGANIZACIÓN

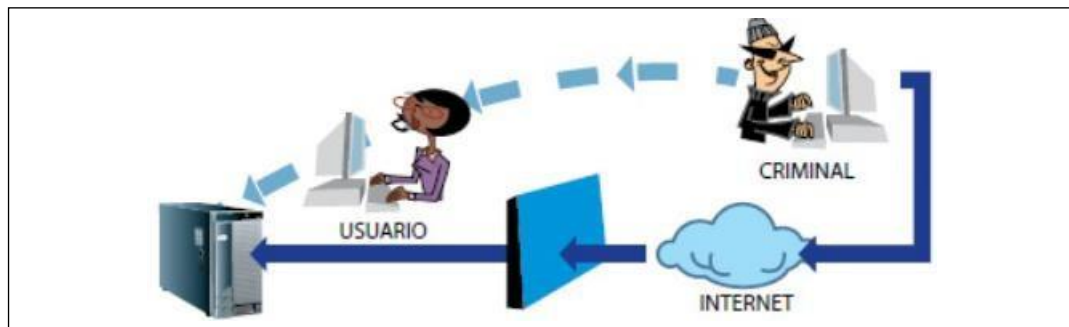


Figura: Business Transformation

Fuente: <http://web1.gbm.net/bt/bt51/tendencias/ingenieria-social.php>

2.17.1 Formas de Ataque de la Ingeniería Social

Las formas en cual la ingeniería social tiene sus ataques son de diferentes formas y dependen de la imaginación del atacante y su interés en conseguir la información deseada. La Ingeniería Social tiene dos niveles el físico describe los recursos o medios que a través de este se pueden llevar los ataques dentro la organización, el psicosocial es el método en cual engaña o seduce la víctima en obtener lo que quiere. Las formas a nivel físico son:

1. Ataque por teléfono. En esta el atacante se realiza una llamada telefónica a la víctima haciéndose pasar por alguien más, como un técnico de soporte o empleado de la organización. Es muy efectivo, ya las expresiones en el rostro no son visualizadas y lo único que se requiere es un teléfono. (Mexico, 2018)

2. Ataque vía Internet. Los ataques más comunes son vía mail adquiriendo la información a través de phishing o infectando el equipo del usuario con virus malware, web solicitando que llenen formularios falsos.

3. Dumpster Diving o Trashing (zambullida en la basura).

Consiste en buscar información en la basura como en agendas telefónicas, agendas de trabajo, organigramas, unidades de almacenamiento.

4. Ataque vía SMS. El intruso envía un mensaje SMS a la víctima haciéndole creer que el mensaje es parte de una promoción o un servicio, para que facilite información personal.

5. Ataque vía correo postal. El atacante envía un correo falso a la víctima, tomando como referencia alguna suscripción de una revista, cupones de descuentos o promociones.

6. Ataque cara a cara. El atacante requiere de una gran habilidad social y muchos conocimientos para poder manejarse en cualquier situación en la que se presente.

Las formas a nivel psicosocial son:

1. Exploit de familiaridad. Es en la que el atacante abusa de la confianza de la gente que tiene a su alrededor amigos y familiares, suplantándose por cualquiera de ellos así obtener la información.

2. Crear una situación hostil. Una situación hostil es cuando el atacante parece estar enojado o loco en el punto que provoquen suficiente estrés para no ser revisado y no responder preguntas de los vigilantes.

3. Conseguir el mismo empleo en el mismo lugar. Las empresas medianas y pequeñas no realizan una revisión de los antecedentes del solicitante de la vacante, por lo que el atacante le resulta muy fácil entrar a laborar dentro de la organización.

4. Leer el lenguaje corporal. El lenguaje corporal es generar pequeños momentos y mejorar la conexión con la otra persona, una vez que la víctima se sienta en un buen ambiente realizar el ataque.

5. Explotar la sexualidad. Técnica casi Infalible. Las mujeres que juegan con los deseos sexuales de los hombres porque poseen una gran manipulación, ya que el hombre baja sus defensas y el acatante puede obtener la información con facilidad. (Mexico, 2018)

FIGURA N° 9
TÉCNICAS DE INGENIERÍA SOCIAL



Figura: Técnicas de Ingeniería Social

Fuente: <https://deepwebiupsm.wordpress.com/2016/06/23/las-tecnicas-de-la-ingenieria-social-y-como-nos-afecta>

2.17.2 Como defenderse con la Ingeniería Social

La mejor forma es de enfrentar este problema es capacitando a todo el personal que trabaje dentro de la Organización.

Mecanismos sugeridos son los siguientes:

- No divulgar información importante con extraños en lugares públicos.
- Si se sospecha que es un engaño, exigir que se identifique y obtener información de esa persona.
- Implementar políticas de seguridad dentro de la organización.
- Realizar controles de seguridad física para reducir el peligro.
- Realizar auditorías semanales o mensuales dentro la organización para detectar huecos de la seguridad.
- Realizar programas de concientización sobre la seguridad de la información.

2.18 Antecedentes Legales

2.18.1 Delitos contra la Seguridad de los activos de los sistemas de información y comunicación dentro de la Organización.

Artículo 229.- Revelación ilegal de base de datos

Los usuarios que revelen información registrada por un tercero que se encuentre almacenada en la base de datos o medios semejantes que se encuentre relacionadas en el sistema informático, electrónico, telecomunicaciones o telemático, que se haya realizado intencionalmente o voluntaria quebrantado la privacidad o intimidad de las personas dueña de la información serán sancionadas con la pena de privación de la libertad por uno o tres años.

FIGURA N°10

DEMOSTRACIÓN DE LA CADENA DE SEGURIDAD

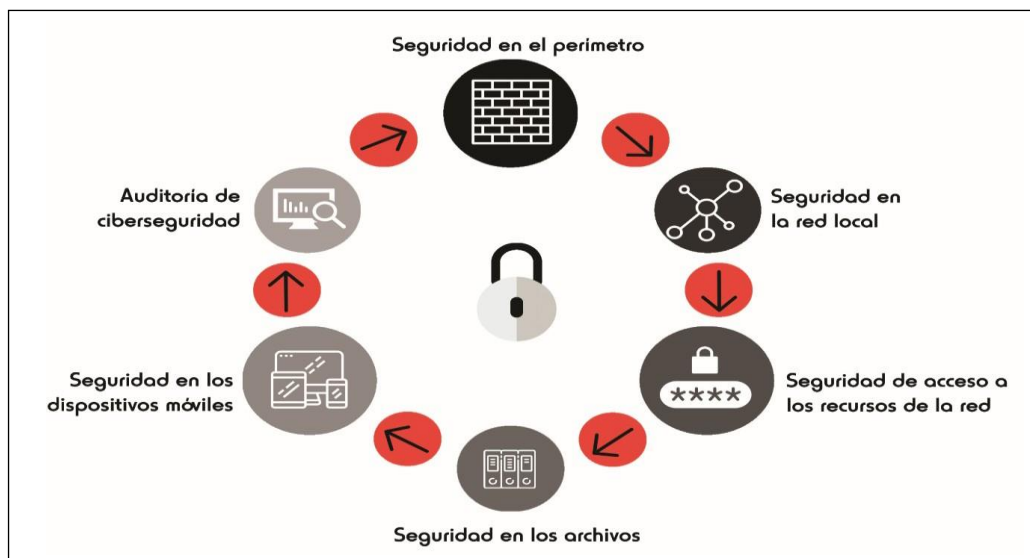


Figura: Ciberseguridad

Fuente: <http://www.fadrell.com/ciberseguridad-defensa-en-capas-para-reducir-el-riesgo/>.

Artículo 230.- Interceptación ilegal de Datos

Los usuarios sin una orden judicial, que desvíe, escuchen, observe u grabe una señal o una transmisión de datos o señales con la finalidad de adquirir la información que se haya registrado o que se encuentre disponible. Si la persona diseña, vende, ejecuta o programe enlaces de ventanas que emerjan y modifiquen el sistema serán sancionados como la pena de tres a cinco años de la privación de la libertad.

Artículo 232.- Ataque a la Integridad de Sistemas Informáticos

Los usuarios que destruyan alteren deteriore, suspenda o provoquen un mal funcionamiento, que suprima datos informáticos o cualquier otro componente lógico que rijan dentro de la organización serán privados de su libertad por tres a cinco años.

Artículo 233.- Delitos contra la Información Pública Reservada Legalmente

Cuando se trata de información o datos que están reservados, y es revelada puede ser comprometido gravemente a la seguridad de la información que se esté utilizando dentro de la organización, será sancionado con la pena de la privación de la libertad de siete a diez años y la separación de un cargo o función pública por seis meses, siempre y cuando la infracción no sea mayor.

Artículo 234.- Acceso no Consentido de un Sistema Informático, Telemático o de Telecomunicaciones

Las personas o usuarios que sin autorización ingresen en todo o en un parte de un sistema informático en contra de la voluntad de las personas que tiene el derecho del ingreso al sistema, para adquirir ilegítimamente información que puede alterar la información o desviarla a terceros para obtener ganancias de proveedores que no estén ligados dentro de la institución será sancionado con la pena de libertad de tres a cinco años.

CAPÍTULO III

METODOLOGÍA

3.1 Diseño de la Investigación

3.1.1 Modalidad de la Investigación

En el presente capítulo se expondrá la figura metodológica de la investigación, las ideas expuestas de la metodología aceptada, en la presente indagación que se está realizando.

De las diferentes metodologías que existen en el campo de la investigación se puede definir con los siguientes métodos; método organizacional, método exploratorio, análisis exploratorio y de observación o comprobación, a este resultado aportara a que la información importante determine que este trabajo es posible en proponer un protocolo de seguridad post-evento informático basado en la norma ISO/IEC-17799 para la Facultad de Ingeniería Industrial de la Universidad de Guayaquil.

3.2 Justificación de elección de Métodos

Las metodologías están orientadas en la investigación del estudio avanzado, para seguir los procedimientos que se deben efectuar en la investigación del proyecto. Se puede indicar que la elección de los procedimientos de la investigación educativa según los objetivos establecidos, obteniendo como un fin principal la resolución de los problemas y mejorar la calidad educacional.

La técnica de investigación es un conjunto de instrumentos y medio a través de los cuales se efectúa el método. Este método proporciona las herramientas, para recorrer el camino de la investigación, esta técnica propone las normas para ordenar las etapas y el proceso de la

investigación, porque permite la recolección, medición, análisis de datos, clasificación para aportar a la ciencia y aplicar el método correcto. (Amador, 2016)

La metodología de la investigación es un proceso que contiene un conjunto de frases sujetas a normas y reglas que dependen de la disciplina científica particular, de la situación o problema del grado de conocimiento y la conceptualización seleccionados para la investigación. (Amador, 2016)

Método de análisis. - Este método permitirá obtener una metodología adecuada en la seguridad de la información dentro de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil.

Método de Organización. - Este método permitirá identificar los puntos importantes en la seguridad de la información y la organización del mismo y fomentar las buenas prácticas dentro de la Facultad de Ingeniería Industrial.

Método de Investigación acción y exploratoria. - Este método aclarará las técnicas necesarias en investigar o explorar la falta de conocimiento de la seguridad de la información dentro de la Facultad de Ingeniería Industrial.

Método de comprobación y de observación. - Este método permitirá actuar en las vulnerabilidades encontradas e identificar las fallas y elaborar un protocolo post-evento informático basado en la norma ISO/IEC-17799 como medida correctiva en la seguridad de información.

Las metodologías de investigación aplicadas en este proyecto, el análisis, la indagación, permitirán elaborar el protocolo y mejorar las buenas prácticas de seguridad de la información.

Método de Campo. - Es considerada de campo porque su lugar de investigación se realiza en las instalaciones donde se encuentran los sistemas que manipulan la información.

3.3 Procedimientos de la Investigación

Esta investigación se llevó a procesar con los siguientes procesos:

- 1.- Determinar la facilidad del estudio.
- 2.- Alcances y limitaciones del proyecto.
- 3.- Legalizar mediante una solicitud la autorización al director de la Carrera para realizar la investigación.
- 4.- Investigación de pruebas realizadas en la infraestructura y red de la seguridad de la información dentro de la Facultad de Ingeniería Industrial.
- 5.-Realizar las debidas conclusiones y definir las políticas de seguridad de la información que se deben implementar.
- 6.- Definir el protocolo de seguridad Post-Evento informático en la seguridad de información de acuerdo con la norma ISO/IEC-17799.
- 7.- Realizar las conclusiones y recomendaciones.
- 8.- Anexos
- 9.- Bibliografías.

3.4 Población y Muestra

Características de la Población

Las características de la población es objeto de estudio debido al avance de la tecnología y de las comunicaciones, los usuarios que exigen la calidad de los servicios de seguridad de la información que ofrecen la tecnología actual y a la vez la capacitación que se está utilizando para que cada usuario tenga conocimiento de las políticas de seguridad existentes dentro de la Facultad de Ingeniería Industrial.

3.5 Delimitación de la Población

La población se encuentra delimitada en los servidores y profesores de las diferentes carreras que se encuentran dentro de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil, ya que son los usuarios que realizan diferentes actividades y operaciones en el sistema informático de la Facultad Ingeniería Industrial, entre las carreras existentes son:

- Ingeniería Industrial
- Ingeniería en Teleinformática
- Licenciatura en Sistemas de Información

3.6 Técnicas e instrumentos

Observación Científica. – En consideración de la observación científica, ayuda a determinar el estado actual en que se encuentra la seguridad informática y de información dentro de la Facultad de Ingeniería Industrial, para determinar las necesidades en la seguridad de información y elaborar el protocolo de seguridad Post-Evento informático basado en la norma ISO/IEC-17799.

Encuesta. - Por medio de la encuesta se obtuvo la información de partes de los usuarios que laboran dentro de la Facultad Ingeniería Industrial de las diferentes carreras acerca de las medidas de seguridad de información que existen en la Facultad.

Estadístico. - Por medio del método estadísticos se puede representar la información obtenida de proceso de investigación sobre las políticas de seguridad de la Facultad de Ingeniería Industrial y se obtendrá conocimientos de esta, por medio de gráficos y tablas estadísticas de fácil visualización y comprensión.

3.7 Tipo de Muestra

El muestreo no probabilístico está considerado en esta investigación pues no se tiene certeza de que la muestra extraída sea representativa, ya todas las personas que intervienen en la Facultad de Ingeniería Industrial no tienen la facilidad de ingresar en la diferentes áreas o sistemas informáticos, por lo tanto, la investigación se basó en una parte de los usuarios administrativos de la Facultad de Ingeniería Industrial. (AG,2015)

3.7.1 Tamaño de la Muestra

El tamaño de la muestra se relaciona por la determinación de las decisiones estadísticas y no estadísticas, la disponibilidad de los recursos, el presupuesto o el equipo que estará en el campo de investigación.

Se determina el tamaño de la muestra de varias cosas:

1.- Tamaño de la población. - Una población está definida de objetos o individuos que tienen características similares, para ellos existe dos tipos: población objetivo tienen diferentes características y es conocida como población teórica, la población accesible es la población sobre la que los investigadores aplicaran las conclusiones. (AG, 2015)

2.- Margen de error (Intervalo de confianza). - El margen de error es una estadística que expresa la cantidad de error de muestreo aleatorio en los resultados de una encuesta, es la medida estadística de número de veces de cada 100, ya que el resultado se espera que este dentro de un rango específico. (AG, 2015)

3.- Nivel de Confianza. - Son los intervalos aleatorios que se usan para acotar un valor con una determinada probabilidad alta. Un intervalo del 95% es una acción que probablemente cubrirá las expectativas el 95% de las veces. (AG, 2015)

4.- La desviación estándar. - Es un índice numérico de la dispersión de un conjunto de datos o población. Mientras mayor es la desviación estándar, mayor es la dispersión de la población. (AG, 2015)

3.7.2 Cálculo del Tamaño de la muestra desconociendo el tamaño de la población.

FIGURA N°11
FÓRMULA PARA CALCULAR EL TAMAÑO DE LA MUESTRA

$$n = \frac{Z_a^2 \times p \times q}{d^2}$$

Figura: Formula del Cálculo de la Muestra

Fuente: <http://www.psyma.com/company/news/message/como-determinar-el-tamano-de-una-muestra>

Simbología:

Z = Nivel de confianza,

P = Probabilidad de éxito, o proporción esperada

Q = Probabilidad de fracaso

D = Precisión de error máximo admisible en términos de proporción.

