



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

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

**ÁREA  
REDES INTELIGENTES**

**TEMA  
“ELABORACIÓN DE UN PLAN DE PROCESOS DE  
RESPALDO Y DETECCIÓN DE  
VULNERABILIDADES BASADO EN NORMATIVAS  
ISO:27001”**

**AUTOR  
CAMPOVERDE PAZMIÑO RUBÉN DARIO**

**DIRECTORA DEL TRABAJO  
LCDA. TELLO ARÉVALO SANDRA ELIZABETH, MG.**

**2018  
GUAYAQUIL – ECUADOR**

## **DECLARACIÓN DE AUTORÍA**

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

**Campoverde Pazmiño Rubén Dario**  
**C.C. 0925636169**

## **AGRADECIMIENTO**

La culminación de esta etapa en nuestras vidas; simboliza el esfuerzo y el deseo de cada uno de nosotros por superarnos en el gran camino de éxitos que tendremos en el futuro. Tanto como profesionales, padres, madres y personas.

Deseo agradecer a cada oportunidad de éxito que se me ha dado hasta ahora, a cada evento fortuito que me ha ayudado a mejorar y a cada situación que me ha permitido llegar hasta este momento.

A mi abuela, que fue el pilar fundamental para poder salir adelante como persona; con sus enseñanzas y consejos.

A mis padres que, aunque no estuvieron cerca, me permitieron seguir mis estudios y apoyaron mis ganas de superarme.

A todos los docentes de la carrera de Ingeniería en Teleinformática que, con todo su conocimiento influenciaron mi crecimiento como estudiante, como persona y como profesional

A la Lcda. Sandra Tello Arévalo, cuya ayuda me permitió elaborar y ejecutar mi proyecto de tesis. Al Ing. Mario Pinos Guerra por sus consejos y guía en el proceso de revisión.

A la Universidad de Guayaquil, por reconocer mi esfuerzo y mis logros en la rama estudiantil IEEE y permitir mi formación como un profesional competente.

## **DEDICATORIA**

Quiero dedicar este trabajo de titulación, al esfuerzo de cada una de las personas que estuvieron en este transcurso de tiempo a mi lado; dándome apoyo y fortaleza.

A mis esfuerzos por seguir una meta autoimpuesta, que me permitirá en el futuro crecer en sabiduría y a mi familia.

## ÍNDICE GENERAL

N°	Descripción	Pág.
	<b>INTRODUCCIÓN</b>	<b>1</b>

### CAPÍTULO I EL PROBLEMA

N°	Descripción	Pág.
1.1	Planteamiento del problema	2
1.1.1	Formulación del problema	4
1.1.2	Sistematización del problema	4
1.2	Objetivos de la investigación	5
1.2.1	Objetivo general	5
1.2.2	Objetivos específicos	5
1.3	Justificación	6
1.4	Delimitación del problema	7
1.5	Alcance	8
1.6	Premisa de la investigación	8
1.7	Variables	8
1.7.1	Variables dependientes	8
1.7.2	Variable independiente	8

### CAPÍTULO II MARCO TEÓRICO

N°	Descripción	Pág.
2.1	Antecedentes	10
2.2	Marco Teórico	12
2.2.1	Norma ISO 27001	12

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
2.2.2	Seguridad de la Información	26
2.2.3	Seguridad Informática	29
2.3	Marco Contextual	31
2.4	Marco Conceptual	31
2.4.1	Seguridad	31
2.4.2	Modelo de Seguridad	32
2.4.3	Estándares de Seguridad	32
2.4.4	Concepto de Norma ISO 27001	32
2.4.5	Escalas de Medición	33
2.4.6	Concepto de amenaza	33
2.4.7	Concepto de vulnerabilidad	33
2.4.8	Concepto de riesgo	34
2.4.9	Riesgo operacional	34
2.4.10	Escala de medición de impacto	34
2.4.11	Escala de medición de probabilidad	34
2.4.12	Concepto de hallazgo	34
2.4.13	Plan de procesos	35
2.4.14	Concepto de procedimiento	35
2.5	Marco Legal	35
2.5.1	Instituto Ecuatoriano de Normalización (INEN)	35
2.5.2	Política de Gestión de Activos	36

### **CAPÍTULO III**

### **METODOLOGÍA**

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
3.1	Modelado de la investigación	37
3.2	Enfoque de la investigación	38
3.2.1	Enfoque cuantitativo	39
3.2.2	Enfoque cualitativo	39
3.2.3	Enfoque documental	39

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
3.2.4	Enfoque descriptivo	40
3.2.5	Enfoque evaluativo	40
3.3	Instrumentos de la investigación	40
3.4	Instrumentos de evaluación para la información	40
3.4.1	Evaluación	41
3.4.2	Inspección	41
3.4.3	Comparación	41
3.4.4	Revisión documental	42
3.4.5	Identificación de activos	42
3.4.6	Agrupación de los activos	43
3.4.7	Dimensiones de la valoración	44
3.4.8	Criterios de valoración	44
3.4.9	Valoración de los activos	49
3.5	Identificación de impactos por activo	56
3.5.1	Auditoría realizada en el área de dirección de carrera de Ingeniería en Teleinformática de la Universidad de Guayaquil	58

## **CAPÍTULO IV**

### **DESARROLLO DE LA PROPUESTA**

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
4.1	Definición del plan de procesos de respaldo	67
4.2	Compromiso del área de dirección de carrera	67
4.2.1	Planificación a futuro para un Sistema de Gestión de Seguridad de la Información (SGSI) en la dirección de carrera	68
4.2.2	Criterios de evaluación del tratamiento de la información	69
4.3	Valoración de los procesos de respaldo según la información	70

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
4.3.1	Información privilegiada	72
4.3.2	Información privada	72
4.3.3	Información pública	72
4.3.4	Información interna	72
4.3.5	Información externa	72
4.3.6	Información directa	73
4.3.7	Información indirecta	73
4.4	Selección de controles para la gestión de la información	73
4.4.1	Controles para la gestión de los respaldos de la información	77
4.5	Pasos para el tratamiento del respaldo de la información	83
4.6	Conclusiones	85
4.7	Recomendaciones	86
	<b>ANEXOS</b>	<b>87</b>
	<b>BIBLIOGRAFÍA</b>	<b>97</b>



## ÍNDICE DE TABLAS

<b>Nº</b>	<b>Descripción</b>	<b>Pág.</b>
1	Operacionalización de las variables	9
2	Identificación de activos	43
3	Escala de valores	45
4	Criterios de valoración	46
5	Valoración de activos	50
6	Amenazas por activo	51
7	Identificación de impactos	56
8	Detección de vulnerabilidades por activo	57
9	Gestión de control de base de datos	61
10	Gestión de control de redes	62
11	Gestión de control de inventarios	63
12	Gestión de control de inventarios (seguridad)	64
13	Gestión de control de seguridad	65
14	Impacto de la información	69
15	Cantidad de la información	70
16	Modelo para la ponderación de la información	70
17	Plan de procesos de respaldo de información	73
18	Selección de objetivos de control ISO 27001	77

## ÍNDICE DE FIGURAS

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
1	Estructura de la nueva ISO/IEC 27001:2013	13
2	Top 10 países con certificación ISO 27001	16
3	Evolución de la serie ISO/IEC 27000 y su ramificación	17
4	Características de la nueva ISO/IEC 27001:2013	22
5	Certificados de la norma ISO 27001 por regiones	23
6	Norma ISO 27001 porcentaje de incremento por región	24
7	Incremento en cifras norma ISO 27001 a nivel mundial	25
8	Cantidad de países certificados en Norma ISO 27001	25
9	Enfoques de la investigación	38

## ÍNDICE DE ANEXOS

<b>N°</b>	<b>Descripción</b>	<b>Pág.</b>
1	Objetivos de control de la Norma ISO/IEC 27001:2013	88

**AUTOR:** CAMPOVERDE PAZMIÑO RUBÉN DARIO  
**TEMA:** ELABORACIÓN DE UN PLAN DE PROCESOS DE  
RESPALDO Y DETECCIÓN DE VULNERABILIDADES  
BASADO EN NORMATIVAS ISO:27001  
**DIRECTORA:** LCDA. TELLO ARÉVALO SANDRA ELIZABETH, MG.

## **RESUMEN**

El presente trabajo de titulación tiene como objeto elaborar un plan de procesos de respaldo y el análisis de vulnerabilidades para la implementación del mismo, dentro del área de la carrera de Ingeniería en Teleinformática de la Universidad de Guayaquil. Este plan de procesos permitirá la correcta gestión de la información, mediante una normativa establecida; clara, concreta y que permitirá un respaldo apropiado por medio de niveles de evaluación para la previa clasificación de la información y un plan estratégico de gestión planteado, para establecer las fechas óptimas para el desempeño de las actividades de respaldo. También permitirá gestionar el área de trabajo con un estándar preestablecido para el control de la información; como es la Norma ISO 27001:2013. La automatización de procesos de respaldo conlleva siempre un estudio previo, que le permita a los evaluadores realizar una serie de procesos metódicos que generen a futuro la mejora en las seguridades de la información, con el objetivo de alcanzar la mejora continua que generalmente es aplicada dentro de los procesos de los sistemas de gestión de la seguridad de la información. Es por esto, que se generó un plan de procesos de respaldo (PPR) bajo un estándar internacional que permitirá reducir o mitigar las inconsistencias en los procesos actuales en el tratamiento de la información.

**PALABRAS CLAVES:** ISO 27001, Seguridad, Información, Informática, Plan de procesos, Respaldos, Vulnerabilidades.

**AUTHOR: CAMPOVERDE PAZMIÑO RUBÉN DARIO**  
**SUBJECT: ELABORATION OF A BACKUP PROCESSES PLAN AND**  
**VULNERABILITY DETECTION BASED ON STANDARDS**  
**ISO:27001**  
**DIRECTOR: LCDA. TELLO ARÉVALO SANDRA ELIZABETH, MG.**

### **ABSTRACT**

The purpose of this research work is to develop a backup process plan and the analysis of vulnerabilities for its implementation, in the area of teleinformatics engineering career in the University of Guayaquil. This process plan will allow the correct management of the information, by means of an established; clear and concrete regulation and that will allow an appropriate support by means of evaluation levels for the previous classification of the information and strategic management plan set up, to establish the best dates for the backup activities performance. It will also allow to manage the work area with a pre-set standard to control the information; as it is the ISO 27001:2013 standard. The automation of backup processes always carries out a previous study, that allows the evaluators to carry out a series of methodical processes that generate the improvement in the future information security, in order to achieve the continuous improvement that it is generally applied within the processes of the information security management systems. That is why a backup process plan (BPP) was generated under an international standard that will allow to reduce or mitigate inconsistencies in current processes in the processing of information.

**KEY WORDS:** ISO 27001, Security, Information, Informatics, Process plan, Backup, Vulnerabilities.

## **INTRODUCCIÓN**

La presente investigación se centra en la elaboración de un plan de procesos de respaldo y el análisis de vulnerabilidades de la dirección de la carrera de Ingeniería en Teleinformática de la Universidad de Guayaquil. Para el correcto manejo, uso y respaldo de la información de todas las sub-áreas de trabajo. Así mismo, se plantea una metodología de trabajo y un cronograma de prioridades, que permitirá la correcta gestión en base a las necesidades del área de trabajo.

Capítulo 1: El presente se encuentra titulado como “El problema”, en el mismo se elabora la sistematización, análisis de viabilidad y factibilidad de la propuesta de un plan de procesos de respaldo y detección de vulnerabilidades. Además, se plantean los objetivos con los cuales se desea obtener el resultado más óptimo, su debida justificación, alcance y las variables que podrían afectar la elaboración del proyecto.

Capítulo 2: Se titula Marco Teórico; dentro del capítulo se encontrarán todos los antecedentes que se utilizarán en la investigación para su correcta elaboración y cumplimiento, además de la Norma Internacional en conjunto a su plan de procesos y un marco legal.

Capítulo 3: También llamado Metodología; es donde se encuentran todos los procesos realizados dentro del proyecto como el análisis de vulnerabilidades, levantamiento de información y auditoría del área de trabajo para el cumplimiento de los objetivos y el alcance.

Capítulo 4: Es donde se detalla el proceso del desarrollo de la propuesta y es donde se plantea la resolución, plan de análisis y esquemas de trabajo para el cumplimiento del plan de procesos de respaldo.

