



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

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

**ÁREA  
SEGURIDAD DE LA INFORMACIÓN**

**TEMA  
“EVALUACIÓN DE LA SEGURIDAD TECNOLÓGICA DE LA  
INFORMACIÓN DE LA CARRERA DE INGENIERÍA EN  
TELEMÁTICA DE LA UNIVERSIDAD DE GUAYAQUIL”**

**AUTORA  
DAQUI LEMA DAYSI JACKELINE**

**DIRECTOR DEL TRABAJO  
ING. TELECOMUNICACIONES VEINTIMILLA ANDRADE JAIRO GEOVANNY, MG.**

**GUAYAQUIL, OCTUBRE 2019**



## ANEXO XI.- FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN



### FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA

<b>REPOSITORIONACIONAL EN CIENCIA Y TECNOLOGÍA</b>			
<b>FICHA DE REGISTRO DE TRABAJO DE TITULACIÓN</b>			
<b>TÍTULO Y SUBTÍTULO:</b>			
Evaluación de la seguridad tecnológica de la información de la carrera de ingeniería en telemática de la Universidad de Guayaquil.			
<b>AUTOR(ES)</b> (apellidos/nombres):		Daqui Lema Daysi Jackeline	
<b>REVISOR(ES)/TUTOR(ES)</b> (apellidos/nombres):		Ing. Ortiz Mosquera Neiser / Ing. Veintimilla Andrade Jairo	
<b>INSTITUCIÓN:</b>		Universidad de Guayaquil	
<b>UNIDAD/FACULTAD:</b>		Facultad de Ingeniería Industrial	
<b>MAESTRÍA/ESPECIALIDAD:</b>			
<b>GRADO OBTENIDO:</b>		Ingeniería en Teleinformática	
<b>FECHA DE PUBLICACIÓN:</b>		9 de junio del 2020	<b>No. DE PÁGINAS:</b> 96
<b>ÁREAS TEMÁTICAS:</b>		Seguridad de la información	
<b>PALABRAS CLAVES/ KEYWORDS:</b>		Seguridad, Información, Norma, Política, Usuario, Amenaza	
<b>RESUMEN/ABSTRACT (100-150 palabras):</b>			
<p>Mediante el siguiente estudio se analizó en la fase IV la seguridad de física, eléctrica y seguridad de la información de la Carrera de Ingeniería Telemática, con la finalidad de identificar las amenazas y vulnerabilidades que posee la institución, realizando una auditoria informática basada en la Norma ISO 27001, es muy importante tener en cuenta las políticas de seguridad que deben ser fortalecidas y que los usuarios se comprometan a cumplir con las mismas al realizar sus labores diarias; en la fase V se procede a evaluar y analizar las vulnerabilidades de acuerdo al anexo A de la normativa la manera se efectúa este estudio es mediante la observación, análisis y entrevista que ayuda a obtener resultados reales de la auditoría realizada a la organización; además de realizar una investigación descriptiva, documental y bibliográfica. El análisis tiene como objetivo principal determinar resultados propicios que ayude a realizar este proyecto, utilizando herramientas que ayuden a mejorar la seguridad de la organización.</p>			

Through the following study, the physical, electrical and information security of the Telematic Engineering Degree were analyzed in phase IV, with the determination to identify the threats and vulnerabilities that the institution has, to carry out a computerized audit based on the Standard ISO 27001, it is very important to take into account the security policies that must be strengthened and that the users commit to comply with them when carrying out their daily tasks; In phase V, the vulnerabilities will be evaluated and analyzed according to Annex A of the regulations. The way this study will be carried out is through observation, analysis and interviews that will help to obtain real results of the audit carried out on the organization; in addition to carrying out descriptive, documentary and bibliographic research. The main objective of the analysis is to determine favorable results that help carry out this project, using tools that help improve the security of the organization.

ADJUNTO PDF:	SI X	NO
CONTACTO CON AUTOR/ES:	Teléfono: 0960756941	E-mail: <a href="mailto:daysij_daquil@hotmail.com">daysij_daquil@hotmail.com</a>
CONTACTO CON LA INSTITUCIÓN:	Nombre: Ing. Ramon Maquilon Nicola, MG	
	Teléfono: 593-2658128	
	E-mail: <a href="mailto:directorTi@ug.edu.ec">directorTi@ug.edu.ec</a>	



**ANEXO XII.- DECLARACIÓN DE AUTORÍA Y DE  
AUTORIZACIÓN DE LICENCIA GRATUITA  
INTRANSFERIBLE Y NO EXCLUSIVA PARA EL USO NO  
COMERCIAL DE LA OBRA CON FINES NO ACADÉMICOS**



**FACULTAD DE INGENIERÍA INDUSTRIAL  
CARRERA INGENIERÍA EN TELEINFORMÁTICA**

---

LICENCIA GRATUITA INTRANSFERIBLE Y NO COMERCIAL DE LA OBRA CON  
FINES NO ACADÉMICOS

Yo, **DAQUI LEMA DAYSI JACKELINE**, con C.C. No. **0604258053**, certifico que los contenidos desarrollados en este trabajo de titulación, cuyo título es “**EVALUACIÓN DE LA SEGURIDAD TECNOLÓGICA DE LA INFORMACIÓN DE LA CARRERA DE INGENIERÍA EN TELEMÁTICA DE LA UNIVERSIDAD DE GUAYAQUIL**” son de mi absoluta propiedad y responsabilidad, en conformidad al Artículo 114 del CÓDIGO ORGÁNICO DE LA ECONOMÍA SOCIAL DE LOS CONOCIMIENTOS, CREATIVIDAD E INNOVACIÓN, autorizo la utilización de una licencia gratuita intransferible, para el uso no comercial de la presente obra a favor de la Universidad de Guayaquil.

A handwritten signature in blue ink that reads "Daysi Daqui".

**DAQUI LEMA DAYSI JACKELINE**

**C.C.No. 0604258053**



## ANEXO VII.- CERTIFICADO PORCENTAJE DE SIMILITUD



### FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA

Habiendo sido nombrado ING. VEINTIMILLA ANDRADE JAIRO GEOVANNY, tutor del trabajo de titulación certifico que el presente trabajo de titulación ha sido elaborado por DAQUI LEMA DAYSI JACKELINE, C.C.: 0604258053, con mi respectiva supervisión como requerimiento parcial para la obtención del título de INGENIERA EN TELEINFORMÁTICA.

Se informa que el trabajo de titulación: **“EVALUACIÓN DE LA SEGURIDAD TECNOLÓGICA DE LA INFORMACIÓN DE LA CARRERA DE INGENIERÍA EN TELEMÁTICA DE LA UNIVERSIDAD DE GUAYAQUIL”**, ha sido orientado durante todo el periodo de ejecución en el programa Antiplagio (URKUND) quedando el 1 % de coincidencia.

[https://secure.orkund.com/old/view/63038088-912079-870036#q1bKLVayijY2i9VRKs5Mz8tMy0xOzEtOVbly0DMwMDlwMzazNLewNDYzMLE0s\\_DCrBQA=](https://secure.orkund.com/old/view/63038088-912079-870036#q1bKLVayijY2i9VRKs5Mz8tMy0xOzEtOVbly0DMwMDlwMzazNLewNDYzMLE0s_DCrBQA=)

**URKUND**

Documento: [Daqui Lema Daysi Jackeline.docx](#) (D65019567)

Presentado: 2020-03-07 18:26 (-05:00)

Presentado por: Jairo Veintimilla Andrade (jairo.veintimillaa@ug.edu.ec)

Recibido: jairo.veintimillaa.ug@analysis.orkund.com

Mensaje: [Mostrar el mensaje completo](#)

1% de estas 34 páginas, se componen de texto presente en 1 fuentes.

Lista de fuentes Bloques	
⊞ Categoría	Enlace/nombre de archivo
⊞	Tesis Gema Valencia y Cristhian Rodriguez.docx
⊞ Fuentes alternativas	
⊞ Fuentes no usadas	



Firmado electrónicamente por:  
**JAIRO GEOVANNY  
VEINTIMILLA  
ANDRADE**

**ING. JAIRO VEINTIMILLA ANDRADE, MG.**  
**C.C. 0922668025**  
**FECHA: 04 DE MARZO DE 2020**



## ANEXO VI. - CERTIFICADO DEL DOCENTE-TUTOR DEL TRABAJO DE TITULACIÓN

**FACULTAD DE INGENIERÍA INDUSTRIAL  
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Guayaquil, 3 de marzo de 2020.

Sr (a).

**Ing. Annabelle Lizarzaburu Mora, MG.**

Director (a) de Carrera Ingeniería en Teleinformática / Telemática

**FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE  
GUAYAQUIL**

Ciudad. -

De mis consideraciones:

Envío a Ud. el Informe correspondiente a la tutoría realizada al Trabajo de Titulación **EVALUACIÓN DE LA SEGURIDAD TECNOLÓGICA DE LA INFORMACIÓN DE LA CARRERA DE INGENIERÍA EN TELEMÁTICA DE LA UNIVERSIDAD DE GUAYAQUIL** del (los) estudiante **DAQUI LEMA DAYSI JACKELINE**, indicando que ha(n) cumplido con todos los parámetros establecidos en la normativa vigente:

- El trabajo es el resultado de una investigación.
- El estudiante demuestra conocimiento profesional integral.
- El trabajo presenta una propuesta en el área de conocimiento.
- El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se adjunta el certificado de porcentaje de similitud y la valoración del trabajo de titulación con la respectiva calificación.

Dando por concluida esta tutoría de trabajo de titulación, **CERTIFICO**, para los fines pertinentes, que el (los) estudiante (s) está (n) apto (s) para continuar con el proceso de revisión final.

Atentamente,



Firmado electrónicamente por:  
**JAIRO GEOVANNY  
VEINTIMILLA  
ANDRADE**

**Ing. Jairo Veintimilla Andrade, MG**  
**C.C. 0922668025**

**FECHA: 3 DE MARZO DE 2020**



**ANEXO VIII.- INFORME DEL DOCENTE REVISOR  
FACULTAD DE INGENIERÍA INDUSTRIAL  
CARRERA INGENIERÍA EN TELEINFORMÁTICA**



Guayaquil, 24 de abril del 2020

Sr (a).

**Ing. Annabelle Lizarzaburu Mora, MG.**

Director (a) de Carrera Ingeniería en Teleinformática / Telemática

**FACULTAD DE INGENIERÍA INDUSTRIAL DE LA UNIVERSIDAD DE  
GUAYAQUIL**

Ciudad. -

De mis consideraciones:

Envío a Ud. el informe correspondiente a la REVISIÓN FINAL del Trabajo de Titulación **EVALUACIÓN DE LA SEGURIDAD TECNOLÓGICA DE LA INFORMACIÓN DE LA CARRERA DE INGENIERÍA EN TELEMÁTICA DE LA UNIVERSIDAD DE GUAYAQUIL** de la estudiante **DAQUI LEMA DAYSI JACKELINE**. Las gestiones realizadas me permiten indicar que el trabajo fue revisado considerando todos los parámetros establecidos en las normativas vigentes, en el cumplimiento de los siguientes aspectos:

Cumplimiento de requisitos de forma:

El título tiene un máximo de 20 palabras.

La memoria escrita se ajusta a la estructura establecida.

El documento se ajusta a las normas de escritura científica seleccionadas por la Facultad.

La investigación es pertinente con la línea y sublíneas de investigación de la carrera.

Los soportes teóricos son de máximo 12 años.

La propuesta presentada es pertinente.

Cumplimiento con el Reglamento de Régimen Académico:

El trabajo es el resultado de una investigación.

El estudiante demuestra conocimiento profesional integral.

El trabajo presenta una propuesta en el área de conocimiento.

El nivel de argumentación es coherente con el campo de conocimiento.

Adicionalmente, se indica que fue revisado, el certificado de porcentaje de similitud, la valoración del tutor, así como de las páginas preliminares solicitadas, lo cual indica el que el trabajo de investigación cumple con los requisitos exigidos.

Una vez concluida esta revisión, considero que el estudiante está apto para continuar el proceso de titulación. Particular que comunicamos a usted para los fines pertinentes.

Atentamente,



Firmado electrónicamente por:  
**NEISER STALIN  
ORTIZ MOSQUERA**

**ING. NEISER ORTIZ M., Mg**

**C.C: 0919522243**

**FECHA: 24/04/2020**

**Declaración de autoría**

“La responsabilidad del contenido de este Trabajo de Titulación, me corresponde exclusivamente; y el patrimonio Intelectual del mismo a la Facultad de Ingeniería Industrial de la Universidad de Guayaquil”

**Daqui Lema Daysi Jackeline**  
**C.C. 0604258053**



### **Dedicatoria**

Agradezco a Dios por un día más de vida y por darme la fortaleza para salir adelante y poner a cada una de las personas maravillosas en mi vida, también dedico a mi mami por darme la vida y el apoyo para llegar hasta aquí ahora que ya es un ángel solo le pido que cada día me cuide y vele cada uno de mis sueños a mis abuelitos por el apoyo incondicional que me han dado si ellos no sería nada en la vida y también agradecerles a cada uno de mis tíos y primos por siempre apoyarme cuando más les necesitaba para no darme por vencida.

### **Agradecimiento**

Dedico a mi madre por cada enseñanza, esfuerzo que ha hecho para que yo sea profesional ahora eres un ángel y este era tu mayor sueño verme toda una Ingeniera ahora solo puedo dedicarte esto a ti, aunque no estés a mi lado.

A mis abuelitos porque ellos han sido como unos padres que han estado al pie del cañón alentándome para levantarme en cada caída y darme la fortaleza cuando más les necesitaba por ser fuertes como yo lo soy.

A mis tíos primos y mi novio porque han influido en mí.

## Índice General

N°	Descripción	Pág.
	Introducción	1

### Capítulo I

#### El problema

N°	Descripción	Pág.
1.1.	Planteamiento del Problema	3
1.2.	Formulación del Problema	4
1.3.	Sistematización del Problema	5
1.4.	Objetivos de investigación	6
1.4.1.	Objetivo General	6
1.4.2.	Objetivos Específicos	6
1.5.	Justificación	7
1.6.	Delimitación del Problema	7
1.6.1.	Delimitación geográfica	7
1.6.2.	Delimitación temporal	7
1.6.3.	Delimitación del conocimiento	8
1.7.	Objeto de estudio	8
1.8.	Alcance	8

### Capítulo II

#### Marco Teórico

N°	Descripción	Pág.
2.1.	Antecedentes de la Investigación	9
2.1.1.	Reseña histórica	12
2.2.	Fundamentación Teórica	12
2.2.1.	Importancia de la Seguridad de la Información	12
2.2.2.	¿Qué es la seguridad de la información?	13
2.2.3.	Seguridad Informática	13

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
2.2.4.	Análisis de Riesgo	14
2.2.5.	Fallos de Seguridad	15
2.2.5.1.	Antivirus o Firewall	15
2.5.2.	¿Quiénes están interesados en la información de la empresa?	15
2.2.5.3.	Wifi	16
2.2.5.4.	Copias de Seguridad	16
2.2.6.	Normas de Seguridad	16
2.2.6.1.	HIPPA	16
2.2.6.1.1.	¿A quién aplica la ley HIPPA?	17
2.2.6.2.	SOX	17
2.2.6.3.	PCI/DSS	18
2.2.6.4.	COBIT	18
2.2.7.	Tipos de Vulnerabilidades	18
2.2.7.1.	Vulnerabilidades de desbordamiento de Buffer.	19
2.2.7.2.	Vulnerabilidades de condición de carrera (race condition).	20
2.2.7.3.	Vulnerabilidades de error de formato de cadena (format string bugs).	20
2.2.7.4.	Vulnerabilidades de Inyección SQL.	20
2.2.7.5.	Vulnerabilidades de Cross Site Scripting (XSS).	20
2.2.7.6.	Vulnerabilidades de denegación del servicio.	21
2.2.7.7.	Vulnerabilidad de ventanas engañosas	21
2.2.8.	Vulnerabilidades Informáticas en Unidades Educativas	21
2.2.9.	Norma ISO/IEC 27001	24
2.2.9.1.	Cómo funciona la ISO 27001	25
2.2.9.2.	Beneficios de la Norma ISO 27001	26
2.2.9.3.	Estructura de la Norma ISO 27001	26

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
2.2.9.4.	Actualización de los controles de la ISO 27001	27
2.2.10.	Dominios de Seguridad de la Norma ISO 27001	28
2.2.11	Actividades más relevantes de la Norma ISO 27001	28
2.2.12.	Gestión de Riesgo de la Empresa con la norma ISO 27001	29
2.2.13.	Enfoque de la Norma ISO 27001	29
2.2.13.1.	Planear	30
2.2.13.2.	Hacer	30
2.2.13.3.	Verificar	30
2.2.13.4.	Actuar	31
2.2.14.	Sistema de Gestión de seguridad de la Información (SGSI)	31
2.2.14.1.	Delitos Informático o Ciberdelitos	32
2.2.14.2.	Delitos Informáticos	32
2.2.14.3.	Delitos Computacionales	32
2.2.14.4.	Delitos Electrónicos	32
2.2.14.5.	Hacking/Hackers	33
2.2.14.6.	Cracking/Crackers	33
2.2.15.	Virus Informático	33
2.2.15.1.	Principales Vías de Infección	33
2.2.16.	Spam	33
2.2.17.	Partes interesadas en el uso de la norma ISO 27001	34
2.3.	Marco Conceptual	34
2.4.	Marco Legal	35

### **Capítulo III**

#### **Metodología**

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
3.1.	Descripción de Proceso Metodológico	36
3.2.	Tipos de Investigación	37

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
3.2.1.	Investigación Bibliográfica	37
3.2.2.	Investigación Descriptiva	37
3.3.	Metodología de Investigación	38
3.3.1.	Investigación de Campo	38
3.3.2.	Investigación Documental	38
3.3.3	Investigación Descriptiva	38
3.4.	Métodos de Investigación	39
3.4.1.	Metodología Cuantitativa	39
3.4.2.	Metodología Cualitativa	39
3.5.	Población y Muestra	39
3.5.1.	Población	39
3.5.2.	Muestra	39
3.6.	Estructura Organizacional de la Universidad de Guayaquil de la Carrera de Ingeniería Telemática	42
3.7.	Cronograma de Auditoria	43
3.8.	Programa de Auditoria	44
3.9.	Plan de Auditoria	46
3.10.	Recolección de Información	53
3.10.1.	Entrevista	54

### **Capítulo III**

#### **Propuesta**

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
4.1.	Modelo PDCA	58
4.2.	Área responsable de la ejecución de controles correctivos y preventivos	58
4.3.	Planificación de entrevista	58
4.4.	Infraestructura tecnológica y física.	59

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
4.5.	Fase IV: Análisis de situación actual del departamento de cómputo de la Universidad de la Carrera de Ingeniería en Telemática.	59
4.5.1.	Análisis de riesgo y diagnóstico de la seguridad de la información de acuerdo al inventario de activos.	59
4.5.2.	Análisis de Vulnerabilidades de acuerdo de inventarios de activos de la Carrera de Ingeniería Telemática.	61
4.5.3.	Evaluación y Determinación de Vulnerabilidades, Amenazas y Riesgos.	64
4.6.	Fase V: Propuesta en la auditoría interna	65
4.6.1.	Seguridad de Respaldo de Información	65
4.7.	Conclusiones	67
4.8.	Recomendaciones	68
	<b>Anexos</b>	69
	<b>Bibliografías</b>	70

## Índice de tablas

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
1	Áreas que debe cubrir la seguridad de Información	8
2	Clasificación de tipo de Vulnerabilidad	19
3	Posibles amenazas, vulnerabilidades y consecuencias de una institución	22
4	Estructura de la Norma ISO 27001	40
5	Cronograma de actividades	43
6	Programa de Auditoria Realizado en la Universidad de Guayaquil en la Carrera de Ingeniería Telemática.	44
7	Plan de Auditoría, Evaluación de Seguridad del Sistema SIUG	46
8	Plan de Auditoría, Evaluación de respaldo de la información	48
9	Plan de Auditoría, Evaluación de la Seguridad al ingresar un estudiante al sistema	49
10	Plan de Auditoría, Evaluación del manejo de medios	50
11	Plan de Auditoría, Evaluación de la Seguridad física	51
12	Plan de Auditoría, Evaluación de Creencias Actualizadas	52
13	Inventario de Activos	53
14	Planificación de entrevista	59
15	Dimensión o criterios de evaluación Seguridad de Información	60
16	Vulnerabilidades obtenidas de la entrevista realizada en el centro de cómputo en la Universidad de Guayaquil de la Carrera en Telemática	61
17	Evaluación de efectividad de la Carrera de Ingeniería Industrial de acuerdo con la ISO 27001	63
18	Hallazgos de la Auditoría interna realizada	64



## Índice de figuras

<b>Nº</b>	<b>Descripción</b>	<b>Pág.</b>
1	División de la Seguridad de la Información	13
2	Protección de Seguridad Informática	14
3	Mayores Amenazas cibernéticas para la Compañías	15
4	Evaluación de COBIT	18
5	Encuesta de empresas Certificadas en Normas ISO 27001	24
6	Estructura de ISO 27001	25
7	Actualización de la estructura de la Norma ISO 27001	26
8	Actualización de los controles de la Normas ISO 27001	27
9	Gestión de Riesgos ISO 27001	29
10	Ciclo de Deming	29
11	Paso para proteger la información	31
12	Los principales interesados de la organización en aplicar la Norma ISO 27001	34
13	Análisis de riesgo de Seguridad de la información	37
14	Imágenes de la Facultad de Ingeniería Industrial donde encuentra la carrera de Ingeniería Telemática.	59
15	Valorización de internos de madurez CRM	63



## ANEXO XIII.- RESUMEN DEL TRABAJO DE TITULACIÓN (ESPAÑOL)



### FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA

---

## “EVALUACIÓN DE LA SEGURIDAD TECNOLÓGICA DE LA INFORMACIÓN DE LA CARRERA DE INGENIERÍA EN TELEMÁTICA DE LA UNIVERSIDAD DE GUAYAQUIL”

**Autora:** Daqui Lema Daysi Jackeline

**Tutor:** Ing. Jairo Geovanny Veintimilla Andrade

### Resumen

Mediante el siguiente estudio se realizó un inventario de activos que permite reconocer las amenazas y vulnerabilidades que presenta el departamento de cómputo de la Carrera de Ingeniería Telemática como: hardware, software, información de redes, seguridad física, eléctrica y seguridad de la información, a través del análisis de la Norma ISO 27001, es muy importante tener en cuenta las políticas de seguridad que deben ser fortalecidas y que los usuarios se comprometan a cumplir con las mismas al realizar sus labores diarias; después de analizar todas las vulnerabilidades se procede a la aplicación de objetivos de control y controles de referencia o también conocido como Anexo A del SGSI; la manera en la que se efectúa este estudio es mediante la observación, análisis y entrevista que ayuda a obtener resultados reales de la auditoría realizada a la organización; además de realizar una investigación descriptiva, documental y bibliográfica. El análisis tiene como objetivo principal determinar resultados propicios que ayude a realizar este proyecto, utilizando herramientas que ayuden a mejorar la seguridad de la organización.