Los 81 usuarios encuestados los dividimos por las tres carreras más el área administrativa de la Facultad de Ingeniería Industrial da un total de 20.25 encuestados por cada carrera y personal administrativo equilibrando el resultado de la muestra.

3.8 Proceso de selección

Se toma en perspectiva que la muestra es de tipo no probabilístico el proceso de toma de la encuesta se realizó de manera voluntaria a los usuarios o población de estudio que se encuentra dentro de la Facultad de Ingeniería Industrial.

3.9 Viabilidad del estudio

El presente estudio se realizará el diseño de un protocolo de seguridad Post-Evento informativo basado en la norma ISO/IEC-17799 para la Facultad de Ingeniería Industrial de la Universidad de Guayaquil.

Permitirá obtener las inseguridades que se encuentre dentro de la estructura de la red por medio de los análisis efectuados de las vulnerabilidades que existen en la red y a la vez fomentar las soluciones que se puedan aplicar en la red y evitar los futuros daños tomando las correctivas necesarias.

El análisis efectuado en la red WI-FI permitió detectar las fallas en la velocidad de transmisión y de velocidad que se genera dentro de la Facultad de Ingeniería Industrial la que permitirá mejorar los puntos clave que se tienen que toman en consideración en colocar las medidas de seguridad.

Se realizará un diseño de un protocolo de seguridad Post-Evento informáticos basado en la norma ISO/IEC-17799 en establecerá las buenas prácticas de seguridad y a su vez la manera de cómo debe proceder al cualquier suceso de inseguridad que haya ocurrido dentro de la Facultad de Ingeniería Industrial

3.10 Alcances y limitaciones del proyecto

En el presente estudio establecerá y se determinará las condiciones en las que se encuentran las redes de estructura física e inalámbricas y se podrá medir el nivel de conocimiento de las medidas de seguridad que actualmente cuenta la Facultad de Ingeniería Industrial.

Entre mis limitaciones que se implementará el diseño del protocolo post-evento informático basado con la norma ISO/IEC-17799 que se especializa en fomentar las buenas prácticas de seguridad de la información y las medidas que se deben ejecutar ante una actividad irregular dentro de la Facultad de Ingeniería Industrial.

3.11 Análisis de los activos

La red LAN de la Facultad de Ingeniería Industrial está distribuida por 16 laboratorios que están interconectados mediante cable UTP, esta distribución se encuentra estructurada de la siguiente manera:

TABLA N°2
LABORATORIOS DE LA FACULTAD DE INGENIERIA INDUSTRIAL

LABORATORIOS	CANT.	SERVICIO
Licenciatura en informática	8	Acceso a Internet
Ingeniería Industrial	1	Acceso a Internet
Ingeniería Teleinformática	10	Acceso a Internet
Total	19	Acceso a Internet

Fuente: Investigación Directa
Realizado por: Parraga Olvera Rene Gregorio

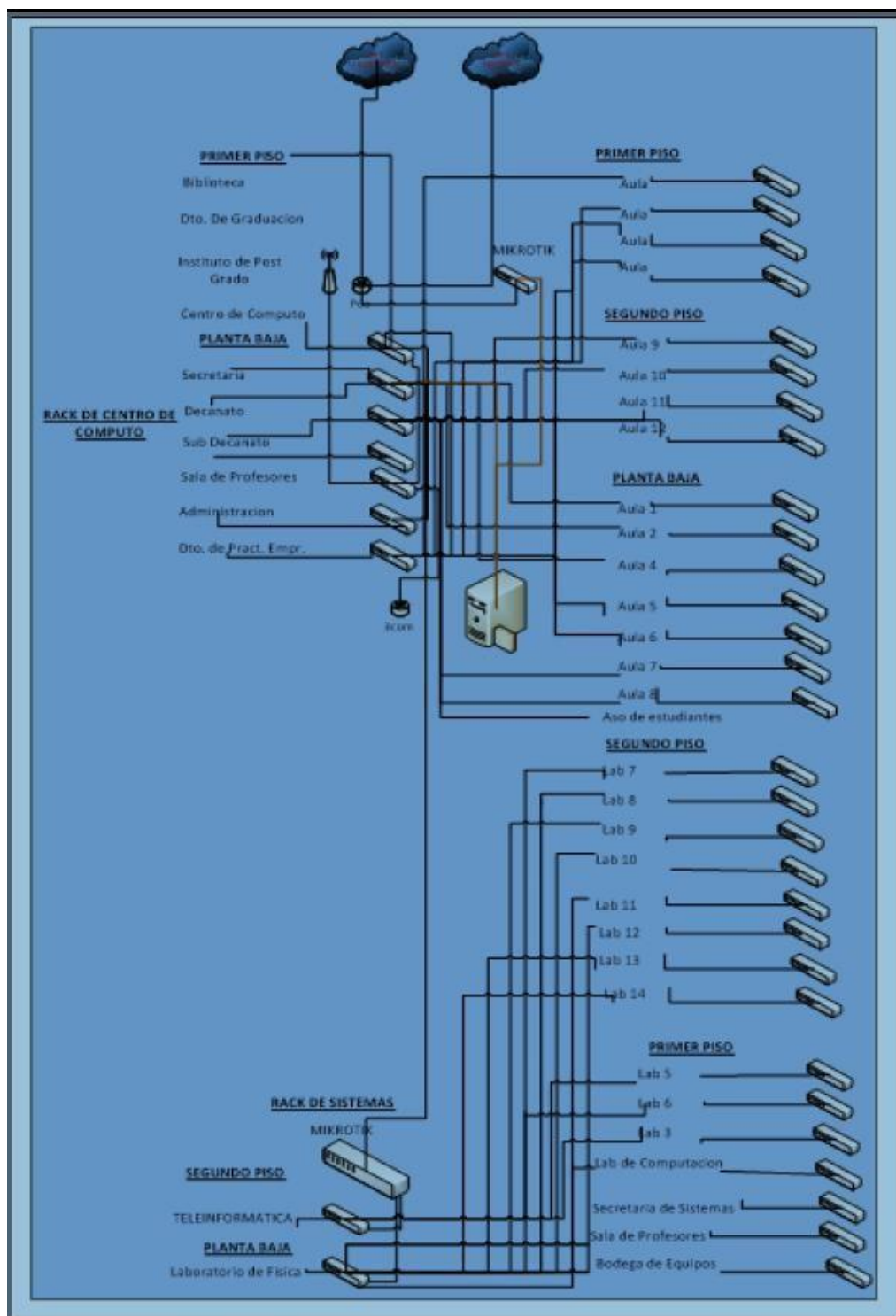
FIGURA N°12
NUMERO DE COMPUTADORAS EN EL AREA ADMINISTRATIVA

ÁREA	Cant.	SERVICIO
Decanato	2	Acceso a internet
Secretaria decanato	1	Acceso a internet
Sub-decanato	1	Acceso a internet
Administradora	4	Acceso a internet
Prácticas empresariales	2	Acceso a internet
Curso de nivelación	3	Acceso a internet
Imprenta	1	Acceso a internet
Secretaria general	10	Acceso a internet
Acreditación	2	Acceso a internet
Dpto. Física arq. Pérez	1	Acceso a internet
Relaciones publicas	1	Acceso a internet
Centro de computo	6	Acceso a internet
Instituto de investigaciones	12	Acceso a internet
Departamento de graduados	4	Acceso a internet
Biblioteca	3	Acceso a internet
Biblioteca consulta de estudiantes	10	Acceso a internet
Biblioteca consulta de profesores	7	Acceso a internet
Carrera licenciatura secretaria	10	Acceso a internet
Graduados	5	Acceso a internet
Operación y mantenimiento	2	Acceso a internet
Coordinación	1	Acceso a internet
Carrera teleinformática área administrativa	4	Acceso a internet
Postgrado	3	Acceso a internet
Área administrativa laboratorios industriales		
Ing. De métodos	2	Acceso a internet
Ensayo	1	Acceso a internet
Eléctrica	3	Acceso a internet
Dibujo	2	Acceso a internet
Metrología básica	3	Acceso a internet
Total	106	Acceso a internet

Fuente: Área Académica

Realizado por: Klever Andrés Arellano Idrovo

FIGURA N°13
ESTRUCTURA DE LA RED DE LA FACULTAD DE INGENIERIA
INDUSTRIAL



Fuente: investigación Directa
 Realizado por: Parraga Olvera Rene Gregorio

TABLA N°3
IDENTIFICACIÓN DE LOS ACTIVOS DE LA FACULTAD DE
INGENIERÍA INDUSTRIAL

CÓDIGO	TIPO/CLASE	NOMBRE	DESCRIPCIÓN
ACT1	Información	Base de Datos	Base de datos de los aplicativos SIUG.
ACT2	Software	SIUG	Conjunto de aplicaciones desarrolladas
ACT3	Hardware	Puestos de trabajos	Equipos de trabajo de la Facultad de Ingeniería Industrial
ACT4	Hardware	Servidores	Servidores permiten realizar las transacciones en la entidad. (Aplicaciones, Proxy, Datos).
ACT5	Red	Router	Permite la conexión con las diferentes redes
ACT6	Red	Switch	Switch Cisco de 24 puertos
ACT7	Red	Patch Panel	Patch Panel 48 puertos Newlink
ACT8	Rack	Rack Panduit y Cabinet	Rack Panduit de 42u Rack Cabinet para servidores de 42u
ACT9	Personal	Empleados administrativos	Cada empleado que elabora dentro de la Facultad de Ingeniería Industrial.

Fuente: investigación Directa

Realizado por: Parraga Olvera Rene Gregorio

3.12 Valoración de la Activos

La valoración de los activos está basada en la metodología Magerit que está establecida por cinco niveles de seguridad que son:

1.- Confiabilidad: La información que está dentro de la institución que no se releva o se dispone a usuarios no autorizados.

2.-Integridad: Es mantener en perfectas condiciones sin alteraciones la información o un activo dentro la institución.

3.- Autenticidad: Garantiza la fuente de donde proviene los datos que se está recibiendo.

4.- Disponibilidad: Que los activos o servicios estén listos cuando se su uso sea necesario para los distintos usuarios.

5.- Trazabilidad: Se permite identificar y verificar qué o quién lo hizo y cuando sucedió la intrusión. (Orozco, 2015)

La valoración de los activos de una institución se realiza de acuerdo con las fallas que afecten en la institución con una calificación de 0 a 10, siendo 0 (Despreciable) y 10 (Daño extremadamente grave). (Orozco, 2015)

TABLA N°4

TABLA DE ESCALA DE VALORACION DE LOS ACTIVOS MEDIANTE CALIFICACIÓN

VALOR	CRITERIO	CRITERIO
10	Extremo	Daño extremadamente grave
9	Muy Alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño Importante

1-2	Bajo	Daño Menor
0	Despreciable	Irrelevante a Efectos Prácticos

Fuente: Manual de Políticas de seguridad de Informática
Realizado por: Lara Orozco Carlos Alfonso

Se procede a realizar la valoración de los activos de la institución de acuerdo con la tabla de escala de valoración.

TABLA N°5
VALORACIÓN DE LOS ACTIVOS DE LA FACULTAD DE INGENIERÍA
INDUSTRIAL DE ACUERDO CON SU ESCALA DE GRAVEDAD

DESCRIPCIÓN							
CÓDIGO	TIPO/CLASE	NOMBRE	Disponibilidad [D]	Integridad [I]	Confidencialidad [C]	Autenticidad [A]	Trazabilidad [T]
ACT1	Información	Base de Datos	9	8	8	8	8
ACT2	Software	SIUG	7	8	9	9	9
ACT3	Hardware	Puestos de trabajos	5	3	3	4	5
ACT4	Hardware	Servidores	8	7	9	6	9
ACT5	Red	Router	5	3	3	2	1
ACT6	Red	Switch	9	4	4	5	5
ACT7	Red	Patch Panel	9	4	4	5	5
ACT8	Rack	Rack Panduit y Cabinet	9	4	4	5	5
ACT9	Personal	Empleados administrativos	7	6	7	5	4

Fuente: investigación Directa
Realizado por: Parraga Olvera Rene Gregorio

3.13 Identificación y Valoración de las Amenazas

El método MAGERIT contiene una diversidad de amenazas que afectan a un activo en específico de la información. Una vez determinadas se procede a realizar la tabla de Frecuencia en la que sucede podría suceder dentro de la Facultad de Ingeniería Industrial.

TABLA N°6
TABLA DE PROBABILIDAD DE FRECUENCIA EN QUE OCURREN LA
AMENAZAS

Valor	Criterio	Criterio
100	Muy Frecuente	A diario
10	Frecuente	Mensualmente
1	Normal	Una vez al año
1/10	Poco Frecuente	Cada varios años
1/100	Muy poco Frecuente	Siglos

Fuente: Magerit versión 3.0 libro i Método
Realizado por: Parraga Olvera Rene Gregorio

Por cada de una de las frecuencias establecidas que pueden presentar como amenazas frecuentes se representara en forma porcentual.

TABLA N°7
TABLA PORCENTUAL DEL NIVEL DE FRECUENCIAS DE LAS
AMENAZAS

PORCENTAJE	CRITERIO
91% - 100%	MUY ALTO (MA)
76% - 90%	ALTO (A)
51% - 75%	MEDIO (M)
21% - 50%	BAJO (B)
0% - 20%	MUY BAJO (MB)

Fuente: investigación Directa
Realizado por: Parraga Olvera Rene Gregorio

De acuerdo con la información obtenida de las frecuencias de riesgo y la valoración de los activos de la información se va a proceder a realizar el respectivo análisis de amenazas de los activos de la información.