## **CAPÍTULO I**

### **EL PROBLEMA**

#### **1.1 Planteamiento del problema**

Según el Instituto Ecuatoriano de Normalización, mediante la norma ISO 27003:2009 define; a la información, sistemas, procesos y redes que la soportan, como activos muy importantes de las entidades o negocios. La definición, el logro, el mantenimiento y la mejora de la seguridad de la información son parte esencial para mantener su alta competitividad. Al igual que, el flujo de caja, la rentabilidad, el cumplimiento de las leyes y la imagen institucional. (NTE INEN-ISO/IEC 27003:2012, 2012)

Las organizaciones, sus sistemas, aplicaciones y redes para el manejo de la información enfrentan constantemente amenazas de seguridad procedentes de una gran cantidad de fuentes, comprendiendo también los fraudes por computador, sabotaje, vandalismo, inundaciones o incendios. Las causas de daño; como los códigos maliciosos o ataques de piratería informática por computador, además de, negación del servicio mejor conocidos como ataques DoS, se han vuelto mucho más comunes.

La seguridad de la información es indispensable para las entidades del sector público y privado, con el fin de resguardar la infraestructura crítica de la información. En ambos sectores, la seguridad de la información actuará como un elemento facilitador, por ejemplo, para lograr, Gobierno en línea (e-government) o negocios electrónicos (e-business) y evitar o mitigar los riesgos. La interconexión de las redes públicas y privadas y compartir los recursos de información incrementan la dificultad para lograr el control del acceso.

La tendencia hacia los sistemas distribuidos de la información también ha debilitado la eficacia del control centralizado y especializado. Muchos sistemas no se han diseñado para ser seguros. La seguridad que se puede lograr a través de los medios técnicos es limitada y debería estar soportada por una buena gestión y por procedimientos apropiados. La identificación de los controles que se deberían establecer; requiere planificación y atención cuidadosa a los detalles. (ISO/IEC 27001, 2015). La gestión de la seguridad de la información requiere, como mínimo, la participación de todos los empleados de una organización. También puede requerir la participación de accionistas, proveedores, terceras partes, clientes u otras partes externas.

De igual modo, puede ser necesaria la asesoría especializada de organizaciones externas. La información es un activo que, como otros activos importantes del negocio, es esencial para las actividades una organización y, en consecuencia, necesita una protección adecuada.

Esto es especialmente importante en el entorno del negocio cada vez más interconectado. Como resultado de esta interconexión creciente, la información se expone a un gran número y variedad de amenazas y vulnerabilidades.

La información puede existir en diversas formas. Se puede imprimir o escribir en papel, almacenar electrónicamente, transmitir por correo o por medios electrónicos, presentar en películas, o expresarse en la conversación. Cualquiera sea su forma o medio por el cual se comparte o almacena, siempre debería tener protección adecuada.

La seguridad de la información es la protección de la misma contra una gran variedad de amenazas, con el fin de asegurar la continuidad del negocio, minimizar el riesgo y así maximizar el retorno de inversiones y oportunidades del negocio.



La seguridad de la información se logra implementando un conjunto apropiado de controles, incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

Estos controles necesitan ser establecidos, implementados, monitoreados, revisados y mejorados, con el fin de asegurar que se cumplan los objetivos específicos de la seguridad y del negocio una organización. Esto debería hacerse en conjunto con otros procesos de gestión del negocio. (Disterer G., 2013)

### **1.1.1 Formulación del problema**

¿En qué beneficiaría la implementación de un plan de procesos de respaldo y la detección de vulnerabilidades al manejo de la información, dentro de la carrera de Ingeniería en Teleinformática?

### **1.1.2 Sistematización del problema**

Hoy en día el correcto manejo de la información, así como los respaldos de la misma son considerados procesos de vital importancia dentro de las organizaciones. Sin embargo, a pesar de su importancia muchas de las instituciones no cuentan con un plan que les permita gestionar y respaldar de una forma óptima la información.

Por esta razón se pretende elaborar un plan de procesos de respaldo y una detección de vulnerabilidades que le permita a la carrera gestionar de forma organizada, detallada y óptima la información que es de vital importancia para la misma.

Dentro de este trabajo de titulación se busca solventar las respuestas a las siguientes interrogantes:

1. ¿Cómo se determina la cantidad de información de una entidad?

2. ¿Qué tipo de información se debe analizar?
3. ¿Cuál es la manera correcta para la valoración de los activos de la información?
4. ¿Qué normativa y qué criterio se utilizará para analizar y elaborar el plan de procesos de este proyecto?
5. ¿Cómo se demostrará la eficacia del plan de procesos y cómo deberá ser aplicado?

## **1.2 Objetivos de la investigación**

### **1.2.1 Objetivo general**

Analizar y elaborar un plan de procesos de respaldo y detección de vulnerabilidades, basado en la Norma ISO 27001, para el correcto manejo y respaldo de la información en la Carrera de Ingeniería en Teleinformática de la Universidad de Guayaquil.

### **1.2.2 Objetivos específicos**

1. Analizar, determinar, ponderar y valorar la cantidad de información.
2. Determinar y planificar el tratamiento de las posibles amenazas y riesgos de los activos de la información.
3. Desarrollar procesos debidos para el control y resguardo del flujo de la información.
4. Establecer una metodología de gestión de la seguridad clara y estructurada.

### 1.3 Justificación

Uno de los activos más valiosos que se encuentran dentro de las organizaciones, es la información y a través del tiempo se presenta una mayor cantidad de amenazas en cuanto a su confiabilidad, confidencialidad y resguardo. Sin embargo, la información es vital para el éxito y sobrevivencia de cualquier entidad en cualquier ámbito.

Es por esto, que el principal objetivo de las organizaciones es el asegurar dicha información, así como también su correcto manejo y utilización.

Para lograr estos objetivos existen normas, procedimientos y estándares que se especializan en el resguardo y seguridad de la información. Dichos estándares se encuentran en la Norma ISO 27000 específicamente dentro de sus ramificaciones especializadas en el manejo y seguridad de la información.

La seguridad no solo es representada a nivel tecnológico sino también físico. Es decir, cada uno de los procesos que se toman como medida de seguridad para respaldar la información física existente, cumplen una función específica para el buen uso y administración de los recursos. (ISO/IEC 27001, 2015)

El análisis de las vulnerabilidades en la seguridad de la información permitirá determinar de manera eficaz las posibles debilidades y amenazas ante la información prioritaria, para que así se pueda asegurar la continuidad del negocio.

Esto permitirá detallar con mayor claridad, cuál será la metodología y el plan de procesos que se implementará para la protección de los activos de la información de un rango amplio de amenazas y minimizar el riesgo de pérdida o mal manejo de los mismos.

La seguridad de los activos de información se logra implementando un correcto conjunto de controles; incluyendo procesos, procedimientos y estructura.

Para realizar un correcto análisis y elaboración de un plan de procesos de respaldo de información se necesita; establecer, implementar, revisar y mejorar los controles y procesos de manejo de la información, para asegurar que se cumplan los objetivos de seguridad pertinente. La correcta gestión de la seguridad de la información debe siempre de apuntar a una estabilidad en los activos.

La estandarización mediante la Norma ISO 27001: “Permite proteger la información en los siguientes términos: (Mejía, 2012)

**Confidencialidad:** Acceso exclusivo para el personal autorizado.

**Disponibilidad:** El usuario y el personal autorizado deben de poder acceder a dicha información en cualquier momento o etapa.

**Integridad:** La información debe de mantener su orden, forma y estructura sin ninguna modificación posterior a la entrega por parte del usuario dueño de la información a menos que este lo preceda.

#### **1.4 Delimitación del problema**

En el presente estudio se tomará en consideración todos los factores detallados anteriormente de los procesos de respaldo y análisis de vulnerabilidades que ofrece la Norma ISO 27001, para realizar el respectivo enfoque y elaboración del plan de procesos que permitirá elevar la seguridad y un mejor manejo de la información logrando hacer del análisis +una fuente de apoyo en el manejo de los activos de información de la Carrera de Ingeniería en Teleinformática.

## **1.5 Alcance**

Dentro del presente proyecto de tesis se realizará:

1. Análisis del uso y tratamiento de la información en la dirección de carrera de Ingeniería en Teleinformática.
2. Detección de vulnerabilidades en el tratamiento de los activos de información.
3. Elaboración de un plan de procesos de respaldo que permitirá el correcto manejo de los activos y su resguardo.

## **1.6 Premisa de la investigación**

En el presente proyecto se demostrará la eficacia y eficiencia en la aplicación de la norma (ISO/IEC 27001, 2015) en la elaboración de un plan de procesos de respaldo y detección de vulnerabilidades, con el cual se desea obtener un mejor manejo en los activos de la información en la carrera de Ingeniería en Teleinformática.

## **1.7 Variables**

### **1.7.1 Variables dependientes**

- Manipulación de la información por terceros.
- Fuga de información.
- Pérdida de información.

### **1.7.2 Variable independiente**

No poseer una norma o estándar internacional de seguridad para el manejo de la información.

**TABLA N°1**  
**OPERACIONALIZACIÓN DE LAS VARIABLES**

VARIABLE	TIPO DE VARIABLE	DEFINICIÓN	CARACTERÍSTICA POR MEDIR	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADOR
No poseer una norma o estándar internacional de seguridad para el manejo de la información.	Independiente	Verificación de los procesos actuales para su valoración	Calidad del manejo de información.	Cualitativo Continuo.	Viabilidad	Excelente Muy bueno Bueno Regular Malo
			Procesos de respaldo.	Cuantitativo Continuo.	Organización	Excelente Muy bueno Bueno Regular Malo
Manipulación de la información por terceros.	Dependiente	Observación del tratamiento de datos personales o de carácter secreto por terceros dentro del ambiente de trabajo.	Categoría de datos.	Mixto Continuo.	Integridad	Excelente Muy bueno Bueno Regular Malo
			Envío de información.	Mixto Continuo.	Disponibilidad	Excelente Muy bueno Bueno Regular Malo
Fuga de información.	Dependiente	Filtrado de información y vulneración de las seguridades actuales por un agente interno o externo.	Ética laboral.	Mixto Continuo.	Responsabilidad	Excelente Muy bueno Bueno Regular Malo
			Compañerismo, trabajo en equipo.	Mixto Continuo.	Comunicación	Excelente Muy bueno Bueno Regular Malo
Pérdida de información.	Dependiente	Mal tratamiento de la información por parte de los encargados de la misma.	Tratamiento de la información.	Mixto Continuo.	Responsabilidad	Excelente Muy bueno Bueno Regular Malo
			Cuidado de la información.	Mixto Continuo.	Respaldo	Excelente Muy bueno Bueno Regular Malo

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

## **CAPÍTULO II**

### **MARCO TEÓRICO**

#### **2.1 Antecedentes**

La presente investigación se orienta a la concepción de una propuesta para la implementación de un plan de procesos de respaldo de información basado en la Norma ISO 27001, para la dirección de carrera de Ingeniería en Teleinformática, siendo necesario conocer la conceptualización científica relacionada con el tema para consolidar una mejor idea en la perspectiva de este proyecto.

En la actualidad la información de todas las entidades u organizaciones tanto académicas como empresariales tiene un alto grado de valor, sin embargo, se suele subestimar o dar poca importancia a la misma, por lo que generalmente es relegada a un segundo plano dentro de las entidades.

Por lo general, el problema de la seguridad se produce por los usuarios o encargados que laboran en las distintas organizaciones, debido a su falta de conocimiento, mala relación en el ambiente laboral, problemas de comunicación, curiosidad por parte de los encargados, etc. Destacando como mayor problema la práctica de otras actividades que no son parte de su actividad laboral.

A esto hay que agregar que, gracias a las Tecnologías de la Información (TI) y al Internet, además de, softwares de última tecnología, se puede acceder remotamente a los dispositivos a cualquier momento del día y a cualquier hora ya que son requeridos para realizar labores que se hacen en el trabajo desde la comodidad del hogar.

Esto genera que la seguridad de la información de todas las organizaciones esté expuestas a niveles muy altos de ataques o amenazas. Ya que, en la mayoría de los casos, no existe un registro o control de las personas que pueden ingresar en los sistemas; ¿Por qué? y ¿Para qué? necesitan acceder a esa información fuera de su horario laboral.