**Palabras Clave:** Seguridad, Información, Norma, Política, Usuario, Amenazas.



## ANEXO XIV.- RESUMEN DEL TRABAJO DE TITULACIÓN (INGLÉS)



### FACULTAD DE INGENIERÍA INDUSTRIAL CARRERA INGENIERÍA EN TELEINFORMÁTICA

---

#### **“EVALUATION OF THE TECHNOLOGICAL SECURITY OF THE INFORMATION OF THE CAREER OF ENGINEERING IN TELEMATICS OF THE UNIVERSITY OF GUAYAQUIL”**

**Autora:** Daqui Lema Daysi Jackeline

**Tutor:** Ing. Jairo Geovanny Veintimilla Andrade

#### **Abstract**

Through the following study, an inventory of assets was carried out to recognize the threats and vulnerabilities presented by the computer department of the Telematic Engineering Degree, such as: hardware, software, network information, physical, electrical and information security, to Through the analysis of the ISO 27001 Standard, it is very important to take into account the security policies that must be strengthened and that the users commit to comply with them when carrying out their daily tasks; after analyzing all the vulnerabilities, we proceed to the application of control objectives and reference controls or also known as Annex A of the ISMS; the way in which this study is carried out is through observation, analysis and interview that helps to obtain real results of the audit carried out on the organization; in addition to carrying out descriptive, documentary and bibliographic research. The main objective of the analysis is to determine favorable results to help carry out this project, using tools that help improve the security of the organization.

**Keywords:** Security, Information, Norm, Policy, User, Threat.

## **Introducción**

Hoy en día el uso del internet es muy importante ya que permite acceder al sistema para obtener información que sea importante, por esa razón es necesario resguardar y proteger la información, para mantener la confidencialidad, la disponibilidad e integridad de datos, el aumento de vulnerabilidades y el amplio espectro de amenazas cibernéticas han dado mucho de qué hablar en los últimos años por el robo de información confidencial ya sea de empresas, instituciones etc. Es fundamental comprender que la información siempre necesita ser protegida y controlada al momento que un usuario ingrese al sistema.

Es importante saber que recursos deben de ser protegidos para de esa manera evitar el robo de información y el alto espectro de amenazas; el campo de la seguridad de la información ha evolucionado drásticamente a partir de la Segunda Guerra Mundial, convirtiéndose en una carrera acreditada a nivel mundial, la auditoria en informática ayuda mucho a las empresas para así conocer las vulnerabilidades y ayudar a proteger la información. (Basaldua, 2016).

Generalmente la informática consiste en garantizar la protección de datos, el material y los recursos de software que permiten almacenar la información que son importantes para las compañías o instituciones, toda esta información debe ser protegida por los administradores y jefes del departamento de TI para de esta manera evitar el fraude informático; no se puede negar que hoy en día en hacking es muy diferente existen diferentes mecanismos de ataque y diferentes técnica para el robo de información, los intrusos analizan las debilidades de la empresa para empezar atacar una vez que el hacker conozca las vulnerabilidad accederá a robar la información más importante. (Villagómez., 2017).

Entendemos que el acceso no autorizado al sistema se constituye en un problema de seguridad grave ya que esa persona o software puede extraer información valiosa de nuestra base de datos y posteriormente perjudicar la organización de formas diferentes. (Seguridad, 2016). La seguridad informática está formado por tecnologías de la información, sustentadas sobre una infraestructura tecnológica con amplio grado de integración de redes, comunicaciones y sistemas de información de punta, para maximizar a través de su soporte logístico el control interno, la contabilidad, y consecuentemente sus resultados, demanda transformaciones en la práctica de la disciplina orientada a ejercer un control superior mediante la auditoria y en especial en la auditoría interna. (Basaldua, 2016)

La auditoría tiene como objetivo general analizar el grado de efectividad de las tecnologías de información dado a que evalúa el grado de seguridad de la información en

todas las dimensiones posibles para garantizar su grado de eficiencia, eficacia, confiabilidad, integridad para tomar decisiones; Su ámbito de acción se centra, en revisar y evaluar: los procesos de planificación; inversión en tecnología; organización; los controles generales y de aplicación en proyectos de automatización de procesos críticos; el soporte de las aplicaciones; aprovechamiento de las tecnologías; sus controles específicos, los riesgos inherentes a la tecnología, como la seguridad de sus recursos, redes, aplicaciones, comunicaciones, instalaciones y otras (Basaldua, 2016).

Según (Villagómez., 2017) “la seguridad informática está conformada por: Integridad, Confidencialidad, Disponibilidad y Autenticación, que asegura que solo los individuos autorizados tengan acceso a los recursos”.

Las amenazas del sistema que se van a evaluar para una mayor seguridad TI pueden proceder del personal encargado, externo, daños en los equipos o caída de enlaces. Un análisis de las vulnerabilidades ayudaría a identificar la ausencia de medidas para reducir los riesgos. Entre las diferentes vulnerabilidades a evaluar se encontrarían, por ejemplo, las de software que aluden a errores de sistemas operativos, aplicaciones o rutinas de acceso no autorizado. (Macías, 2017).

## Capítulo I

### El Problema

#### 1.1. Planteamiento del Problema.

La seguridad informática es un conjunto de medidas preventivas y reactivas que deben resguardar la información y proteger por el bien de las Instituciones, es muy importante mantener la privacidad para de esta manera evitar el acceso indebido a información confidencial que poseen las organizaciones, cada área debe conocer la seguridad que tiene cada departamento sus objetivos y diferentes actividades que se realicen.

Se debe tener en cuenta que la seguridad informática se ha convertido en una de las principales preocupaciones de la empresa ya que es la encargada de crear técnicas de protección para evitar el robo de información y reducir las vulnerabilidades. Por otro lado la seguridad de la información es una disciplina que ayuda a reconocer los riesgos, las amenazas a la que está expuesta la información, análisis de escenarios, buenas prácticas y esquemas normativos que nos asegura el nivel de protección del almacenamiento de información, transmisión y recuperación de información; dicho de otro modo son políticas de uso y medidas que afectan a los datos que se manejan en las organizaciones, los individuos somos conscientes de lo importante que es mantener la privacidad de la información ya que es un bien invaluable para las empresas.

Las unidades educativas a nivel mundial deben contar con un SGSI (Sistema de Gestión de Seguridad de la Información) para evitar el mal uso, abuso de información organizacional que contienen las instituciones para hurtar actividades malintencionadas que tengan algunos individuos como: robar o destruir información importante que provoque la caída del sistema y denegar servicios, la tecnología de ahora evita las vulnerabilidades de cualquier sistema y nos permite proteger con un nivel de seguridad más elevado que el anterior. En Ecuador hoy en día existen diferentes pequeñas y grandes empresas e instituciones que todavía no consiguen la seguridad de la información a nivel empresarial, sin embargo, el gobierno da la iniciativa para que las entidades públicas cumplan con un SGSI que permita proteger la información con las Normas ISO27001 el cual garantiza que toda la información sea estandarizada, regulada y controlada para combatir el acceso a información confidencial de las instituciones. (Praxis, 11 Julio 2019).

**“En todos los sectores esta norma es fundamental e importante en las instituciones educativas, en las organizaciones que se dedican a la educación, hoy en día, emplean cada vez más sistemas informáticos para**

**llevar a cabo sus actividades, por ello es necesario asegurar la protección de su información y de sus sistemas informáticos de cualquier clase de amenaza como accesos no autorizados, virus, etc. Para llevar a cabo dicha protección lo ideal y recomendable es adoptar un sistema de gestión de la seguridad que se base en la norma ISO-27001". (ISOTools, 2019).**

De esta manera se analizará la seguridad de la información mediante el estudio de las Normas ISO27001 donde se conocerá la confiabilidad, integridad, disponibilidad y mejora continua de la información que maneja la Carrera de Ingeniería Telemática para así conocer las falencias y proponer un SGSI que ayude a proteger la información de acuerdo a los controles de la norma para ver si cumple o no; el departamentos de TI de la organización, tienen la obligación de ratificar la buena utilización y supresión de los riesgos a los que diariamente se somete la información.

## **1.2. Formulación de problema**

Analizar el sistema de seguridad tecnológico de la carrera y comprobar si utilizar correctamente las Normas ISO27001.

## **1.3. Sistematización del problema**

Hoy en día en base a la falta de seguridad en las empresas e instituciones, los crackers se aprovechan de este afán para robar información confidencial, así afectando a la seguridad y el acceso no autorizado a los sistemas, por lo cual siempre es necesario realizar un análisis para conocer las amenazas y debilidades teniendo en cuenta las Normas ISO27001 en el cual esta norma permite el aseguramiento, la confidencialidad e integridad de los datos que tiene la empresa siendo así un estándar para analizar los sistemas SGSI permitiendo evaluar los riesgos y las aplicaciones de los controles necesarios para mitigarlos o eliminarlos, donde ayudará a verificar qué tan segura esta la información que posee las organizaciones y en caso de que no se no cumpla con cierta seguridad la empresa deberá realizar auditoria para conocer las vulnerabilidades.

Esto conlleva a que por medio de este proyecto se plantee las siguientes interrogantes:

1. ¿La universidad cuenta con algún sistema de seguridad?
2. ¿La universidad está preparada en caso de que se realice un ataque a la información que posee?
3. ¿Es posible aplicar la ISO27001 en caso de que no esté aplicada?
4. ¿Por qué la ISO27001 es la solución para proteger la información?

5. ¿Hace cuánto tiempo se realizó una auditoria?
6. ¿Qué tan complejo es aplicar esta norma?

#### **1.4. Objetivos de Investigación.**

##### **1.4.1. Objetivo General.**

Analizar la gestión de seguridad de la Carrera de Ingeniería Telemática mediante las Normas ISO/IEC27001.

##### **1.4.2. Objetivos Específicos.**

1. Realizar un estudio bibliográfico sobre los temas concernientes a la seguridad tecnológica de la información.
2. Analizar la situación actual de la carrera referente a la seguridad de sus activos de información.
3. Determinar la situación actual de la institución mediante el análisis de la Norma ISO 27001.

#### **1.5. Justificación.**

Las instituciones educativas no cuentan con un sistema de seguridad implementado solo toman medidas preventivas para evitar ataques, pero eso no quiere decir que garantice la correcta gestión y protección de los datos e información que por lo que otras instituciones o personas mal intencionadas se aprovechan de las vulnerabilidades y acceden a información sin tener autorización, es por esos que las instituciones se acoplan al uso las dichas Normas como la ISO27001 donde ayudara con la confidencialidad e integridad de toda la información que sea manejada internamente cuyo estándar cuenta con pautas para aplicar correctamente un SGSI. (VIU, 2018).

Todos saben que ninguna empresa tiene su información 100% protegida ya que siempre existirá brechas de seguridad y las Instituciones Educativas grandes como esta cuentan con una gran cantidad de información que debe ser confidencial por lo que se considera evaluar y verificar si existe alguna medida de protección que garantice el respaldo de la información. Luego de que se realice el respectivo diagnostico se conocerá la situación de seguridad del departamento de TI y se procederá a la mejora continua.

Esta información se puede encontrar de varias formas ya sea impresa, archivada, escrita, digital, en correos o incluso grabada en conversaciones ya que la tecnología de hoy en día a avanzado, siempre es considerable tener respaldos de cada documento en caso de algún



desastre natural o tiempo severo es ahí donde se debe aplicar la seguridad de ambiente cerrado o seguridad de aire libre.

Se desea definir, lograr mantener y mejorar la seguridad de la información de la Carrera de Ingeniería Telemática a través de la aplicación de la ISO27001 donde ayudará con el correcto manejo de la seguridad de la información, aplicando estándar y anexos de la normativa ISO 27001:

- El campo de aplicación no ayuda aportando a la orientación sobre el uso, finalidad y modo de aplicación para la correcta seguridad.
- El primer requisito para el uso de esta norma es el contexto de la organización en el cual indica sobre el correcto uso de este estándar para alcanzar el SGSI.
- Todos los empleados deben contribuir al establecimiento de la norma para demostrar el liderazgo y compromiso que tiene con la empresa.
- La planificación muestra que tan importante es la determinación de riesgos y oportunidades a la hora de planificar un SGSI.
- El soporte permite ver qué tan bueno es el funcionamiento de la seguridad de la información que posee la empresa.

Es importantes recalcar que quienes forman parte de la Carrera deben tener en cuenta la correcta gestión de seguridad, para mostrar resultados positivos de esta estructura de seguridad del departamento encargado de la información y así evitar el robo de información e implementar controles seguidos de seguridad, evaluar y tratar los riesgos la correcta gestión de la misma producirá una serie de ventajas para la carrera.

## **1.6. Delimitación del Problema.**

La evaluación de las seguridades tecnológicas de la información ayudará a comprobar la protección de los datos que tiene en el Sistema de las Carrera mediante el estudio del estándar ISO27001 o conocido como Sistema de Gestión de Seguridad de la Información donde ayuda a mejorar el resguardo de la base de datos de los estudiantes tomando en cuenta sus falencias.

### **1.6.1. Delimitación geográfica.**

El presente proyecto de investigación se ejecutado en la Carrera de Ingeniería Telemática de la Universidad de Guayaquil.

### **1.6.2. Delimitación Temporal**

La elaboración del análisis de seguridad de la información es de 5 meses a partir de la fecha de aprobación del tema

### **1.6.3. Delimitación del conocimiento**

Es necesario tener conocimiento de las Normas ISO27001 ya que está orientada para evaluar y analizar los riesgos mediante una matriz FODA para disminuir las debilidades del ambiente interno y externo para saber a qué riesgos está expuesta la información.

En este proyecto se analizar la seguridad de la información que posee la Carrera de Ingeniería Telemática mediante la norma ISO 27001, realizando encuestas y entrevistas para conocer las vulnerabilidades y aplicar los anexos de acuerdo a las debilidades que presente la institución.

## **1.7. Objeto de estudio**

Mediante el presente trabajo de investigación se evaluará la seguridad tecnológica de la información basado en la Norma ISO27001.

Para alcanzar los objetivos propuestos:

1. Analizar el contexto de la institución de educación superior e identificar los riesgos y oportunidades.
2. Realizar un estudio bibliográfico para la recopilación de información.
3. Determinar de forma breve y concisa la aplicabilidad del sistema de seguridad informática.
4. Desarrollar un sistema de gestión de seguridad basado en el estándar ISO27001.
5. Establecer pasos a seguir para la seguridad de la información de forma breve y concisa para que se lleve a cabo en un futuro en la organización.

## **1.8. Alcance**

Para cumplir con los objetivos propuestos se debe tener en cuenta el estudio de seguridad que se realizará en la institución y analizar las vulnerabilidades, amenazas que posee la organización y proponer una solución basado en el SGSI (Sistema de Gestión de Seguridad de la Información) aplicado en el departamento de TI teniendo en cuenta las cuatro áreas principales que debe cubrir la seguridad de la información teniendo en cuenta que una vulnerabilidad se debe identificar para saber a qué se están exponiendo, recuperar la información que fue víctima de ataque, responder a los ataques de una forma correcta dependiendo de la parte de la información afectada, detectar al intruso y combatir al virus

encargado en dañar la información, y por último se debe tener un plan de protección para que no vuelva a ocurrir lo mismo :

**Tabla 1.** Áreas que debe cubrir la seguridad de la información.

<b>Confidencialidad</b>	<b>Integridad</b>	<b>Disponibilidad</b>	<b>Autenticación</b>
<ul style="list-style-type: none"> <li>• Sólo los usuarios autorizados pueden acceder a datos e información.</li> </ul>	<ul style="list-style-type: none"> <li>• Sólo el personal autorizado debe ser capaz de modificar los datos cuando sea necesario.</li> </ul>	<ul style="list-style-type: none"> <li>• Los datos deben estar disponibles para los usuarios cuando sea necesario.</li> </ul>	<ul style="list-style-type: none"> <li>• Asegura que solo los individuos autorizados tengan acceso a los recursos</li> </ul>

*Información tomada de la revista universidadviu, Equipo de Expertos, Elaborado por el autor.*

## **Capítulo II**

### **Marco Teórico**

#### **2.1. Antecedentes de la Investigación.**

A final de la década de los 80 los sistemas informáticos no eran tomados en cuenta ya que eran solo de uso militar, pero poco a poco fueron evolucionando hasta convertirse en una de las herramientas más importantes de las empresas, instituciones educativas y hogares. Las organizaciones se han preocupado por mejorar sus sistemas informáticos sin tomar en cuenta las vulnerabilidades que presenta la seguridad tecnológica de la información; las debilidades de los sistemas computacionales o del internet ha sido aprovechado por ciberdelincuentes para crear agujeros que permiten que el atacante acceda a información confidencial ocasionando la caída del sistema. (Molina, 2015).

Con el pasar de los años los errores que presentan ciertos sistemas han ido disminuyendo, pero todavía existen sistemas operativos, programas que están formados por un lenguaje de programación débil en el cual los hackers se aprovechan de las fallas y roban o alteran la información confidencial, desafortunadamente el mal diseño de un software perjudica a la empresa. (Molina, 2015).

En la actualidad es importante implementar medidas de seguridad en las empresas que ayude a la protección de la información de las personas buscando así la confiabilidad, integridad y disponibilidad de los datos para evitar la pérdida o modificación de los mismos. Siempre es importante realizar análisis de seguridad a las organizaciones para conocer las vulnerabilidades, las amenazas y dar una solución que ayude a la continuidad de negocios controlando a través de normas contando con herramientas que ayude a evitar ataques.

Existen diferentes casos de vulnerabilidades en la seguridad informática como los sistemas operativos Microsoft Windows, exploradores de internet son muy populares, pero no cuentan con la seguridad necesaria para evitar el robo de información este tipo de fallos son producidos por los malos diseños del software. La población accede de cualquier modo a las pagina de internet sin tener en cuenta que no todas son seguras, hoy en día estas páginas poseen publicidades llamativas en las cuales piden datos importantes y es ahí donde se produce el robo de información.

Las amenazas, en un entorno dinámico de interconectividad, pueden venir de cualquier parte, sea interna o externa, e íntimamente relacionada con el entorno de las organizaciones. Las vulnerabilidades son una debilidad en la tecnología o en los procesos asociados con la información, y como tal, se consideran características propias de los sistemas o de la infraestructura que lo soporta. (Ciberseguridad, 2019).