TABLA N°8
TABLA DE ANÁLISIS DE AMENAZAS DE LOS ACTIVOS DE
INFORMACIÓN

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
Activos Esenciales								
1.ACT1 Base de datos								
1.1 Revelación de información	10			100%			100%	MA
1.2 Destrucción de información	10	50%					50%	A
1.3 Modificación deliberada de la información	10		100%				100%	MA
1.4 Acceso no autorizado	100		10%	50%			30%	M
1.5 Abuso de privilegios de acceso	10	1%	10%	50%			21%	M
1.6 Suplantación de la identidad del usuario	10		10%	50%	100%		53%	A
1.7 Fugas de información	1			12%			12%	B
1.8 Alteración accidental de la información	1		2%				1%	B
1.9 Errores del administrador	1	22%	22%	22%			22%	B
1.10 Errores de los usuarios	10	16%	16%	16%			16%	B
Servicios Internos								
Aplicaciones								
2. ACT2 APLICACIONES								
2.1 Manipulación de programas	1	50%	100%	100%			83%	A
2.2 Revelación de información	1			51%			51%	M
2.3 Destrucción de información	1	51%					51%	M

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
2.4 Modificación deliberada de la información	1		50%				50%	M
2.5 Acceso no autorizado	1		10%	51%			31%	A
2.6 Difusión de software dañino	1	100%	100%	100%			100%	M
2.7 Uso no previsto	1	2%	11%	11%			8%	B
2.8 Abuso de privilegios de acceso	1	2%	11%	11%			8%	B
2.9 Suplantación de la identidad del usuario		50%	51%	100%			68%	M
2.10 Errores de mantenimiento/ actualización de programas	1	2%	2%				2%	B
2.11 Vulnerabilidades de los programas	1	1%	21%	21%			15%	B
2.12 Fugas de información	1			11%			11%	B
2.13 Alteración accidental de la información.	1		2%				2%	B
2.14 Errores del administrador	1	21%	20%	20%			20%	B
2.15 Errores de los usuarios	1	2%	10%	11%			8%	B
2.16 Avería de origen físico o lógico	1	51%					51%	M
Equipamiento								
Equipos								
3.ACT3Puesto de Trabajo								
3.1 Ataque destructivo	1	100%					100%	A
3.2 Robo de Equipos	10	6%		10%			9%	B
3.3 Denegación de servicios	1	100%					100%	MA
3.4 Manipulación de hardware	1	50%		51%			50%	B
3.5 Acceso no autorizado	1	10%	10%	50%			23%	B

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
3.6 Uso no previsto	1	10%	1%	11%			8%	B
3.7 Abuso de privilegios de acceso	1	11%	10%	50%			23%	B
3.8 Pérdida de equipos	5	6%		10%			9%	B
3.9 Caída de sistemas por agotamiento de recursos	10	50%					50%	A
3.10 Errores de mantenimiento/ actualización de equipos	1	10%					10%	B
3.11 Errores del administrador del sistema	1	20%	20%	20%			20%	B
3.12 Emanaciones electromagnéticas	1			1%			1%	B
3.13 Condiciones inadecuadas de temperatura o humedad	1	100%					100%	A
3.14 Corte del suministro eléctrico	1	100%					100%	A
3.15 Avería de origen físico o lógico	1	50%					50%	M
3.16 Contaminación electromagnética	1	10%					10%	B
3.17 Contaminación medioambiental	1	50%					50%	B
3.18 Desastres industriales	1	100%					100%	M
3.19 Daños por agua	1	50%					50%	B
3.20 Fuego	1	100%					100%	M
3.21 Desastres naturales	1	100%					100%	M
3.22 Daños por agua	1	50%					50%	M
3.23 Fuego	1	100%					100%	M
4. Act4 Servidores								
4.1 Ataque destructivo	1	100%					100%	A
4.2 Robo de Equipos	1	100%		100%			100%	M
4.3 Denegación de servicios	2	100%					100%	MA
4.4 Manipulación de hardware	0	50%		50%			50%	B

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
4.5 Acceso no autorizado	1	11%	100%	100%			71%	M
4.6 Uso no previsto	1	10%	10%	100%			40%	B
4.7 Abuso de privilegios de acceso	1	10%	100%	100%			70%	M
4.8 Pérdida de equipos	1	100%		100%			100%	A
4.9 Caída de sistemas por agotamiento de recursos	10	50%					50%	A
4.10 Errores de mantenimiento/ actualización de equipos	1	10%					10%	B
4.11 Errores del administrador del sistema	1	20%	20%	20%			20%	B
4.12 Emanaciones electromagnéticas	1			2%			2%	B
4.13 Condiciones inadecuadas de temperatura o humedad	1	100%					100%	A
4.14 Corte del suministro eléctrico	1	100%					100%	A
4.15 Avería de origen físico o lógico	1	51%					51%	M
4.16 Contaminación electromagnética	1	11%					11%	B
4.17 Contaminación medioambiental	1	51%					51%	B
4.18 Desastres industriales	1	99%					99%	M
4.19 Daños por agua	1	51%					51%	B
4.20 Fuego	1	99%					99%	M
4.21 Desastres naturales	1	99%					99%	M
4.22 Daños por agua	1	51%					51%	B
4.23 Fuego	1	99%					99%	M
Comunicaciones								
5. ACT5 ROUTER								
5.1 Fuego	1	99%					99%	M
5.2 Daños por agua	1	51%					51%	B
5.3 Desastres naturales ocasionados el mundo	1	99%					99%	M

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
5.4 Desastres industriales	1	99%					99%	M
5.5 Errores del administrador del sistema	1	21%	21%	21%			21%	B
5.6 Emanaciones electromagnéticas	1			1%			1%	B
5.7 Condiciones inadecuadas de temperatura o humedad	1	99%					99%	A
5.8 Corte del suministro eléctrico	1	99%					99%	A
5.9 Avería de origen físico o lógico	1	49%					49%	M
5.10 Contaminación electromagnética	1	11%					11%	B
5.11 Contaminación medioambiental	1	51%					51%	B
5.12 Errores de re-encaminamiento	1			11%			11%	B
5.13 Errores de secuencia	1		11%				11%	B
5.14 Alteración de la información	1		1%				1%	B
5.15 Fuga de Información	1		11%				11%	B
5.16 Errores de mantenimiento/ actualización de equipos(hardware)	1	11%					11%	B
5.17 Caída del sistema y agotamiento de recursos	1	51%					51%	M
5.18 Pérdida de equipos	1	21%		50%			35%	B
5.19 Suplantación de la identidad	1		11%	51%	99%		53%	M
5.20 Abuso de privilegios de acceso	1	11%	11%	50%	100%		44%	B
5.21 Uso no previsto	1	11%	11%	11%			115	B
5.22 Re-encaminamiento de mensajes en el dispositivo	1			10%			10%	B

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
5.23 Alteración de secuencia	1		11%				11%	B
5.24 Acceso no Autorizado	1	11%	11%	51%	100%		44%	B
5.25 Análisis de tráfico	1			3%			3%	B
5.26 Interceptación de información	1			6%			6%	B
5.27 Modificación de la información	1		11%				11%	B
5.28 Destrucción de la información	1	51%					51%	M
5.29 Revelación de información	1			51%			51%	M
5.30 Manipulación de hardware	1	100%		50%			75%	M
5.31 Denegación de servicio	10	51%					51%	A
5.32 Robo de equipos	1	21%		50%			36%	MB
5.33 Ataque destructivo	1	99%					99%	A
6. ACT6 Swicth								
6.1 Fuego	1	99%					99%	M
6.2 Daños por agua	1	51%					51%	B
6.3 Desastres naturales	1	99%					99%	M
6.4 Desastres industriales	1	100%					100%	M
6.5 Errores del administrador del sistema	1	21%	21%	21%			21%	B
6.6 Emanaciones electromagnéticas	1			2%			2%	B
6.7 Condiciones inadecuadas de temperatura o humedad	1	99%					99%	A
6.8 Corte del suministro eléctrico	1	100%					100%	A
6.9 Avería de origen físico o lógico	1	51%					51%	M
6.10 Contaminación electromagnética	1	11%					11%	B

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
6.11 Contaminación medioambiental	1	51%					51%	B
6.12 Errores de re-encaminamiento	1			10%			10%	B
6.13 Errores de secuencia	1		11%				11%	B
6.14 Alteración de la información	1		2%				2%	B
6.15 Fuga de Información	1			11%			11%	B
6.16 Errores de mantenimiento/ actualización de equipos(hardware)	1	10%					10%	B
6.17 Caída del sistema y agotamiento de recursos	1	51%					51%	M
6.18 Pérdida de equipos	1	21%		51%			36%	B
6.19 Suplantación de la identidad	1		11%	51%	99%		54%	M
6.20 Abuso de privilegios de acceso	1	11%	11%	51%	99%		44%	B
6.21 Uso no previsto	1	11%	11%	11%			11%	B
6.22 Re-encaminamiento de mensajes	1			11%			11%	B
6.23 Alteración de secuencia	1		11%				11%	B
6.24 Acceso no Autorizado	1	11%	11%	51%	99%		44%	B
6.25 Análisis de tráfico	1			3%			3%	B
6.26 Interceptación de información	1			6%			6%	B
6.27 Modificación de la información	1		10%				10%	B
6.28 Destrucción de la información	1	51%					51%	M
6.29 Revelación de información	1			50%			50%	M
6.30 Manipulación de hardware	1	99%		50%			76%	M

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
6.31 Denegación de servicio	10	51%					51%	A
6.32 Robo de equipos	1	21%		51%			36%	MB
6.33 Ataque destructivo	1	99%					99%	A
7. ACT7 Patch Panel								
7.1 Fuego	1	99%					99%	M
7.2 Daños por agua	1	51%					51%	B
7.3 Desastres naturales	1	99%					99%	M
7.4 Desastres industriales	1	99%					99%	M
7.5 Contaminación electromagnéticas	1	11%					11%	B
7.6 Contaminación medioambiental	1	51%					51%	B
7.7 Condiciones inadecuadas de temperatura o humedad	1	99%					99%	A
7.8 Corte del suministro eléctrico	1	99%					99%	A
7.9 Avería de origen físico o lógico	1	51%					51%	B
7.10 Emanaciones electromagnéticas	1			2%			2%	B
7.11 Errores de mantenimiento/ actualización de equipos(hardware)	1	11%					11%	B
7.12 Caída del sistema y agotamiento de recursos	10	51%					51%	A
7.13 Pérdida de equipos	1	21%		50%			36%	B
7.14 Abuso de privilegios de acceso	1	11%	11%	51%			23%	B
7.15 Uso no previsto	1	11%	2%	11%			8%	B
7.16 Acceso no Autorizado	1	10%	11%	51%			23%	B
7.17 Manipulación del hardware	1	99%		51%			76%	M
7.18 Denegación de servicio	2	99%					99%	MA

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
7.19 Robo de Equipos	1	21%		51%			36%	MB
7.20Ataque Destructivo	1	99%					99%	A
Servicios subcontratados								
8. ACT8 Acceso a Internet								
8.1 Fallo de servicios de comunicaciones	1	51%					51%	M
8.2 Interrupción de otros servicios o suministros esenciales	1	50%					50%	M
8.3 Errores del administrador del sistema de la seguridad	1	21%	21%	21%			21%	B
8.4 Errores de re-encaminamiento	1			11%			11%	B
8.5 Errores de secuencia	1		11%				11%	B
8.6 Alteración de la información	1		2%				2%	B
8.7 Denegación de servicio	10	51%					51%	A
8.8 Revelación de información	1			51%			50%	M
8.9 Destrucción de la información	1	50%					50%	M
8.10 Modificación de la información	1		11%				11%	B
8.11 Interceptación de información	1			6%			6%	B
8.12 Repudio negación de actuaciones	1					99%	99%	A
8.13 Análisis de tráfico	1			3%			3%	B
8.14 Acceso no autorizado	1		11%	50%	99%		54%	M
8.15 Alteración de secuencia	1		10%				10%	B
8.16 Re-encaminamiento de mensajes	1			10%			10%	B
8.17 Uso no previsto	1	11%	11%	11%			11%	B

Amenazas de Activos	FREQ	[D]	[I]	[C]	[A]	[T]	PROM	RIESGO
8.18 Abuso de privilegios de acceso	1		11%	50%	99%		53%	M
8.19 Suplantación de la identidad	1		10%	50%	99%		53%	M
8.20 Caída del sistema por agotamiento de recursos	1	51%					51%	M
8.21 Fugas de información	1			10%			10%	B
Personal								
9. ACT9 Empleados								
9.1 Alteración de la información	1		11%				11%	B
9.2 Destrucción de la información	1	2%					2%	B
9.3 Fugas de información	1			11%			11%	B
9.4 Indisponibilidad del personal	1	10%					10%	B
9.5 Modificación de la información	1		51%				51%	M
9.6 Destrucción de la información	1	11%					11%	B
9.7 Revelación de información	10			20%			20%	M
9.8 Extorsión	1	10%	21%	21%			18%	MB
9.9 Ingeniería social	1	11%	20%	21%			18%	MB

Fuente: Desarrollo e implementación de manual de políticas de seguridad

Realizado por: Parraga Olvera Rene Gregorio

Realizado el análisis de cada una de las amenazas posibles que pueden afectar los niveles de seguridad y de riesgos que pueden afectar la seguridad de información de la Facultad de Ingeniería Industrial, en donde se puede visualizar el nivel de riesgos de acuerdo con la escala establecida.

TABLA N°9
NIVEL DE RIESGO TOTALIZADO DE ACUERDO CON SU NIVEL DE AMENAZA

DESCRIPCIÓN	TOTAL
MUY ALTO	5
ALTO	26
MEDIO	55
BAJO	97
MUY BAJO	5

Fuente: Desarrollo e implementación de manual de políticas de seguridad
Realizado por: Parraga Olvera Rene Gregorio

3.14 Importancia de la implementación de un protocolo de seguridad Post-evento informático en la Facultad de Ingeniería Industrial.

Para la Facultad de Ingeniería Industrial de la Universidad de Guayaquil es necesario la implementación de protocolos de seguridad de la información post-evento, que sirva como un direccionamiento para los empleados en fomentar la seguridad de la información y que sean establecidos para cada uno de los integrantes de la institución.

Cuando se implementan las políticas de seguridad de la información tiene sus defectos ya que los usuarios dentro de la institución no las llevan a cabo por lo tanto no se toma las medidas correctivas, hay que entender que cada institución o organización es un mundo distinto de acuerdo a las necesidades que se mantiene dentro la organización, para ello se tiene procesos y procedimientos, organigramas, instalaciones, normativa entre otros, también es posible que falle debido a que no se asignan responsables a la seguridad de la información que el empleado conozca sus respectivas actividades y que tengan clara cada una de sus actividades y que activos de la información se deben proteger. Estas Políticas deben

ser consideradas importantes para en la organización porque permiten un soporte de seguridad de la información en la Facultad de Ingeniería Industrial. (Orozco, 2015)

El documento que contendrá el protocolo de Seguridad post-evento informático basado en la norma ISO/IEC-17799, tendrá el siguiente parámetro de Políticas de seguridad de la Información basado a los riesgos existentes dentro de la organización.

- Políticas de la Organización de la Seguridad de la Información
- Políticas de Seguridad de los Recursos Humanos
- Políticas de Gestión de Activos de Información
- Política de Control de Acceso
- Políticas de Criptografía
- Políticas de Seguridad Física y del Entorno
- Políticas de Seguridad de las Operaciones
- Políticas de seguridad de las Comunicaciones
- Políticas de Gestión de Incidentes de Seguridad de la Información
- Políticas de Administración de Servidores
- Sanciones

Cada una de estas políticas representan un conjunto de protocolos que se forman de acuerdo con las necesidades de la organización es decir que cada una de ellas fortalecerá las debilidades de cada uno de los departamentos y motivara el entorno de seguridad de la información y como debe actuar en cada evento no previsto.

CAPÍTULO IV

CONCLUSIONES Y RECOMENDACIONES

4.1 Título de la Propuesta

“Diseño de un protocolo de seguridad post-evento informático basado en la norma ISO/IEC-17799 para la Facultad de Ingeniería Industrial”

4.2 Objetivos de la propuesta

4.2.1 Objetivo General

Propuesta de un protocolo de seguridad post-evento informático basado en la norma ISO/IEC-17799 en la Facultad de Ingeniería Industrial, ya que la norma está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información con un enfoque de nuevas técnicas de seguridad.

4.2.2 Objetivos específicos.

1. Analizar las Metodologías de Seguridad Implementadas en la Facultad de Ingeniería Industrial.

2. Identificar los puntos importantes que se deben considerar para establecer las buenas prácticas en la gestión de la seguridad de la información en la Facultad de Ingeniería Industrial.

3. Diseñar un protocolo de seguridad post-evento informático basado en la norma ISO/IEC-17799 para que se considere como medidas correctivas en la Facultad de Ingeniería Industrial.

4.3 Elaboración de la propuesta

4.3.1 Análisis de las posibles fallas de seguridad en la Facultad de Ingeniería Industrial

De acuerdo a la investigación que se realizó en el capítulo anterior en la Facultad de Ingeniería Industrial no cuenta con políticas de seguridad post-evento informático que permitan actuar al responsable de la seguridad de la información de la manera correcta y ejecutar los protocolos vigentes de la seguridad de la información, para tomar las correcciones apropiadas dentro de la Facultad de Ingeniería Industrial y fomentar la confidencialidad, disponibilidad y integridad.