“La nueva forma de trabajar de los usuarios en las organizaciones provoca que los negocios estén cada vez más expuestos a ataques que pueden llegar desde cualquier lugar.” Esto ocurre debido a que generalmente en el área de seguridad de las entidades u organizaciones, el usuario siempre es el eslabón con mayor debilidad. (Acevedo, J., 2015)

A esto se le agrega la falta de ética, interés y colaboración del personal en cuanto al manejo de la información de la organización y la información del usuario o encargado, que, generalmente es colocada por ellos en el mismo equipo o dispositivo que utilizan para realizar sus actividades laborales. Generando así, un filtrado de su información personal y terminando la mayoría de las veces, en problemas de robo o pérdida por parte de otros encargados o usuarios.

La privacidad y la seguridad en Internet son las principales preocupaciones de los usuarios, cada vez que se conectan a la red. Sin embargo, una encuesta realizada por Mozilla revela; que no se sabe cómo gestionar estas dos prioridades: la compañía afirma que un tercio del total siente que no tiene control sobre su información online. Los resultados de la encuesta revelan los pensamientos de 30.000 usuarios de Internet con los que se ha llegado a una conclusión: no se está pendiente de que los elementos de protección (antivirus, antimalware) estén al día y se suele ofrecer datos de forma automática, cada vez que se navega por la red. (Mañero, 2017)

¿Por qué los usuarios tienen tan poco cuidado con su información?



La respuesta del estudio realizado revela; que la ignorancia tecnológica junto a la falta de interés de los usuarios son la causa genérica del problema.

Aproximadamente un 90% de los encuestados declara que la información que poseen sobre su seguridad y la de su información online es insuficiente pero no hacen ni solicitan nada para poder remediarlo. Un tercio de estas personas afirma que no poseen conocimiento alguno de cómo protegerse.

Actualmente existen organizaciones que poseen estándares internacionales cuya finalidad es la de cumplir con los objetivos respectivos al resguardo, manejo y seguridad de la información, como son las Normas ISO, en sus diferentes versiones.

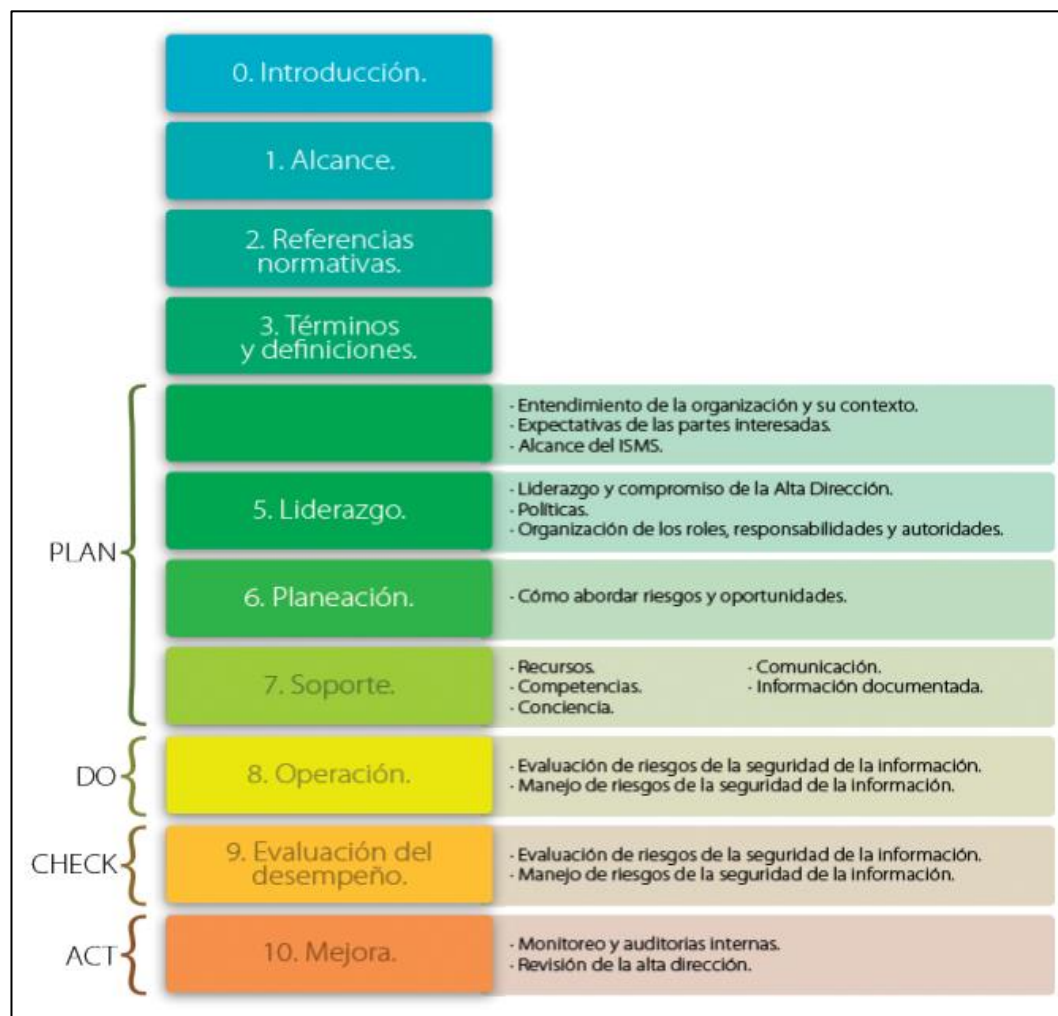
Uno de estos estándares es la Norma Internacional ISO/IEC 27001:2013, que posee todos los parámetros necesarios para elaborar e implementar un plan de procesos de respaldo, analizar sus vulnerabilidades y gestionar las medidas correctivas para el mejor control y manejo de la información aplicando un sistema de gestión y un árbol de procesos.

## **2.2 Marco Teórico**

### **2.2.1 Norma ISO 27001**

Según el portal oficial de la Organización Internacional de Normalización, la norma ISO 27001, es una solución de mejora continua en base a la cual puede desarrollarse un Sistema de Gestión de Seguridad de la Información (SGSI). Este permite evaluar todo tipo de riesgos o amenazas susceptibles de poner en peligro la información de una organización, tanto propia como datos de terceros. (ISOTools, 2015)

**FIGURA N°1**  
**ESTRUCTURA DE LA NUEVA ISO/IEC 27001:2013**



Fuente: <http://www.magazcitum.com.mx/?p=2397#.WNqJjIXhDIU>

Elaborado por: Campoverde Pazmiño Rubén Dario

Además, (ISOTools, 2015) también infiere que, ISO 27001 es una norma internacional que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan. El estándar ISO 27001:2013 para los Sistemas Gestión de la Seguridad de la Información, permite a las organizaciones la evaluación del riesgo y la aplicación de los controles necesarios para mitigarlos o eliminarlos. Su aplicación significa una diferenciación con respecto al resto, ya que mejora la competitividad y a su vez, la imagen corporativa. Siendo esta norma complementada con las buenas prácticas y controles establecidos en la norma ISO 27002.

### **2.2.1.1 ¿En qué consiste la Norma ISO 27001?**

Según el portal de (ISOTools, 2015) la información es la columna vertebral de las organizaciones, por lo tanto, necesita ser convenientemente protegida ante cualquier amenaza o vulnerabilidad que puede poner en peligro la integridad de las empresas, tanto públicas como privadas y de cualquier sector, puesto que, de ser el caso contrario podría quedar seriamente dañada la salud y la integridad empresarial ante el mercado. Un remedio eficiente y eficaz contra estos peligros lo constituye la Norma ISO 27001.

Este enfoque exige, en primer lugar, un análisis y gestión de los riesgos y vulnerabilidades de sistemas de información realista y orientado a los objetivos, metas y porvenir de la organización para posteriormente, evaluar el riesgo y aplicar los debidos controles adecuadamente establecidos por los estándares de la (UNE ISO/IEC 27002, 2007).

Consistentemente la Norma (ISO/IEC 27001, 2015) permite establecer los controles, planes o estrategias más adecuadas para mitigar o eliminar los posibles peligros que se pueden presentar en el manejo de la información y a su vez, permite realizar un respaldo de la misma, con la finalidad de resguardar la información y mitigar los errores del personal encargado de dicha información.

Como generalmente ocurre con todas las Normas ISO, la 27001 maneja un sistema basado en el PHVA enfocado en el ciclo de mejora continua o de Deming conocido también como PDCA por sus siglas en ingles.

### **Evaluación de riesgos según ISO 27001**

El análisis y gestión de los riesgos que se proponen por la ISO 27001 está basado en procesos de negocio y servicios de Tecnologías de la

Información, por tanto, esta norma se convierte en una de las herramientas más útiles para la correcta evaluación y control de una organización con respecto a los riesgos y vulnerabilidades en sus sistemas de información.

Este sistema de gestión de la información está basado en el ciclo de (Planear, Hacer, Verificar, Actuar) con la finalidad de generar, mantener, mejorar gestionar e implementar los Sistemas de Gestión de la Seguridad en la Información, y a su vez, cumplir de manera complementaria a la mejora y respaldo de las buenas prácticas en el ambiente laboral.

#### **2.2.1.2 ISO 27001 en el mundo**

A nivel global, los datos en el año 2017 muestran un aumento constante del número de certificados en ISO 27001 emitidos. En total, se estima que su crecimiento es aproximadamente un 45% con respecto al año anterior.

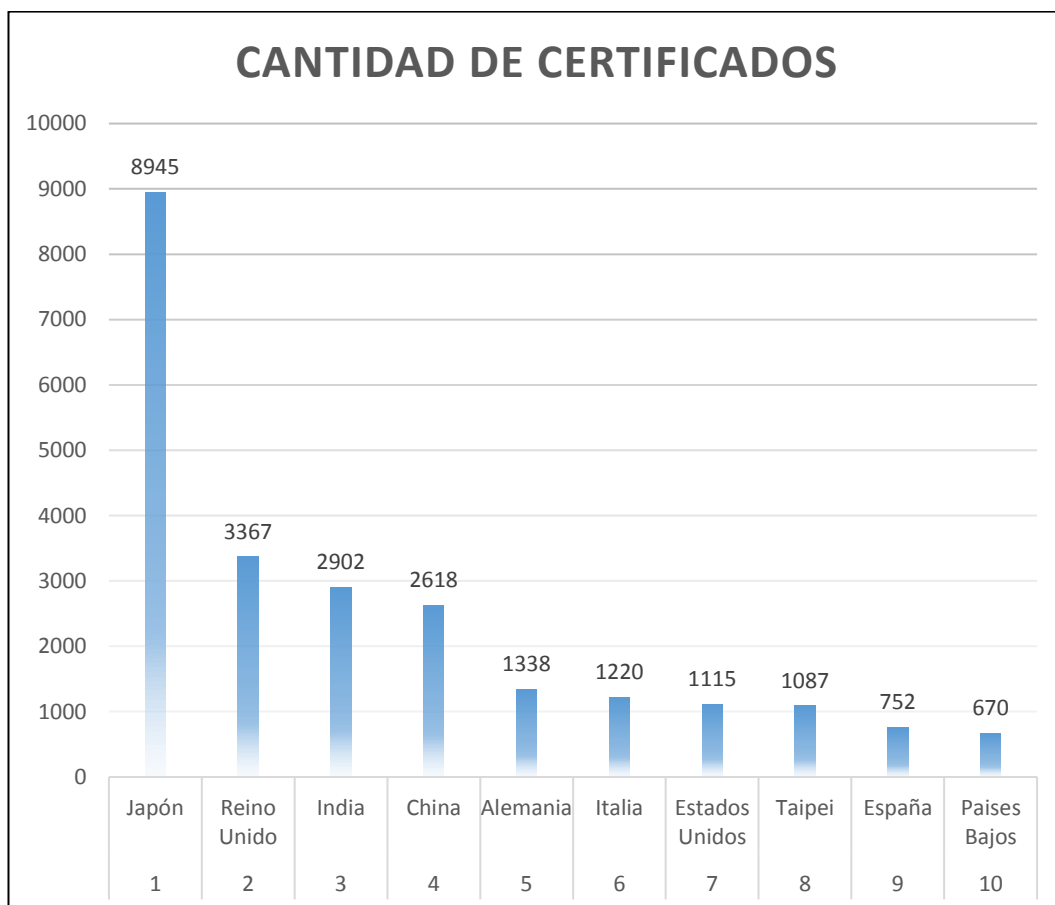
La certificación en Sudamérica ha llevado una progresión creciente, en el año 2006 sólo existían 18 certificados, en 2010 ya eran 117 y en el año 2016 la cifra ascendió a 564 certificados. Esto supuso un incremento del 1,7% en 10 años. (SGSI, ISOTools, 2017).