Los hackers dirigen su mirada hacia las vulnerabilidades que poseen dichos sistemas para aprovecharse de eso, en el 2017 un virus ataco mediante mail a más de 99 países en el cual los ciberataques afectaron a las infraestructuras informática alcanzando a docenas de hospitales de Reino Unido donde pedían dinero a cambio de liberarles. Este ataque se produjo aprovechándose de la falla de documentos filtrados por NSA (Agencia de Seguridad Nacional). (Gutierrez, 2019).

Más del 90% de las empresas de servicios básicos de Estados Unidos, Inglaterra, Alemania, Australia, México, Japón y otros países fueron víctimas de ataques a información confidencial, en el cual hubo secuestros de expertos encargados de la seguridad. Un ataque realizado en navidad del 2015 demostró que los hackers son perfectamente capaces de paralizar infraestructuras críticas en la red eléctrica de Ucrania, un empleado de la empresa fue víctima de este suceso en el cual abrió un programa malicioso desde un correo electrónico, que instaló el malware y provocó gradualmente el fallo de los sistemas. (Gutierrez, 2019).

En el 2017 WannaCry sufrió uno de más grandes ataques producidos por Ransomware este programa malicioso ingreso al sistema encripto los archivos y luego pidió dinero a cambio de devolver al usuario la posibilidad de ingresar a la información. Más de 230 mil computadoras fueron víctimas del ataque en más de 150 países producido por este software malicioso los siguientes países fueron los más perjudicados “Rusia; Ucrania; India; Gran Bretaña, donde se vio comprometido el servicio nacional de salud; España, por el ataque a Telefónica y Alemania, donde la empresa ferroviaria alemana Deutsche Bahn AG fue el principal blanco.” (Jaimovich, 2018). Estos ciberatacantes lograron recolectar 140.000 dólares en bitcoin por detener la información y pedir rescate de la misma esto no se logró expandir por la ayuda de Marcus Hutchins también conocido como Malware Tech que logro detener que sigan encriptando la información de las empresas y prohibiendo su acceso, lo que hizo fue que mediante un código de programación del malware encontró un botón de apagado, evitando la propagación de WannaCry registrando un nombre de dominio al que, aparentemente el gusano podía cifrar los archivos del equipo que fue infectado. (Jaimovich, 2018).

WannaCry se infectó debido a la vulnerabilidad que presentaba Windows EternalBlue, o MS17-010 este error es producido debido a que el Windows de Microsoft es viejo como Windows XP esta vulnerabilidad ocurre cuando este virus ingresa a un equipo empieza a escanear la red y a buscar otras direcciones IP aleatoriamente es ahí cuando se produce este tipo de ataques infectando a varias máquinas de la empresa, este tipo de errores es producido porque Microsoft poco después lanzo un parche para el sistema EternalBlue antes de lanzar

el programa WannaCry y es ahí donde empezó todas las empresas no habían instalado el parche por eso quedo vulnerable y se produjo el ataque. (Jaimovich, 2018) afirma que. “Según el último reporte de ciberseguridad de Cisco, los ataques de ransomware están creciendo a una tasa anual del 350%. Usualmente los delincuentes piden rescates de entre USD 500 y 200 por usuario”. (Jaimovich, 2018).

Una de las instituciones más grandes Equifax es víctima de robo de información de más de 143 millones de usuarios en Estados Unidos, Canadá y Reino Unido este ataque es uno de los más importantes, superando el de Target en el 2013, este expulso información de más de 41 millones de clientes lo que produjo que la compañía por este ataque tuviera que pagar aproximadamente 18,5 millones de dólares debido a las demandas realizada por los usuarios, aun no se ha podido calcular la gran pérdida económica que sufrió la empresa Equifax. Esta compañía era la responsable de comprobar los riesgos crediticios o determinar si el usuario está apto para realizar algún préstamo, comprar una casa o un coche, es por esa razón que la empresa poseía información muy importante de millones de clientes como nombres completos, direcciones, números telefónicos, historial crediticio, números de tarjetas de crédito, fecha de nacimiento, números de seguridad social y hasta números de licencias de conducir, todo esto había sido robado esta vulnerabilidad ocurrió en la aplicación web de la empresa es ahí donde se detectó al intruso que obtuvo la información, dentro del robo destacan 209.000 números de tarjetas de crédito y más de 182.000 documentos de disputa, pero esto no se compara al ataque que tuvo Yahoo donde más de 1.500 millones de personas fueron afectadas . (Álvarez, 2018).

Yahoo fue víctima de los hackers su débil medida de seguridad hizo que exista un hackeo masivo el cual no fue informado a sus usuarios, desde los últimos yahoo tiene mala fama por sus vulnerabilidades, Jouko Pynnonen fue la persona que descubrió la falla que permitía el acceso del hacker a cualquier cuenta y leer los mails. Lo que el atacante hacia es que enviaba un correo infectado de malware en el cual no era necesario descargar ni hacer clic en ningún lado con tan solo abrir el correo ya era infectado el equipo. (Espinoza, 2016).

Trend Micro es uno de los programas que está rastreando la infección del equipo producido por ransomware o también conocido como Bad Rabbit este software malicioso lo que hace es bloquear toda la información de la empresa y para desbloquear piden dinero a cambio esto se produce a través de unas supuestas actualizaciones falsas de Adobe Flash engañando a los Usuarios para que hagan clic y así infectar con el malware. Bad Rabbit incorpora el uso de Mimikatz que posee un código abierto como Admin, Guest, User, root.

### **2.1.1. Reseña histórica.**

La Universidad de Guayaquil es una institución pública localizada en la ciudad de Guayaquil una de las más antiguas con 148 años tiene varias extensiones en cual nos vamos a enfocar en la facultad de Ingeniería Industrial donde se encuentra la carrera de Ingeniería Telemática, se realizará un análisis de riesgo en la que está expuesta información basado en la norma ISO27001. El objetivo principal es realizar el análisis de vulnerabilidad, conocer la capacidad de solucionar cualquier tipo de problema, riesgos a los que este expuesto la organización, saber si el personal tiene conocimiento de la política de la institución como:

#### **Misión**

“La misión de la Facultad de Ingeniería Industrial es proporcionar a nuestros estudiantes un entorno educativo de excelencia e innovador, para preparar ingenieros emprendedores e integrales que sirvan y se adapten a las necesidades del desarrollo futuro del País de una forma ética, humana y sustentable”. (Gomez, 2019).

#### **Visión**

“La Facultad de ingeniería Industrial será reconocida por su nivel de excelencia en la formación de profesionales en ingeniería, con programas de estudio de la más alta calidad académica, con sólidos conocimientos científicos y con un gran compromiso social que permita contribuir al desarrollo del país en el cambio de la matriz productiva, orientándose a las necesidades de la industria y los mercados”. (Gomez, 2019).

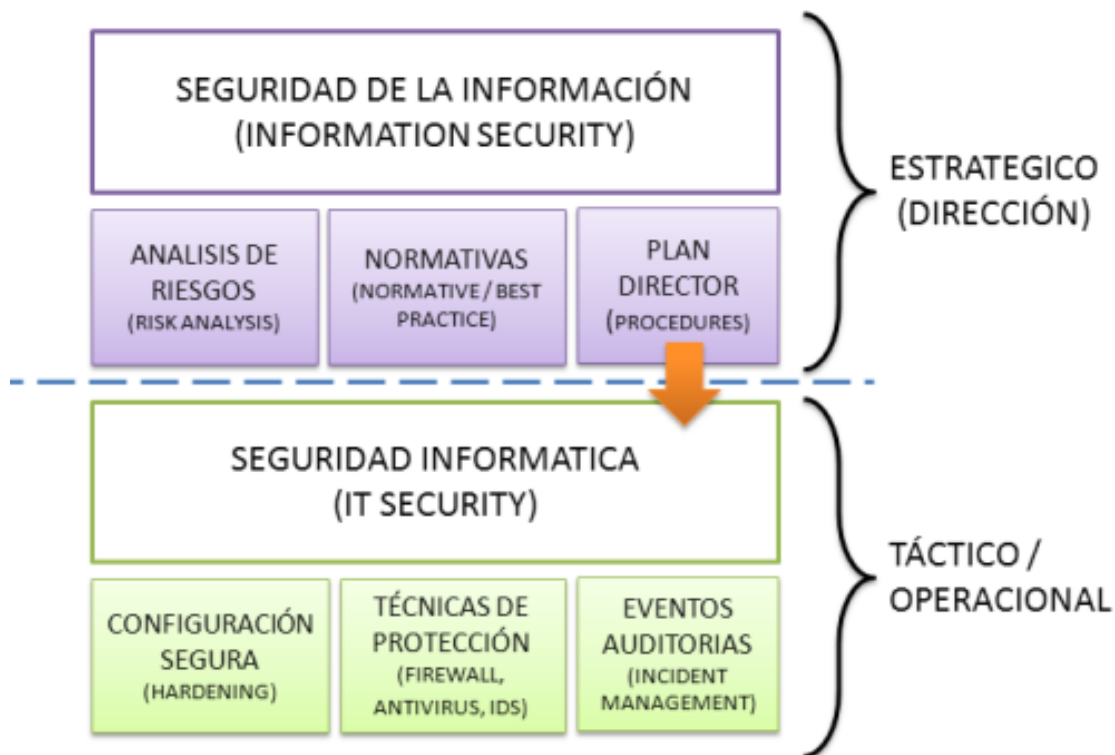
## **2.2. Fundamentación Teórica.**

### **2.2.1. Importancia de la seguridad en la Información.**

Se debe tener en cuenta la seguridad de la información como un conjunto de disciplinas que se encarga de proteger todo tipo de información, ayuda a establecer una serie de fallar parciales y totales. La ciberseguridad se describe también como la distinción táctica y operacional de la seguridad en el cual permite proteger la información que se encuentra en línea y está en riesgo. (Rodríguez, 2016).

Es muy importante la seguridad de la información porque permite asegurar la identificación, valoración y gestión de los activos de información y analizar sus riesgos, mediante el uso de las tecnologías de la información y comunicación (TIC), de esta manera se evita la frecuencia de los ciberatacantes y disminuir las consecuencias graves que provocan en los sistemas, todos estos ataques que se realizan ayuda a reconocer las falencias que presentan programas, sistemas o páginas web en el cual se encuentra información confidencial del usuario para prevenir y evitar que ocurran nuevamente el ingresos de estos a sistemas sin autorización. (Rodríguez, 2016). Permite llevar a cabo una serie de soluciones

técnicas para proteger la información, creando un plan de acción y adecuación para minimizar los riesgos, bajo la normativa o las buenas prácticas con el objetivo de asegurar la confidencialidad, integridad y disponibilidad del manejo de la información. Los empresarios deben tener en cuenta que tipo de información es importante para los ciberdelincuentes. (Rodríguez, 2016).



**Figura 1:** División de la Seguridad de la Información. Información Tomada Academy 27001. Elaborado por el Autor.

### 2.2.2. ¿Qué es la Seguridad en la Información?

La seguridad de la información engloba un conjunto de técnicas y medidas que permite controlar los datos que manejan las instituciones y asegurar que no van a ser mal utilizados, la tecnología de hoy en día ayuda a proteger la información y que solo tengan acceso personas autorizadas sin embargo estas personas no podrán hacer ningún tipo de modificaciones a no ser que sean realizados por personal autorizado. (ISOTools, 2015).

Para garantizar la seguridad de la información se debe realizar un proceso que sea documentado correctamente y tener conocimiento toda la organización, en caso de que la información sea expuesta y obtenga un número alto de amenazas se debe realizar una auditoria en el departamento de TI para someter de diferentes formas al espionaje, fraude y sabotaje al que haya sido sometidos. (ISOTools, 2015).



### 2.2.3. Seguridad Informática.

Son normas diseñadas para garantizar la confidencialidad, integridad, disponibilidad de la infraestructura de un hardware o software de una empresa.



**Figura 2:** Protección de la Seguridad Informática. Información tomada de HSI. Elaborada por el Autor.

### 2.2.4. Análisis de Riesgo.

Es un proceso de identificación, evaluación los riesgos y toma de decisión para reducir los mismos a un nivel aceptable mediante un elemento que forma parte del programa de gestión de continuidad de negocios. El análisis de riesgo tiene como meta proteger la organización y la habilidad de manejar su misión, visión y el alcance de la institución toda la información debe ser considerado en el contexto del negocio e identificar el impacto, las vulnerabilidades, activos informáticos, amenazas y probabilidad de ocurrencia. Para realizar un análisis de riesgo se debe generar un documento “matriz de riesgo”, evaluar los riesgos a los que están expuestos, identificación los activos, identificación de los requisitos legales y de negocios que son relevantes para realizar la identificación de las amenazas y vulnerabilidades, calcular el riesgo, las empresas siempre están expuestas a diferentes tipos de vulnerabilidades y estas pueden ser cualitativas y cuantitativas. (ISO, 2017).

**Método cualitativo:** este es el método más utilizado al momento de tomar decisiones importantes para la organización cuando los niveles de riesgo son muy bajos y no justifica en tiempo para realizar un análisis completo.

**Método cuantitativo:** en este método permite asignar valores a los diferentes riesgos para así calcular en nivel de riesgo de la empresa.



**Figura 3:** Mayores amenazas cibernéticas para las compañías. Información tomada del Sistema de Seguridad Tecnológica de la Información. Elaborada por el Autor.

### 2.2.5. Fallos de Seguridad.

Existen diferentes fallos de seguridad en las empresas, se suele encontrar información muy importante y confidencial de la organización afectada, la mayoría de los fallos de seguridad informáticas PYMES más frecuentes se pueden generar en el sistema informático de una empresa. A continuación, se analizará algunas ideas erróneas y problemas de seguridad que se generan en las empresas y se conocerá unas posibles soluciones.

#### 2.2.5.1. Antivirus o Firewall.

Muchas de las empresas piensan que tener un antivirus o un firewall está bien protegida pero no es suficiente. Las herramientas de seguridad lo que hacen es evitar que los softwares espías, intrusos o malware que tengan idea de cómo acceder al sistema, si los antivirus no

son actualizados entonces existirá agujeros de seguridad y es ahí donde existe robo de información por los intrusos o conocidos como hackers. (FM, 2019).

#### ***2.2.5.2. ¿Quiénes están interesados en la información de la empresa?***

Ya sea una pequeña o grande empresa siempre tiene información confidencial importantes y personas que están interesados en obtener información, el este caso existe varios hackers interesados en organizaciones grandes ya que estas empresas son las que menos invierten en la seguridad informática. Se debe tener en cuenta que cualquier organización está expuesta sufrir un ataque por el cual la empresa debe estar preparada para evitar cualquier vulnerabilidad. (ISOtools, 2018).

#### ***2.2.5.3. Wifi.***

Hoy en día todas las empresas manejan sus negocios por internet, pero ¿Cuántas empresas se han preocupado por comprobar su nivel de seguridad? Ninguna empresa se preocupa por eso cualquier persona puede conectarse a su red y obtener datos es necesario encriptar para tener más seguridad en sus archivos. (ISOtools, 2018).

Para evitar este tipo de incidencias informáticas es necesario capacitar el personal para que tenga cuidado al momento de acceder a cualquier página web y conocer su responsabilidad, lo que puede o no puede hacer dentro de la empresa y del sistema.

#### ***2.2.5.4. Copia de seguridad.***

La copia de seguridad se debe realizar constantemente es la única manera de mantener a salvo la información de la empresa en caso de que la maquina llega a sufrir algún problema desde otra se podrá ingresar al sistema realizar la restauración de la información. (Pores).

### **2.2.6. Normas de Seguridad.**

Son marcos de referencia que establecen un equilibrio socioeconómico entre los diferentes agentes que participan en las transacciones comerciales, en base de cualquier economía del mercado. Son patrones necesarios en brindar confianza al cliente y proveedor.

Ofrece un lenguaje común entre empresas, administración pública, los usuarios y consumidores. El hecho de cumplir con las normas no necesariamente garantiza su seguridad informática. Lo que detiene a un ataque es la configuración técnica de las barreras de seguridad. Ejemplos de normas de seguridad.

- HIPAA
- SOX

- PCI/DSS
- COBIT

#### **2.2.6.1. HIPAA**

Esta ley fue creada el 21 de agosto del año de 1996 para ayudar a la seguridad de la información de los pacientes en hospitales, clínicas y ayude a combatir el despilfarro, fraude y abuso de las mismas. Establece pauta para proteger, la confidencialidad y privacidad de la información del paciente y sus datos médicos, mejorar la portabilidad de la cobertura del seguro médico y simplificar la administración de la atención médica. (Rouse, 2019)

Todos los trabajadores deben tener conocimiento del uso correcto de la norma para evitar huecos en el cual puedan acceder los ciberdelincuentes a la información, las violaciones de HIPAA pueden resultar bastante costosas para las organizaciones de atención médica. (Rouse, 2019)

##### **2.2.6.1.1. ¿A quién les aplica la ley HIPAA?**

En la actualidad los doctores, enfermeras, laboratorios almacenan la información de los pacientes en el correo electrónico, o algún sistema desarrollado especialmente para la unidad por el cual la información es enviada o guardada en estos medios; esta norma garantiza los derechos a la seguridad de la información del paciente adoptando procedimientos que ayuden a la privacidad teniendo por escrito quien accede a la información, como fue utilizada. (Rouse, 2019).

#### **2.2.6.2. SOX**

Es una ley de protección a fraudes financieros impulsada por USA la información es lo más importante para la empresa, esta norma tiene como propósito proteger inversiones evitando informes fraudulentos.

**“Los escándalos de la pérdida de información provocados por las empresas WorldCom, Enron, Parmalat, Royal Dutch Shell; causaron desconfianza a los usuarios ya que su información fue obtenida y divulgada por ciberdelincuentes, viéndose así afectados los inversionistas por su dedil seguridad informática. Este fraude financiero hizo que el gobierno norteamericano retomará el tema de seguridad informática dando origen a la Ley Sarbanes Oxley en Julio de 2002, a través de los reglamentos, estándares y controles más estrictos para evitar el fraude informático,**

**financiero y fortalecer la información aplicando la norma ISO 27001”.**

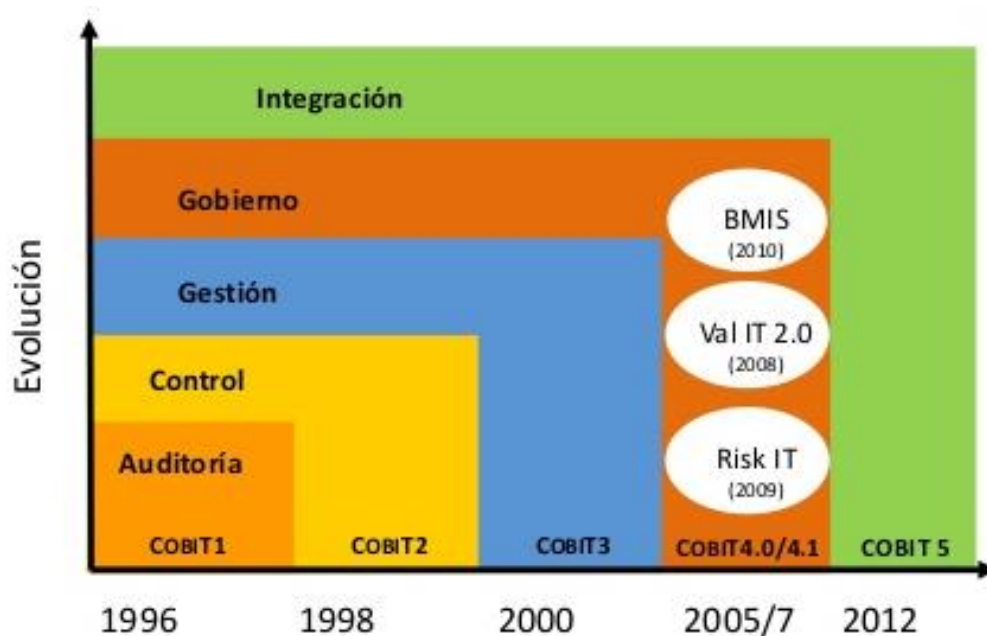
(Auditool, 2014).

El fraude informático ocurrió en las empresas ENRON y WORLDCOM de Estados Unidos en el cual fueron involucrados a empleados y a directivos que tienen acceso a equipos tecnológicos que contiene información confidencial, así facilitando el ingreso de individuos para producirse ataques hace que empresas nacionales como internacionales dejen de crecer, por esa razón el gobierno de EE. UU ha creado esta norma para ayudar a proteger la información. (Auditool, 2014).