Cabe indicar que el nodo principal de la Facultad de Ingeniería Industrial, la infraestructura se encuentra desactualizada por los problemas de conectividad que presenta y los problemas de latencia como consecuencia al tiempo de vida máxima que contiene el cableado. (jose, 2017)

4.4 Vulnerabilidades encontradas

Se detallan las vulnerabilidades con algún problema específico que se encuentre en cada una de las áreas administrativas dentro de la Facultad desde Ingeniería Industrial y su posible solución de los riesgos encontrados.

TABLA N°10
NIVEL DE RIESGO DE LAS VULNERABILIDADES ENCONTRADAS EN
LA FACULTA DE INGENIERIA INDUSTRIAL

CONCEPTO	NIVEL	PROBLEMA	VULNERABILIDAD	POSIBLE SOLUCIÓN
RED WIFI	ALTA	CNT_EXCELECIA_UG RED ABIERTA	FACIL INSTRUSION A LOS DISPOSITIVOS CONECTADOS A ELLA	IMPLEMENTAR CONTRASEÑAS COMO MEDIDA DE SEGURIDAD
RED LAN	ALTA	PUERTOS ABIERTOS	CONEXIÓN UN DISPOSITIVO MEDIANTE ENVENENAMIENTO	IMPLEMENTAR EL FORTALECIMIENTO
RACKS	ALTA	FACILIDAD ACCESO A LOS DISPOSITIVOS	RACKS DESCUBIERTOS SIN PROTECCIÓN FÍSICA	COLOCAR GABINETES CERRADOS
CABLEADO	MEDIO	LATENCIA, RETARDO EN LA CONEXIÓN	NO EXISTEN NORMAS EN EL CABLEADO	IMPLEMENTACIÓN DE UNA NORMA DE CABLEADO

Fuente: García Álvarez María José

Realizado por: Parraga Olvera Rene Gregorio

4.5 PROTOCOLOS DE SEGURIDAD DE LA INFORMACIÓN

DISEÑO DE UN PROTOCOLO DE SEGURIDAD POST-EVENTO INFORMÁTICO BASADO EN LA NORMA ISO/IEC-17799 PARA LA FACULTAD DE INGENIERÍA INDUSTRIAL

4.5.1 INTRODUCCIÓN

Con la necesidad de equipos informáticos en la actualidad y su demanda por los servicios que ofrecen, el uso de los equipos de computación y de la diferentes software y aplicaciones que se está utilizando dentro de la Facultad de Ingeniería Industrial, se hace importante

mantener un control en los diferentes dispositivos tanto como los hardware y software, mejorando la ventajas del uso y evitar el mal funcionamiento que se puedan presentar en la Facultad de Ingeniería Industrial de la Universidad de Guayaquil.

El presente documento contiene protocolos de seguridad de información que servirá y dará lineamientos de cumplimiento del uso correcto de los diferentes equipos de cómputo, sistemas operativos y sistemas que manipulan la información importante dentro de la institución y dar conciencia de la sensibilidad de los datos que son importantes y no deben ser entregados a ninguna persona extraña.

4.5.2 ALCANCE

Las políticas que se establecerán en el presente documento, es una implementación que deben realizar cada uno de los usuarios que laboren en la Facultad de Ingeniería Industrial, que hacen uso indirecta o directamente a los diferentes medios de tecnológicos que manipulan la información y los equipos de comunicaciones.

4.5.3 COMPROMISO DE LA DIRECCIÓN

El compromiso de la alta dirección de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil con el diseño e implementación del protocolo de seguridad de la información en la entidad apruebe las políticas que están en este documento, y contiene material de apoyo en:

1. Fomenta una cultura activa en la seguridad de la información en los servidores públicos, estudiantes, proveedores y partes interesadas dentro de la institución.
2. Una constante verificación de las políticas presente en que se cumplan dentro de la institución.
3. Mantiene una constata retroalimentación de las políticas de seguridad a los servidores públicos, estudiantes, proveedores y partes interesadas dentro la institución.

4.5.4 ACTUALIZACIÓN

Para que este documento tenga nuevos correctivos en base a las necesidades de la institución se requiere una revisión de este cada seis meses para mantenerlo actualizado de las diferentes amenazas que hayan evolucionado tanto sea hardware como software que manipulan la información de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil.

4.5.5 LINEAMIENTOS DE POLÍTICAS DE SEGURIDAD

Toda la información que sea manipulada en los equipos computacionales e ingresada en los sistemas operativos que se utilizan en la Facultad de Ingeniería Industrial de la Universidad de Guayaquil, será de carácter confidencial, es decir que ningún funcionario de la Facultad de Ingeniería Industrial no podrá utilizar esta información como uso personal y tampoco no entregarla a ninguna persona externa ajena de la Facultad de Ingeniería Industrial.

Los dispositivos o equipos computadoras designadas cada funcionario público son de uso exclusivo y con fines laborales, siendo responsable de los daños al equipo o al sistema operativo dentro de la computadora. Será un agravante si el sistema o equipo de cómputo es utilizado para lucro personal indebido.

4.6 POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

4.6.1. Políticas de la Organización de la Seguridad de la Información

1. Política de Estructura Organizacional de la Seguridad de la Información

La política de estructura Organizacional de la Información está conformada por la Alta Dirección de la Facultad de Ingeniería Industrial, Comité de Seguridad de la Información y además un Profesional de la Seguridad de la Información.

Responsabilidades de cada una de las áreas y personal de la Facultad de Ingeniería Industrial:

Alta Dirección de la Facultad de Ingeniería Industrial:

1. La alta dirección de la Facultad de Ingeniería Industrial debe aprobar los roles y responsabilidades a los relacionados con la seguridad de la información.
2. La alta dirección de la Facultad de Ingeniería Industrial debe formar el comité de seguridad de información dentro de la institución.

3. La alta dirección de la Facultad de Ingeniería Industrial debe elaborar una carta de compromiso en donde cuente con todo el apoyo de las actividades relacionadas en la seguridad de la información.
4. La alta dirección de la Facultad de Ingeniería Industrial de revisar y aprobar los protocolos de seguridad Post-evento informático contenido en este manual.
5. La alta dirección de la facultad de Ingeniería Industrial debe promover la cultura de seguridad de la información en la Institución.
6. La alta dirección de la Facultad de Ingeniería Industrial debe facilitar la difusión de las Políticas de seguridad de la información a todos los servidores públicos, estudiantes y partes interesadas

Comité de Seguridad de la información:

1. El comité de seguridad de la información de la Facultad de Ingeniería Industrial debe revisar, constantemente las políticas de seguridad de la información contenidas en el protocolo de seguridad.
2. El comité de seguridad de la información de la Facultad de Ingeniería Industrial debe analizar los incidentes que hayan sucedido y activar los procedimientos de seguridad de la información.

3. El comité de seguridad de la información de la Facultad de Ingeniería Industrial debe verificar el cumplimiento de las políticas establecidas dentro de la Institución.

Profesional de Seguridad de la información:

1. El profesional de la seguridad de la información de la Facultad de la Ingeniería Industrial debe liderar la gestión de las políticas o protocolos de seguridad de la información.
2. El profesional de la seguridad de la información de la Facultad de la Ingeniería Industria debe monitorear de forma periódica los controles establecidos en la institución.

2. Política de Uso de Dispositivos Móviles

La política de uso de dispositivos móviles será parte del área informática y comunicaciones de la Facultad de Ingeniería Industrial para el control de los dispositivos móviles institucionales y personales que hagan uso de los sistemas operativos o aplicaciones de la institución garantizando la seguridad de la información.

1. El área informática y de comunicaciones debe tener opciones de protección de los diferentes dispositivos móviles institucionales y personales que hagan uso de los servicios que proviene de la institución.
2. El área informática y de comunicaciones debe implementar las debidas configuraciones para los dispositivos móviles y personales que hagan uso de los servicios que proporciona la institución.

3. El área informática y de comunicaciones debe implementar sistemas de bloqueo de los dispositivos móviles institucionales, para que solo el usuario pueda activar el dispositivo mediante las diferentes formas de desbloqueo que existente ya sean estas por contraseñas, patrones, reconocimiento de vos, biométrico entre otros.
4. El área informática y de comunicaciones debe contar con la opción de cifrado de información en la memoria del dispositivo móvil institucional, haciendo que sea imposible la copia o extracción de la información en el dispositivo.
5. El área informática y de comunicaciones debe de instalar antivirus en los dispositivos móviles institucionales y personales que hacen uso de los servicios que proporciona la institución.
6. El área informática y de comunicaciones debe contar la configuración de borrado remoto para evitar la salida de información en caso de perdido o robo del dispositivo.
7. Los dispositivos móviles institucionales deben evitar ser usados en lugares que nos ofrezcan las garantías de seguridad para evitar el robo y pérdida de estos.
8. Los dispositivos móviles institucionales no se debe instalar programas, que vengan de fuentes desconocidas, únicamente deben instalar aplicaciones que estén bajo el permiso de la institución.

9. Los dispositivos móviles institucionales no deben conectarse a redes de acceso público, solo a redes protegidas al igual a puertos USB que no estén dentro de la institución.
10. Los dispositivos móviles institucionales no deben almacenar información personal, fotografías, videos entre otros archivos que no sean parte de la institución.
11. Solo el personal del área de sistemas de la Facultad de Ingeniería Industrial está calificado de desarmar, cambiar, abrir o instalar piezas nuevas en el equipo de cómputo de la Facultad de Ingeniería Industrial.

3. Política para el uso de conexiones Remotas

La política de conexiones remotas garantiza que los niveles de la red LAN sean idóneos y que la ejecución de los mismos sea la correcta en las actividades que se realizan en la institución.

1. El área de informática y comunicaciones debe implementar método de seguridad en las conexiones remotas.
2. El área informática y de comunicaciones debe restringir el Acceso en periodos determinados en el que el personal autorizado realice sus labores en el tiempo establecido.
3. Todos los servidores públicos que realicen conexiones remotas en la LAN deben contar con aprobaciones requeridas para establecer conexión dentro de la red.
4. Todos los servidores públicos que realicen conexiones remotas en la LAN deben de ser de computadores que estén

registradas en la institución, no de computadores personales o provenientes de otros lugares.

4.6.2. Políticas de Seguridad de los Recursos Humanos

1. Política Antes de Asumir el Empleo

Esta política garantiza los acuerdos o cláusulas de confidencialidad y Aceptación de las Políticas de seguridad de la información, sean incluidas en los contratos o cualquier otra forma de vinculación laboral para la Facultad de Ingeniería Industrial.

1. El área de talento humano debe confirmar la información brindada por el candidato aspirante a la vacante laboral dentro de la institución.
2. El área de contratación de la Facultad de Ingeniería Industrial debe contar con las cláusulas de confidencialidad y aceptación de las políticas de seguridad de la información vigentes en la institución antes de otórgale acceso a las instalaciones y a los sistemas.

2. Política Durante la Ejecución del Empleo

Esta política garantiza que los todo los servidores públicos y partes interesadas, que acceso a las diferentes instalaciones de sistemas de información, reciban capacitaciones en temas de seguridad de la información.

1. La alta dirección de la Facultad de Ingeniería Industrial debe promover el interés sobre la importancia de la seguridad de la información y el cumplimiento de las normas, procedimientos y estándares establecidos para la seguridad de la información.
2. La alta dirección de la Facultad de Ingeniería Industrial debe definir establecer el proceso disciplinario para las infracciones ocurridas a las políticas de seguridad de la información que hayan sido infringidas.
3. El profesional de la seguridad de la información debe ejecutar de forma permanente los programas de concienciación de la seguridad de información.
4. El profesional de la seguridad de la información debe llevar un control de asistencia de todas las personas que asistan a las reuniones.

3. Política determinación y cambio de Empleo

Esta política garantiza que todos los servidores públicos que terminen su contrato de forma voluntaria, por separación de la institución, tome de licencia o vacaciones se desvincule de la institución es decir que su acceso sea inhabilitado del sistema.

1. El área de talen humano debe realizar el proceso de separación o cambio de posición laboral del servidor público saliente.

2. El área de informática y comunicaciones debe realizar los procedimientos de cancelación de cuentas de usuarios en los equipos de cómputos que estuvo a su cargo el usuario saliente.
3. El área de informática y comunicaciones cuando servidor de la institución cambio de cargo se debe realizar los procedimientos de revisión de las funciones del nuevo cargo para modificar los permisos y privilegios que se obtiene del nuevo cargo.
4. Una vez emitida la orden del área de informática y comunicaciones el servidor público no tendrá acceso a ninguna área física o acceso a los sistemas de información.

4.6.3 Políticas de Gestión de Activos de Información

1. Políticas de Responsabilidad por los Activos

Esta política garantiza que todos los activos de la información que poseen un propietario dentro de la institución garanticen la preservación de la integridad, disponibilidad y confidencialidad de la información en cada una de las áreas de la institución.

1. Los usuarios de cada Activo de la información deben revisar periódicamente la validez de los usuarios y sus perfiles de acceso a los sistemas de información.
2. Los usuarios de los activos de la información deben ser conscientes del uso de los recursos y de sus procedimientos en el proceso de información.

3. Los activos de la información deben de tener verificados los niveles de acceso a la información definidos y a aprobados por la Alta dirección de la Facultad de Ingeniería Industrial.
4. El área de Informática y Comunicaciones deben tener la autorización de la instalación, cambio o eliminación de componentes dentro de los sistemas operativos de la institución.
5. El área de Informática y Comunicaciones debe preparar las portátiles de los servidores públicos con todos los accesos a la información establecida.
6. El profesional de la seguridad de la información debe de llevar un inventario de los todos los activos de la información.
7. Los servidores públicos deben de utilizar los dispositivos de la información de forma ética cumpliendo las leyes y reglamentos que estén vigentes, con la finalidad de evitar daños o pérdidas de información dentro de la institución.
8. Los servidores públicos no deben utilizar sus equipos móviles o de cómputo personales, en actividades laborables.
9. Los servidores públicos no deben de utilizar software que no se encuentren autorizados por la Facultad de Ingeniería Industrial.
10. En el momento que el usuario se separe de la institución o cambio de labores debe de entregar el activo de información

en perfectas condiciones sin quebrantar las políticas de seguridad vigentes.

4.6.4 Política de Control de Acceso

1. Política de Acceso a Redes y Recursos de red

La política de accesos a redes y recursos de red garantiza que todo servidor público que tenga necesidad de acceso a las redes de la institución, lo realicen siguiendo los procesos de políticas de seguridad preservando la disponibilidad, integridad y confidencialidad de la información.

1. El área de informática y comunicaciones, deben implementar los procedimientos de autorización de acceso a la red de Facultad de Ingeniería Industrial, para proteger la información que se manejan en red de la institución.
2. El área de informática y comunicaciones deben asegurar que las redes wi-fi cuenten con métodos de autenticación y evite el acceso no autorizados.
3. El área de informática y comunicaciones deben autorizar la creación o modificación de las cuentas de acceso a las redes o a sus recursos.
4. El profesional de seguridad de la información debe verificar que los controles de acceso de dichos usuarios tengan acceso permitido únicamente aquellos recursos de la red para los que fueron autorizados.

5. Todos los servidores públicos de la Facultad de Ingeniería Industrial, antes de tener acceso a los servicios y a la red de datos deben tener firmadas las cláusulas de confidencialidad y de aceptación de las políticas de seguridad de Información de la Facultad de Ingeniería Industrial.

2. Política de Administración de Acceso de Usuarios

Esta política garantiza que todas las áreas respectivas realicen una administración adecuada y optima de todos los recursos informáticos y de los sistemas de información de la Facultad de Ingeniería Industrial de acuerdo sus niveles de acceso en red de Información.