En Ecuador la única entidad con certificación ISO 27001 es la Corporación Nacional de Telecomunicaciones (CNT). La cual la legitima como una empresa que “dispone de un sistema de Seguridad de la Información conforme a la Norma UNE-ISO/IEC 27001:2007”.

Según (Roberto Almeida, 2015), gerente general de AENOR ECUADOR recalca que: “La CNT sigue siendo la única empresa pública en haber recibido este reconocimiento y se ubica en el tipo de empresas de categoría mundial, que no solo buscan calidad, sino, que se preocupan por la seguridad en la información que manejan”.

En el mundo existe un top de los 10 países con mayor cantidad de certificaciones en ISO 27001, los cuales son:

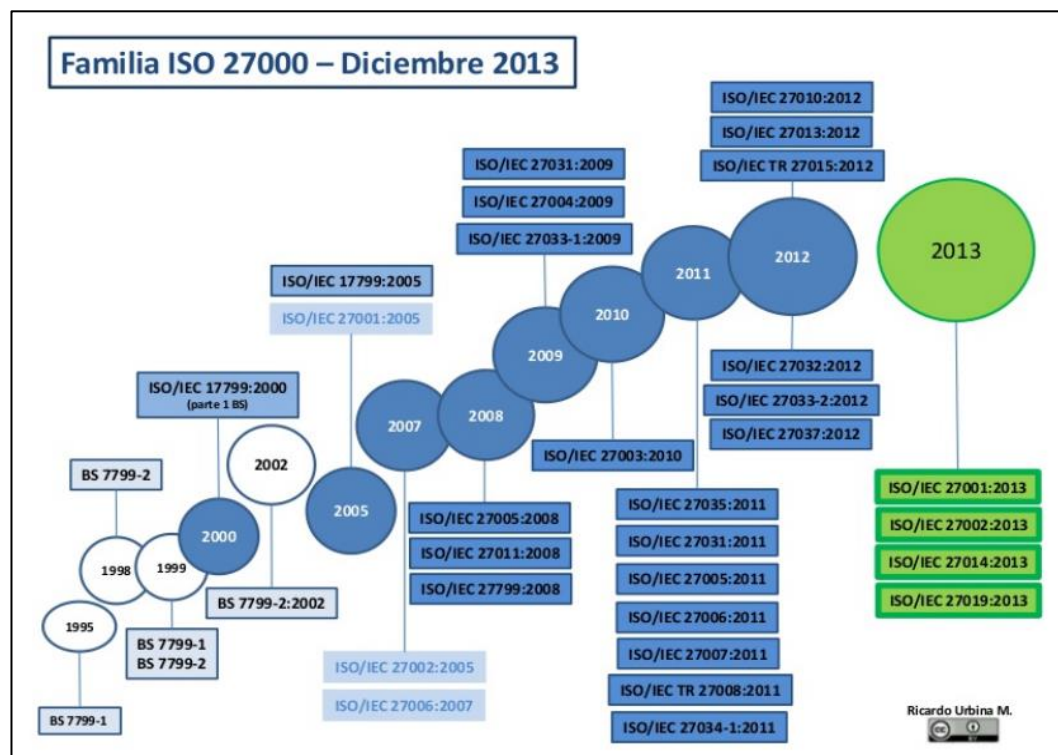
**FIGURA N°2**  
**TOP 10 PAÍSES CON CERTIFICACIÓN ISO 27001**



Fuente: <http://www.pmg-ssi.com/2017/09/situacion-norma-iso-27001-sudamerica/>  
Elaborado por: Campoverde Pazmiño Rubén Dario

Se aprecian en la FIGURA N°2, los países con una mayor cantidad de certificaciones ISO 27001 a nivel mundial, donde se puede observar que, Japón posee la mayor cantidad de certificaciones. Demostrando que la estandarización es parte primordial de su industria y que cumple el objetivo de garantizar uno de los primeros puestos a nivel comercial en el mundo, debido a su eficiencia, eficacia y variedad de mercado.

**FIGURA N°3**  
**EVOLUCIÓN DE LA SERIE ISO/IEC 27000 Y SU RAMIFICACIÓN**



Fuente: <https://www.slideshare.net/RicardoUrbinaM/iso27000estado>

Elaborado por: Campoverde Pazmiño Rubén Dario

En efecto, el objetivo primordial de cada empresa, organización u entidad pública o privada es la seguridad y disponibilidad de su activo más importante que es la información. A su vez, poseer una alta rentabilidad solo pudiendo ser lograda al cumplir con los tres pilares fundamentales para el resguardo de la información como lo son; la disponibilidad, integridad y de la confidencialidad en el manejo de su información.

Se sabe que, en un mundo de cambios constantes en la tecnología, la seguridad y resguardo de la información es una meta dificultosa para todas las entidades, debido al manejo inadecuado de la misma. Debido a esto se precisan nuevos métodos o planes de procesos de seguridad para poder respaldar esa información, ya que, si no es resguardada correctamente podría generar mayores riesgos al momento de transferir la información, originado por el mínimo nivel de protección ante las amenazas y vulnerabilidades que toman la mayoría de entidades.

La consecuencia de la falta de resguardo por lo general se refleja como pérdidas y desventajas en el ambiente competitivo obteniendo un bajo o nulo nivel de tratamiento de la información. Trayendo consigo problemas legales o desaparición en el mercado laboral.

Para un adecuado control y gestión de la información es necesario implementar un plan de procesos con una metodología rigurosa, basado en normas preestablecidas que permitan el fácil y adecuado manejo de la información a todos los miembros de la organización para asegurar la confiabilidad, disponibilidad y seguridad de la información.

La norma ISO mediante su estándar 27001 promueve y promulga la correcta gestión de la seguridad además de su control, respaldo, verificación en cualquier tipo de información.

Se afirma que, la norma ISO 27001 tiene como objetivo primordial: “Mitigar o reducir las vulnerabilidades de una institución con riesgos en la seguridad de la información”.

Un SGSI es un proceso de mejora continua y de gran flexibilidad frente a los cambios que se pueden producir en la empresa refiriéndonos a los procesos de negocio y a la tecnología, ya que ésta avanza a una gran velocidad. (Cardona, 2015)

Por lo tanto, la Norma ISO 27001 posee un marco referencial de gestión de seguridad de toda la información que se maneja dentro de una organización que permite a las distintas entidades generar un árbol de control de procesos de información tanto para su respaldo como para su manejo cotidiano, logrando como objetivo principal el manejo constante de la información de manera segura, integra y con una alta disponibilidad en todas las áreas que sea requerida. La presencia masiva de los sistemas informáticos en la actualidad tan solo en la sistematización de la

información crea un gran agujero de vulnerabilidades, dejando así expuesta información esencial para las actividades dentro de las áreas de trabajo, sin llevar control de los riesgos que se presentan y generan una pérdida.

“El objetivo de la seguridad informática será mantener la Integridad, Disponibilidad, Privacidad (sus aspectos fundamentales) Control y Autenticidad de la información manejada por computadora”. (Aldegani, 1997)

A su vez, la firma de ISMS Forum Spain Empresas Certificadas ISO 27001 expresa que; la certificación del Sistema de Gestión de Seguridad de la información, bajo la norma ISO 27001, permite a una organización posicionarse con un valor añadido en la prestación de sus servicios. En este registro figurarán organizaciones que velan por mantener sus operaciones y la prestación de sus servicios alineados con las buenas prácticas de Seguridad de la Información. Además de brindar la satisfacción a sus usuarios. (D'Antonio, 2007-2016)

La iniciativa se ajusta a los distintos instrumentos estratégicos y normativos dentro de la organización, que permitirán promover la certificación como un mecanismo para la generación de confianza, fiabilidad y gestión de riesgos como pilar del cumplimiento.

El objetivo de esta iniciativa es:

Incentivar una mejora en la imagen de las organizaciones, que han logrado implementar mejores prácticas de Seguridad de la Información, apoyadas en la Norma ISO 27001.

Promover la certificación de los Sistemas de Gestión de Seguridad de la Información para el correcto manejo de los activos de la información en las empresas.



A su vez, ampliar la visión y el reconocimiento de todas las organizaciones certificadas. Con la finalidad de ser conocidas como un referente en las actividades económicas de sus países y difundir la mejora obtenida con su certificación.

Siendo esta, una ventaja comercial para una organización, ya que poseer una Norma ISO ante sus afiliados, en este caso alumnado. Demostrando a los mismos que mantienen su información segura.

La filosofía principal de las Normas ISO en especial la 27001, es controlar y evitar que se generen incidentes de seguridad a gran o pequeña escala. Debido al costo monetario elevado que se podría suscitar y la poca credibilidad que generan estas pérdidas de información.

### **Confidencialidad de la información**

Este proceso permitirá demostrar al usuario o empleado de la entidad, verificar la garantía de la seguridad al momento de acceder a la información, sin divulgar la misma a personas ajenas a la organización.

### **Disponibilidad de la información**

Permite el acceso, gestión y verificación de la información de una entidad, en la mayor brevedad posible. Con la finalidad de que solo el personal o usuarios encargados puedan; actualizar, respaldar y verificar todos los datos útiles para prevenir la pérdida de información.

### **Integridad de la información**

Supone una referencia a toda la información que se encuentra en la organización y que no puede ser alterada por ningún tipo de personal. Para eso se hace necesario poseer un tipo seguridad que ayude a erradicar sucesos de esta índole para el beneficio propio de la empresa.

### **2.2.1.3 Beneficios de la Norma ISO 27001**

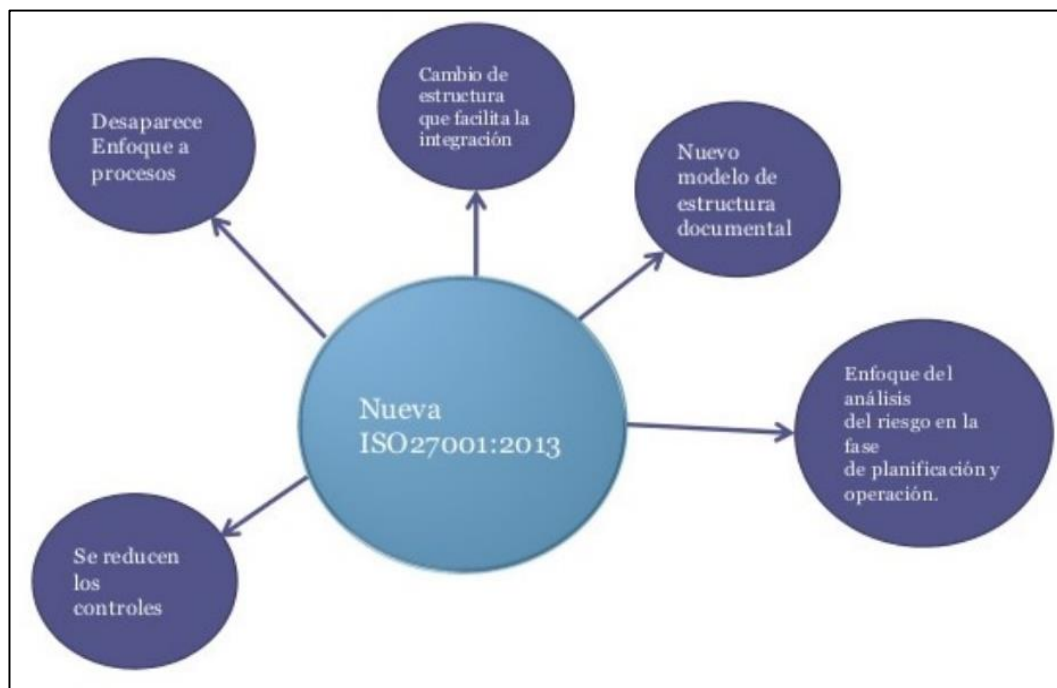
Permite garantizar las buenas prácticas en temas la seguridad de la información, determinando leyes, normas y procesos a seguir. Y así proporcionar ventaja en el cumplimiento de requisitos y convenios con otras empresas o entidades, brindando a sus usuarios una información de forma rápida y eficaz. Además, establece los requisitos para plantear y aplicar con éxito un Sistema de Gestión de Seguridad de la Información o SGSI, evitando de este modo riesgos y mejorando los procesos para el resguardo de la información.