#### **2.2.6.3. PCI/DSS**

Ayuda a proteger la información de las tarjetas de crédito almacenando los datos de los titulares son estándares de seguridad diseñada para encriptar los números de las tarjetas de crédito ya que están almacenados en base de datos. Todas las organizaciones que trabajen con tarjetas de crédito deben cumplir con esta norma de protección de datos del usuario, el PCI SSC estableció 12 estándares para guiar los esfuerzos generales para lograr y mantener el cumplimiento. (ISOTools, 2015).

#### **2.2.6.4. COBIT**



**Figura 4:** Evolución de COBIT. Información tomada de Blog COBIT. Elaborada por el Autor.

Esta norma tiene como misión investigar y desarrollar un diseño que ayuda a la comunidad de auditoría financiera a navegar mejor en el crecimiento de los entornos de TI. Existen

varias versiones de cobit en el cual va mejorando, cada versión se implementada con diferentes estándares. Esta norma permite evaluar el departamento informático de una organización. (simplilearn, 2019).

### 2.2.7. Tipos de Vulnerabilidades

Los problemas de vulnerabilidades por ningún caso deben ser tomados a la ligera, ya que todos los sistemas acarrear problemas de seguridad, aunque no utilicemos datos o documentos de gran importancia como en el caso de las empresas siempre es importante proteger la información de cualquier virus. Las vulnerabilidades se clasifican en 4 Tipos:

**Tabla 2.** Clasificación de tipo de Vulnerabilidades.

Clasificación	Definición
<b>Crítica</b>	Este tipo de vulnerabilidad permite la propagación de amenazas sin que sea necesaria la participación del usuario.
<b>Importante</b>	Este tipo de vulnerabilidad es capaz de poner en riesgo la confidencialidad, integridad o disponibilidad de los datos de los usuarios, como así también, la integridad o disponibilidad de los recursos de procesamiento que este disponga.
<b>Moderna</b>	Este es uno de los tipos de vulnerabilidades más sencillas de combatir, ya que el riesgo que presenta se puede disminuir con medidas tales como configuraciones predeterminadas, auditorías y demás.
<b>Baja</b>	Este tipo de vulnerabilidad es realmente muy difícil de aprovechar por un atacante, y su impacto es mínimo, ya que no afecta a una gran masa de usuarios.

*Información tomada de la revista Tecnología informática. (Díaz Montenegro & Castro Zambrano, 2019).  
Elaborado por el autor.*

Este cuadro clasifica el tipo de peligro de cada una de las vulnerabilidades de acuerdo al grado de daño que puede causar. A continuación, detallaremos de manera más clara y en que consiste cada una de estas vulnerabilidades.

#### **2.2.7.1. Vulnerabilidades de desbordamiento de Buffer.**

Se produce por el desbordamiento de memoria asignado a un sistema operativo, este tipo de vulnerabilidad ocurre cuando existe un error en el Software o no pasan adecuadamente los datos que se copian en una memoria reservada llamada (Buffer). “Estos fallos son utilizados por ciberdelincuentes para lograr ejecutar código arbitrario en un equipo, de manera que en muchos casos logran tomar control del equipo víctima o ejecutar un ataque de Denegación de Servicios (**DoS**)”. (Pérez, 2014).

Este tipo de ataques se produce cuando no se tiene instalado correctamente los controladores de seguridad con sus respectivos códigos, para realizar este tipo de desbordamiento de memoria se debe tener los conocimientos adecuados de arquitectura de sistemas operativos, el desbordamiento de memoria se realiza en el procesador en donde se ejecuta una aplicación vulnerable, ya sea de 32 o 64 bits. “Todos estos datos que son ingresados se almacenan en el Buffer si el programa es diseñado correctamente se debería estipular el tamaño máximo para los datos de entrada y garantizar que no superen ese valor”. (Pérez, 2014).

Los ciberdelincuentes pueden crear una dirección de memoria sobrescrita que corresponda a una real para que sea confuso al momento que desee acceder el usuario y así el atacante poder tener acceso a todos los datos. Como hemos visto estas vulnerabilidades se pueden encontrar en cualquier sistema operativo, aplicaciones o protocolos. (Pérez, 2014).

#### **2.2.7.2. Vulnerabilidades de condición de carrera (race condition).**

Este tipo de vulnerabilidades son bastante frecuentes y ocurren cuando varios procesos tienen acceso a la información de la empresa y es utilizado de mal forma este recurso es compartido de forma simultánea. (Blog InternetLab, 2013).

#### **2.2.7.3. Vulnerabilidades de error de formato de cadena (format string bugs).**

Son problemas de seguridad que proviene del programa ya diseñado, la causa principal de la cadena de errores es que ingresan sin la necesidad de la aprobación del usuario. El lenguaje de programación que más vulnerabilidades tiene por la cadena de errores es C++, un ataque utilizando este método definitivamente conduce a la ejecución de código arbitrario y al robo de información y datos del usuario. (Diaz Montenegro & Castro Zambrano, 2019).

#### ***2.2.7.4. Vulnerabilidades de Inyección SQL.***

Es un método en el cual el intruso ingresa un código malicioso para adquirir información o acceder a documentos, datos de base sin tener la aprobación del usuario alterando el funcionamiento normal del programa. (Díaz Montenegro & Castro Zambrano, 2019).

#### ***2.2.7.5. Vulnerabilidades de Cross Site Scripting (XSS).***

Son agujeros de seguridad que se encuentran en aplicaciones web en el cual permite que una tercera persona inyecte algún virus malicioso para infectar a persona que accedan a los lenguajes como VBScript o JavaScript es posible encontrar en equipos que no protejan su navegador web y no se encuentre debidamente protegido contra estos ataques. (Díaz Montenegro & Castro Zambrano, 2019). Estas vulnerabilidades también son llamadas Phishing la cual consiste básicamente en la suplantación de un sitio web verdadero por otro que no lo es.

#### ***2.2.7.6. Vulnerabilidades de denegación del servicio.***

Al momento en el que aparece este tipo de vulnerabilidad básicamente produce un ataque de denegación de servicio “es la pérdida de la conectividad de la red de la víctima del ataque por el excesivo consumo del ancho de banda de la red o de los recursos conectados al sistema informático”. (Díaz Montenegro & Castro Zambrano, 2019).

#### ***2.2.7.7. Vulnerabilidad de ventanas engañosas.***

Estas vulnerabilidades son muy conocidas por los usuarios sin embargo hay veces que no se sabe diferenciar estas ventanas maliciosas que son mostradas como notificaciones o publicidades, también son conocidas como “Windows Spoofing”. (Díaz Montenegro & Castro Zambrano, 2019).

### **2.2.8. Vulnerabilidades Informáticas en Unidades Educativas.**

Hoy en día las redes de datos son cada vez más importantes para las entidades y como organización se debe tener en cuenta las amenazas a las que están expuestas, estas vulnerabilidades por más pequeñas que sean con el tiempo pueden llegar a ocasionar grandes problemas en la Unidad Educativa Zapotal ubicada en el cantón Ventanas cuenta son 600 alumnos donde se maneja sistemas y la plataforma del Ministerio de Educación para el registro de calificación, asistencia, contiene información confidencial de los estudiantes



como: historial académico, información de su disciplina, dirección domiciliar, entre otros. (Aviles, 2017).

La seguridad es uno de los pasos fundamentales para el funcionamiento adecuado de la red de datos en este caso se analizará la seguridad de la red para indagar, estudiar y analizar el funcionamiento de los equipos, así facilitando el estudio de las vulnerabilidades. En esta institución nunca se había realizado una auditoria de seguridad por el que no hay documentos en el que justifique el uso de equipos y software que posee la institución, la investigación se realizó al director de la TIC'S de la Unidad Educativa Zapotal en el cual se observó, que la información que se encontraba en la red de datos era difícil de controlar al momento de ser atacado ya que los equipos de la institución no contaban con la seguridad necesaria y son propensos a ataques ya sea por software o por códigos maliciosos, por lo que lo ciberatacantes tienen como objetivo obtener información y generar pérdidas de las mismas. (Aviles, 2017). Después del estudio realizado se obtuvo los siguiente:

**Tabla 3.** Posibles amenazas, vulnerabilidades y consecuencias de una institución.

<b>Amenazas</b>	<b>Vulnerabilidades</b>	<b>Consecuencias</b>
<b>Fenómenos naturales</b>	No cuenta con programas de contingencia.	Ocasiona daños en los equipos.
<b>Desperfecto eléctrico</b>	Falla en ciertos reguladores de voltaje usado para los equipos de computación. Desorganización de los cables de energía y red.	Los equipos se pueden quemar.
<b>Suciedad</b>	Falta de mantenimiento a equipos.	Los equipos podrían bajar su rendimiento o dejar de funcionar
<b>Sobrecalentamiento de equipos</b>	Déficit de acondicionamiento de aire para los equipos.	
<b>Delito informático</b>	Insuficiente personal especializado en el área de seguridad informática. No existen políticas de seguridad. No utilizan sistemas de detección de intrusos para	La información correría el riesgo de bajar los niveles óptimos de confidencialidad, integridad y disponibilidad.

	identificar los ataques a la seguridad.	
<b>Desperfecto de los equipos</b>	<p>No se encuentran registrados los equipos con mal funcionamiento.</p> <p>No existe un cambio regular de los equipos deteriorados.</p> <p>Insuficiente personal para resolver los inconvenientes ante cualquier desperfecto.</p> <p>Los equipos de red como el cableado, conmutador o switch, conexiones a internet no se encuentran en lugares cerrados y con llave.</p>	<p>Los equipos estarían en riesgo de perder su funcionalidad con eficiencia.</p>
<b>Deficiencia en el servicio de internet</b>	Inestabilidad del servicio de internet.	La conectividad de la red de datos queda inactiva temporalmente.
<b>Desprotección contra virus</b>	Uso de software antivirus desactualizado.	La información podría ser dañada por la infección de virus y afectar su

---

*Información tomada del repositorio de la Universidad Técnica de Babahoyo. (Aviles, 2017). Elaborado por el Autor.*

En el análisis de vulnerabilidad a los servicios web de la intranet en la Universidad Técnica de Babahoyo se encontró con varias debilidades, errores no controlados por ataques, esta institución presenta inconvenientes con la red WAN, como se puede observar este tipo de vulnerabilidades y amenazas ocasiona robo de la información ya que la red no cuenta con una contraseña y eso abre puerta a ciberdelincuentes al acceso a información confidencial, cifrar la información almacenada en los soportes para que en caso de robo no sea legible, realizar copias de seguridad para restaurar la información perdida, uso de programas de chequeo del equipo, SiSoft Sandra 2000, TuneUp, etc. Firewall, autorizando y auditando las conexiones permitidas. (Geovanny Vega Villacís, 2017).

Hoy en día toda institución maneja una base de datos de sus estudiantes en este caso no es la excepción la Institución Educativa Departamental Luis Carlos Galán de Yacopí Cundinamarca utiliza una plataforma llamada SIMAT en el que contiene un registro con toda la información necesaria de los estudiantes, las calificaciones, asistencias pero en los últimos años han presentado dificultades al momento de registrar las notas de los estudiantes la unidad educativa tiene como idea principal proteger los riesgos informáticos a los que están expuestos utilizando la Norma ISO 27000. (Retamoso, 2017).

De acuerdo a la investigación realizada en la Universidad Estatal de Milagro (UNEMI) se analizó los riesgos a los expuesto de acuerdo a la norma 27001, con el objetivo de determinar la capacidad de vulnerabilidad durante una situación de emergencia por riesgos naturales, evaluando la infraestructura y escaso conocimiento de la política de la organización sobre el riesgo de incendios y sus posible consecuencias, además analizar los factores que inciden en la seguridad de las personas (medidas preventivas, medidas de protección). (Granizo, Noboa Romero , & Buchelli Carpio, 2014).

La Unidad Educativa “Luciano Andrade Marín” de Quito está expuesta a sufrir amenazas naturales y de ámbito social, es muy necesario evaluar todo tipos de riesgos y vulnerabilidades, estar capacitados para actuar de manera correcta a cualquier tipo riesgo. Más del 70% de los desastres naturales son producidos por el clima, terremotos, inundaciones, es por eso que se debe tomar conciencia de todo a lo que está expuesto una organización al momento de ocurrir un desastre natural como perdida de información, daños materiales entro otros. (Simbaña, 2018).

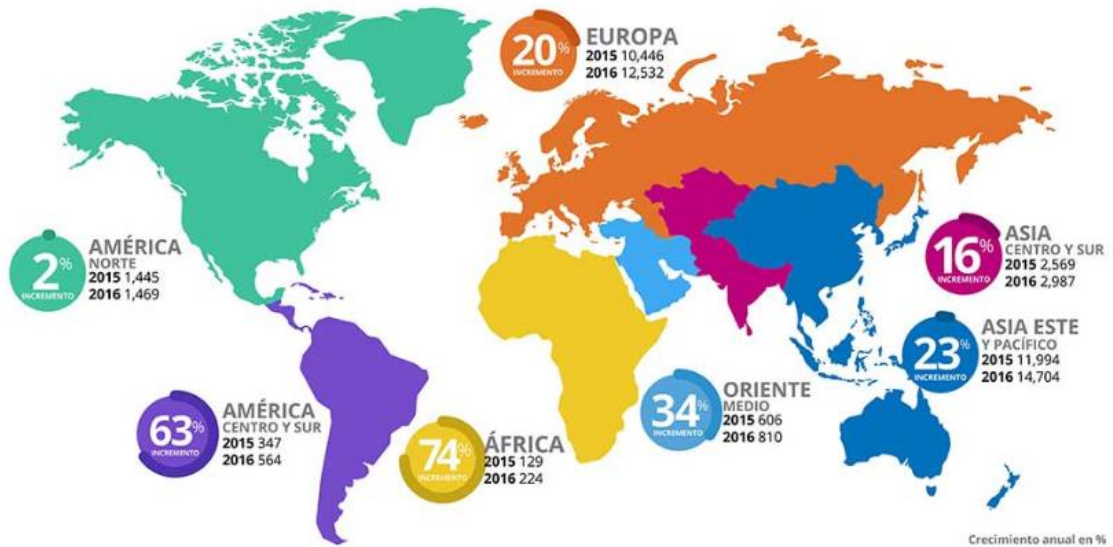
#### **2.2.9. Norma ISO/IEC 27001.**

La ISO 27001 es una norma internacional certificable forma parte de la familia de ISO 27000 ayuda a mantener segura la información de los usuarios y controlar continuamente las brechas de seguridad, tiene la capacidad de responder a cualquier vulnerabilidad, la última revisión de la norma fue en el 2013 y la primera fue en el 2005. (Academy 27001, 2019).

Esta norma puede ser implementada en cualquier tipo de organización ya se pública o privada, grande o pequeña, ya que permite mantener segura la información y corregir las vulnerabilidades que posee, también permite que las empresas sean certificadas con esta norma de seguridad. (Academy 27001, 2019).



## ISO 27001 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN ESTADÍSTICA DE CERTIFICADOS EN 2016



**Figura 5:** Encuestas de empresas certificadas en la Norma ISO 27001. Información tomada de advisera. Elaborado por el autor.

ISO 27001 es una norma muy usada a nivel mundial para proteger la información de la empresa, usuarios, clientes. Como se puede ver en la Figura 4 según la encuesta realizada en cada año existe más empresas certificadas en esta Norma que ayuda a la Seguridad de la Información.

### 2.2.9.1. *Cómo funciona la ISO/IEC 27001.*

Como idea principal de esta norma se centra en proteger información de la empresa, esto hace que la información que se encuentre en el sistema esté respaldada, y estar pendientes de los problemas que podrían afectar en caso de que exista algún tipo de vulnerabilidad, tener el conocimiento necesario en caso de que se produzca algún ataque. La ISO 27001 se basa en la gestión de riesgos de una organización, investigando donde está el riesgo para luego tratarlo sistemáticamente. (Academy 27001, 2019).

Las medidas de seguridad de la información deben estar bajo las políticas de seguridad de la empresa; al implementar medidas de protección técnica en el softwares y hardware la mayoría de las empresas no tendrían problemas de vulnerabilidades, pero el caso es que sus empleados no saben usar correctamente el sistema o no actualizan los antivirus es ahí donde quedan huecos de seguridad y los intrusos se aprovechan de los mismos. (Academy 27001, 2019). La ISO 27001 es importante para la empresa porque contiene ventajas esenciales que toda empresa debe tener para implementar de una forma correcta su seguridad:

1. Cumplir con los requerimientos legales: Cada vez hay más normas, leyes y reglas que se deben cumplir para proteger la información, en este caso la ISO 27001 es la norma más completa que puede ayudar a la empresa.
2. Una de las ventajas más importantes es que al momento de que una empresa obtenga la certificación, los clientes se interesan más por su seguridad.
3. Teniendo la certificación de la norma ISO 27001 ayuda a evitar incidentes de seguridad por lo que se reducirá los costos económicos de la empresa.



**Figura 6:** Estructura de ISO 27001. Información tomada adversera. Elaborado por el Autor.

#### **2.2.9.2. Beneficio de la Norma ISO 27001.**

Ayuda a disminuir los riesgos de seguridad en las empresas evitando y corrigiendo todo tipo de vulnerabilidades, así manteniendo segura la información de los clientes, estableciendo metodologías claras y bien estructuradas para reducir las pérdidas y robos de información brindando así confiabilidad y confianza para tener una mejor organización.

#### **2.2.9.3. Estructura de la Norma ISO 27001**

La estructura de la ISO 27001:2005 fue actualizada a la ISO 27001:2013, pero esta no puede ser cambiada sin cambiar la ISO 27002, ya que estas normas están alineadas por ende si se cambia la una también ocurre cambios en la otra. A continuación, se conoce la estructura.



**Figura 7:** Actualización de la estructura de la norma ISO 27001. Información tomada slideplayer pág.14. Elaborado por el Autor.

1. Objeto y Campo de aplicación: es la orientación de la empresa, hacia donde se proyecta.
2. Referencia de la Normativa: revisión de los documentos más importantes para la norma.
3. Términos y Definiciones: se basa a toda la terminología del estándar.
4. Contexto de la Organización: son indicaciones sobre el conocimiento de la organización y conocer sus necesidades y el alcance.
5. Liderazgo: la persona encargada del liderazgo es el responsable de conocer sus necesidades y elaborar una política de seguridad; realizar capacitación donde se dé a conocer a toda la organización y asignar roles, responsabilidades y autoridades dentro de la misma.
6. Planificación: es importante conocer los riesgos y las oportunidades a la hora de planificar un sistema.
7. Soporte: señalar el buen funcionamiento del sistema de gestión de seguridad, la organización deberá tener respaldado toda la información.
8. Operación: al momento de cumplir con la norma se debe tener en cuenta que cumpla con la norma y sus principales ideas de planificar, implementar y controlar en el proceso de la organización.
9. Evaluación del desempeño: en este paso se debe tener en cuenta el desempeño del sistema mediante una auditoría interna y la revisión por la dirección del SGSI.
10. Mejora: son las obligaciones que tendrá que cumplir una organización para mantener la mejora continua.

#### **2.2.9.4. Actualización de controles de la ISO27001:2005 a ISO 27001:2013.**

Ahora se centra en los cambios de los controles como era de esperar, el número de secciones ha aumentado de 11 secciones que contienen los controles en el viejo estándar a 14 en el nuevo. Número de controles: sorprendentemente, el número de controles ha disminuido de 133 a sólo 111 en el 2005 fueron borrados 21 controles, pero en el 2013 se crearon 14 nuevos controles como:

- A.10 Criptografía.
- A.13 Seguridad de las comunicaciones.
- A.15 Relaciones con los Proveedores.

#### **2.2.10. Dominios de seguridad de la norma ISO 27001.**

Los Dominios Tecnológicos de Seguridad incorporan los activos de la información que van a proteger y cumplir totalmente.

- “Política de seguridad de la información.
- Seguridad organizacional.
- Gestión de activos.
- Seguridad de recursos humanos.
- La seguridad física y del ambiente.
- Gestión de las operaciones y comunicaciones.
- Control de acceso.
- Gestión de incidentes de seguridad de la información.
- Gestión de la continuidad del negocio”. (Coelho, Araújo, & Bezerra, Gestion de la seguridad de la informacion, 2014).

#### **2.2.11. Actividades más relevantes de la ISO 27001.**

- Orientar a la organización.
- Definir el alcance del SGSI
- Crear políticas de seguridad.
- Formar personal competente
- Concientizar al personal de la información que maneja
- Comunicación constata en la organización
- Análisis y evaluación de resultado.
- Implementación del inventario activos.
- Demostrar liderazgo y riesgo.

- Evaluación de riesgo y tratamiento del riesgo.
- Reconocer las amenazas, vulnerabilidades e impactos.
- Conocer los controles para dar tratamiento a los riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Capacitación al personal para dar a conocer las políticas
- Implementas un plan para tratar el riesgo.
- Aplicación de controles, políticas, procedimientos e instrucciones de trabajo.
- Monitorear constantemente la seguridad del sistema.
- Revisar las no conformidades
- Aceptar los riesgos
- Realización de auditorías internas.
- Mejora continua del SGSI.
- Prevenir los riesgos después de corregir.