1. El área de informática y Comunicaciones de la Facultad de Ingeniería Industrial debe garantizar la administración de cuentas usuarios como la creación, modificación, eliminación o bloqueo de las cuentas de usuarios de los servidores públicos.
2. El área de informática y de comunicaciones tiene que tener conocimiento de los procedimientos de autorizaciones a la red institucional de la Facultad de Ingeniería Industrial que debe ser revisado por la alta dirección de la Facultad.
3. El área de informática y de Comunicaciones debe de tener la facilidad de creación, modificación o finalización a las cuentas de acceso de los diferentes usuarios una vez que departamento de recursos humanos notifique alguna novedad con algún servidor público.
4. El área informática y comunicaciones deben definir las configuraciones de contraseñas al acceso a la plataforma de

información de la Facultad Ingeniería Industrial y dichas configuraciones deben estar basadas con la complejidad, longitud, control histórico, cambio histórico, cambio de contraseñas en el primer acceso y bloqueo por número de intentos fallidos al ingreso al sistema.

3. Políticas de Responsabilidades de Acceso de los Usuarios

La Política de Responsabilidades de acceso de los usuarios ser aplicada a todos los servidores dentro de la Facultad de Ingeniería Industrial para que cada uno de ellos se responsabilicen por el uso adecuado y correcto de las cuentas de usuarios y contraseñas que se encuentren definidas dentro la red institucional de la Facultad de Ingeniería Industrial.

1. Todos los servidores públicos de la Facultad de Ingeniería Industrial se deben responsabilizar por las acciones causadas dentro de la red tecnológica o las base datos que manejen de acuerdo a su nivel de acceso de cuenta de usuario y de contraseña.
2. Todos los servidores públicos de la Facultad de Ingeniería Industrial no deben compartir por ningún motivo sus cuentas de usuarios o contraseñas a terceras personas, ya que su uso es para solo las personas autorizadas con fines institucionales.
3. Todos los servidores públicos deben de seguir los lineamientos de seguridad de la información por las configuraciones de acceso de cuentas de usuarios y contraseñas.

4.6.5 Políticas de Criptografía

1. Política de controles Criptográficos

La política de controles criptográficos garantiza que toda la información que se transmite, almacenada y recibida llegue de manera segura, garantizando la confidencialidad de la integridad de la información dentro de la Facultad de Ingeniería Industrial.

1. El área de informática y comunicaciones debe de cifrar la información que se almacene, transmita o se etiquete con el propósito de proteger de proteger la información que se envía dentro de la red.
2. El área de informática y comunicaciones debe realizar verificaciones a los sistemas de información que cuenten con mecanismo de cifrados en la transmisión de información.
3. El área de informática y comunicaciones debe implementar estándares para controles de envío de información a través de la red de la Facultad de Ingeniería Industrial.

2. Políticas de seguridad Física y del Entorno

La política de seguridad física y entorno es que todo servidor público, estudiante, ciudadano o parte interesada realice su ingreso o salida de las instalaciones cumpla con los procedimientos de seguridad física aprobadas por alta dirección de la Facultad de Ingeniería Industrial.

1. El área de informática y comunicaciones de la Facultad de Ingeniería Industrial debe de autorizar las solicitudes de acceso a cualquier departamento de donde se maneja información, data center, centro de cableado o cuarto de servidores y deben estar acompañados por un servidor público durante su visita dentro de las instalaciones.

2. El área de informática y comunicaciones de la facultad Ingeniería Industrial debe registrar todos los accesos que se realicen en los diferentes departamentos de data center, centro cableado o cuarto de servidores.
3. El área de informática y comunicaciones de la Facultad de Ingeniería Industrial debe de tener las condiciones físicas y medioambientales, para certificar la protección de los equipos informáticos ubicados en la Facultad; como sistemas de control ambiental de temperatura y humedad, sistemas de detección y extinción de incendios, sistemas de vigilancia, sistema de descarga eléctrica y alarmas en caso de detectarse condiciones ambientales no apropiadas.
4. El área de informática y de comunicaciones de la Facultad de Ingeniería Industrial debe contar como sistemas contra fallas de interrupciones eléctricas que sucedan en cualquier departamento informático.

3. Políticas de Escritorio Limpio y Pantalla Limpia

Las políticas de escritorio limpio y pantalla limpian tiene como lineamiento es de mantener los escritorios libres de documentos o de dispositivos móviles de almacenamiento de información, depositándolos en lugares seguros durante y después de su jornada laboral y que los escritorios de los equipos computacionales se encuentren sin acceso directo a la documentación o información confidencial de la institución.

1. Mantener actualizado el inventario de los hardware o equipos de cómputo de la Facultad de Ingeniería Industrial.

2. Garantizar que los equipos se encuentren registrados en la base datos del área informática y comunicaciones de la Facultad de Ingeniería Industrial.
3. Establecer bloqueos de usuarios cuando haya pasado cierto tiempo de inactividad en el equipo.
4. Garantizar que la ubicación del equipo de cómputo no sea ubicada en un lugar, que se pueda visualizar las pantallas por personas no autorizadas.
5. Garantizar que el acceso a los equipos de cómputo se requiera cada vez que el equipo se bloquee, encienda o reinicie.
6. Garantizar que las áreas de las oficinas o puestos de trabajo cuenten con archivadores necesarios para almacenar toda la documentación necesaria, que requiere ser protegida.
7. No deben de ingresar con ningún tipo de alimentos o bebidas cerca de los equipos de cómputos.
8. Cuando se ausente de su puesto de trabajo debe de bloquear la sesión de usuario, para proteger la documentación valiosa que se encuentre.
9. Cerrar correctamente la sesión del equipo de cómputo y apagar de forma correcta cuando finalice la jornada de trabajo, garantizando una desconexión satisfactoria de la red institucional de la Facultad de Ingeniería Industrial.
10. Evitar colocar accesos directos de documentos importantes en la pantalla, para mantener limpio y seguro la pantalla del equipo.

11. Retirar toda documentación física que se encuentre en impresoras, fax o escáner, evitando la exposición de la información documentado a personas no autorizadas.

4.6.6 Políticas de Seguridad de las Operaciones

1. Política de Protección contra Códigos Maliciosos

La política de protección de códigos maliciosos es decir que posean software antispam, antivirus, antimalware y antispyware instalados de esta forma se encuentre protegidos de cualquier software malicioso que intente poner en riesgo la información confidencial que se maneja en la red de la Facultad de Ingeniería Industrial.

1. El área de informática y comunicaciones debe contar con las herramientas necesarias que reduzcan el nivel de infección de un software malicioso y respalden la seguridad de la información dentro de la Facultad de Ingeniería Industrial.
2. El área de informática y comunicaciones debe garantizar que todos los softwares de antivirus cuenten con licencias de uso requeridas, certificando su autenticidad.
3. Se debe escanear toda la información contenida o almacenada en el software antivirus incluyendo la información contenida en los correos electrónicos.
4. El área de informática y comunicaciones debe garantizar que los equipos de cómputo no se pueda realizar cambios en su configuración del software antivirus, antispyware, antimalware, antispam que se encuentre instalados.
- 5.

6. El área de informática y comunicaciones debe garantizar que se posea las últimas actualizaciones de software antivirus, antispyware, antimalware, antispam para minimizar las vulnerabilidades dentro de los equipos de cómputo de la Facultad de Ingeniería Industrial.

2. Política de Copias de Respaldo de la Información

La política de copias de respaldo de información garantiza que todos los datos se encuentren respaldados, mediante copias de seguridad, preservar la disponibilidad de la información y la integridad de los mismo en la Facultad Ingeniería Industrial.

1. El área de informática y comunicaciones debe elaborar procedimientos para la ejecución y restauración en las copias de respaldo que deben realizar cada uno de los usuarios de la información que manejan en la Facultad de Ingeniería Industrial.
2. El área de informática y comunicaciones debe de disponer recursos de identificación y de disposición de medios de almacenamiento, permitirán el respaldo de la información de la Facultad de Ingeniería Industrial.
3. El área de informática y de comunicaciones debe definir las copias de respaldos y de restauración en cual se efectuarán por tiempos determinados.

4.6.7 Políticas de seguridad de las comunicaciones

1. Política de uso del Correo Electrónico Institucional

La política de uso de correo institucional garantiza que se siga los lineamientos de seguridad y contribuyan la confidencialidad, preservación y buenas prácticas del uso de este en la Facultad de Ingeniería Industrial.

1. Todos los servidores públicos y estudiantes deben ser conscientes que el correo institucional es de carácter individual es decir que no puede utilizar otra cuenta de correo que no sea la que fue asignada por la institución.
2. El correo electrónico institucional no debe ser utilizado con fines de uso personales o de otro interés que no forme parte de la institución y los buzones de mensajes solo deben contener información de acuerdo con el cargo que manejan.
3. Todos los servidores públicos y estudiantes no deben enviar cadenas de mensajes que argumente cualquier tipo de información no relacionada con la institución.

2. Política de Uso Adecuado de Internet

La política de uso adecuado de internet garantiza que todos los servidores públicos, estudiantes y partes interesadas, utilicen el servicio de internet de manera adecuada, evitando que su uso sea personal o que vayan contra las políticas establecidas.

1. El área de informática y de comunicaciones de la Facultad de Ingeniería Industrial es de diseñar un mecanismo que permita que el servicio de internet tenga una continuidad sin afectar las actividades tanto externo como interno.
2. El área de informático y de comunicaciones de la Facultad de Ingeniería Industrial debe definir los controles de descarga de los softwares no autorizados o códigos maliciosos que provienen de internet.
3. Todos los servidores públicos, estudiantes no deben acceder a páginas como drogas, alcohol, web proxys, hacking, pornografías que atenten como la ética moral, dentro de la Facultad de Ingeniería Industrial.
4. Todos los servidores públicos y estudiantes tienen restringido el acceso a los servicios comunitarios o mensajería como son las siguientes Facebook, kazzaa, MSN, Yahoo, Sype y otros similares que tengan que intercambiar información por esos medios.
5. Todos los servidores públicos y estudiantes tienen restringido descargar, intercambiar, usar juegos, películas, música, protectores o fondos de pantalla o cualquier otro tipo de software que atente con la integridad, confidencialidad de los sistemas de información de la Facultad de Ingeniería Industrial.

4.6.8 Políticas de Gestión de Incidentes de Seguridad de la Información

1. Política de Gestión de Incidentes y Mejoras en la Seguridad de la Información

La política de gestión de incidentes y mejoras en la seguridad de la información deben garantizar una seguridad optima que deben mitigar los riesgos que se hayan identificados o reportados, que afecten la disponibilidad, integridad y confidencialidad en la Facultad de Ingeniería Industrial.

1. El área de informática y de comunicaciones debe dar una respuesta rápida, efectiva y ordenada a cualquier evento de seguridad de la información ocurrido en la Facultad de Ingeniería Industrial.
2. El área de informática y de comunicaciones debe examinar los incidentes ocasionados en la seguridad de la información y llevar un informe a las personas encargadas de la seguridad información de la Facultad de Ingeniería Industrial.
3. Se debe asignar al personal calificado, para que realice una investigación adecuada de los incidentes de seguridad reportados y que se proporcione las soluciones necesarias del caso.
4. Se debe crear un base de conocimiento de los incidentes de seguridad que se hayan presentados con sus respectivas soluciones, con la finalidad de reducir el tiempo de reacción de incidentes futuros en la Facultad de Ingeniería Industrial.

4.6.9 Política de administración de Servidores

En la relación a los servidores que se encuentran en la Facultad de Ingeniería Industrial se establecerán las siguientes políticas.

1. El área de informática y de comunicaciones debe tener el acceso restringido a los servidores o medios de comunicación para que solo personal autorizado tenga permitido ingresar.
2. Cualquier persona externa que ingrese a las instalaciones donde se encuentren los sistemas de información debe registrarse en una bitácora de ingreso en donde se encuentre la información personal.
3. Queda prohibida la manipulación de los equipos informáticos y de comunicación como servidores, rack entre otros de personal no autorizado.
4. Las copias de seguridad de información de los servidores deben ser trasladada de forma segura a otro sitio.
5. Todos los equipos informáticos deben estar conectados a una alimentación de corriente eléctrica ininterrumpida para evitar fallas en el sistema.
6. La habitación en donde se encuentra los equipos informáticos como los servidores, racks entre otros deben contar con la temperatura adecuada manteniendo un segundo aire acondicionado de respaldo en la habitación de sistemas.

4.6.10 Sanciones

Todo el personal que labore en la Facultad de Ingeniería Industrial que no cumpla con los protocolos de seguridad de la información será

sancionado de forma legal o disciplinaria. Las sanciones van desde un llamado de atención por escrito hasta la finalización de sus labores, dependiendo de la gravedad de la falta cometida además del nivel de información que pudo ser extraída.

La ley establecida en Ecuador por los delitos de seguridad de Información que ha afectado la disponibilidad, integridad y confidencialidad de la información manipulada, por cual se regirá de acuerdo con las leyes establecidas.

4.7 Conclusiones

Conclusiones que se obtuvieron del proyecto en la elaboración de un protocolo post-evento informático de seguridad de la información basado en norma ISO/IEC-17799.

En la Facultad de Ingeniería Industrial se pudo encontrar debilidades de seguridad que pueden afectar al activo importante que es la información o datos que se manejan dentro de la Facultad de Ingeniería Industrial para ello se indago en cada una de las políticas existentes en la seguridad de la información y se estudió la forma correcta de aplicarlas mediante un comité responsable que deben saber cada una de sus tareas específicas y el campo de acción que ellos interactúan para estar preparados en cualquier post-evento informático que se presente en la organización y así las interrupciones que se hayan presentado sean corregidas de manera efectiva sin interrumpir las actividades de los diferentes usuarios dentro de la organización.

Los equipos informáticos de transferencias de información como racks, Switch entre otros que se encuentran en los diferentes laboratorios y departamentos no se encuentran protegidos con su estructura física metálica ya que cualquier persona extraña puede manipular los equipos y ocasionar daños como pérdida de información y desconfiguración de los equipos informáticos.

Por lo tanto, el diseño de un protocolo de seguridad de la información que permita evaluar los riesgos de seguridad y tomar las debidas correcciones y los pasos que se deben de seguir inmediatamente en algún evento que intenten quebrantar la seguridad física y lógica dentro de la Facultad de Ingeniería Industrial.

4.8 Recomendaciones

Las recomendaciones se establecerán de acuerdo con los puntos que están presentes en las conclusiones anteriores:

Se recomienda fortalecer las políticas de seguridad de la información en todas las áreas que manipulan información importante que puedan afectar la organización capacitando a los usuarios con los protocolos de seguridad vigentes en la Facultad de Ingeniería Industrial basado con los siguientes puntos que se deben tomar en consideración:

- Políticas de la Organización de la Seguridad de la Información
- Políticas de Seguridad de los Recursos Humanos
- Políticas de Gestión de Activos de Información
- Política de Control de Acceso

- Políticas de Criptografía
- Políticas de Seguridad Física y del Entorno
- Políticas de Seguridad de las Operaciones
- Políticas de seguridad de las Comunicaciones
- Políticas de Gestión de Incidentes de Seguridad de la Información
- Políticas de Administración de Servidores
- Sanciones

Se recomienda mantener la estructura metálica de todos los equipos como Switch, racks cubiertos para evitar manipulación de personas externas y la acumulación de polvo que puedan perjudicar al equipo y dañarlo ocasionando un gran problema cuando se está laborando dentro de la red de la Facultad de Ingeniería Industrial.

Se recomienda que se realice mantenimientos en la red de la Facultad de Ingeniería Industrial que permitan detectar cables dañados u obsoletos que impidan la transferencia de información y que perjudiquen a los diferentes usuarios en sus actividades diarias.

ANEXOS

ANEXO N°1

Encuesta a al Personal Administrativo y Profesores de las distintas carreras de la Facultad de Ingeniería Industrial de la Universidad Estatal de Guayaquil

1. ¿Conoce las funciones que debe desempeñar en su puesto de trabajo?