### **2.2.1.4 Características de la Norma ISO 27001**

1. Mejora continua en el plan de procesos del mismo Sistema de Gestión de Seguridad de la Información.
2. Establecimiento de los requisitos para documentación, tratamiento y manejo de la información.
3. Valoración de riesgos potenciales, vulnerabilidades y procedimientos de gestión acorde al modelo de trabajo PHVA.
4. Flexibilidad en el manejo de la información de cada entidad u organización.
5. Determina el compromiso del personal administrativo, corporativo y colectivo de la entidad con la seguridad de la información.
6. Consolidación para la correcta gestión de la seguridad de la información por medio de un planteamiento de alta disponibilidad.
7. Estructura generalizada para la elaboración de procesos de respaldo dentro de un SGSI.

8. Estipular los riesgos dentro de la entidad que estén perfectamente identificados, los cuales serán analizados y gestionados al momento en que se establezcan los procesos.
9. Presencia de una armonía de trabajo con otros estándares ISO para el cumplimiento de requisitos específicos de cada entidad, como pueden ser ISO 9001, ISO 27040 e ISO 14001.

**FIGURA N°4**  
**CARACTERÍSTICAS DE LA NUEVA ISO/IEC 27001:2013**



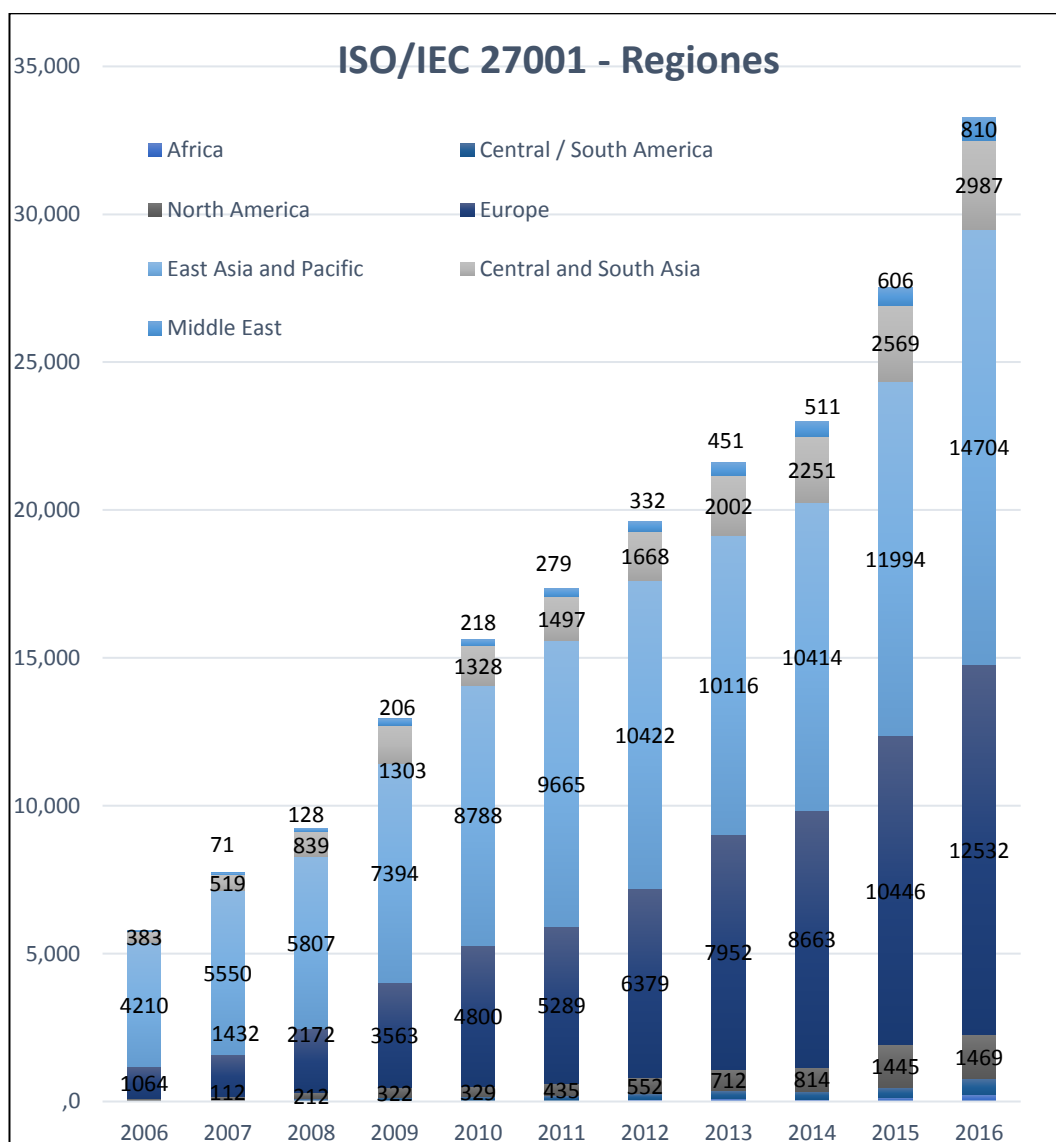
Fuente: <https://es.slideshare.net/georgepereira01/ntc-isoiec-27001-jorge-h-gaviria-y-shernndra-ocampo>

Elaborado por: Campoverde Pazmiño Rubén Dario

#### 2.2.1.5 Importancia de la Norma ISO 27001

La norma ISO 27001 a nivel mundial se ha convertido en la fuente principal de guía para la correcta gestión de la seguridad de la información. Debido a que, una gran cantidad de organizaciones públicas y privadas han sido certificadas a través del cumplimiento en los procesos que realizan en las mismas para la correcta gestión, organización, verificación y mejora en todos los procesos de seguridad de la información.

**FIGURA N°5**  
**CERTIFICADOS DE LA NORMA ISO 27001 POR REGIONES**

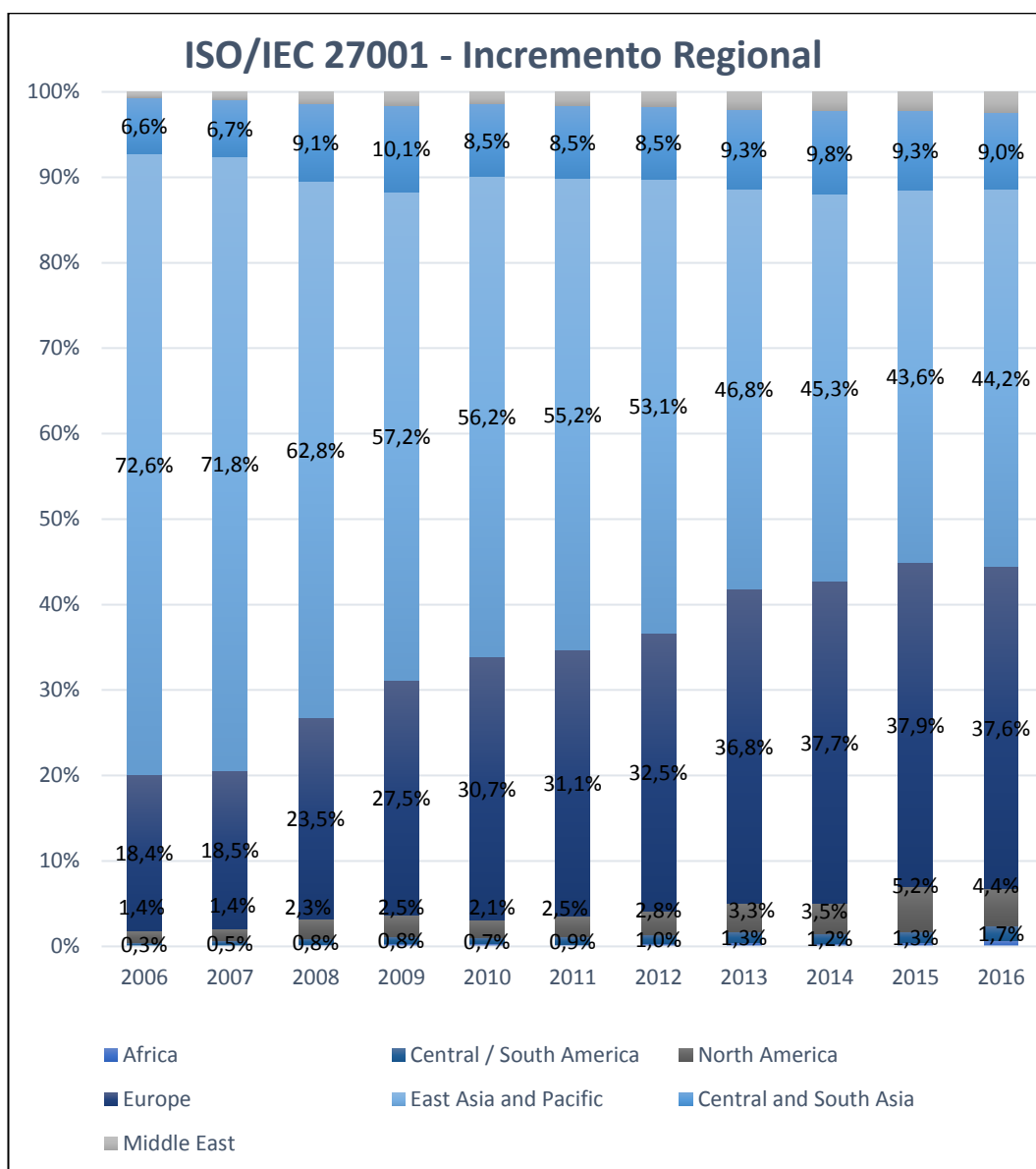


Fuente: [www.isotc.iso.org](http://www.isotc.iso.org)

Elaborado por: Campoverde Pazmiño Rubén Dario

Se puede apreciar en los datos expresados en la FIGURA N°5 que, anualmente se registra un incremento exponencial de certificaciones de la Norma ISO 27001 dando como resultado la veracidad en el valor agregado que proporciona esta normativa a las distintas entidades alrededor del mundo. Además de, la eficacia en el control y cuidado que se genera en cada una de ellas para el manejo de su información; podemos apreciar que, en el año 2016 hay una cantidad de 32.502 certificados en todo el mundo superando por mucho el año 2015.

**FIGURA N°6**  
**NORMA ISO 27001 PORCENTAJE DE INCREMENTO POR REGIÓN**

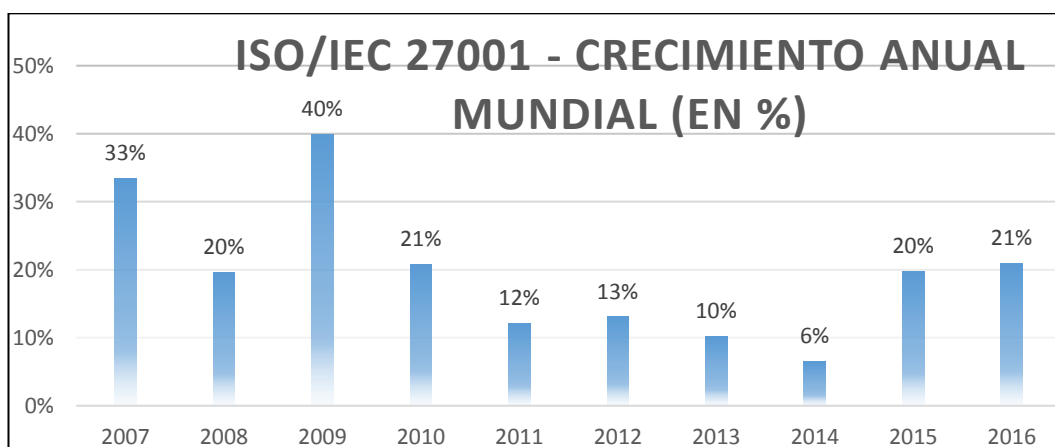


Fuente: [www.isotc.iso.org](http://www.isotc.iso.org)

Elaborado por: Campoverde Pazmiño Rubén Dario

Se aprecia en la FIGURA N°6, el porcentaje de incremento total de la Norma ISO 27001 por regiones, se muestra que en Centro y Sur América hay un crecimiento del 0.3% en el año 2006 pero que exponencialmente empieza a crecer hasta llegar a un total de 1.7% en el año 2016, demostrando así que las distintas organizaciones Latinoamericanas empiezan a consolidar un mercado con ayuda de la norma ISO 27001 dando como apertura otros mercados.