#### 2.2.12. Gestión de riesgo de la empresa con la norma ISO 27001.

Básicamente la seguridad de la información forma parte de la gestión global de riesgos de una empresa.



**Figura 8:** Gestión de riesgo ISO 27001. Información tomada adversera. Elaborado por el Autor.

#### 2.2.13. Enfoque de la Norma ISO 27001.

Esta norma se enfoca a la seguridad de la información basada en la versión 2013 ayuda a la información para establecer, implementar, operar, monitorear, revisar, mantener y mejorar. (Guzman, 2016).





**Figura 9:** Ciclo de Deming. Información tomada repositorio Espol. Elaborado por el Autor.

#### **2.2.13.1. Planear.**

- Definición de políticas y directrices de la seguridad de la información.
- Definición de la metodología de la evaluación de riesgos.
- Identificación de riesgos.
- Análisis y evaluación de riesgos.
- Tratamiento de riesgos.
- Selección de objetivos de controles y aplicación de los controles del anexo A de la norma.
- Aprobación por parte de la dirección de riesgos y la implementación del SGSI.
- Declaración de aplicabilidad (SOA).

#### **2.2.13.2. Hacer.**

- Implantación del plan de tratamiento de riesgos.
- Implementación de los controles seleccionados en la fase de planificación.
- Definición de un sistema de métricas/indicadores para la medición eficaz de los controles implementados.
- Implementación del sistema de seguridad física.
- Asignación de actividades al personal.
- Implantación de procedimientos y controles preventivos, de detección y correctivos ante los incidentes de seguridad de la información.

#### **2.2.13.3. Verificar.**

- Ejecución de procedimientos de monitoreo.
- Detección de errores en el procesamiento de la información.

- Identificación de brechas e incidentes de seguridad.
- Detección y prevención de eventos e incidentes de seguridad mediante el uso de indicadores. Revisión regular de la efectividad del SGSI en función del cumplimiento de los objetivos. Medición de la efectividad de los controles implementados.
- Revisión regular en intervalos planificados las evaluaciones de riesgo, los riesgos residuales y sus niveles aceptables.
- Realización periódica de auditorías internas del SGSI en lapsos planificados.
- Revisión periódica del SGSI por parte de la dirección para garantizar que el alcance definido y las mejoras del SGSI son los adecuados.
- Actualización de los planes de seguridad en función de los resultados y los nuevos Hallazgos en el monitoreo.
- Registra de acciones y eventos de seguridad para analizar el impacto de estos en el SGSI.

#### **2.2.13.4. Actuar.**

- Implantación de las mejoras identificadas en el SGSI.
- Ejecución de las acciones preventivas en contra de amenazas externas.
- Comunicar cambios en la organización a todos sus empleados
- Verificación de que las mejoras planteadas alcanzarán los objetivos previstos.

#### **2.2.14. Sistema de Gestión de Seguridad de la Informática (SGSI).**

El SGSI o también conocido como ISO27001 ayuda a la protección de información para evitar el acceso, utilización, divulgación y destrucción del sistema sin tener la autorización, la seguridad de la información o seguridad informática garantiza la protección de la información a la que se accede constantemente con la finalidad de: Identificar, Recuperar, Responder, Detectar y Proteger la información de la empresa. (ISOTools, 2015). El gobierno, empresas grandes o pequeñas, instituciones, hospitales tienen una gran cantidad de información importante que debe ser protegida por el bien de la organización, esta información confidencial debe ser encargadas a personas responsables. En caso de realizar una auditora para dar seguimiento a la seguridad y responsabilidad de los gerentes o empleados encargado del departamento de TI, la información debe estar en regla para que en cualquier momento sea revisada y analizada por un auditor anualmente.

Si la información llega a caer en manos de organizaciones de la competencia sin autorización puede existir graves consecuencias como: perder clientes por mala protección

de su información, direcciones, teléfonos, números de cedula, información de sus propiedades e incluso tener perdidas en el negocio o demandas por divulgar la información. Toda empresa debe brindar: confidencialidad, la integridad y la disponibilidad. (ISOTools, 2015).



**Figura 10:** Paso para Proteger la Información. Información tomada del Sistema de Gestión de Seguridad informática. Elaborado por el Autor.

#### **2.2.14.1. Delitos Informáticos o Ciberdelitos.**

Navegar en la web conlleva a una serie de riesgos informáticos o también conocidos como Ciberdelitos, la utilización de Tecnologías de la Información y Comunicación (TIC) son utilizados frecuentemente por ciberdelincuentes para realizar sus actos delictivos y extraer información de las empresas, instituciones u organizaciones.

Los usuarios hoy en día navegar en internet es de mucha responsabilidad ya que estos peligrosos delincuentes Hackers se encuentra navegando en internet buscando cualquier tipo de vulnerabilidades o huecos de seguridad para cometer sus infracciones, se debe tener en cuenta que este tipo de conductas ilícitas son cometidas bajo un anonimato. (Verdezoto, 2018) En 1983 se dieron a conocer los primeros delitos informáticos que se definió como comportamiento no ético o no autorizado, troyano fue el primer virus masivo a partir de ahí Estados Unidos creo una ley específica para la protección de la información, los delitos informáticos son cometidos a través del departamento de TIC. (Verdezoto, 2018).

#### **2.2.14.2. Delitos Informáticos.**

Afectan a la información y datos de la empresa, toda la información de un usuario es protegida jurídicamente por leyes ya que son datos importantes que no pueden ser divulgados. (Verdezoto, 2018).

#### **2.2.14.3. Delitos Computacionales.**

Son delitos producidos por la implementación de tecnología para sacar beneficios de los mismo como el robo, el hurto, la defraudación, la estafa. Por ejemplo: cuando un ciberdelincuente envía un correo que contenga información idéntica de un banco para poder obtener contraseñas, usuarios y realizar una estafa electrónica. (Verdezoto, 2018).

#### **2.1.14.4. Delitos Electrónicos**

Este tipo de delitos tiene que ver mucho con ciberterrorismo donde se utiliza dispositivos electrónicos y pulsaciones electromagnéticas para detonar bomba en un avión, carro, casa, local comercial, etc. (Verdezoto, 2018).

#### **2.2.14.5. Hacking/Hackers.**

Son personas que cometen infracciones como acceder sin autorización a programas y sistemas estos delincuentes conocen su funcionamiento y son silenciosos, buscan indagar a las víctimas con el fin de descifrar y obtener la información necesaria y producir un ataque cibernético. (Verdezoto, 2018).

#### **2.2.14.6. Cracking/Crackers.**

Son delincuentes cibernéticos que ingresan a un programa o sistema con el fin de destruir la información y denegar el ingreso a los usuarios legítimos y causar daños al sistema, estos con conocidos también como piratas informáticos. Cabe recalcar que un Cracker es una versión violenta y utilizan algunas técnicas hacking para ingresar sin consentimiento al sistema. (Verdezoto, 2018).

Una de las principales diferencias entre Hackers y Cracker utilizan programas extraídos de la web mientras que los Hackers crean sus propios programas ya que tienen conocimiento de programación. (Verdezoto, 2018).

#### **2.2.15. Virus Informático.**

Son programa malicioso (Malware) son usado por los ciberatacantes para modificar o eliminar información de las instituciones, alterando el funcionamiento del equipo.

### 2.2.15.1. Principales vías de infección.

- Redes Sociales
- Sitios web
- Redes
- Dispositivos USB, CD, DVD
- Correos no deseados.

### 2.2.16 Partes interesadas en el uso de la norma ISO 27001.

Para definir el alcance de la norma se debe tener en cuenta quienes son los interesados en aplicar el SGSI.



**Figura 11:** Los principales interesados de las organizaciones en aplicar la Norma ISO 27001. Información tomada (Aviles, 2017). Elaborado por el Autor.

### 2.2.17. Spam.

Son mensajes basura enviados por el atacante para que el usuario acceda y el hacker obtenga información.

## 2.3. Marco Conceptual.

“Se analizará la seguridad de la información de la carrera de ingeniería telemática de la Universidad de Guayaquil realizando un estudio bibliográfico sobre la seguridad de la información y analizando cualquier tipo de vulnerabilidades que pese el sistema, siempre teniendo en cuenta los sistemas de gestión normalizados, modelos de excelencia, gestión de riesgos, gestión de estrategia”. (ISOTools, 2019).

“Y conocer la actualización de la norma ISO 27001:2018 ya que se va actualizando la norma con respecto a la seguridad de la información esta nueva versión cuenta con un

vocabulario al igual que la ISO 9000 toda la información se puede encontrar en formato digital ya que es un formato que está más divulgado” (ISOTools, 2019).

Según (ISOTools, 2019) “se da cumplimiento a los requisitos basados en el ciclo PHVA (Planear – Hacer – Verificar – Actuar) para establecer, implementar, mantener y mejorar el Sistema Gestión de la Seguridad en la Información, así como se da cumplimiento de manera complementaria a las buenas prácticas o controles establecidos en la ISO 27001:2013”.

**SGSI:** Sistema de Gestión de Seguridad de la Información.

**Vulnerabilidad:** Incapacidad de proteger una información.

**IEC:** Comisión Electrotécnica Internacional.

**Normas:** Son principios que permite el cumplimiento de las políticas de una organización.

**Riesgo:** Vulnerabilidades que son aprovechadas por delincuentes para sacar beneficio.

**Controles:** “Una práctica, procedimiento o mecanismo que reduce el riesgo” (Romero, SlidePlayer, 2017).

## 2.4. Marco Legal.

En los últimos años a nivel mundial han existido diferentes tipos de ataques cibernéticos, en el que se ha visto afectado la seguridad de la información y sistemas de la empresa causando daños graves que perjudican tanto a empresarios como al gobierno.

En el presente proyecto habla sobre la seguridad informática del instituto público y educativo que se da en caso de robo de información o ingreso sin autorización a sistemas de pequeñas o grandes empresas.

“Según el Art 186 sesión 1 denominado como estafa se aplicará pena máxima de 5 a 7 años personas que realicen fraude mediante tarjetas de crédito y débito ya se por clonación, duplicada, hurto, robo u obtenida sin el consentimiento del propietario” (Barrezueta, 2014), (Ecuador, 2019).

“En el Art 186 sesión 2 mediante el uso de dispositivos electrónicos se realice algún tipo de estafa será sancionado con máximo 7 años privado de la libertad” (Barrezueta, 2014), (Ecuador, 2019).

“El Art 178 toda persona que acceda sin autorización legal intercepte, examine, retenga, grabe, reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y vídeo sin autorización de propietario será sancionado de 1 a 3 años privado de libertad” (Barrezueta, 2014), (Ecuador, 2019).

“Art 190 La persona que ingresen fraudulentamente a un sistema informático o redes electrónicas para facilitar la apropiación de un bien ajeno o que procure la transferencia no

consentida de bienes, valores o derechos y alteren el funcionamiento de la información del propietario, sistemas informáticos serán sancionados de 1 a 3 años” (Barrezueta, 2014), (Ecuador, 2019).

“Art 231 el cracker que altere manipule o modifique el funcionamiento de programa o sistema informático, telemático o mensaje de datos, para realizar cualquier tipo de vulnerabilidades en las empresas será sancionado de 3 a 5 años” (Barrezueta, 2014), (Ecuador, 2019).

“Art.234 Acceso no consentido a un sistema informático, telemático o de telecomunicaciones. - 3 a 5 años” (Barrezueta, 2014), (Ecuador, 2019).

“Art.232 Ataque a la integridad de sistemas informáticos. - 3 a 5 años” (Barrezueta, 2014), (Ecuador, 2019).

“Art.233 Delitos contra la información pública reservada legalmente. - 5 a 7 años” (Barrezueta, 2014), (Ecuador, 2019).

## Capítulo III

### Metodología

#### 3.1. Descripción del Proceso Metodológico

En el presente capítulo se analizará la situación actual del sistema de gestión de seguridad de la información en Carrera de Ingeniería Telemática de la Universidad de Guayaquil, donde muestre a los usuarios que su información esta correctamente protegida ya sea que este almacenada en papel, en alguna base de datos o a través de la red.

Esta norma de seguridad de la información ayuda a identificar cualquier riesgo de seguridad y a reducirlo para brindar confiabilidad a los usuarios, es muy importante que la institución tenga en cuenta los riesgos a los que están expuestos a diario y evitarlos. En caso de que la esta institución no cuente con un sistema de seguridad lo más recomendado es proponer un sistema que ayuda a la protección de la privacidad de la información mediante la Norma ISO 27001 ya que esta norma brinda una mejora continua para el bien de la organización.

Toda organización ya sea pública o privada debe contar con un plan de gestión de riesgos para evitar los ataques cibernéticos o fraudes informáticos, lo primero que se debe hacer es:

- **Establecer el contexto:** Calificando los riesgos y estableciendo si son internos o externos. ( ISOTools, 2017)
- **Identificación del riesgo:** es importante reconocer los riesgos describirlos y obtener la información completa de cada uno, siempre se debe tener en cuenta cualquier evento que pueda alterar, acelerar o reducir cualquier información. ( ISOTools, 2017)
- **Análisis de riesgo:** en este punto debemos analizar los riesgos las amenazas y consecuencias tanto negativas como positivas, el análisis de riesgo siempre tiene la estigmatización de entender el riesgo y el impacto que ocurra en caso de suceder cualquier fraude informático. ( ISOTools, 2017)
- **Evaluación:** es una valoración cuantitativa que ayuda en la toma de decisiones de los encargados de la organización. ( ISOTools, 2017)
- **Tratamiento:** después de haber evaluado y tomado una decisión la organización es importante que realice algún plan que ayude a la empresa en la protección de la información. ( ISOTools, 2017)
- **Comunicación y consulta:** toda la información obtenida al momento de realizar cada uno de los pasos deben ser informados a través de diálogos, foros, debates a los integrantes de la organización. ( ISOTools, 2017)

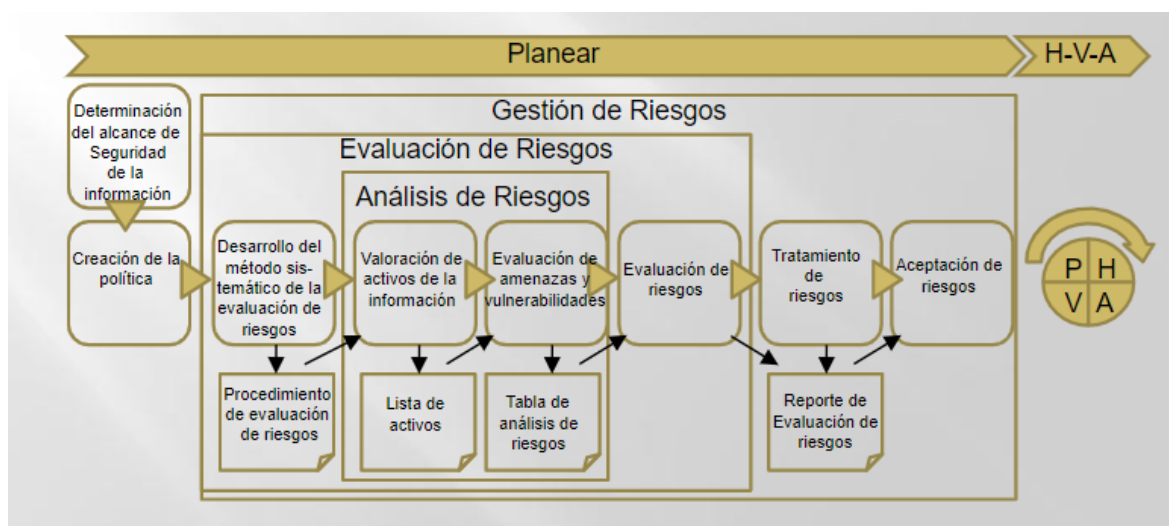


### 3.2. Tipo de investigación

#### 3.2.1. Investigación Bibliográfica.

La metodología que se utilizará para realizar el análisis de la seguridad de la información que posee la carrera de ingeniería telemática será basado en las políticas, misión y visión de la institución. “La ISO 27001 será utilizada como un apoyo bibliográfico ya que contiene requisitos para el establecimiento, mantenimiento y mejora continua del sistema de seguridad de la información que brinda a las organizaciones, este sistema preserva la confidencialidad, integridad y disponibilidad de toda la información que posee la empresa, así brindando confianza a las partes interesadas. Esta norma que se utilizara tiene como objetivo especificar los requisitos para establecer, implementar, mantener y mejorar continuamente”. (ISO/IEC 27001, 2013).

- **“Análisis de Riesgos:** Evaluación de amenazas y vulnerabilidades de los activos de información.” (Romero, SlidePlayer, 2017).
- **“Evaluación de Riesgos:** Todo el proceso de análisis y evaluación de riesgos” (Romero, SlidePlayer, 2017).
- **“Gestión de Riesgos:** Proceso de identificación, control y reducción o eliminación de riesgos de seguridad que pueden afectar los sistemas de información” (Romero, SlidePlayer, 2017).



**Figura 12:** Análisis de riesgo de seguridad de la información. Información tomada Slideplayer pág.9. Elaborado por el Autor.

#### 3.2.2. Investigación Descriptiva.

Esta metodología ayudará a conocer a los usuarios que tan segura esta su información, y a la organización a saber si cumple con cada una de las políticas, propuestas y si es así

declarar conformidad con la privacidad de la información cumpliendo con los requerido en la norma ISO 27001 sin excluir ninguno de los requisitos especificados en los numerales del 4 al 10. (ISO/IEC 27001, 2013). Según (Chacon Mejia, 2008) dice que “siempre es importante utilizar métodos cuantitativos en el cual el primero nos da agilidad en los procesos y facilidad al momento de asignar valores de impacto o riesgo y el segundo nos ayuda a tomar valores con mayor precisión y exactitud”

### **3.3. Metodología de investigación**

#### **3.3.1. Investigación de Campo**

Se visito el departamento de cómputo donde se analizará la seguridad de la información de los usuarios y asegurar que cumple con todas las cláusulas del 4 al a10 y controles.

Este tipo de investigación es obtenida mediante un análisis del lugar donde se desarrolla las reuniones de los directivos, gerentes y supervisores de cada área para hablar sobre la seguridad de la información de cada uno de los usuarios.

#### **3.3.2. Investigación Documental**

Es la recopilación del material de trabajo recopilado ya sea escrito, audiovisual o cualquier otro tipo de investigaciones que sirva como muestra. En este caso la investigación realiza se basa a documentos guardados.

#### **3.3.3. Investigación Descriptiva**

Aquí se detalla cada una de las actividades que se lleva a cabo, conociendo si cumplen con los objetivos de estudio desarrollados por la institución y las políticas para así tener como resultado las falencias que presente la organización, este estudio se aplicó para dar a conocer los diferentes tipos de vulnerabilidades que presente la empresa.

Se realiza la estructura organizacional de la carrera de ingeniería industrial para tener encuentra como está formada la organización y conocer el departamento en el que se va a realizar la auditoria basado en la Norma ISO 27001.

#### **3.3.4. Cronograma de Auditoria**

Una de las herramientas más importantes para realizar un estudio, es crear un cronograma de actividades en el cual ayuda a fijar el tiempo que lleva en elaborar un proyecto, por lo general este tipo de documentos son realizados en la última etapa del proyecto, cuando ya se han definido los objetivos que se desea alcanzar.

### **3.3.5. Plan de auditoria**

El plan de auditoria es realizado para ir detallando cada una de las actividades fijadas en el cronograma y ver si cumple todo lo documentado en el cronograma. El plan de auditoria debe estar suficientemente detallado con cada una de las actividades realizadas para que al momento de ser revisada por un auditor externo entienda las conclusiones que se ha llegado obtener.

## **3.4. Métodos de investigación**

### **3.4.1. Metodología cuantitativa**

Este tipo de metodología nos permite obtener información de datos de manera numérica, revela los resultados empleados mediante encuestas y luego permitir establecer conclusiones de acuerdo a la información adquiridas

### **3.4.2. Metodología cualitativa**

La investigación cualitativa es empleados a través de un encuestador y de un encuestado, en el cual el encuestador ya tiene una serie de preguntar listas para ser interrogadas y de esa manera adquirir la información; las preguntas son respondidas de manera subjetiva acumulando así una serie de información importante.

## **3.5.Población y Muestra**

### **3.5.1. Población**

Mediante esta investigación se dio a conocer los empleados que forman parte de la carrera de ingeniería teleinformática.