TABLA N°11

NIVEL DE CONOCIMIENTO DE SUS FUNCIONES LABORABLES

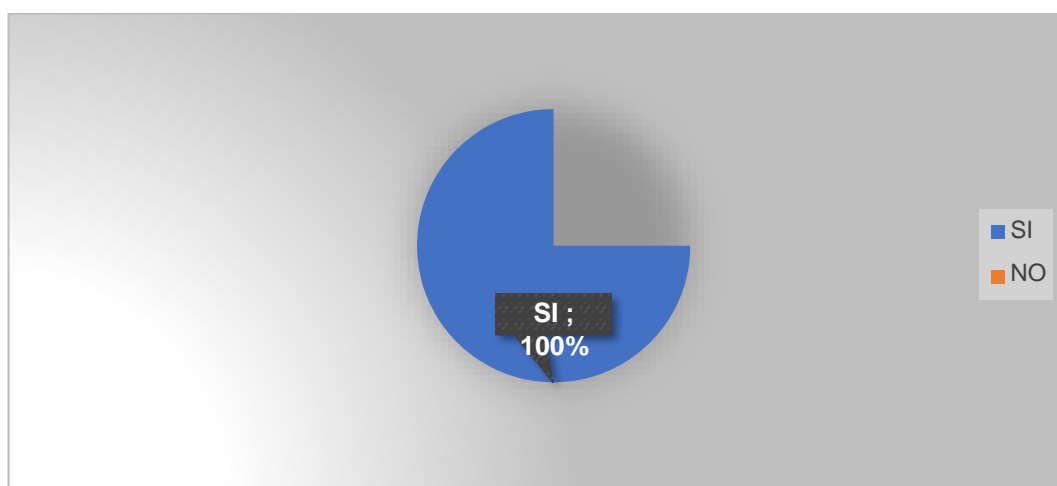
Opción	Cantida d	Porcentaj e
SI	81	100%
NO	0	0%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°1

RESULTADO DE NIVEL DE CONOCIMIENTO DE SUS FUNCIONES LABORABLES



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 100% de los encuestados conoce las funciones que deben realizar en su puesto de trabajo.

2. ¿La Facultad de Ingeniería Industrial cuenta con políticas de seguridad de información?

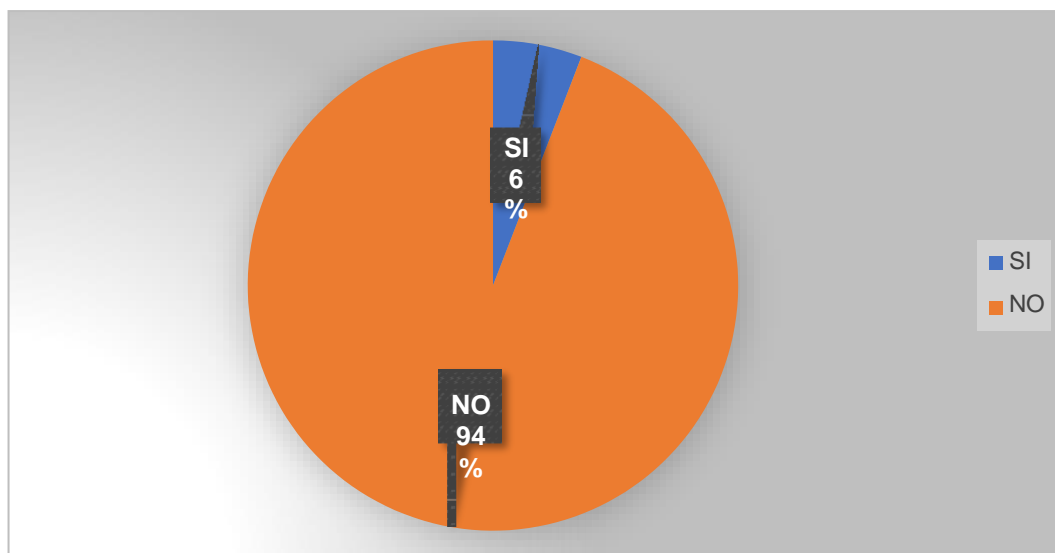
TABLA N°12
NIVEL DE CONOCIMIENTO QUE HAY POLÍTICAS DE SEGURIDAD DE LA FACULTAD DE INGENIERÍA INDUSTRIAL

Opción	Cantidad	Porcentaje
SI	72	94%
NO	9	6%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°2
RESULTADO DE NIVEL DE CONOCIMIENTO QUE HAY POLÍTICAS DE SEGURIDAD DE LA FACULTAD DE INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 94% de los encuestados indican que no conocen las políticas de seguridad de la información de Facultad de Ingeniería

Industrial mientras que el 6% indica que si conocen las políticas de seguridad de la Facultad de Ingeniería Industrial.

3. ¿Conoce alguna Políticas?

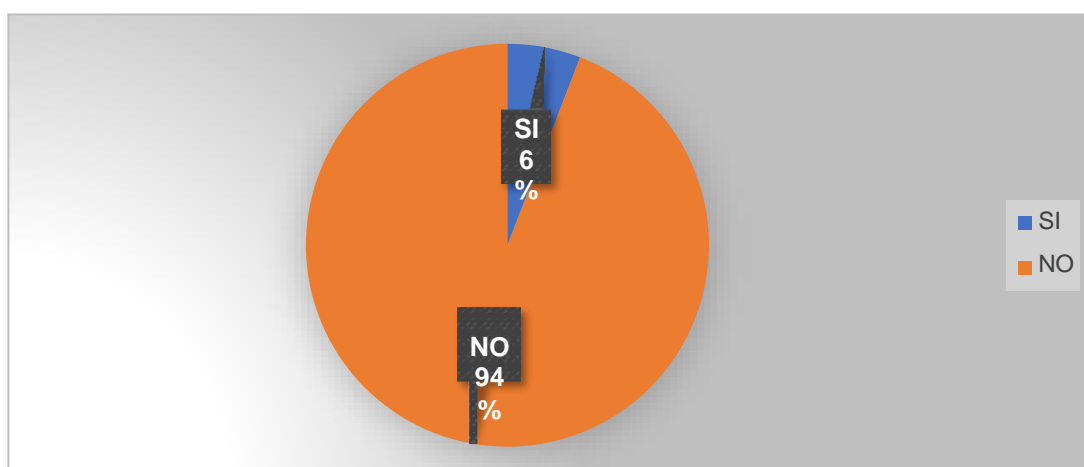
TABLA N°13
NIVEL DE CONOCIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA FACULTAD DE INGENIERÍA INDUSTRIAL

Opción	Cantidad	Porcentaje
SI	72	94%
NO	9	6%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°3
RESULTADO DE NIVEL DE CONOCIMIENTO DE LAS POLÍTICAS DE SEGURIDAD DE LA FACULTAD DE INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 94% de los encuestados indican que no conocen las políticas de seguridad de la información de Facultad de Ingeniería Industrial mientras que el 6% indica que si conocen las políticas de seguridad de la Información indicaron que saben algunas de ellas Facultad de Ingeniería Industrial.

4. ¿Ha recibido capacitación al respecto de las políticas de seguridad de información?

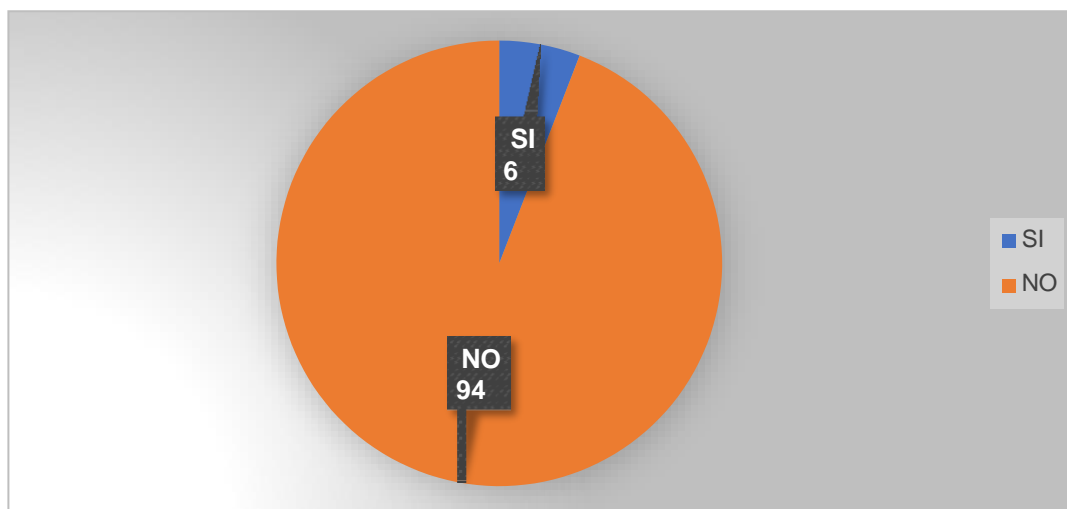
TABLA N°14
NIVEL DE CAPACITACIÓN DE LAS POLÍTICAS DE SEGURIDAD DE INFORMACIÓN LA FACULTAD DE INGENIERÍA INDUSTRIAL

Opción	Cantidad	Porcentaje
SI	72	94%
NO	9	6%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°4
RESULTADO DE NIVEL DE CAPACITACIÓN DE LAS POLÍTICAS DE SEGURIDAD INFORMACIÓN DE LA FACULTAD DE INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 94% de los encuestados indican que no conocen las políticas de seguridad de la información de Facultad de Ingeniería Industrial mientras que el 6% indica que si conocen las políticas de seguridad de la

Información indicaron que saben algunas de ellas Facultad de Ingeniería Industrial.

5. ¿Maneja o tiene a su cargo activos Informáticos?

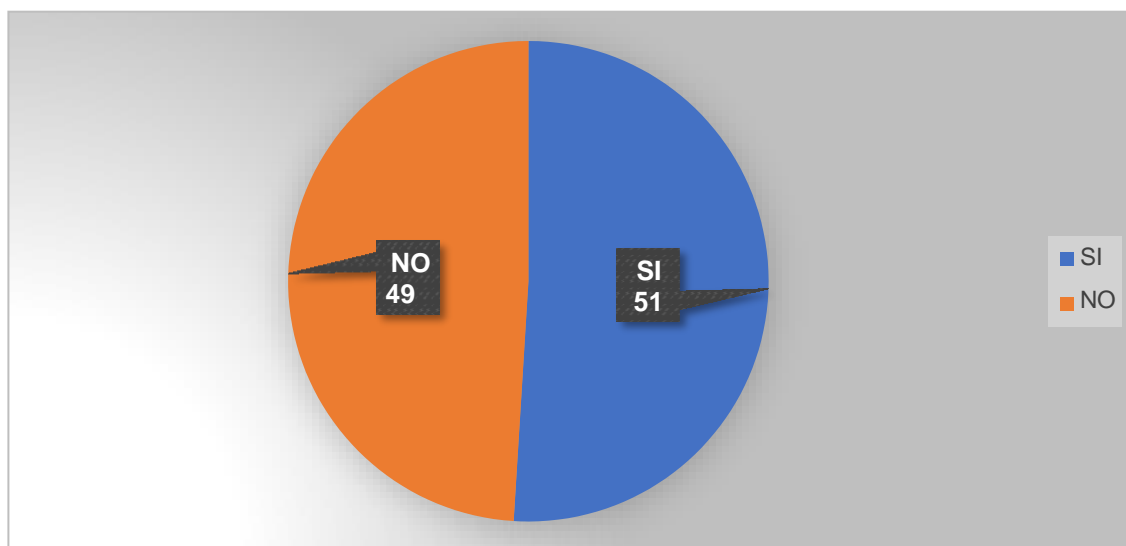
TABLA N°15
MANEJO DE ACTIVOS INFORMÁTICOS LA FACULTAD DE
INGENIERÍA INDUSTRIAL

Opción	Cantida d	Porcentaj e
SI	39	49%
NO	43	51%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°5
RESULTADO DEL MANEJO DE ACTIVOS INFORMÁTICOS DE LA
FACULTAD DE INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 49% de los encuestados indican que no manejan activos informáticos como base datos e información importante de la

Facultad de Ingeniería Industrial mientras que el 51% indica que si maneja activos informáticos o bases de datos en la Facultad de Ingeniería Industrial.

6. ¿Tiene acceso a Internet desde su computador o laptop?

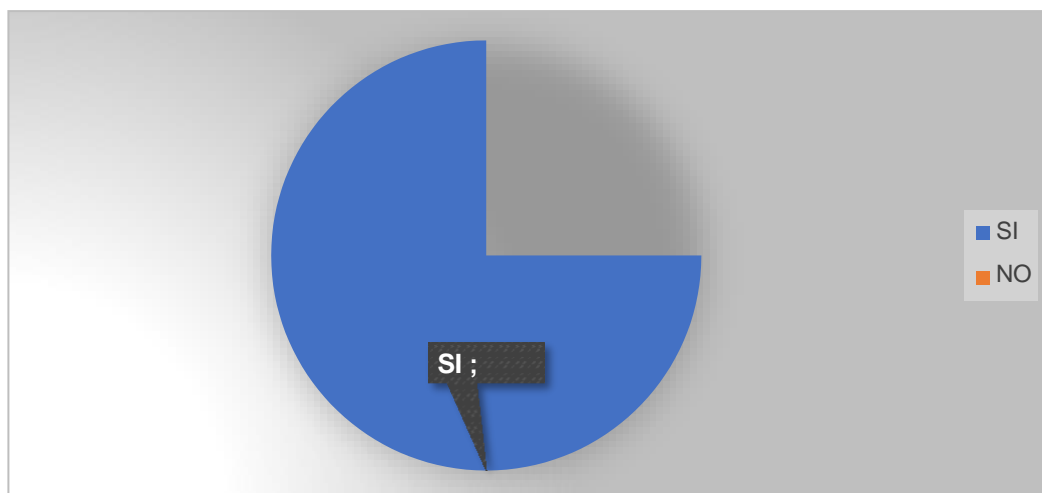
TABLA N°16
NIVEL DE ACCESO DE LOS USUARIOS A INTERNET DESDE
COMPUTADOR O LAPTOP EN LA FACULTAD DE INGENIERÍA
INDUSTRIAL

Opción	Cantidad	Porcentaje
SI	81	100%
NO	0	0
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°6
RESULTADO NIVEL DE ACCESO DE LOS USUARIOS A INTERNET
DESDE COMPUTADOR O LAPTOP DE LA FACULTAD DE
INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 100% de los encuestados indican que tienen acceso a internet de sus computadoras y laptop.

7. ¿Almacena información confidencial en su computador?