**FIGURA N°7**  
**INCREMENTO EN CIFRAS NORMA ISO 27001 A NIVEL MUNDIAL**

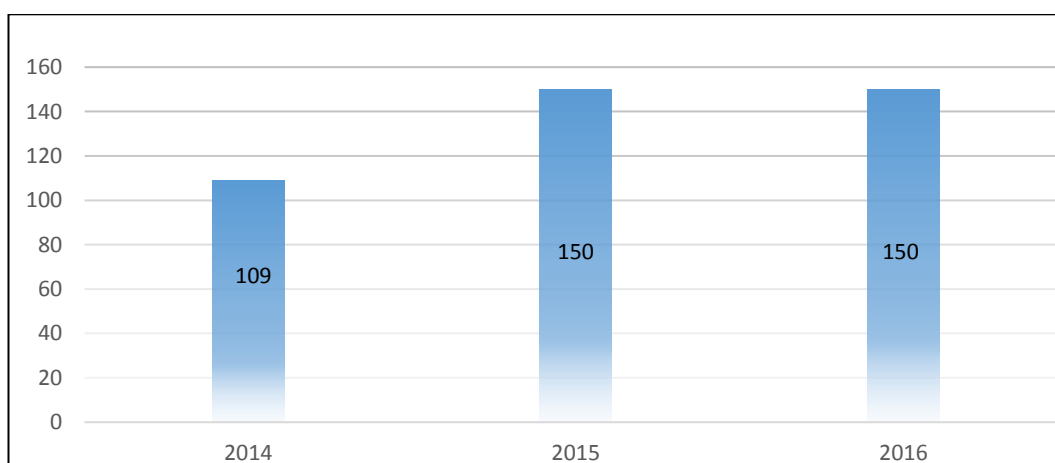


Fuente: [www.isotc.iso.org](http://www.isotc.iso.org)

Elaborado por: Campoverde Pazmiño Rubén Dario

Se aprecia en la FIGURA N°7, el crecimiento que posee la Norma ISO 27001 porcentualmente alrededor del mundo desde el año 2007 hasta el 2016. Se observa que, en dicha figura hay un nivel fluctuante de crecimiento en la norma, esto debido a que la misma con el paso del tiempo ha ido adoptando nuevos procesos en el mejor manejo y tratamiento de la información evolucionando a la par con los nuevos avances tecnológicos y por su puesto el avance de la Norma ISO 27001 como un estándar globalizado.

**FIGURA N°8**  
**CANTIDAD DE PAÍSES CERTIFICADOS EN NORMA ISO 27001**



Fuente: [www.s bqconsultores.es](http://www.s bqconsultores.es)

Elaborado por: Campoverde Pazmiño Rubén Dario

En la FIGURA N°8, podemos observar la cantidad de países que cuentan con una certificación en la Norma ISO 27001 en los años 2014, 2015 y 2016, se puede apreciar que, en el año 2016 no se ha incrementado la cantidad de países con esta norma, debido a que, para que una empresa pueda certificarse dentro de la norma debe de cumplir una cantidad de requisitos estrictamente establecidos y esto hace que dentro de muchos países solo las grandes y medianas entidades cuenten con una certificación como la ISO 27001.

### **2.2.2 Seguridad de la Información**

“Se basa en que la información va mucho más allá de la netamente procesada por equipos informáticos y sistemas; es decir, también abarca aquello que pensamos, que está escrito en un papel, que decimos, etcétera”. (Jara, H., & Pacheco, F., 2012)

“Sin importar su forma o estado, la información requiere de medidas de protección adecuadas de acuerdo con su importancia y criticidad”. (Mendoza, 2015)

También se puede definir como “conjunto de medidas técnicas, organizativas y legales que permiten a la organización asegurar la confidencialidad, integridad y disponibilidad de su sistema de información”. (Mifsud, 20102)

Antes del auge tecnológico y el uso de los sistemas informáticos dentro de las entidades u organizaciones, toda la información era almacenada en grandes bodegas con una estructura de archivadores que permitían la clasificación masiva de información según el tipo y la fecha de ingreso. Gracias a la implementación de estos sistemas se digitalizó la información permitiendo su análisis y proceso de una forma mucho más sencilla.

Pero, a su vez, aparecieron nuevos inconvenientes, ya que a pesar de que se facilitó el transporte de la información, también se generaron muchas posibilidades de la pérdida de la misma en el camino. Debido a que, si es mucho más sencillo acceder a ésta, también se vuelve mucho más sencilla la modificación o alteración del contenido original.

Esto implica que, la seguridad de la información está basada en metodologías, técnicas, herramientas, normas, estructuras, tecnologías, procesos, planes, etc., que son destinados específicamente a la protección y resguardo de la información.

Además, se debe contar con un Sistema de Gestión de Seguridad de la Información (SGSI) para la aplicación y gestión de las medidas de seguridad apropiadas y que se adapten a la entidad u organización.

Expresado de otra manera, la Seguridad de la Información se encarga de regular y declarar las pautas necesarias que deben seguirse para la protección de toda la información dentro de una organización.

Comúnmente la Seguridad de la Información se estructura mediante una Política de Seguridad, la cual se estructura por medio de la elaboración de un Plan Director de Seguridad o una Directriz de Seguridad y está será basada específicamente en la dirección que tiene la organización por medio de sus líneas estratégicas en lo referente a la seguridad y mediante el Plan Director para elaborar las medidas de procesos de tratamiento y respaldo como las técnicas que se utilizarán para ese fin, con la finalidad de poder garantizar los objetivos que se encuentran en la Política de Seguridad.

Los encargados de la gestión de las tácticas y operaciones serán los administradores o encargados de los sistemas y de la seguridad, los cuales deberán implementar las medidas necesarias para que se cumpla la Política de Seguridad.



### 2.2.2.1 Objetivos de la Seguridad de la Información

Los principales objetivos que tiene la seguridad de la información son:

1. Deben ser reportados.
2. Deben estar completamente ligados con las políticas de seguridad de la información.
3. Deben poder ser evaluables siempre que sea posible.
4. Deben resguardar la mayor cantidad o totalidad de la información posible.
5. Deben regirse a una cadena preestablecida de resguardo de información, con la finalidad de poder mantener la integridad de la misma.
6. Deben ser renovados siempre que sea necesario.
7. Deben siempre tener en consideración los requisitos y procesos establecidos, así como también las estrategias y resultados que se obtengan de las evaluaciones y tratamiento de los riesgos.

Para poder alcanzar todos los objetivos, la seguridad de la información se apoya en las normas o estándares establecidos y en la seguridad informática, la cual está regida por directrices orientadas a la seguridad de la información.

Dicho de otra manera, quien regula y da las pautas necesarias que deben de seguirse para la protección de la información es la seguridad de la información mediante su plan estratégico.

### 2.2.3 Seguridad Informática

La seguridad informática se puede definir como: Un conjunto de normas, procesos, procedimientos y herramientas que se encargan de asegurar la integridad, disponibilidad y privacidad de la información dentro de un sistema informático e intentar reducir la cantidad de amenazas que pueden afectar o generar un peligro potencial en el mismo. La seguridad informática intenta resguardar el almacenamiento, procesamiento y transmisión de todo tipo de información digital, así como también la buena práctica del uso de dicha información.

La seguridad informática generalmente abarca dos conceptos fundamentales que son: seguridad lógica y seguridad física.

Dentro de la seguridad lógica se encuentra la aplicación de los procedimientos para proteger el acceso a la información, y que, solo los usuarios encargados de la misma puedan ser autorizadas al acceso.

Sus objetivos son:

1. Controlar el acceso total de los usuarios para su verificación y validación.
2. Evitar que los usuarios no autorizados puedan alterar la información o programas para el manejo de la misma.
3. Garantizar que la información esté siendo utilizada de manera correcta con el plan de procesos adecuado para la gestión de los datos.
4. Garantizar la integridad total de la información al ser enviada y recibida por el usuario correcto sin llegar a manos de un tercero.

5. Garantizar la alta disponibilidad por medio de una estructura organizacional.
6. Mitigar la pérdida de la información cuando sea enviada por vías alternas si llega a existir un fallo en la vía principal.
7. Condicionar el acceso a la información, su uso y alteración.

La seguridad física generalmente en el área de seguridad informática suele ser relegada a un segundo plano en cuanto se realiza un sistema informático. Sin embargo, cuando es tomado en consideración, consiste en la utilización de barreras físicas en conjunto a procesos y planes de control de resguardo, ante las posibles amenazas o peligros a los que se encuentran expuestos los recursos y la información.

Sus amenazas principales son:

- Desastres naturales como tormentas, inundaciones, terremotos, etc.
- Amenazas ocasionadas por el hombre de manera involuntaria.
- Robos, disturbios, fraudes y sabotajes.
- Extracción de información por parte de usuarios internos.
- Atentado contra la ética.

#### 2.2.3.1 Objetivos de la Seguridad Informática

La seguridad informática se define por cinco objetivos principales:

**Integridad:** Consiste en garantizar que los datos no hayan sufrido ningún tipo de alteración al momento de ser enviados o receptados.

**Disponibilidad:** Garantiza que los recursos y la información estén siempre disponibles.

**Confidencialidad:** Se deberá confirmar que el ingreso a los recursos será exclusivamente para aquellas personas que estén debidamente autorizadas.

**No repudio:** Evita que la información que se maneja dentro del área de trabajo pueda ser negada por los usuarios que la manejan, es decir, que se guardará un registro o control de las personas que utilizan la información con la finalidad de resguardar la seguridad de la misma, sin que las personas involucradas puedan negar en el futuro una operación realizada.

**Autenticación:** Es utilizado para la confirmación en la veracidad de la identidad del usuario, es decir, si realmente es la persona que dice ser. Con esto, se busca garantizar que sólo las personas con una previa autorización tengan acceso a los recursos.

## **2.3 Marco Contextual**

Se desea elaborar un plan de procesos de respaldo y el análisis de información para la verificación de vulnerabilidades que le genere a la Carrera de Ingeniería en Teleinformática tener un plan estratégico de respaldo que le permita organizar la información. Mediante la toma de decisiones con una base fundamentada en la Norma ISO 27001:2013 y el análisis de los datos que se obtengan dentro de la dirección de carrera por medio de una entrevista de Auditoría que permita categorizar la información obtenida y priorizarla según la escala de importancia que se haya obtenido.

## **2.4 Marco Conceptual**

### **2.4.1 Seguridad**

El concepto de seguridad se aplica a todos los entornos de la vida cotidiana, de tal manera que, el ser humano siempre se ha visto en la

necesidad de inventar distintos mecanismos que aseguren sus recursos, los cuales, en este caso, viajarán a través de una red informática o un medio de almacenamiento electrónico de forma segura, los cuales deberán llegar a los respectivos receptores sin ser modificados en el proceso de envío.

#### **2.4.2 Modelo de Seguridad**

Los modelos de seguridad generalmente son los mecanismos, procesos, estándares, protocolos, procedimientos o actividades que se generan dentro de un plan de procesos para desarrollar y mantener el control frente a las posibles amenazas que se presentan en una entidad ante los avances del auge tecnológico.

#### **2.4.3 Estándares de Seguridad**

Los estándares de seguridad son la base fundamental que nos proporciona los mecanismos que debemos de seguir para crear un plan estratégico de seguridad en base a políticas y procesos de seguridad previamente establecidos con un alto margen de probabilidad en cuanto a la mejora de los procesos que se posean actualmente dentro de la organización, garantizando que proporcionarán la ayuda necesaria para desempeñar las funciones en distintas áreas.