- Centro de computo

Cuya población cuenta con 5 Empleados

### **3.5.2. Muestra**

En esta investigación se realizó un muestreo donde se obtuvo lo siguiente:

- Directivos del departamento de cómputo tienen un amplio conocimiento acerca del sistema que se utiliza en la universidad, el cual son encargados de la seguridad de la información que contiene el mismo ayudando así a los estudiantes a mantener seguras sus cuentas y en caso de sufrir un robo de información brindar ayuda a recuperar toda la información.

- Personal encargado de manipular la información para llevar a cabo actividades que estén programadas.

Es factible que con 5 Empleados encargados del departamento de cómputo se pueda lograr la seguridad de la información.

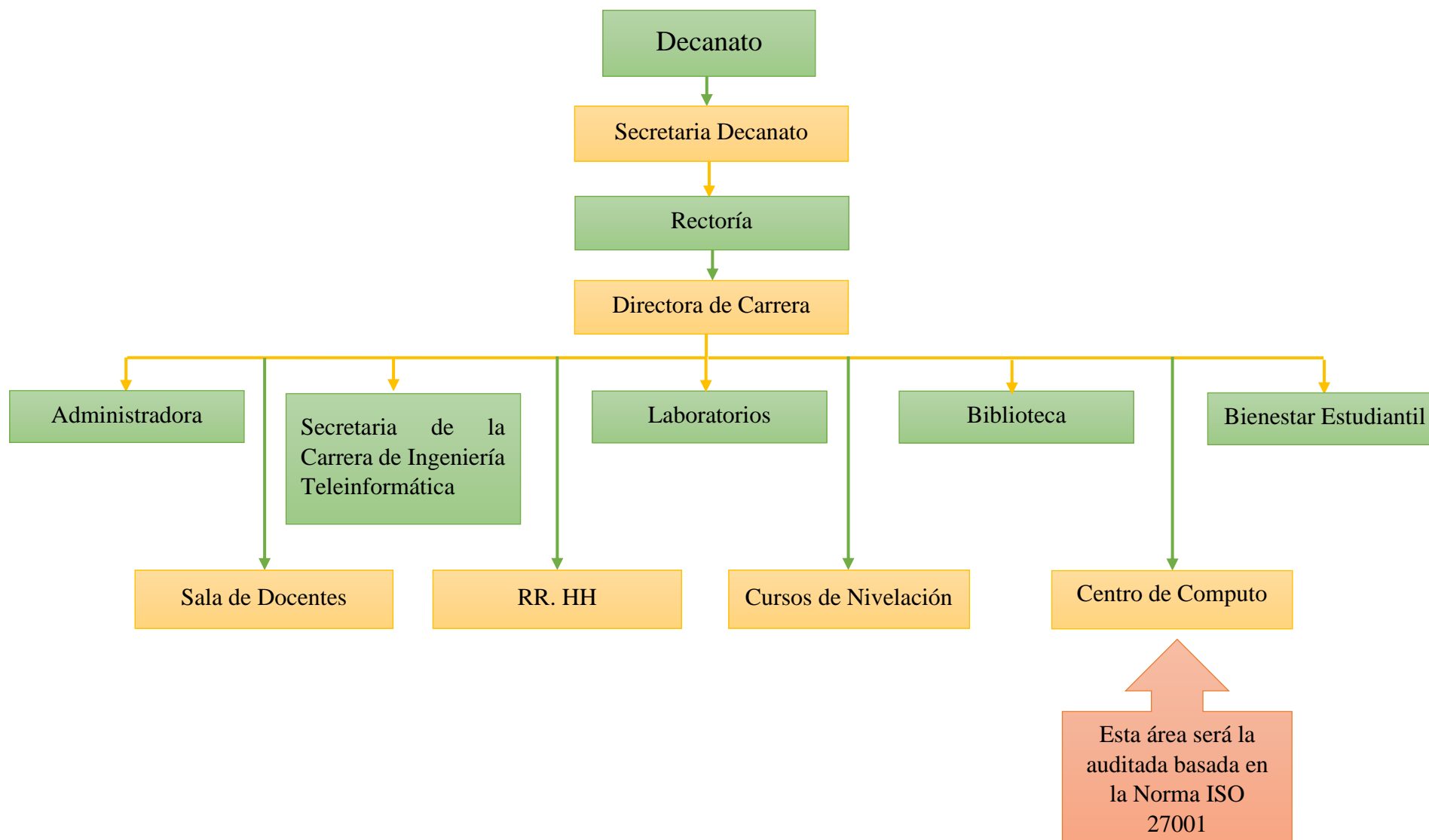
**Tabla 4.** Estructura de la Norma ISO27001.

<b>ESTRUCTURA DE LA NORMA ISO 27001</b>	
<b>4. Contexto de la organización</b>	<p>4.1 “Conocimiento de la organización y de su contexto.</p> <p>4.2 Comprensión de las necesidades y expectativas de las partes interesadas.</p> <p>4.3 Determinar el alcance del SGSI.</p> <p>4.4 Sistema de gestión de seguridad de la información” (SGSI, 2014).</p>
<b>5. Liderazgo</b>	<p>5.1 Liderazgo y compromiso.</p> <p>5.2 Política.</p> <p>5.3 Roles, responsabilidades y autoridades en la organización.</p>
<b>6. Planificación.</b>	<p>6.1 Acciones para tratar riesgos y oportunidades.</p> <p>6.1.1. Generalidades.</p> <p>6.1.2. Valoración de riesgos de la seguridad de la información.</p> <p>6.1.3. Tratamiento de riesgos de la seguridad de la información.</p> <p>6.2 Objetivo de la seguridad de la información y planes para lograrlos.</p>

<b>7. Soporte</b>	7.1 Recursos. 7.2 Competencia. 7.3 Toma de conciencia. 7.4 Comunicación. 7.5 Información documentada. 7.5.1. Generalidades. 7.5.2. Creación y actualización. 7.5.3. Control de la información documentada.
<b>8. Operación</b>	8.1 Planificación de control operacional. 8.2 Valoración de riesgos de la seguridad de la información. 8.3 Tratamiento de riesgo de la seguridad de la información.
<b>9. Evaluación del desempeño</b>	9.1 Seguimiento, medición, análisis y evaluación. 9.2 Auditoría Interna. 9.3 Revisión por la dirección
<b>10. Mejora</b>	10.1 No conformidades y acciones correctivas. 10.2 Mejora continua.

*Información tomada de la norma técnica colombiana NTC- (ISO/IEC 27001, 2013). Elaborado por el Autor.*

### 3.6. Estructura Organizacional de la Universidad de Guayaquil de la carrera de Ingeniería Telemática




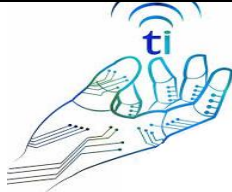
### 3.6. Cronograma de actividades.

**Tabla 5.** Cronograma de actividades.

Actividades	Enero				
	6	13	14	27	29
Constitución del equipo auditor					
Contexto general y situación de la empresa					
Delimitar área auditar					
Realización de plan de auditoria					
Ejecución de auditoria					
Recopilación de información					
Procesamiento de información					
Análisis de la información					
Formulación de informe de auditoria					

### 3.7. Programa de auditoria.

**Tabla 6.** Programa de Auditoria Realizado en la Universidad de Guayaquil en la Carrera de Ingeniería Telemática.



		<b>Programa de Auditoria</b>							
<b>Objetivo de programa</b>		Establecer actividades para llevar a cabo el correcto proceso de auditoría.		<b>Procedimiento</b>		Auditoría Interna		<b>Año</b>	2020
<b>N°</b>	<b>Proceso</b>	<b>Dependencia</b>	<b>Objetivo</b>	<b>Alcance</b>	<b>Inicia</b>	<b>Finaliza</b>	<b>Criterio</b>	<b>Recursos</b>	<b>Equipo Auditor</b>
1	Evaluación de la seguridad del sistema SIUG	Centro de Computo	Verificar la seguridad de la Información de los estudiantes que pertenecen a la institución.	Proteger la información privada de todos los estudiantes de la institución.	13/1/2020	14/1/2020	Norma ISO27001(SGSI)	Norma, Banco de preguntas, Grabadora, Computadora.	Daysi Daqui
2	Evaluar el respaldo de la información	Centro de computo	Verificar que todo este documentado y respaldado.	Proteger información documentada tanto física como digital.	13/1/2020	14/1/2020	Norma ISO27001(SGSI)	Norma, Banco de preguntas, Grabadora, Computadora.	Daysi Daqui



N°	Proceso	Dependencia	Objetivo	Alcance	Inicia	Finaliza	Criterio	Recursos	Equipo Auditor
3	Evaluar la seguridad al ingresar los estudiantes al sistema SIUG.	Centro de computo	Verificar la responsabilidad de los estudiantes al acceder al sistema SIUG	Cambio de contraseña constante	13/1/2020	14/1/2020	Norma ISO27001(SGSI)	Norma, Banco de preguntas, Grabadora, Computadora.	Daysi Daqui
4	Evaluación de manejo de medios	Centro de computo	Verificar que la información no sea divulgada ni manipulada	Confidencialidad	13/1/2020	14/1/2020	Norma ISO27001(SGSI)	Norma, Banco de preguntas, Grabadora, Computadora.	Daysi Daqui
5	Evaluación de seguridad Física	Centro de computo	Verificar la seguridad del control de acceso a oficinas	Implementación del sistema de seguridad física	13/1/2020	14/1/2020	Norma ISO27001(SGSI)	Norma, Banco de preguntas, Grabadora, Computadora.	Daysi Daqui
6	Evaluación de licencias actualizadas	Centro de computo	Verificar el plan de actividades sobre el mantenimiento de licencias	Aplicación anual	13/1/2020	14/1/2020	Norma ISO27001(SGSI)	Norma, Banco de preguntas, Grabadora, Computadora.	Daysi Daqui
7	Investigar si se realiza anualmente auditorias.	Centro de computo	Conocer las vulnerabilidades que presenté y corregirlas	Aplicación de mejora continua	13/1/2020	14/1/2020	Norma ISO27001(SGSI)	Norma, Banco de preguntas, Grabadora, Computadora.	Daysi Daqui


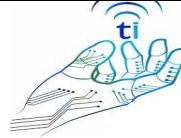
### 3.8. Plan de auditoria.

**Tabla 7.** Plan de Auditoria, Evaluación de la seguridad del sistema SIUG.


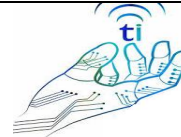
		<b>Plan de Auditoria</b>					
<b>Departamento a Auditar</b>	Área de computo	<b>Área</b>	Centro de computo	<b>Líder del Proceso</b>	Jefe del centro de computo	<b>Equipo Auditor</b>	Daysi Daqui
<b>Objetivo de la Auditoria</b>	Verificar la documentación que posee el departamento de computo	<b>Alcance de la Auditoria</b>	Proteger la información privada de todos los estudiantes de la institución.		<b>Criterio de la Auditoria</b>	Norma ISO 27001 Sistema de Gestión de Seguridad de la Información	
N°	Actividades	Fecha	Hora Inicio	Hora Final	Lugar	Equipo Auditor	Recursos
1	Aviso de realización de auditoria	6/1/2020	13:00	13:25	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
2	Reunión de apertura de Auditoria	13/1/2020	8:00	8:20	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
3	Revisión de las políticas de la Universidad	13/1/2020	8:25	9:00	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.

N°	Actividades	Fecha	Hora Inicio	Hora Final	Lugar	Equipo Auditor	Recursos
4	Revisión de la seguridad de la información colgada en el sistema SIUG.	13/1/2020	9:05	9:30	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
5	Revisión del correcto funcionamiento del sistema	13/1/2020	9:30	10:00	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
6	Verificación de la Seguridad del acceso al sistema	13/1/2020	10:20	11:00	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
8	Análisis del sistema de redes de la Universidad	13/1/2020	11:05	11:20	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
9	Seguridad del servidor	13/1/2020	11:25	12:00	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.


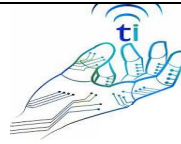
**Tabla 8.** Plan de Auditoria, Evaluación del respaldo de la información.

		<b>Plan de Auditoria</b>					
<b>Proceso a Auditar</b>	Revisión de documentación.	<b>Área</b>	Centro de computo	<b>Líder del Proceso</b>	Jefe del centro de computo	<b>Equipo Auditor</b>	Daysi Daqui
<b>Objetivo de la Auditoria</b>	Verificar que todo este documentado y respaldado.	<b>Alcance de la Auditoria</b>	Proteger información documentada en carpetas.		<b>Criterio de la Auditoria</b>	Norma ISO 27001 Sistema de Gestión de Seguridad de la Información	
<b>N°</b>	<b>Actividades</b>	<b>Fecha</b>	<b>Hora Inicio</b>	<b>Hora Final</b>	<b>Lugar</b>	<b>Equipo Auditor</b>	<b>Recursos</b>
1	Verificación de información documentada física.	13/1/2020	13:00	15:00	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
2	Verificación del respaldado de información.	13/1/2020	15:05	15:25	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
3	Comprobar que la información archivada en físico se encuentre digitalizada	13/1/2020	15:30	15:45	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.



**Tabla 9.** Plan de Auditoria, Evaluación de la seguridad al ingresar un estudiante al sistema.

		<b>Plan de Auditoria</b>							
<b>Proceso a Auditar</b>		Seguridad de acceso al sistema		<b>Área</b>	Centro de computo	<b>Líder del Proceso</b>	Jefe del centro de computo	<b>Equipo Auditor</b>	Daysi Daqui
<b>Objetivo de la Auditoria</b>		Verificar la responsabilidad de los estudiantes al acceder al sistema SIUG		<b>Alcance de la Auditoria</b>	Cambio de contraseña constante		<b>Criterio de la Auditoria</b>	Norma ISO 27001 Sistema de Gestión de Seguridad de la Información	
<b>N°</b>	<b>Actividades</b>	<b>Fecha</b>	<b>Hora Inicio</b>	<b>Hora Final</b>	<b>Lugar</b>	<b>Equipo Auditor</b>	<b>Recursos</b>		
1	Dar a conocer la política de seguridad del sistema SIUG a los estudiantes.	13/1/2020	15:50	16:20	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.		
2	Verificar el cambio constante de contraseña para su seguridad	13/1/2020	16:25	16:40	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.		
3	Verificar el plan de seguridad en caso de riesgos tales como: hackeo, crackeo, etc.	13/1/2020	16:45	17:30	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.		


**Tabla 10.** Plan de Auditoria, Evaluación del manejo de medios.

		<b>Plan de Auditoria</b>					
<b>Proceso a Auditar</b>	Manipulación de información	<b>Área</b>	Centro de computo	<b>Líder del Proceso</b>	Jefe del centro de computo	<b>Equipo Auditor</b>	Daysi Daqui
<b>Objetivo de la Auditoria</b>	Verificar que la información no sea divulgada ni manipulada	<b>Alcance de la Auditoria</b>	Confidencialidad		<b>Criterio de la Auditoria</b>	Norma ISO 27001 Sistema de Gestión de Seguridad de la Información	
<b>N°</b>	<b>Actividades</b>	<b>Fecha</b>	<b>Hora Inicio</b>	<b>Hora Final</b>	<b>Lugar</b>	<b>Equipo Auditor</b>	<b>Recursos</b>
1	Constatar las responsabilidades que tienen al transferir información	14/1/2020	8:00	8:20	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
2	Conocer las reglas para ingresar de forma segura a cualquier información	14/1/2020	8:25	9:00	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
2	Evaluar la confidencialidad de usuarios y contraseñas de los estudiantes	14/1/2020	9:10	9:50	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
3	Tener un plan en caso del robo de información de docentes y estudiantes.	14/1/2020	9:55	10:30	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.

**Tabla 11.** Plan de Auditoria, Evaluación de la seguridad física.

		<b>Plan de Auditoria</b>					
<b>Proceso a Auditar</b>	Seguridad física	<b>Área</b>	Centro de computo	<b>Líder del Proceso</b>	Jefe del centro de computo	<b>Equipo Auditor</b>	Daysi Daqui
<b>Objetivo de la Auditoria</b>	Verificar la seguridad del control de acceso a oficinas.	<b>Alcance de la Auditoria</b>	Implementar un sistema de seguridad física.		<b>Criterio de la Auditoria</b>	Norma ISO 27001 Sistema de Gestión de Seguridad de la Información	
<b>N°</b>	<b>Actividades</b>	<b>Fecha</b>	<b>Hora Inicio</b>	<b>Hora Final</b>	<b>Lugar</b>	<b>Equipo Auditor</b>	<b>Recursos</b>
1	Verificación del control acceso de personas particulares.	14/1/2020	11:00	11:30	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
2	Verificación del control de acceso de estudiantes a equipos sin autorización por falta de seguridad	14/1/2020	11:33	11:50	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
3	Constatar el registro ingreso y salida de los estudiantes al centro de información.	14/1/2020	11:55	12:30	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
4	Confirmar las responsabilidades de docentes y demás autoridades	14/1/2020	12:33	13:00	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.

**Tabla 12.** Plan de Auditoria, Evaluación de licencias actualizadas.

		<b>Plan de Auditoria</b>					
<b>Proceso a Auditar</b>	Culminación de auditoria	<b>Área</b>	Centro de computo	<b>Líder del Proceso</b>	Jefe del centro de computo	<b>Equipo Auditor</b>	Daysi Daqui
<b>Objetivo de la Auditoria</b>	Evaluación de licencias actualizadas	<b>Alcance de la Auditoria</b>	Aplicación anual.			<b>Criterio de la Auditoria</b>	Norma ISO 27001 Sistema de Gestión de Seguridad de la Información
<b>N°</b>	<b>Actividades</b>	<b>Fecha</b>	<b>Hora Inicio</b>	<b>Hora Final</b>	<b>Lugar</b>	<b>Equipo Auditor</b>	<b>Recursos</b>
1	Corroborar los documentos sobre plan de aplicación de licencias anuales	14/1/2020	14:00	14:30	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
2	Revisar su cumplimiento.	14/1/2020	14:30	15:00	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.
3	Reunión de cierre de auditoria	14/1/2020	15:00	15:20	Facultad de Ingeniería Industrial	Daysi Daqui	Laptop, Grabador de voz, Norma ISO 27001, Banco de preguntas.



### 3.9. Recolección de información

**Fase I. Inventario de activos:** En esta fase se procede a crear una tabla de inventario de activos para comprobar el funcionamiento de hardware, software, redes, seguridad física de las oficinas, seguridad lógica, como está estructurada y conocimiento sobre el personal interno y externo de la institución.

**Tabla 13.** Inventario de Activos.

<b>Inventario de Activos Importantes</b>	
<b>Tipos de Activos</b>	<b>Nombre de Activos</b>
<b>Activos de información Hardware.</b>	<p><i>Comprende elementos (físicos, accesorios, periféricos) que soportan el procesamiento de datos de la institución.</i></p> <ul style="list-style-type: none"> <li>• Respaldo de documentos físicos.</li> <li>• Servidores</li> <li>• Laptop</li> <li>• Pc</li> <li>• Impresoras</li> <li>• Disco duro removibles</li> <li>• Cd de instalación de programas</li> <li>• Memorias USB</li> </ul>
<b>Activo de información Software</b>	<p><i>Comprende todos los programas de computadora desarrollados internamente o adquiridos que son utilizados para realizar actividades informáticas tanto para el personal administrativo como para los estudiantes de la institución.</i></p> <ul style="list-style-type: none"> <li>• Sistemas operativos</li> <li>• Software para tareas administrativas</li> <li>• Sistema de monitoreo de red.</li> <li>• Sistema de seguridad</li> <li>• Antivirus</li> <li>• Filtrado de contenido web</li> </ul>
<b>Activo de información de redes</b>	<p><i>Son todos los dispositivos físicos de telecomunicaciones para interconectar varias computadoras remotas.</i></p> <ul style="list-style-type: none"> <li>• Puentes (bridge),</li> </ul>

	<ul style="list-style-type: none"> <li>• Enrutadores (router),</li> <li>• Hubs,</li> <li>• Switches,</li> <li>• Firewall,</li> <li>• IDS,</li> <li>• Balanceador de carga</li> <li>• Adaptadores de red (tarjeta de red).</li> </ul>
<b>Seguridad Física</b>	<ul style="list-style-type: none"> <li>• Control de acceso a oficinas</li> <li>• Control de acceso a equipos del personal administrativo</li> </ul>
<b>Seguridad lógica</b>	<ul style="list-style-type: none"> <li>• Control de acceso a sistemas</li> </ul>
<b>Personal</b>	<p><i>Comprenden todas las personas que forman parte de la institución.</i></p> <ul style="list-style-type: none"> <li>• Estudiantes</li> <li>• Docentes</li> <li>• Departamento de computo</li> <li>• Secretaria</li> <li>• Personal administrativo</li> </ul>

---

*Información tomada de la revista tecnológica ESPOL. Elaborado por el Autor.*

### **3.9.1. Entrevista**

Se realiza una entrevista para obtener información importante realizada mediante una pequeña auditoria para obtener resultados sobre la seguridad de la información, este proceso será analizado mediante fases donde se investigará las diferentes vulnerabilidades que posee la institución, en cada una de estas etapas se verá el cumplimiento de los objetivos que han sido desarrollados por la organización e investigar si el personal tiene conocimiento de las políticas de la misma, toda la investigación será realizada en el centro de cómputo para conocer el estado de seguridad del sistema de SIUG en el cual se encuentra información de los docentes y estudiantes.