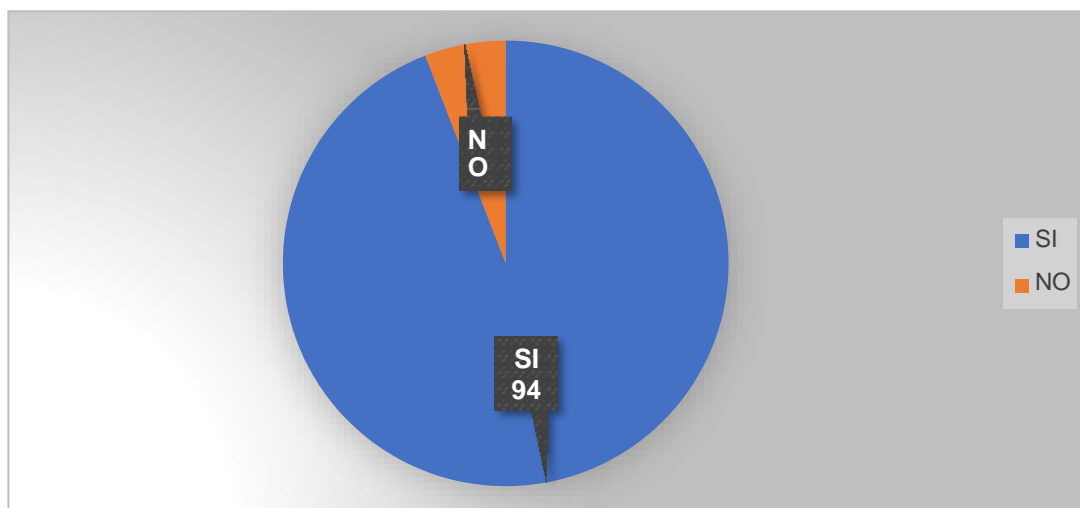
TABLA N°17
ALMACENA INFORMACIÓN CONFIDENCIAL EN SU COMPUTADOR
DE LA FACULTAD DE INGENIERÍA INDUSTRIAL

Opción	Cantidad	Porcentaje
SI	72	94%
NO	9	6%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°7
RESULTADO DE ALMACENA INFORMACIÓN CONFIDENCIAL EN SU
COMPUTADOR DE LA FACULTAD DE INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 6% de los encuestados indican que no almacena información confidencial de la Facultad de Ingeniería Industrial mientras

que el 94% indica que si almacena información confidencial de la Facultad de Ingeniería Industrial.

8. ¿Comparte esta información por algún medio sin cifrarla?

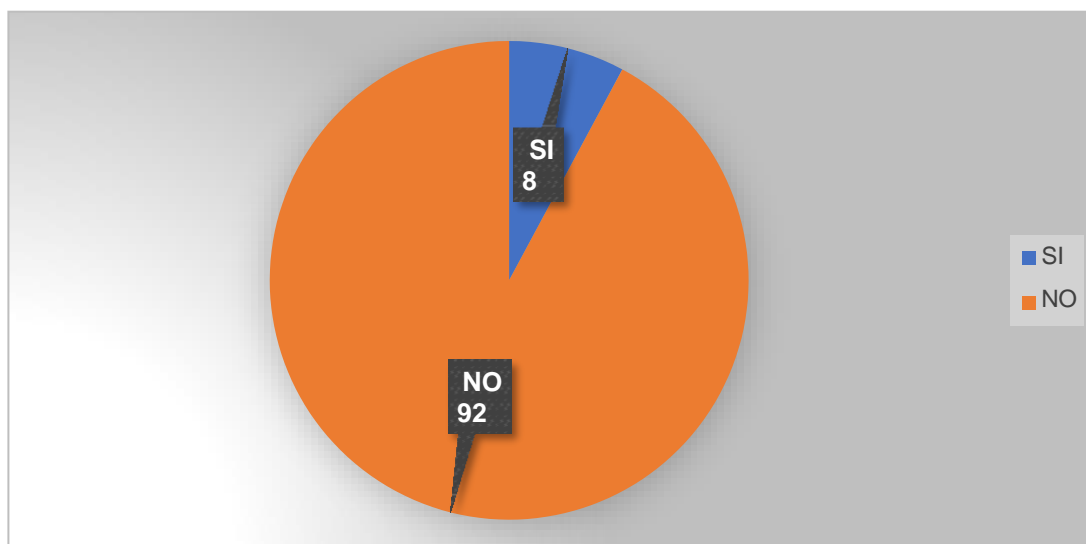
TABLA N°18
COMPARTE ESTA INFORMACIÓN SIN CIFRARLA POR ALGÚN
MEDIO INFORMÁTICO

Opción	Cantida d	Porcentaj e
SI	10	8%
NO	71	92%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°8
RESULTADO DE COMPARTIR INFORMACIÓN SIN CIFRARLA POR
ALGÚN MEDIO INFORMÁTICO



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 92% de los encuestados indican que no envía información confidencial de la Facultad de Ingeniería Industrial cifrándola

mientras que el 8% indica que si envían información sin cifrarla de la Facultad de Ingeniería Industrial.

9. Realiza periódicamente copias de seguridad de la información

TABLA N°19

SE REALIZA COPIAS DE SEGURIDAD DE LA INFORMACIÓN EN EL COMPUTADOR DE LA FACULTAD DE INGENIERÍA INDUSTRIAL

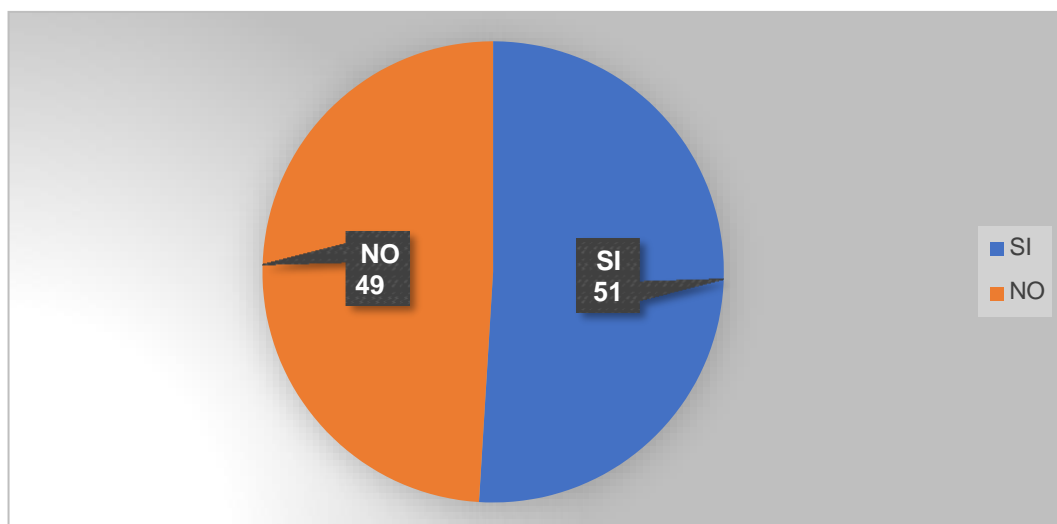
Opción	Cantidad	Porcentaje
SI	26	51%
NO	25	49%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°9

RESULTADO SE REALIZA COPIAS DE SEGURIDAD DE LA INFORMACIÓN EN EL COMPUTADOR DE LA FACULTAD DE INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 49% de los encuestados indican que no realizan copias de seguridad información confidencial de la Facultad de Ingeniería Industrial mientras que el 51% indica que realizan copias de seguridad de la información de la Facultad de Ingeniería Industrial.

10. ¿Tiene cuenta de correo electrónico institucional?

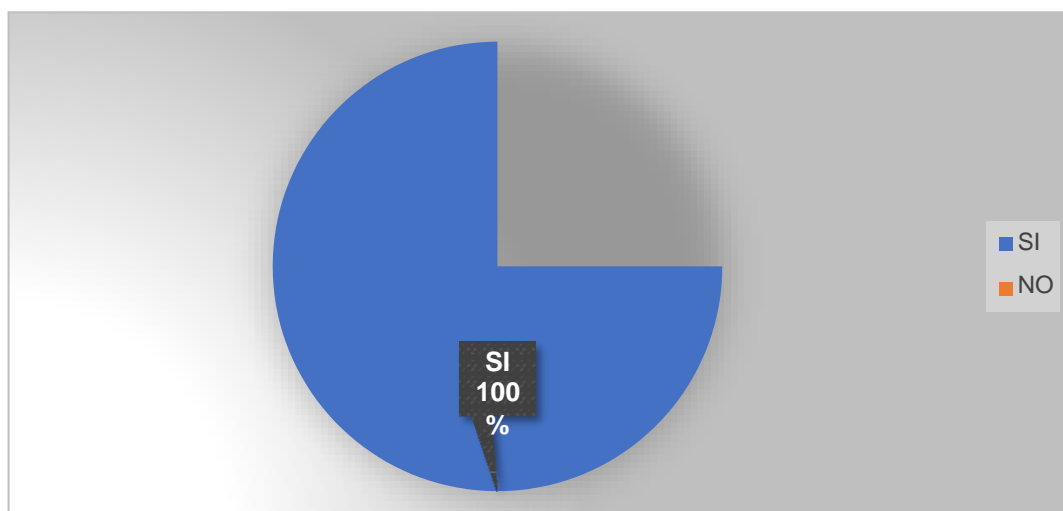
TABLA N°20
TIENE CUENTA DE CORREO ELECTRONICO INSTITUCIONAL
FACULTAD DE INGENIERÍA INDUSTRIAL

Opción	Cantidad	Porcentaje
SI	81	100%
NO	0	0%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°10
RESULTADO DEBE TENER CUENTA DE CORREO ELECTRONICO
INSTITUCIONAL FACULTAD DE INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 100% de los encuestados indican que tienen correo institucional de la Facultad de Ingeniería Industrial Universidad de Guayaquil.

11. ¿Conoce la clave de acceso a su correo institucional?

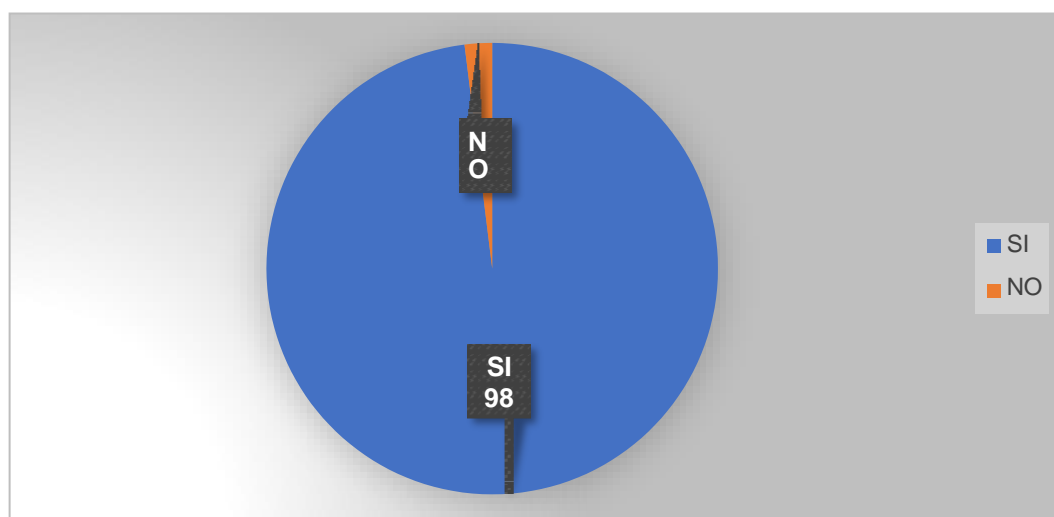
TABLA N°21
CONOCE LA CLAVE DE SU CORREO ELECTRONICO
INSTITUCIONAL FACULTAD DE INGENIERÍA INDUSTRIAL DE LA
UNIVERSIDAD DE GUAYAQUIL

Opción	Cantida d	Porcentaj e
SI	80	98%
NO	1	2%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°11
RESULTADO DE CONOCE LA CLAVE DE SU CORREO
ELECTRONICO INSTITUCIONAL FACULTAD DE INGENIERÍA
INDUSTRIAL DE LA UNIVERSIDAD DE GUAYAQUIL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 2% de los encuestados indican que no saben cuál es su clave de acceso al correo institucional de la Universidad de Guayaquil mientras que el 98% indica que si conocen su clave de acceso a su correo institucional de la Universidad de Guayaquil.

12. ¿Posee clave para acceso al equipo de trabajo?

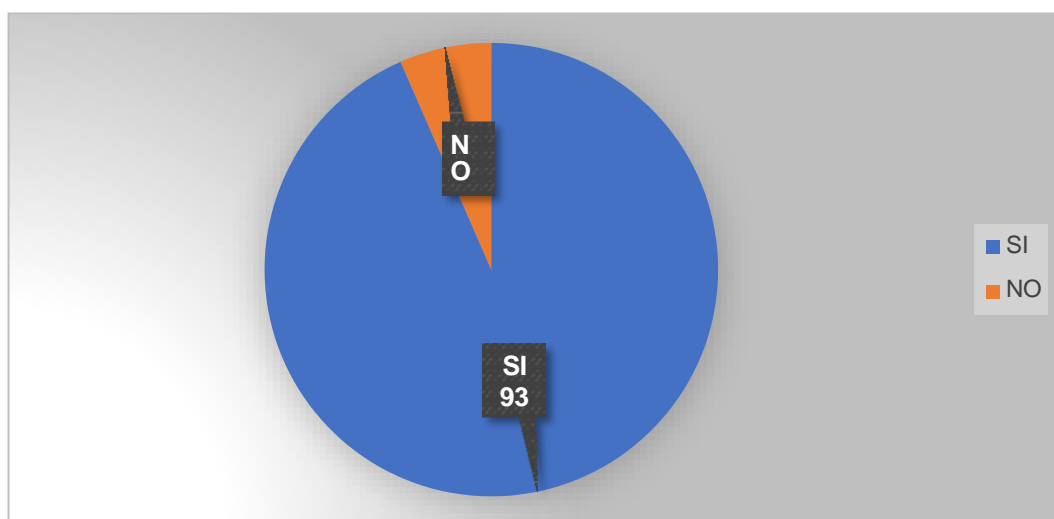
TABLA N°22
CUENTA CON CLAVE DE ACCESO A SU COMPUTADOR DE
TRABAJO EN LA FACULTAD DE INGENIERÍA INDUSTRIAL

Opción	Cantidad	Porcentaje
SI	75	93%
NO	6	7%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°12
RESULTADO DE CUENTA CON CLAVE DE ACCESO A SU
COMPUTADOR DE TRABAJO EN LA FACULTAD DE INGENIERÍA
INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 7% de los encuestados indican que no poseen claves de acceso a sus equipos de trabajos en la Facultad de Ingeniería Industrial mientras que el 93% indica que si poseen su clave de acceso a sus equipos de trabajo en la Facultad de Ingeniería Industrial.

13. ¿Cambia de forma periódica las claves de acceso al equipo y/o al correo?

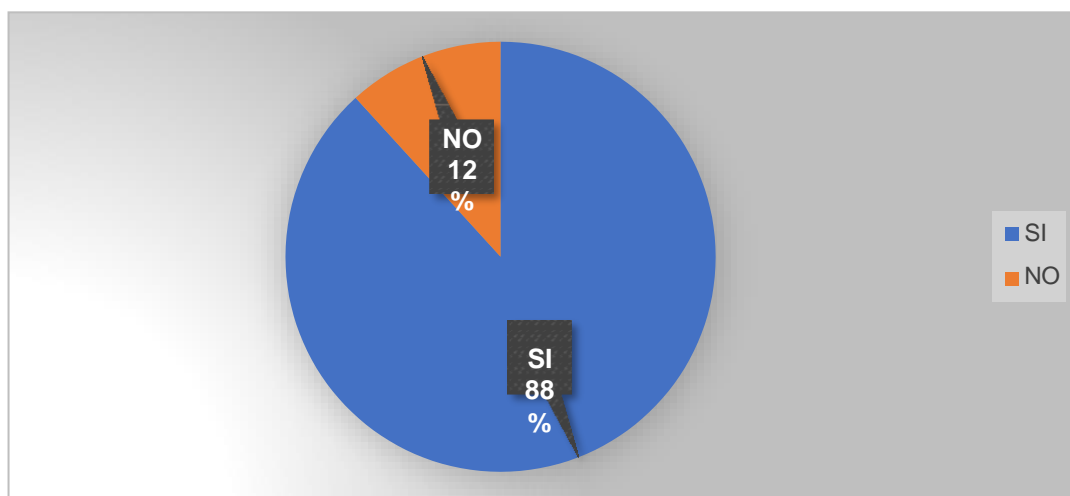
TABLA N°23
CAMBIA PERIÓDICAMENTE LAS CLAVE DE ACCESO A SU
COMPUTADOR DE TRABAJO O CORREO EN LA FACULTAD DE
INGENIERÍA INDUSTRIAL

Opción	Cantidad	Porcentaje
SI	68	88%
NO	13	12%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°13
RESULTADO DE CAMBIA PERIÓDICAMENTE LAS CLAVE DE
ACCESO A SU COMPUTADOR DE TRABAJO O CORREO EN LA
FACULTAD DE INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 12% de los encuestados indican que no cambian claves de acceso a sus equipos de trabajos o correos institucionales en la Facultad de Ingeniería Industrial mientras que el 98% indica que si cambian periódicamente las claves de acceso a sus equipos de trabajo y a los correos institucionales de la Facultad de Ingeniería Industrial de la Universidad de Guayaquil.