A su vez, un estándar de seguridad permite llevar un control parcial o total de toda la información dentro de un área de trabajo, generando confianza en el cumplimiento de los compromisos y visión de la institución.

#### **2.4.4 Concepto de Norma ISO 27001**

La Norma ISO 27001, fue creada por la Organización Internacional de Normalización (ISO), la cual detalla la manera en la que se debe gestionar la seguridad de la información para cualquier organización

pública o privada, al ser parte de la familia ISO 27000, marca como punto inicial la elaboración de un SGSI, además de ser la pauta principal para su aplicabilidad en la Norma ISO 27002.

Por consiguiente, al ser una norma internacional, las distintas entidades pueden certificarse para garantizar a sus usuarios que cumplen con todos los estándares y normas internacionales necesarias de seguridad.

#### **2.4.5 Escalas de Medición**

Son procesos que permiten asignar un valor a un elemento a observarse, permitiendo al analista que este elemento se desplace en diferentes escalas para su interpretación e identificación. Por lo tanto, se tomará en consideración los distintos tipos de información para verificar cada vulnerabilidad y amenaza, para poder clasificarla en una matriz de riesgo para su respectivo control.

#### **2.4.6 Concepto de amenaza**

Se conoce como amenaza a todo aquello que pueda generar una posibilidad de que se ocurra un evento, incidente o fenómeno que pueda o no causar daño tanto material como inmaterial sobre un objeto, generalmente causado por un factor externo.

#### **2.4.7 Concepto de vulnerabilidad**

Se define a vulnerabilidad como la incapacidad que posee una entidad u organismo de anticipar, resistir, prever, asimilar y recuperarse de un incidente causado ya sea por una catástrofe natural o un acto humano, ya sea, producido por un factor externo.

#### **2.4.8 Concepto de riesgo**

Se conoce como riesgo a toda posibilidad que pueda producir un contratiempo u incidente y que pueda preceder un gran daño o pérdida de la estructura física, humano o de información.

#### **2.4.9 Riesgo operacional**

Se entiende por riesgo operacional, al riesgo de pérdidas resultantes de la falta de adecuación o fallas en los procesos internos, de la actuación del personal o de los sistemas o bien aquellas que sean producto de eventos externos. El objetivo de la gestión del riesgo operacional es la identificación, evaluación, seguimiento, control y mitigación de este riesgo. (Morgan, 2014)

#### **2.4.10 Escala de medición de impacto**

Esta herramienta tiene como objetivo analizar los elementos observados para prever un posible riesgo con la finalidad de minimizar el impacto que puede generar en el proceso.

#### **2.4.11 Escala de medición de probabilidad**

Es un proceso de medición numérica que se puede encontrar en un intervalo de 0 a 1 o una escala de 1 a 5 que permite observar la posibilidad que ocurra un evento aun poseyendo un plan estratégico de procesos.

#### **2.4.12 Concepto de hallazgo**

Un hallazgo es un proceso de evaluación frente a información evidenciada ya sea novedosa u original de un aspecto escalable entre una debilidad o fortaleza frente a un proceso.

### **2.4.13 Plan de procesos**

Este permite generar, idear o crear el modo o accionar que se va a llevar a cabo por medio de procedimientos o conjuntos de operaciones dentro de un plan estratégico.

### **2.4.14 Concepto de procedimiento**

Se conoce como concepto de procedimiento a la ejecución de una determinada acción, por medio de un proceso consecutivo, estructurado y sistemático, llegando a cumplir de forma metódica el objetivo impuesto desde el inicio del proceso.

## **2.5 Marco Legal**

### **2.5.1 Instituto Ecuatoriano de Normalización (INEN)**

Con el apoyo de varios ministerios e instituciones del sector público, desde el año 2010, se ha procurado definir los lineamientos que regularicen la implementación de SGSI en nuestro país. (Lanche C., 2015)

De esta forma, de acuerdo a la información que se muestra en la página web del Instituto Ecuatoriano de Normalización (INEN), en el periodo 2010-2011 el subcomité técnico de "Tecnologías de la Información" había propuesto al menos siete normas de la familia ISO/IEC 27000 para que sean adoptadas como normativa ecuatoriana, las cuales han sido revisadas por los Ministerios de Telecomunicaciones, Ministerio de Industrias y Productividad, Subsecretaría de Industrias, Productividad e Innovación Tecnológica. (Lanche C., 2015)

Mediante acuerdos ministeriales publicados en el Registro Oficial No. 804 del 29 de julio de 2011 y No. 837 del 19 de agosto de 2011, La



Secretaría Nacional de Administración Pública crea la Comisión para la Seguridad Informática y de las Tecnologías de la Información y Comunicación. Dentro de sus atribuciones tiene la responsabilidad de establecer los lineamientos de seguridad informática, protección de infraestructura computacional, incluyendo la información contenida, para las entidades de la Administración Pública Central e Institucional. En respuesta a esta tarea, la Comisión desarrolla el Esquema Gubernamental de Seguridad de la Información (EGSI) basado en la Norma NTE INEN ISO/IEC 27002. (Lanche C., 2015)

Con estos antecedentes y contando con una normativa nacional vigente, el Gobierno Ecuatoriano, dispone a las entidades de la administración pública central, institucional y que dependen de la función ejecutiva, el uso obligatorio de las normas técnicas ecuatorianas serie NTE INEN-ISO/IEC 27000 para la Gestión de Seguridad de la Información. Esta disposición fue publicada en el Segundo Suplemento del Registro Oficial 088 del 19 de septiembre de 2013. (Lanche C., 2015)

### **2.5.2 Política de Gestión de Activos**

1. Los activos de red deben estar debidamente inventariados.
2. Los equipos de red por ningún motivo serán utilizados con fines personales o didácticos.
3. Se prohíbe la destrucción, adjudicación o modificación deliberada de la información y/o configuración existente en los equipos de red.
4. Los equipos de red no deben ser desconectados o reubicados sin autorización del Propietario del Activo y las Jefaturas.

## **CAPÍTULO III**

### **METODOLOGÍA**

La elaboración de este capítulo tiene como objetivo, expresar de una manera detallada cada uno de los procesos que se llevaron a cabo para el desarrollo de este proyecto. Las distintas metodologías y técnicas empleadas en el mismo, además de los procesos para el tratamiento y análisis de la información.

#### **3.1 Modelado de la investigación**

El proceso con el cual se elaboró el presente proyecto fue una metodología mixta, ya que se necesitó realizar un análisis; cualitativo, cuantitativo, documental, descriptivo y evaluativo para el tratamiento de la información obtenida. Sobre la cual se va a elaborar el plan de procesos de respaldo y con la misma se analizarán las distintas vulnerabilidades por medio de cuestionarios de evaluación en distintos procesos que se llevan a cabo en la dirección de carrera de Ingeniería en Teleinformática.

Por consiguiente, en el análisis realizado para la elaboración del mismo, se utiliza como referencia: Metodología cualitativa, cuantitativa, documental, descriptiva y evaluativa; y a su vez se utilizan cuestionarios de control de auditoría para la obtención de los puntos favorables y desfavorables para el análisis de las vulnerabilidades, ayudando de esta forma a la aplicación de las técnicas de investigación como a la documental y descriptiva. Adquiriendo finalmente una cantidad considerable de datos que fueron analizados mediante una valoración de datos.

Todos los procesos, preguntas y datos realizados y adquiridos se basan fundamentalmente en la norma ISO 27001:2013 con la finalidad de

llevar una guía que permita la ponderación más exacta y eficaz de los datos dentro del presente trabajo de titulación.

### 3.2 Enfoque de la investigación

En el libro “Metodología de la investigación”, detallan que los trabajos de investigación se encuentran sustentados en dos enfoques principales, los cuales son; el enfoque cuantitativo y el enfoque cualitativo, los mismos que de manera conjunta componen un tercer enfoque; El enfoque mixto. (Hernández, Fernández, & Baptista, 2010)

Un enfoque de investigación siempre tiende a variar dependiendo del tipo de investigación que se desea realizar. Está estrechamente ligado al éxito de la misma, la correcta selección de los métodos de evaluación dentro del enfoque de la investigación permitirá la mejora a futuro y que los resultados obtenidos sean más favorables.

**FIGURA N°9**  
**ENFOQUES DE LA INVESTIGACIÓN**



Fuente: <http://normasapa.net>

Elaborado por: Campoverde Pazmiño Rubén Dario

### **3.2.1 Enfoque cuantitativo**

Se hace referencia al enfoque cuantitativo de la investigación al estudio a partir del análisis de cantidades pueden ser estas de información, personas u objetos, es decir, que involucra un proceso de estudio numérico que tiene como objetivo un planteamiento estadístico.

Se utiliza en la recolección de datos para comprobar una hipótesis ya planteada, enfocándose mucho más en la investigación que en el resultado, por eso solo debe de ser aplicado en pequeñas muestras que permitan un resultado claro y conciso de la información obtenida.

### **3.2.2 Enfoque cualitativo**

El enfoque cualitativo se centra en realizar un análisis no estadístico de los datos para la futura formulación de una propuesta. Se basa en el buen juicio del investigador y en este caso del auditor de la información, quien es el que decide de la manera más ideal posible plantear un esquema o estructura de trabajo. Puede interpretarse como un enfoque más subjetivo del estudio del problema, sin embargo, no implica que el auditor pueda afirmar o denegar la información sin un fundamento previo, es por esto, que este enfoque se liga estrechamente a los procesos de las normas ISO 27001:2013, que le permitirán ser una guía lógica y coherente en la toma de decisiones.

### **3.2.3 Enfoque documental**

Se apoya en documentación obtenida directamente en el área o lugar en el que se vaya a realizar la investigación, generalmente se la toma en consideración al momento de analizar el estado actual del área que se desea explorar, y permite obtener datos reales que pueden formar parte importante de la investigación.

### **3.2.4 Enfoque descriptivo**

Mediante este tipo de metodología de la investigación se logrará caracterizar un objeto de estudio para gestionar una situación concreta, es decir, se podrá señalar las características y propiedades en el tratamiento de la información para poder agruparla, ordenarla, clasificarla y sistematizarla con la finalidad de poder detallar de una forma mucho más estructurada la resolución que se debe de adoptar para poder mitigar los problemas en el tratamiento de la información.

### **3.2.5 Enfoque evaluativo**

Este tipo de metodología tiene como objetivo la evaluación de los resultados de las distintas aplicaciones de procesos utilizados dentro de la investigación.

Tiene como objetivo la medición de los efectos que se producen en la aplicación de los distintos procesos para compararlos con los alcances o metas que se proponen, con la finalidad de proponer soluciones para la mejora en una futura ejecución.

## **3.3 Instrumentos de la investigación**

Se conoce a los instrumentos de la investigación como las herramientas que el investigador utiliza para recabar la información que necesita dentro de la muestra seleccionada y así poder plantear una solución sustentable ante el problema.

## **3.4 Instrumentos de evaluación para la información**

Permitirá en la investigación seguir un criterio claro por medio de una auditoría de la información y la ponderación de los datos mediante cinco

criterios, como son: evaluación, inspección, confirmación, comparación y revisión documental.

### **3.4.1 Evaluación**

Consiste en el análisis mediante pruebas de cumplimiento y calidad las actividades que se realizan en una área u organización. Se utilizan para valorar todo tipo de información que se maneje en el área de trabajo.

Esta es aplicada para investigar algún hecho, comprobar algún detalle, verificar el funcionamiento de los procesos, evaluar la aplicación correcta de métodos, técnicas o procedimientos de trabajo, verificar los resultados obtenidos y comprobar la operación correcta del personal encargado de todos los puestos de trabajo dentro de un área.

### **3.4.2 Inspección**

Permite evaluar la eficiencia y eficacia del plan de procesos o del sistema implementado, en cuanto a operaciones y procesamiento de la información para reducir las amenazas o riesgos que se puedan presentar.

Se puede realizar una inspección o cualquier dato, proceso, estrategia, operación, actividad, componente, área de trabajo o trabajador con la finalidad de verificar el cumplimiento óptimo en su estructura o esquema de trabajo.

### **3.4.3 Comparación**

Una de las técnicas más utilizadas en la auditoría de la información y la auditoría en general es la comparación de datos obtenidos en un área de trabajo y cotejar esa información con datos iguales o con características similares de otra área de trabajo que tenga características semejantes.