**Fase II. Entrevista Realizado Autoridades Encargados del Departamento de Computo.**

- *Normativa 4.1. Conocimiento de la Organización y de su Contexto.*

---

**1. ¿Cuáles son las partes internas y externas de la Carrera de Ingeniería Telemática?**


---

<b>Personal entrevistado</b>	<b>Respuesta</b>
Irwin Fernández Avilés	Las partes internas son los Docentes y las externas los Estudiantes.

---

**Análisis:** De acuerdo a la normativa la organización siempre debe estar conformada por partes internas y externas el cual en la Universidad de Guayaquil está conformada por docentes y estudiantes, los docentes son las partes internas y los estudiantes las partes externas, para cumplir con los resultados previstos en el sistema de gestión de seguridad.

---

**2. ¿Tienen acuerdos de confidencialidad con los docentes y demás autoridades?**


---

<b>Personal entrevistado</b>	<b>Respuesta</b>
Irwin Fernández Avilés	Solo para evaluación a docentes de firma un acuerdo de confidencialidad.

---

**Análisis:** es importante revisar y establecer acuerdos de confidencialidad para así evitar la divulgación de información y proteger la organización.

---

**3. ¿Quiénes pueden acceder a la información sobre el desempeño de los estudiantes?**


---

<b>Personal entrevistado</b>	<b>Respuesta</b>
Irwin Fernández Avilés	Las personas que tienen acceso a información de calificación y rendimiento del estudiante son los Docentes de cada materia.

---

**Análisis:** Es muy importante controlar el personal que accede a la información de los usuarios para evitar la divulgación de información.

---

**4. ¿Poseen de una planificación estratégica en caso de robo de información?**


---

<b>Personal entrevistado</b>	<b>Respuesta</b>
Irwin Fernández Avilés	La facultad y en especial la carrera no cuenta con una planificación estratégica en caso de robo de información, existe una para la Ciudadela en la administración central DGTI, pero no tiene conocimiento de si está documentada o no.

---

**Análisis:** Es muy importante contar con plan de riego el cual nos ayude a controlar y prevenir el acceso a robo de información confidencial.

- *Normativa 4.2. Comprensión de las necesidades y expectativas de las partes interesada.*

---

**5. ¿Los docentes tiene tiempo límite en subir notas?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	Si, este documento en el VIFAC.
------------------------	---------------------------------

---

**Análisis:** toda la información debe estar documentado y respaldado en caso de presentarse vulnerabilidades

---

**6. ¿Tanto docentes como estudiantes tienen acceso o conocimiento de las políticas?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	SI, se encuentran en las pagina de SIUG.
------------------------	--

---

- *Normativa 4.3. Determinación del alcance del sistema de gestión de la seguridad de la información.*

---

**7. ¿Tiene documentado de quienes nomas puede acceder al sistema SIUG?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	SI, eso maneja el DGTI.
------------------------	-------------------------

---

**Análisis:** El departamento de TI de toda la universidad es el encargado de manejar el acceso al sistema de SIUG donde se encuentra información confidencial de docentes y estudiantes.

---

**8. ¿Qué pasos debe cumplir el estudiante para ingresar al sistema, son seguros?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	Se implementó la seguridad del cambio de contraseña cada 3 meses para mayor protección y no la pueden repetir, se procedió a realizar esto por el acceso de terceras personas
------------------------	---

---

**Análisis:** en la institución ha existido varios tipos de vulnerabilidades al momento de acceder al sistema ya que las contraseñas eran vulnerables o por falta de seguridad por parte de los estudiantes, ya que exista casos de estudiantes que daban las contraseñas a terceras personas y accedían al sistema a causar cualquier daño a la información como: anulación de materias, cambio de paralelos, cancelación de documentos de tercera matrícula, etc.

- *Normativa 4.4. Sistema de gestión de seguridad de la información.*

---

#### 9. ¿De qué manera protegen el sistema?

---

Personal entrevistado	Respuesta
Irwin Fernández Avilés	Los encargados de la protección del sistema es DGTI con plataformas de seguridad Check Point y Base de Datos.

---

**Análisis:** La institución maneja diferentes plataformas de seguridad para evitar cualquier tipo de vulnerabilidades y proteger la información.

---

#### 10. ¿Cada cuánto tiempo actualizan las licencias de equipos y sistemas?

---

Personal entrevistado	Respuesta
Irwin Fernández Avilés	La universidad posee un convenio de compras de licencias anuales.

---

**Análisis:** Por lo general todo tipo de instituciones actualizan sus licencias cada año para evitar cualquier tipo de huecos informáticos de permita el robo de información

- *Normativa 5.1. Liderazgo y Compromiso.*

---

#### 11. ¿La persona encargada del compromiso y liderazgo conoce las políticas de seguridad y el plan de seguridad?

---

Personal entrevistado	Respuesta
Irwin Fernández Avilés	No hay plan de seguridad manejan normas de control interno creada en el 1996. No poseen reglamentos de seguridad interno.

---

**Análisis:** De acuerdo con la investigación realizada se puede observar que no existe normas de seguridad, los últimos controles internos que aún son utilizados por la institución fueron creados en 1996; hoy en día la tecnología avanzado muchísimos por el cual estas normas no abastecen para la seguridad de la información de los usuarios.

- *Normativa 5.3. Roles y Responsabilidades.*

---

**12. ¿Capacitan a los docentes sobre las responsabilidades que deben tener?**


---

Personal entrevistado	Respuesta
Irwin Fernández Avilés	Los encargados de las capacitaciones de docentes es VIFA

---

**Análisis:** Es importante recalcar que la capacitación a docentes sobre la seguridad de la información que manejan es muy importante ya que de esa manera se podrá disminuir las vulnerabilidades y dar la seguridad a los usuarios de que su información está protegida.

---

**13. ¿Capacitan al docente en caso de cambiar algo en el sistema?**


---

Personal entrevistado	Respuesta
Irwin Fernández Avilés	SI lo hace VIFAP

---

- *Normativa 6.1. Acción para tratar riesgos.*

---

**14. ¿En caso de que intenten ingresar al sistema cual es el plan de para evitar el riesgo?**


---

Personal entrevistado	Respuesta
Irwin Fernández Avilés	La carrera no posee su propio plan para evitar riesgos por lo cual tienen que esperar a que el DGTI reaccione, como seguridad del sistema se utiliza un Check Point.

---

**Análisis:** Toda institución debe contar con un plan de seguridad que ayude a reducir riesgos o prevenir a cualquier tipo crisis que provoque la perdida de información confidencial.

---

**15. ¿Cuentan con proceso de valoración de riesgos?**


---

Personal entrevistado	Respuesta
Irwin Fernández Avilés	No

---

**Análisis:** Es muy importante recalcar que en una institución es importante realizar una valoración de riesgos, que ayude a identificar los riesgos o posibles riesgos a los que están expuestos y así corregirlos.

---

**16. ¿Disponen de información documentada sobre los objetivos para proteger la información?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

---

Irwin Fernández Avilés	Maneja el DGTI.
------------------------	-----------------

---

**Análisis:** Es importante recalcar que cada área de una institución debe contar con información documentada de como protege su información.

- *Normativa 7.1.*

---

**17. ¿Disponen con algún plan de actividades a cumplir sobre el mantenimiento de licencias e instalación de programas?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

---

Irwin Fernández Avilés	SI, cada año se realiza un plan.
------------------------	----------------------------------

---

**Análisis:** Es importante contar con un plan de actividades cada 6 meses para analizar vulnerabilidades que existan y corregirlas a tiempo.

- *Normativa 7.2. Creación y actualización.*

---

**18. ¿Se actualiza el sistema?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

---

Irwin Fernández Avilés	SI.
------------------------	-----

---



---

**19. ¿Reciben capacitación sobre seguridad del sistema?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

---

Irwin Fernández Avilés	NO
------------------------	----

---

**Análisis:** Es importante recalcar que la seguridad del sistema es un tema muy importante ya que protege toda la información

- *Normativa 7.3. Control de la información documentada.*

---

**20. ¿Se ha realizado charlas para dar a conocer las políticas a los estudiantes?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

---

Irwin Fernández Avilés      SI al iniciar clases.

**Análisis:** Capacitar al usuario sobre la seguridad con la que deben manejar el sistema

**21. ¿Cuentan con algún tipo de software el cual contengan programas para los estudiantes?**

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	No
------------------------	----

**Análisis:** Incentivas al personal a prepararse y crear competitividad

**22. ¿Cuentan con respaldo de información documentada en papel?**

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	NO
------------------------	----

- *Normativa 8. Planificación y control operacional.*

**23. ¿Tienen planificado e implementado algún plan y control operacional?**

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	NO posee ninguno
------------------------	------------------

**24. ¿Alguna vez se han valorado los riesgos que tiene la carrera?**

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	NO
------------------------	----

**25. ¿Cuentan con un tratamiento de riesgos?**

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	NO
------------------------	----

- *Normativa 9.1. Seguimiento, medición, análisis y evaluación.*

**26. ¿Cuentan con alguna certificación ISO?**

Personal entrevistado	Respuesta
-----------------------	-----------



Irwin Fernández Avilés	NO
------------------------	----

---

**27. ¿Han sido auditados alguna vez?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	NO
------------------------	----

---

**Análisis:** Es importante realizar auditorías en la organización para encontrar y analizar los riesgos y aplicar una mejora continua.

---

**28. ¿Qué tipo de falencias posee la Carrera?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	Sistema Eléctrico, comunicaciones, seguridad.
------------------------	---

---



---

**29. ¿Cree que los errores que posee la Carrera han sido corregidos?**

---

Personal entrevistado	Respuesta
-----------------------	-----------

Irwin Fernández Avilés	NO ninguno.
------------------------	-------------

---

**Análisis:** La Carrera de Telemática posee muchas falencias en estructura de red, infraestructura de seguridad, el cableado de red no está seguro; poseen documentos de cambio de carreras, anulación de materias, terceras matriculas.

**Fase III. Análisis de riesgo:** En esta fase se procede realizar un análisis sobre el sistema de gestión de seguridad de la información, en el cual se detalla cada una de las vulnerabilidades encontradas dando un valor de acuerdo a los daños que presenta la institución, toda la información fue obtenida de la entrevista; la institución no cuenta con respaldos de la información física por lo que al momento de ocurrir un desastre natural se puede perder la información, el servidor está ubicado en un data center, los antivirus son actualizados anualmente (Kaspersky), no posee con respaldos en disco duro. (Solarte, Rosero, & Ruano, 2015 ).

Los equipos que son utilizados por los estudiantes cuentan con Windows 8.1 y 10; para enviar sus tareas existen diferentes plataformas como Edmodo, office 365, entre otros; una de las vulnerabilidades más grandes es que no cuentan con sistemas de seguridad, tampoco dispone de protección para los equipos del personal administrativo ya que la contraseñas con las que son protegidas pueden ser obsoletas y de fácil acceso. La política de la universidad se encuentra en la página web.

## **Capítulo IV**

### **Propuesta**

Al finalizar el levantamiento de la información del presente estudio y ser analizada la seguridad de la información, se procede a plantear una propuesta con la finalidad reducir los riesgos expuestos anteriormente, aplicando la Norma ISO 27001 el cual ayudará a reducir las vulnerabilidades y amenazas identificadas.

El proceso central que fue analizado en el departamento de cómputo el cual se encuentra toda la información tanto de estudiantes como de docentes, esta área es considerada como una de las más importantes ya que tiene almacenada información confidencial, es importante recalcar que se analizó el grado de concientización en la seguridad de la información que brinda la institución a estudiante y docentes.

#### **4.1. Modelo PDCA.**

PDCA (PLAN – DO – CHECK – ACT) en español significa: planear, hacer, verificar y actuar, es un modelo que ayuda a las empresas a la mejora continua, para la implementación de un SGSI, ya que ayuda a la organización y documentación correcta para evitar cualquier tipo de vulnerabilidades.

#### **4.2. Área responsable de la ejecución de controles correctivos y preventivos.**

El departamento encargado de la seguridad de la información de los estudiantes de la carrera de ingeniería telemática de la Universidad de Guayaquil es el área de cómputo, después de evaluar con los controladores de la norma ISO27001 se dio a conocer que la información no estaba brindando la protección correcta, por ende, se procederá a implementar un sistema que ayude a la seguridad de la información.

**Ejecutan:** Departamento de cómputo encargados de la seguridad de la información de los estudiantes.

#### **4.3. Planificación de entrevista**

Se coordinó la entrevista con el personal encargado del departamento de cómputo para obtener resultados reales, actuales sobre la seguridad de la información de la institución para lo cual se programó 3 visitas al departamento donde se obtuvo toda la información importante.

**Tabla 14.** Planificación de entrevista

<b>Fecha</b>	<b>Nombre</b>	<b>Cargo</b>
6-enero-2020	Ing. Irwin Fernández Avilés	Analista de Computo
13-enero-2020	Ing. Irwin Fernández Avilés	Analista de Computo
14-enero-2020	Ing. Irwin Fernández Avilés	Analista de Computo
27-enero-2020	Ing. Irwin Fernández Avilés	Analista de Computo

#### **4.4. Infraestructura tecnológica y física.**

La carrera de ingeniería teleinformática cuenta con una infraestructura acorde a sus necesidades actuales para la transmisión de datos, tiene pequeños déficits que producen fallas al momento de transferir información, la institución cuenta con todas las licencias actualizadas, pero con equipos obsoletos y antiguos, uno de los problemas más grandes de la infraestructura es la falta de seguridad física y del entorno, falta de seguridad criptográfica para la protección de información, falta de seguridad de equipos para evitar pérdidas, daños y robo de información.

#### **4.5. Fase IV: Análisis de situación actual del departamento de cómputo de Universidad de Guayaquil de la Carrera de Ingeniería Telemática.**

En esta fase se realizará el análisis de toda la información obtenida de acuerdo con el SGSI, se analizará los riesgos de seguridad encontrados.

##### **4.5.1. Análisis de riesgo y diagnóstico de la seguridad de la información de acuerdo con el inventario de activos.**

El análisis realizado para conocer los riesgos que presenta la institución da a conocer, que no cuenta con la seguridad necesaria para evitar que ciberdelincuentes accedan y manipulen la información del personal, cerraduras con huella en lugares donde se tiene información importante como el centro de cómputo, secretaria y decanato, que son sitios donde se encuentran información importante de los estudiantes como calificación base de datos de los mismo e información de los docentes, también se puede recalcar que nunca se ha realizado un análisis de riesgo el cual permite identificar y corregir las vulnerabilidades; por otra parte es muy importante recalcar que la seguridad de ingeniería eléctrica es otro punto negativo para la institución por lo que debería ser corregido y aplicar una mejora continua de acuerdo con la norma estudiada ISO 27001, . En este análisis se utilizará una técnica que permite conocer los riesgos ya que está relacionada con medios electrónicos,

informáticos y telemáticos dando seguridad a la información; de esta manera se identificarán las causas de robo de la información y definir un sistema de seguridad de acuerdo con las vulnerabilidades encontradas. A continuación, se mostrará la **“Escala de valoración de los activos informáticos de acuerdo al daño que se pueda causar en ellos: Daño catastrófico: 10; Daño grave: 7 – 9; Daño moderado: 4 – 6; Daño Leve: 1 – 3; Daño Irrelevante: 0”**. (Solarte, Rosero, & Ruano, 2015 ).

**Tabla 15.** Dimensiones o criterios de evaluación seguridad de la información.

<b>Tipo de nombre</b>	<b>Nombre de activo</b>	<b>Confidencialidad. Daño: Divulgación de información</b>	<b>Integridad Perjuicio: Falta de seguridad.</b>	<b>Disponibilidad: Degradación al acceder al sistema informático.</b>	<b>Autenticidad Perjuicio: Protección de información</b>
Hardware	Respaldo de información documentada.	9	9	--	10
	Servidores	5	4	10	6
Software o aplicación	Seguridad de sistemas operativos	8	9	9	8
	Sistema de seguridad	9	10	8	6
Instalación eléctrica	Fallas del sistema eléctrico	9	--	6	--
Seguridad Física	Control de acceso a oficinas	9	10	8	8

**“Relación entre amenazas, vulnerabilidades y pérdida**

**(Amenaza) X (Vulnerabilidad) = (Pérdida)**

**Virus X no tener instalado software antivirus = destrucción.”** (Romero, Análisis de riesgos DE seguridad de la información, 2016).

#### 4.5.2. Análisis de Vulnerabilidades de acuerdo con el inventario de activos de la Carrera de Ingeniería Telemática.

Las vulnerabilidades de la información es uno de los principales peligros más frecuentes en las organizaciones, por lo que se procede a evaluar la Carrera de Ingeniería Telemática de acuerdo a los controles de la norma ISO27001; esta información es analizada mediante un inventario de activos donde se identifica las vulnerabilidades, amenazas a las que están expuestas

**Tabla 16.** Vulnerabilidades obtenidas de la entrevista realizada al centro de cómputo en la Universidad de Guayaquil de la carrera de Ingeniería en Telemática.

<b>Hardware</b>		
<b>Vulnerabilidades</b>	<b>Amenazas</b>	<b>Riesgos Potenciales</b>
No cuenta con respaldo de información documentada en papeles.	Perdida de información por desastres naturales: <ul style="list-style-type: none"> <li>• Incendios</li> <li>• Inundación</li> <li>• Terremotos</li> </ul>	Perdida de información importante, falta de respaldos en caso de daños en equipos.
Deficiencia de control de acceso a la Pc, no cuentan con seguridad	Ingreso a información confidencial, acceso de personas inadecuadas	Robo de información. Alteración o destrucción de la información.
No cuentan con respaldo en discos duros removibles	En caso de dañarse los equipos no cuentan con respaldos de información	Perdida de información
<b>Software</b>		
No cuentan con sistema de seguridad en equipos.	Acceso de personas inapropiadas al equipo que contienen sistemas operativos antiguos.	Obtención de información de docentes y estudiantes.
<b>Información de Redes</b>		
No disponen de puentes (bridge)	La institución no cuenta con este tipo de interconexión para realizar transferencias de información de un lado a otro.	Alteración al momento de transferir información de un

		equipo a otro sin autorización.
<b>Seguridad Física</b>		
No posee control de sistema de seguridad acceso a oficinas.	Al no existir ningún tipo de control de acceso, tanto a oficinas como, al sistema de docentes los estudiantes pueden aprovecharse de la vulnerabilidad y acceder.	Acceso inadecuado de personas no autorizadas.
No cuenta con el control de seguridad necesario para proteger el acceso de los estudiantes a equipos de personal administrativo	Los equipos del personal administrativo no cuentan con la seguridad adecuada para evitar el acceso inapropiado.	<ul style="list-style-type: none"> <li>• Destrucción</li> <li>• Manipulación de información</li> <li>• Robo de claves etc.</li> </ul>
<b>Seguridad Lógica</b>		
Deficiencia de control de acceso a los sistemas	Acceso directo a información y editar o alterar contraseñas tanto de equipos como de cuentas se estudiantes y de docentes	<ul style="list-style-type: none"> <li>• Pérdida de información.</li> <li>• Alteración de información.</li> </ul>

Procedemos a evaluar las cláusulas de acuerdo a la situación de la seguridad de la información de la carrera basando en el modelo de madurez de capacidad (CMM).

Valor	Efectividad	Significado	Descripción
L0	0%	Inexistente	Carencia completa de cualquier proceso reconocible. No se ha reconocido siquiera que existe un problema a resolver.
L1	10%	Inicial / Ad-hoc	Estado inicial donde el éxito de las actividades de los procesos se basa la mayoría de las veces en el esfuerzo personal. Los procedimientos son inexistentes o localizados en áreas concretas.
L2	50%	Reproducible, pero intuitivo	Los procesos similares se llevan en forma similar por diferentes personas con la misma tarea. Se normalizan las buenas prácticas en base a la experiencia y al método.
L3	90%	Proceso definido	La organización entera participa en el proceso. Los procesos están implantados, documentados y comunicados
L4	95%	Gestionado y medible	Se puede seguir con indicadores numéricos y estadísticos la evolución de los procesos. Se dispone de tecnología para automatizar el flujo de trabajo, se
L5	100%	Optimizado	Los procesos están bajo constante mejora.