14. ¿Tiene un comité de seguridad de la información a nivel de alta dirección?

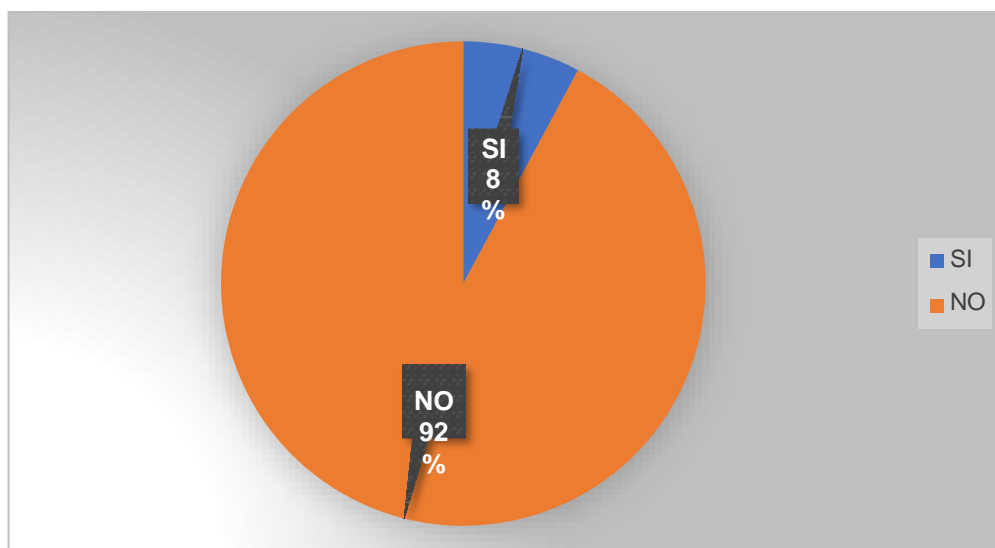
TABLA N°24
CUENTA CON UN COMITÉ DE SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE INGENIERÍA INDUSTRIAL

Opción	Cantidad	Porcentaje
SI	4	8%
NO	77	92%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°14
RESULTADO DE CUENTA CON UN COMITÉ DE SEGURIDAD DE LA INFORMACIÓN EN LA FACULTAD DE INGENIERÍA INDUSTRIAL



Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 92% de los encuestados indican que no cuentan con un comité de seguridad de la información de alta dirección en la Facultad de Ingeniería Industrial mientras que el 8% indica que si cuentan con un comité de seguridad de la información alta dirección de la Facultad de Ingeniería Industrial.

15. ¿Realizan evaluaciones de seguridad de la información a través de entidades públicas o privadas?

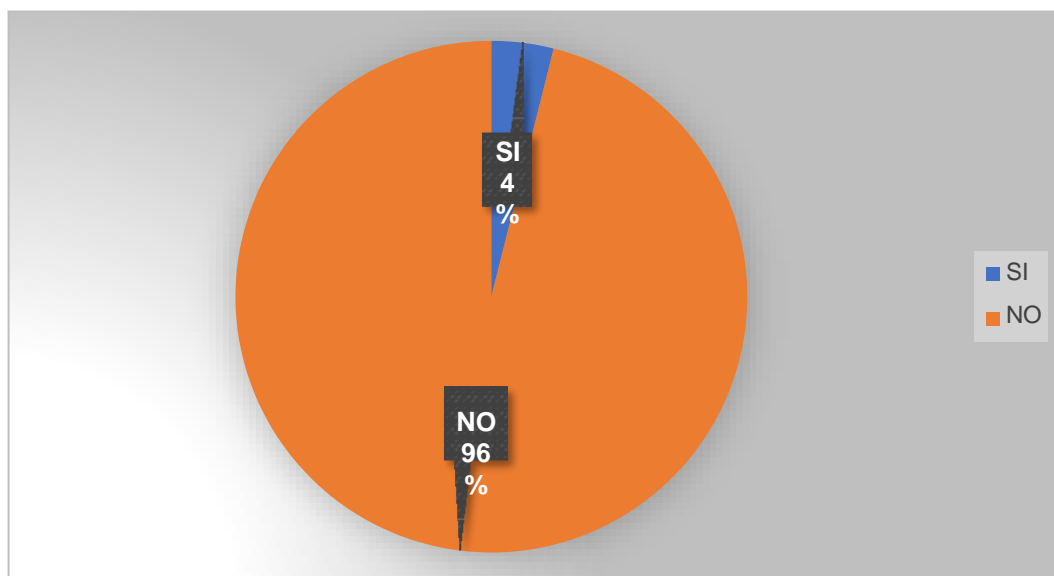
TABLA N°25
SE REALIZAN EVALUACIONES DE SEGURIDAD POR ENTIDADES
PÚBLICAS O PRIVADAS EN LA FACULTAD DE INGENIERÍA
INDUSTRIAL

Opción	Cantida d	Porcentaj e
SI	2	4%
NO	79	96%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°15
RESULTADO DE SE REALIZAN EVALUACIONES DE SEGURIDAD
POR ENTIDADES PÚBLICAS O PRIVADAS EN LA FACULTAD DE
INGENIERÍA INDUSTRIAL



Fuente: Encuesta
Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 96% de los encuestados indican que no se realizan evaluaciones de seguridad por ninguna entidad pública o privada Facultad de Ingeniería Industrial mientras que el 4% indica que si se realizan evaluaciones de seguridad por alguna entidad pública o privada en la Facultad de Ingeniería Industrial.

16. ¿Si suceden incidentes de seguridad en los sistemas de información se encuentra usted preparado?

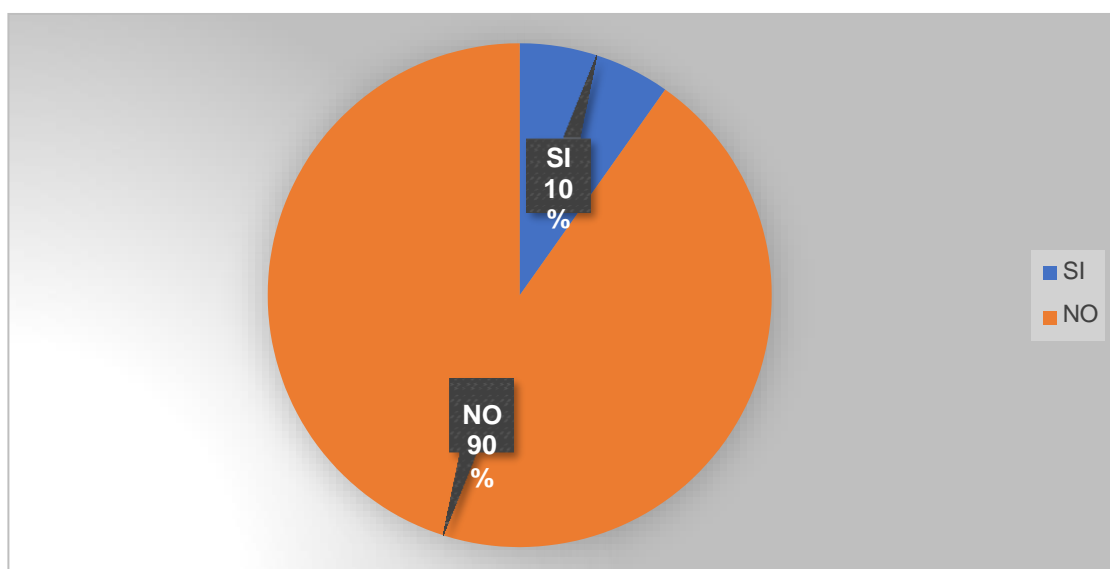
TABLA N°26
SE ENCUENTRA PREPARADO POR INCIDENTES QUE SUCEDAN EN
LOS SISTEMAS DE INFORMACIÓN EN LA FACULTAD DE
INGENIERÍA INDUSTRIAL

Opción	Cantida d	Porcentaj e
SI	8	10%
NO	73	90%
TOTAL	81	100%

Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

GRÁFICO N°16
RESULTADO DE ENCUESTA PREPARADO POR INCIDENTES QUE
SUCEDAN EN LOS SISTEMAS DE INFORMACIÓN EN LA FACULTAD
DE INGENIERÍA INDUSTRIAL




Fuente: Encuesta

Realizado por: Parraga Olvera Rene Gregorio

Análisis. - El 90% de los encuestados indican que no se encuentra preparado si suceden incidentes de seguridad en los sistemas de información Facultad de Ingeniería Industrial mientras que el 10% indica que si se encuentra preparado si suceden incidentes de seguridad en los sistemas de información Facultad de Ingeniería Industrial.



ANEXO N°2

**PRUEBAS DE LAS POLÍTICAS DE SEGURIDAD DE LA
INFORMACIÓN PARA LOS EMPLEADOS DE LA FACULTAD DE
INGENIERÍA INDUSTRIAL**

 <p style="text-align: center;">UNIVERSIDAD DE GUAYAQUIL FACULTAD DE INGENIERÍA INDUSTRIAL</p> <p style="text-align: center;">PRUEBAS DE POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN PARA LOS EMPLEADOS DE LA FACULTAD DE INGENIERÍA</p>				
Num	Aspecto a evaluar	SI	NO	Observaciones
1	¿Conoce las funciones que debe desempeñar en su puesto de trabajo?			
2	¿La Facultad de Ingeniería Industrial cuenta con políticas de seguridad de información?			
3	¿Conoce alguna Políticas? (Mencione al menos dos)			
4	¿Ha recibido capacitación al respecto de las políticas de seguridad de información?			
5	¿Maneja o tiene a su cargo activos Informaticos?			
6	¿Tiene acceso a Internet desde su computador o lapto?			
7	¿Almacena información confidencial en su computador?			
8	¿Comparte esta información por algun medio sin cifrarla?			
9	Realiza periódicamente copias de seguridad de la información			
10	¿Tiene cuenta de correo electrónico institucional?			
11	¿Conoce la clave de acceso a su correo institucional?			
12	¿Posee clave para acceso al equipo de trabajo?			
13	¿Cambia de forma periódica las claves de acceso al equipo y/o al correo?			
14	¿Tiene un comité de seguridad de la información a nivel de alta dirección?			
15	¿Realizan evaluaciones de seguridad de la información a través de entidades públicas o privadas?			
16	¿Si suceden incidentes de seguridad en los sistemas de información se encuentra usted preparado?			

ANEXO N°3

FORMATO DE REPORTE DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN

	Facultad de Ingeniería Industrial de la Universidad de Guayaquil Formato Reporte de Incidentes de la Seguridad de la Información				
Datos de Inicio del Reporte					
Fecha:		Hora:		Consecutivo:	
Datos de Incidente					
Fecha:		Hora:			
Departamento donde se ocasiono el incidente:					
Descripción del Incidente:					
<div style="border: 1px solid black; padding: 5px;"> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> <div style="border-bottom: 1px solid black; height: 15px; margin-bottom: 5px;"></div> </div>					
Quien Reporta:				Quien recibe el reporte:	
Nombre:		Nombre:			
Firma:		Firma:			

ANEXO N°4

FORMATO DE INGRESO Y ELIMINACIÓN DE USUARIOS

[illegible]

BIBLIOGRAFÍA

AG, P. g. (04 de 11 de 2015). *Company industries topics cases y perspectives offices career*. Sitio web de Como determinar el tamaño de la muestra: <http://www.psymba.com/company/news/message/como-determinar-el-tamano-de-una-muestra>

Amador, M. G. (2016). *Metodologia de la Investigacion*. Sitio web de Guia Metodológica: <http://manuelgalan.blogspot.com/p/guia-metodologica-para-investigacion.html>

bortnik, s. (13 de 03 de 2010). *esecurity*. Blog de Que es la fuga de Informacio: <https://www.welivesecurity.com/la-es/2010/04/13/que-es-la-fuga-de-informacion>

Caldas, U. D. (marzo de 2017). *seguridad de la informacion*. Artículo de portalws udistrital.edu: https://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf

Central, E. T. (19 de 04 de 2017). *Manual de Politicas de Seguridad y Privacidad de la Informacion*. Manual de Politicas: <http://www.itc.edu.co/archives/manualpiliticassi.pdf>

consite. (s.f.). *Bienvenido a nuestro Blog*. Sitio web de www.cosinte.com: <http://www.cosinte.com/protocolos-de-seguridad/>

Datos, E. e. (27 de 11 de 2013). *Razones por la que se pierde la integridad de los datos*. Sitio web de power data: <https://blog.powerdata.es/el-valor-de-la-gestion-de-datos/bid/349170/razones-por-las-que-se-pierde-la-integridad-de-los-datos>

Ecuador, P. N. (21 de 03 de 2018). *Los Activos de la Seguridad de la Informacion y sus Riesgos*. Artículo de Policía Nacional del Ecuador:

<http://www.policiaecuador.gob.ec/los-activos-de-la-seguridad-de-la-informacion-y-sus-riesgos>

Elcas21. (07 de 30 de 2015). *scribd*. Sitio web de Resumen iso 17799:
<https://www.scribd.com/document/272998312/Resumen-ISO-17799>

Gabriel, D. (2015). Artículo del *fortalecimiento de seguridad*. Guayaquil.

informacio, i. P. (2 de 06 de 2016). *guia metodologica de analisis de riesgos de seguridad y privacidad de la informacion superintendencia nacional de salud*. bogota d.c: 2/06/2016.

institute, s. e. (1 de 10 de 2014). *Seguridad Informatica*. Sitio web de
https://issuu.com/michelwebivan/docs/seguridad_informatica

jose, G. A. (25 de mayo de 2017). *repositorio* de la universidad de guayaquil:
<http://repositorio.ug.edu.ec/bitstream/redug/27168/1/GARCÍA20ÁLVAREZA%20MARÍA%20JOSÉ.pdf>

Iujan, U. n. (s.f.). *Departamento de seguridad informatica*. Repositorio de seguridad informatica:
<http://www.seguridadinformatica.unlu.edu.ar/?q=node/12>

Medina, F. (17 de mayo de 2017). *El comercio*. Blog de El ciberataque:
<http://www.elcomercio.com/actualidad/ciberataque-wannacry-impacto-ecuador-hackeo.html>

Mexico, U. N. (2018). *Universidad Nacional Autonoma de Mexico*. Repositorio de Seguridad cultura de prevencion para TI:
<https://revista.seguridad.unam.mx/numero-10/ingenier%C3%AD-social-corrompiendo-la-mente-humana>

Orozco, C. A. (05 de 05 de 2015). *Universidad Nacional Abierta y a Distancia*. Repositorio de Desarrollo e implemtacion del manual de politicas de seguridad informatica.

PMG. (21 de 05 de 2015). *BLOG DE SISTEMAS DE GESTION DE SEGURIDAD*. Blog de SGSI: <https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion>

Target, T. (2016). *search data center*. Blog de Gestion de riesgos de seguridad de la informacion:
<https://searchdatacenter.techtarget.com/es/consejo/Gestion-de-riesgos-de-seguridad-de-la-informacion-Comprension-de-los-componentes>