**Figura 13:** Valoración de criterios de madurez CMM. Información tomada tesis Fundación Universitaria San Mateo. Elaborado por el Autor.

**Tabla 17.** Evaluación de efectividad de la Carrera de Ingeniería Industrial de acuerdo a la ISO 27001.

Clausula	Dominio	Calificación actual	Calificación objetivo
A.5	Políticas de seguridad de la Información	80	100
A.6	Organización de la seguridad de la información	45	100
A.7	Seguridad de los Recursos Humanos	30	100
A.8	Gestión de activos	60	100
A.9	Control de Acceso	10	100
A.10	Criptografía	10	100
A.11	Seguridad física y ambiental	20	100
A.12	Seguridad Operacional	60	100
A.13	Seguridad de las Comunicaciones	50	100
A.14	Adquisición, desarrollo y mantenimiento de Sistemas	80	100

A.15	Relaciones con los proveedores	75	100
A.16	Gestión de Incidentes en Seguridad de la Información	30	100
A.17	Aspectos de Seguridad de la Información de la gestión de la continuidad del negocio	20	100
A.18	Cumplimiento	0	100

#### 4.5.3. Evaluación y Determinación de Vulnerabilidades, Amenazas y Riesgos:

Las preguntas realizadas a analistas sobre el respaldo de información y el resto de las vulnerabilidades que presente la universidad son corregidas; debido al estudio realizado se observó que los procesos y archivos no están clasificados, documentados, no posee ningún sistema de seguridad de ingreso al departamento.

**Tabla 18.** Hallazgos de la Auditoría interna realizada.

<b>Auditoría Interna</b>			
<b>Institución</b>	Universidad de Guayaquil	<b>Fecha</b>	6-enero-2020
<b>Área</b>	Departamento de computo	<b>Auditado</b>	Ing. Juan Dolet Washbrum
<b>Cláusulas</b>	Descripción de NO CONFORMIDAD		
<b>4.1, 4.3 ISO 27001</b>	La organización no cuenta con información respaldada sobre planificación para evitar el robo de información. No contiene el alcance documentado		
<b>6.1.2, 6.1.3, 6.2 ISO 27001</b>	La organización no posee valoración de riesgo, es decir, no identifican el nivel de vulnerabilidad o la pérdida de información por la falta de confidencialidad. La institución no contiene tratamiento de riesgos después de los resultados obtenidos		
<b>7.2. ISO 27001</b>	El departamento no cuenta con capacitación para crear competencia basándose en la educación y formación del personal		



<b>7.5.2, 7.5.3 ISO 27001</b>	Varios estudiantes de la carrera supieron manifestar que no cuentan con actualización de software que son de mucha necesidad para ellos. Se observó que no existe respaldo de información documentada, protegida adecuadamente contra la pérdida de confidencialidad e integridad.
<b>8.1, 8.2, 8.3: ISO 27001</b>	La institución no posee una planificación para evitar el robo de información por ciberdelincuentes.
<b>9.1. ISO 27001</b>	El centro de cómputo de la carrera de ingeniería telemática no cuenta la certificación de la norma ISO 27001, que ayude al seguimiento de la seguridad de la información.

#### 4.6. Fase V: Aplicación de objetivos de control y controles de referencia ANEXO A.

**Tabla 19.** Solución a no conformidades mediante el ANEXO A.

<b>4.6.1. Seguridad de respaldo de información.</b>		
<b>Objetivo:</b> Proteger contra la perdida de información aplicando medidas criptográficas para evitar pérdidas, daños, robo y fácil acceso a softwares.		
<b>Controles</b>	<b>Descripción del control</b>	<b>Descripción</b>
A.10.1.1	Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.	Evitar robo o perdida de información por falta de respaldo físico y digital. Las medidas criptográficas son algoritmos de autenticidad con el fin de evitar el fácil acceso a softwares.
A.12.3.1	Se debe hacer copias de respaldo de la información, software e imágenes de los sistemas y ponerlas a pruebas regularmente de acuerdo con una política de copias de respaldo acordadas.	
<b>Objetivo:</b> Definir los criterios de vulnerabilidad y aceptación de riesgos, estableciendo grados de valoración para evitar la pérdida de confidencialidad e integridad de la organización.		

A.12.6.1	Se deberá obtener oportunamente información acerca de las vulnerabilidades técnica de los sistemas de información que se usen; evaluar la exposición de las organizaciones a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	Los criterios de vulnerabilidades deben ser clasificados dependiendo de la magnitud del problema para tomar medidas preventivas según el caso y así implementar la mejora continua.
<b>Objetivo:</b> Implementar un plan de concientización al personal sobre la seguridad de la información que maneja, realizando capacitación, charlas y auto preparación.		
A.7.2.2	Todos los empleados de la organización y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada y actualizaciones regulares sobre la política y procedimientos de la organización pertinentes a su cargo.	Es importante formar personal competente basándose en la formación y experiencias obtenidas, asegurándose que los empleados comprendan sus responsabilidades al momento de manejar la información
<b>Objetivo:</b> Ejecutar un plan preventivo de acceso físico a oficinas de personas no autorizadas, implementando medidas de bioseguridad.		
A.11.1.2	Las áreas seguras se deben proteger mediante controles de acceso apropiado para asegurar que solo permite el acceso de personal autorizado.	Es importante proteger la información que se encuentra en ciertas áreas, por ende, es necesario el uso de dispositivos de seguridad para personal autorizado.
A.11.1.3	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.	
<b>Objetivo:</b> Prevenir riesgos del cableado de red, para evitar interrupciones al momento de transferir información. Instalación		
A.11.2.2	Los equipos de deben proteger contra fallas de energía y otras interrupciones causadas por fallas en los servicios de suministros.	El cableado de red en la organización es muy importante ya que permite

A.11.2.3	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interrupción, interferencias o daños.	transferir información sin interferencia.
<b>Objetivo:</b> Constatar que la institución implemente y opere de acuerdo a las políticas establecidas por el mismo.		
A.18.2.2	Los directores deben revisar con regularidad el cumplimiento del procesamiento de información dentro de su área de responsabilidad con las políticas y normas de seguridad apropiadas y cualquier otro requisito de seguridad.	La organización debe mejorar continuamente la conveniencia adecuada y eficacia del sistema de gestión de la seguridad de la información

#### 4.7. Conclusiones

Mediante la utilización del método de valoración de criterios de madures, se pudo observar las principales vulnerabilidades que atraviesa la organización, es la falta de respaldo de información que posee la institución, lo cual puede ocasionar pérdidas de documentación física por causa de desastres naturales debido a la infraestructura no es la adecuada y no posee el respaldo de la documentación física en digital.

El análisis realizado después entrevista al departamento de cómputo, demuestra que la situación actual dentro de la institución refleja grandes índices de riesgos como: robos de información, la falta de seguridad física a las áreas, débil acceso a equipos de cómputo, causando así impactos negativos a la organización.

Uno de los principales beneficios es la seguridad que posee el servidor ya que se encuentra en un Data Center respaldado con todas las normas de seguridad como: alarma contra incendios, piso falso y respaldo de la información en la nube con la empresa Telconet, teniendo en cuenta que dispone de licencias actualizadas.

Los riesgos más graves que atraviesa la Carrera de Ingeniería Telemática es la falta de seguridad física y del entorno, ya que puede acceder cualquier persona a las oficinas, manipular los equipos y obtener información confidencial. Es importante recalcar que la institución no cuenta con una planificación estratégica para evitar el robo de información, no posee procesos de valoración de riesgos para dar un tratamiento adecuado y brindar la seguridad necesaria teniendo en cuenta la confiabilidad, disponibilidad e integridad.

La infraestructura de red no está protegida correctamente por el cual existe problemas de inferencia, también posee falla eléctrica donde se pierde conexión con la red de SIUG y hace imposible el ingreso a la página web, dando así un hueco para que ciberdelincuentes accedan sin permiso y obtener información confidencial.

#### **4.8. Recomendaciones**

La seguridad total no existe, pero se puede controlar el manejo de información para evitar la divulgación de esta. El propósito de la aplicación del SGSI (sistema de gestión seguridad de la información) de la carrera de ingeniería telemática es conocer las vulnerabilidades y riesgos a los que están expuestos, para reducirlos con la aplicación de la norma ISO 27001 teniendo en cuenta las cláusulas y controles que se deben aplicar a medida que se encuentra una no conformidad.

Se recomienda la elaboración y uso de las políticas de seguridad, creación de un plan y cronograma de actividades de seguridad de la información, también es importante la implementación de un control de acceso físico evitando el ingreso del personal no autorizado.

Crear conciencia en directivos a través de capacitaciones, donde se de conocer las responsabilidades de seguridad a cada uno de los empleados y los riesgos a los que estén expuestos, para garantizar que la información de la empresa sea manejada y procesada correctamente.

Se recomienda que el seguimiento de auditoría interna sea realizado por lo menos cada 6 meses, así se podrá identificar cualquier tipo de vulnerabilidad y corregirlas a tiempo, creando así una mejora continua.

Realizar mantenimiento a las redes eléctricas de la institución ya que se encuentran en mal estados y realizar constantes revisiones por parte de ingenieros de servicios para cumplir con los puntos claves de la seguridad de infraestructura de la norma.

Se debe considerar todas las políticas de seguridad establecidas en el estudio de la auditoria, teniendo en cuenta los propuestos en la certificación. Considerar nuevos métodos de seguridad tanto física como digital.

# ANEXOS

## Bibliografías

ISOTools. (2017). Pasos para implementar un plan de Gestión de Riesgos de acuerdo a ISO 31000. *ISOTools*, <https://www.isotools.org/2017/05/14/10-pasos-para-implementar-un-plan-de-gestion-de-riesgos-de-acuerdo-a-iso-31000/>.

Academy 27001. (2019). *Advisera*. ¿Qué es norma ISO 27001?: [https://advisera.com/27001academy/es/que-es-iso-27001/?fbclid=IwAR1OQ-\\_6QXADnLkdAgFjYHc4bopeF1W9rYOW7AMM17F0kimHOxSEux3Zt0s](https://advisera.com/27001academy/es/que-es-iso-27001/?fbclid=IwAR1OQ-_6QXADnLkdAgFjYHc4bopeF1W9rYOW7AMM17F0kimHOxSEux3Zt0s)

Álvarez, R. (11 de enero de 2018). *xataka*. Los datos de 143 millones de personas filtrados ante el hackeo a Equifax, una de las mayores agencias crediticias: <https://www.xataka.com/seguridad/hackean-equifax-una-de-las-mayores-agencias-de-informes-crediticios-afectando-a-143-millones-de-usuarios>

Auditool. (14 de abril de 2014). *Auditool*. Lo que todo Auditor debe conocer de SOX: <https://www.auditool.org/blog/control-interno/2651-lo-que-todo-auditor-debe-conocer-de-sox>

Aviles, D. S. (2017). *Repositorio de la Universidad Tecnica de Babahoyo*. Estudio de las Vulnerabilidades en la Red de Datos de la Unidad Educativa Zapotal: <http://dspace.utb.edu.ec/bitstream/49000/2514/1/-E-UTB-FAFI-SIST-000038.pdf>

Barrezueta, H. E. (10 de febrero de 2014). *Codigo Organico Integlar Penal*. Leyes de Teleinformatica: [https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT\\_CEDAW\\_ARL\\_ECU\\_18950\\_S.pdf](https://tbinternet.ohchr.org/Treaties/CEDAW/Shared%20Documents/ECU/INT_CEDAW_ARL_ECU_18950_S.pdf)

Basaldua, L. D. (2016). *Universidad Iberoamerica*. Seguridad en Informatica (Auditoria de SIstemas): <http://www.bib.uia.mx/tesis/pdf/014663/014663.pdf>

Blog InternetLab. (2013). *InternetLab*. La condición de carrera: <https://www.internetlab.es/post/2548/condicion-de-carrera/>

Chacon Mejia, P. (Septiembre de 2008). *Sistema de gestion de seguridad*. Escuela Politecnica Nacional : <https://bibdigital.epn.edu.ec/bitstream/15000/7807/1/CD-4189.pdf>

Ciberseguridad. (10 de enero de 2019). *BTOB Consultores*. Amenazas y vulnerabilidades de los sistemas informáticos: <http://btob.com.mx/ciberseguridad/amenazas-y-vulnerabilidades-de-los-sistemas-informaticos/>

Coelho, F. E., Araujo, L. G., & Bezerra, E. K. (2014). *Gestión de la seguridad de la informacion*. Bogota Colombia: <https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI8.pdf>.

Coelho, F. E., Araújo, L. G., & Bezerra, E. K. (2014). *Gestion de la seguridad de la informacion*. Colombia: <https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/GTI8.pdf>.

Diaz Montenegro, G., & Castro Zambrano, G. (2019). Vulnerabilidades informáticas. *tecnologia informatica*, <https://tecnologia-informatica.com/vulnerabilidades-informaticas/>.

Espinoza, F. (10 de diciembre de 2016). *tekcrispy*. Vulnerabilidad crítica en el correo de Yahoo permitía que cualquiera hacker se infiltrará en las cuentas: <https://www.tekcrispy.com/2016/12/10/vulnerabilidad-critica-correo-yahoo-permitia-hacker-se-infiltrara-las-cuentas/>

FM, Y. (2019). Firewall: qué es un cortafuegos, para qué sirve y cómo funciona. *Xataka*, <https://www.xataka.com/basics/firewall-que-cortafuegos-sirve-como-funciona>.

Geovanny Vega Villacís, R. A. (14 de Marzo de 2017). *Ciencias*. Vulnerabilidades y amenazaas de la web de intranet de la Universidad Tecnica de Babahoyo.: <https://www.3ciencias.com/wp-content/uploads/2017/03/ART5.pdf>

Gomez, J. R. (2019). Misión y Visión de todas las facultades de la Universidad de Guayaquil. *Universidad de Guayaquil*, <http://jhonromerogomez.blogspot.com/2018/05/mision-y-vision-de-la-universidad-de.html>.

Granizo, V. G., Noboa Romero, P., & Buchelli Carpio, L. (2014). *scribd*. Analisis de vulnerabilidad de la universidad estatal de Milagro ante factores de riesgo: <https://es.scribd.com/document/336955391/Analisis-de-Vulnerabilidad-de-La-Universidad-Estatal-de-Milagro-Durante-Una-Emergencia>

Gutierrez, M. (02 de 09 de 2019). *spamina*. ¿Por qué tus datos son tan valiosos?: <https://spamina.com/category/blog/seguridad-de-la-informacion>

Guzman, M. L. (2016). *Escuela Superior Politecnica del Litoral*. Desarrollo de un sistema de informacion ISO27001: <https://www.dspace.espol.edu.ec/retrieve/98956/D-106133.pdf>

ISO, C. (16 de mayo de 2017). *Metodología para el Análisis de Riesgos ISO 9001*. Obtenido de Nueva ISO 9001: <https://www.nueva-iso-9001-2015.com/2017/05/metodologia-analisis-de-riesgos-iso-9001/>

ISO/IEC 27001. (2013). *Norma tecnica NTC-ISO-ICE-27001*. Bogota: ICONTEC.

ISOTools. (21 de mayo de 2015). *SGSI*. ISO 27001: ¿Qué significa la Seguridad de la Información?: [https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/?fbclid=IwAR1r87sb2\\_nJPJkwB5njU9CTuc2Sv4eDwG0b0ZJsg2vaueHC3XXPUmHUqwM](https://www.pmg-ssi.com/2015/05/iso-27001-que-significa-la-seguridad-de-la-informacion/?fbclid=IwAR1r87sb2_nJPJkwB5njU9CTuc2Sv4eDwG0b0ZJsg2vaueHC3XXPUmHUqwM)

ISOTools. (2018). Fallos de seguridad. *SGSI*, <https://www.pmg-ssi.com/2018/08/cuales-son-los-fallos-de-seguridad-que-mas-suelen-repetirse/>.

ISOTools. (31 de Octubre de 2019). *Blog especializado en Sistemas de Gestión*. Seguridad de la información y caso Fnac: <https://www.pmg-ssi.com/2019/10/seguridad-de-la-informacion-y-caso-fnac/>

ISOTools. (2019). Software ISO Riesgos y Seguridad. *ISOTools*, <https://www.isotools.org/normas/riesgos-y-seguridad/iso-27001/>. Sistemas de Gestión de Riesgos y Seguridad.

Jaimovich, D. (12 de mayo de 2018). *Infobae*. Cómo surgió y se propagó WannaCry, uno de los ciberataques más grandes de la historia: <https://www.infobae.com/america/techo/2018/05/12/como-surgio-y-se-propago-wannacry-uno-de-los-ciberataques-mas-grandes-de-la-historia/>

Macias, R. (6 de Noviembre de 2017). *Prakmatic*. Evaluación de la Seguridad Informática, esencial para tu empresa: <https://www.prakmatic.com/gestion-ti/evaluacion-de-la-seguridad-informatica-esencial-para-tu-empresa/>

Molina, K. G. (Marzo de 2015). *Universidad Politecnica Salesianas Sede Guayaquil*. Analisis de seguridad Informatica Basada en la Norma ISO 27001 en las Empresas de Servicio Financiero.

Pérez, I. (5 de Noviembre de 2014). *welivesecurity*. Que son y cómo funcionan los Buffer Overflow: <https://www.welivesecurity.com/la-es/2014/11/05/como-funcionan-buffer-overflow/>

Pores, M. (s.f.). Copias de seguridad. *Informática*, <https://www.informatica-hoy.com.ar/seguridad-informatica/Fallos-de-Seguridad-en-la-Informacion.php>. Copias de seguridad.

Praxis. (11 Julio 2019). El SGSI bajo la norma ISO 27001 hacia las unidades educativas ecuatorianas. *Capital de praxis*, [https://issuu.com/praxisconsulting5/docs/el\\_sistema\\_de\\_gesti\\_n\\_de\\_seguridad](https://issuu.com/praxisconsulting5/docs/el_sistema_de_gesti_n_de_seguridad).

Retamoso, J. E. (2017). *Repositorio UNAD*. Auditoria de Seguridad de la Institucion Educativa Departamental Luis Carlos Galán : <https://repository.unad.edu.co/bitstream/handle/10596/17390/10188295.pdf;jsessionid=28AF1B7D2E7D9FE33A4FE232FA75B917.jvm1?sequence=1>

Rodríguez, A. (18 de Enero de 2016). *Trustdimension*. La importancia de la Seguridad Informática: <https://www.trustdimension.com/la-importancia-de-la-seguridad-informatica/>

Romero, L. (2016). Análisis de riesgos DE seguridad de la información. *slideplayer*, <https://slideplayer.es/slide/3881802/>.

Romero, L. (2017). *SlidePlayer*. Análisis de riesgos de seguridad de la información: <https://slideplayer.es/slide/3881802/>

Rouse, M. (2019). HIPAA. *Techtarget*, <https://searchhealthit.techtarget.com/definition/HIPAA>.

Seguridad, S. (24 de Junio de 2016). *Solvetic*. Tipos de ataques informáticos e intrusos y cómo detectarlos: <https://www.solvetic.com/page/recopilaciones/s/profesionales/tipos-de-ataques-informaticos-e-intrusos-y-como-detectarlos>

SGSI. (16 de Julio de 2014). *Blog especializado en Sistemas de Gestión de seguridad Informatica*. ISO 27001:2013 Contexto de la organización: <https://www.pmg-ssi.com/2014/07/iso-270012013-contexto-de-la-organizacion/>

Simbaña, A. L. (2018). *Repositorio de la Universidad Central del Ecuador*. Obtenido de Evaluación de riesgos, amenazas y vulnerabilidades en la Unidad Educativa Luciano Andrade Marín: <http://www.dspace.uce.edu.ec/bitstream/25000/16451/1/T-UCE-0020-CDI-044.pdf>

simplilearn. (2019). COBIT. *simplilearn*, <https://www.simplilearn.com/what-is-cobit-significance-and-framework-rar309-article>.

Solarte, F. N., Rosero, E. R., & Ruano, M. d. (2015 ). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001 . *Revista Tecnológica ESPOL* , <http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456/321>.

Verdezoto, A. J. (2018). *Derechoecuador*. Obtenido de DELITOS INFORMÁTICOS O CIBERDELITOS: <https://www.derechoecuador.com/delitos-informaticos-o-ciberdelitos>

Villagómez., C. (27 de Septiembre de 2017). *CCM*. Introducción a la seguridad informática: <https://es.ccm.net/contents/622-introduccion-a-la-seguridad-informatica#introduccion-a-la-seguridad>

VIU. (21 de 3 de 2018). *Universidad Internacional de Valencia*. ¿Qué es la seguridad informática y cómo puede ayudarme?: <https://www.universidadviu.com/la-seguridad-informatica-puede-ayudarme/>