Se puede realizar una comparación en los resultados obtenidos en el sistema y los datos que se obtienen en el procesamiento manual de la misma información, con el objetivo de determinar si son iguales o si hay alguna posibilidad de modificación de terceros o errores entre los datos.

#### **3.4.4 Revisión documental**

Se utiliza frecuentemente en la revisión de los documentos que sirven como soporte de los registros de operaciones y actividades realizadas por los usuarios encargados del sistema dentro de un área de trabajo o una organización.

Dentro de la revisión se realiza un análisis del registro de actividades y operaciones plasmadas directamente en documentos y archivos formales, con la finalidad de que dentro de la entidad se tenga conocimiento de las acciones realizadas por cada uno de los encargados, resultados u otros aspectos que puedan llevarse a cabo en el desarrollo de las funciones y actividades dentro del área laboral.

Para una correcta ejecución dentro de una revisión documental es común la revisión de manuales, procedimientos, instructivos, funciones y actividades, además de, las políticas y normas planteadas para el control y verificación de los documentos, estadísticas de resultados y la interpretación de los acuerdos que posee cada área de trabajo y su función específica.

#### **3.4.5 Identificación de activos**

Para la obtención de la información e identificación de los activos se solicitó a la dirección de carrera de Ingeniería en Teleinformática de la Universidad de Guayaquil el permiso correspondiente para la obtención de información en los procesos de trabajo dentro del área laboral.

Los activos del área de trabajo dentro de dirección de carrera actualmente son:

**TABLA N°2**  
**IDENTIFICACIÓN DE ACTIVOS**

No.	ACTIVO	USUARIO	FUNCIONES
1	Dirección de Carrera-001	Ing. Miguel Veintimilla	<ul style="list-style-type: none"> <li>Verificación de documentación legal</li> <li>Aprobación de documentos</li> <li>Elaboración de cronogramas de trabajo</li> <li>Planificación de las actividades de la carrera</li> <li>Gestión de las funciones de los docentes</li> <li>Responsable del área de trabajo</li> </ul>
2	Dirección de Carrera-002	Ing. José Ulloa	<ul style="list-style-type: none"> <li>Aprobación de documentos</li> <li>Planificación anual</li> <li>Operatividad de acreditación</li> </ul>
3	Dirección de Carrera-003	Ing. Iván Morejón	<ul style="list-style-type: none"> <li>Planificación anual</li> <li>Planificación de horarios</li> </ul>
4	Secretaría de Dirección	Sra. Xiomara Zambrano	<ul style="list-style-type: none"> <li>Redacción de documentos</li> <li>Manejo de oficios</li> </ul>
5	Secretaría Académica	Sra. María Galarza	<ul style="list-style-type: none"> <li>Recepción de solicitudes de estudiantes</li> <li>Verificación de malla</li> </ul>
6	Secretaría de Titulación	Ing. María Aguilar	<ul style="list-style-type: none"> <li>Manejo de actas</li> <li>Recepción de documentos de titulación</li> </ul>

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

### 3.4.6 Agrupación de los activos

Se clasifica a los activos identificados en la topología de la dirección de carrera y se los agrupa según:

- PC/Laptop
- Equipos de oficina
- Infraestructura de red
- Información



- Aplicaciones

### **3.4.7 Dimensiones de la valoración**

Se considera como la característica o atributo que hace valioso a un activo. Se considera como dimensión a una faceta o aspecto del activo, independientemente de los otros.

Se utilizan para dar un valor a las consecuencias que podría generar una amenaza y tener una escala aproximada o exacta del perjuicio que puede generarse si el activo se ve dañado o modificado según su nivel de importancia.

Para dimensionar la valoración se tomará como base de la escala los siguientes aspectos:

- Disponibilidad [D]
- Integridad [I]
- Confidencialidad [C]

### **3.4.8 Criterios de valoración**

Para la valoración de los activos, se tomarán como referencia los siguientes aspectos dentro de la escala:

1. Escala común utilizada en todas las dimensiones, otorgando una comparativa de los riesgos.
2. Escala logarítmica, enfocada en la diferenciación relativa del valor.
3. Criterio homogéneo que permite una valoración personalizada del área.

Se elige como base una escala detallada con una valoración de 10, donde, el valor de 0 indica lo que sería un valor sin ningún tipo de relevancia.

**TABLA N°3**  
**ESCALA DE VALORES**

VALOR		CRITERIO
<b>10</b>	<b>Muy alto</b>	Daño extremadamente grave al área de trabajo.
<b>7 – 9</b>	<b>Alto</b>	Daño muy grave al área de trabajo.
<b>4 – 6</b>	<b>Medio</b>	Daño importante al área de trabajo.
<b>1 – 3</b>	<b>Bajo</b>	Daño menor al área de trabajo.
<b>0</b>	<b>Ninguno</b>	Ningún daño aparente, irrelevante para efectos prácticos.

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

Comúnmente los activos reciben únicamente un tipo de valoración por cada dimensión en la que se es necesario. Sin embargo, de ser el caso, pueden y deben ser fortificados como en la valoración de la disponibilidad, en la que las consecuencias tienden a variar con respecto al tiempo que pueda durar una interrupción o un corte.

En estos casos, las dimensiones no recibirán una calificación única, sino las que sean consideradas más relevantes al momento de hacer la evaluación de los datos.

Dada la cantidad de mediciones dentro de los criterios de valoración se tomarán ciertos criterios de evaluación, como un punto de referencia, acorde al tipo de información que se maneje; tanto en el área de trabajo como en el resto de áreas que puedan suponer un dato relevante para la medición concreta de los activos de la información.

**TABLA N°4**  
**CRITERIOS DE VALORACIÓN**

VALOR	CRITERIO	
10	[dso]	Posibilidad de un incidente que ocasione daños serios a la eficiencia, eficacia y seguridad operacional dentro del área.
	[dsl]	Posibilidad de un incidente que ocasione daños graves a procesos de alta criticidad de logística o información.
	[sg]	<b>Seguridad:</b> Probabilidad de que sea una incidencia extremadamente seria o que dificulte la revisión e investigación de incidentes que de alto impacto.
	[st]	Posibilidad excepcionalmente grande de una interferencia entre protocolos de trabajo con las demás áreas.
	[dai]	Datos clasificados como alto impacto o secretos.
9	[iat]	Posibilidad de una interrupción prolongada de las actividades dentro del área de trabajo.
	[pna]	Probabilidad de generación de una publicidad negativa por parte del área de trabajo que afecte a las demás, pudieran generar el colapso o cierre de las demás áreas.
	[pef]	Causa de pérdidas económicas o fondos de trabajo.
	[csd]	Causa significativa para despidos dentro del área de trabajo.
	[ini]	Posibilidad de incumplimiento con las normas de trabajo dentro de la institución.
8	[dce]	Datos con clasificación de importancia elevada.
	[pii]	Probabilidad de interrupción ante la investigación de incumplimiento en el área de trabajo.
	[ies]	Incumplimiento altamente elevado de las obligaciones de la seguridad de la información proporcionada por agentes externos del área de trabajo.
	[pis]	Posibilidad de una interrupción seria a las actividades dentro del área de trabajo.
	[ili]	De enorme interés laboral y de relaciones con otras áreas de trabajo de la institución.

7	[plo]	Posibilidad de limitación en las actividades operativas del área de trabajo.
	[pds]	Probabilidad de incidencia que genere daños serios a las actividades de información.
	[psa]	Posibilidad de un daño significativo en las relaciones del área de trabajo con la institución.
	[dcc]	Datos clasificados como confidenciales
	[sg]	<b>Seguridad:</b> Probabilidad de que sea una incidencia grave de seguridad o que dificulte la revisión e investigación de incidentes que puedan ser serios.
6	[ip1]	<b>Información personal:</b> Posibilidad de una incidencia que pueda afectar a un gran grupo de individuos externos al área de trabajo. Estudiantes o cuerpo docente.
	[ip2]	<b>Información personal:</b> Posibilidad de una incidencia que quebrante la ley de protección de información personal de personal interno o externo del área de trabajo.
	[spa]	<b>Seguridad de personas:</b> Probabilidad de daños con un índice considerable de impacto a un individuo dentro del área.
	[cpa]	Causa de presión o manifestación de agentes externos.
	[del]	Datos clasificados como emisión limitada para personal netamente autorizado.
5	[cic]	Posibilidad de una causa que interrumpa una cantidad de actividades propias del área de trabajo que puedan causar impacto en otras áreas.
	[pan]	Probabilidad de acciones que puedan afectar negativamente las relaciones con otras áreas.
	[rel]	Posibilidad de reducción en la eficiencia o seguridad en procesos logísticos o de información fuera del área.
	[ipr]	Impacto posible en las relaciones con autoridades externas.
	[del]	Datos clasificados como emisión limitada para personal netamente autorizado.

4	[ip1]	<b>Información personal:</b> Posibilidad de una incidencia que pueda afectar a un grupo pequeño de individuos. Estudiantes o cuerpo docente.
	[ip2]	<b>Información personal:</b> Posibilidad de una incidencia que quebrante la ley de protección de información personal de personal interno o externo del área de trabajo.
	[spa]	<b>Seguridad de personas:</b> Probabilidad de daños con un índice menor de impacto a un individuo dentro del área.
	[del]	Datos clasificados como emisión limitada para personal netamente autorizado.
	[oii]	Dificultad para la obtención de información que pueda haber generado una incidencia en el área de trabajo.
3	[inr]	Posibilidad de incidencia que afecte negativamente las relaciones internas del área de trabajo.
	[pme]	Posibilidad de mermar la eficiencia de un proceso local dentro del área de trabajo.
	[cip]	Causa de ineficiencia en procesos de cierto interés para otras áreas de trabajo.
	[pri]	Causa de pérdida de respaldo de información con un grado medio de importancia.
	[iol]	Incumplimiento leve de las obligaciones en el manejo de la seguridad de la información proporcionada por agentes externos del área.
2	[pic]	Probabilidad de incidencia que genere una inconformidad o pérdida menor de confianza dentro del área de trabajo.
	[ip1]	<b>Información personal:</b> Posibilidad de una incidencia que pueda causar molestias a un individuo.
	[ip2]	<b>Información personal:</b> Posibilidad de quebrantar levemente la ley de protección de información personal de personal interno o externo del área de trabajo.
	[spa]	<b>Seguridad de personas:</b> Probabilidad de daños con un índice mínimo de impacto a un individuo dentro del área.
	[ngc]	Datos sin ningún nivel o grado de clasificación.

1	[pia]	Posibilidad de causar una interrupción corta a una actividad del área de trabajo.
	[adm]	<b>Administración y gestión:</b> Probabilidad de impedimento operativo de un sector aislado dentro del área de trabajo.
	[ias]	Pudiera causar alguna interrupción mínima al accionar operativo o de seguridad.
	[pic]	Probabilidad de incidencia que genere una inconformidad o perdida menor de confianza dentro del área de trabajo.
	[ngc]	Datos sin ningún nivel o grado de clasificación.
0	[1]	No produce una afección al área de trabajo
	[2]	Posibilidad de una causa que pueda generar inconveniencias mínimas a un individuo del área.
	[3]	No generaría un daño en la imagen o reputación del área de trabajo ante la institución.
	[4]	Supondría perdidas mínimas o ninguna en la gestión de la seguridad de la información.
	[5]	Generaría perdidas casi imperceptibles de fondos económicos.

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

### 3.4.9 Valoración de los activos

Para la valoración de los activos se tomarán datos de todas las tablas previas con el criterio de medición y una debida justificación que permita al encargado del área corroborar la veracidad y efectividad de la valoración para arrojar un resultado claro de los niveles más críticos y puntos clave dentro de la institución que puedan suponer una gran pérdida para el correcto manejo de la información y su seguridad.

**TABLA N°5**  
**VALORACIÓN DE LOS ACTIVOS**

NOMBRE DEL ACTIVO	DISPONIBILIDAD		INTEGRIDAD		CONFIDENCIALIDAD		VALOR TOTAL
	VALOR	JUSTIFICACIÓN	VALOR	JUSTIFICACIÓN	VALOR	JUSTIFICACIÓN	
Dirección de Carrera-001	10	[dso], [dsl]	9	[iat], [pna], [pef], [csd], [ili]	10	[dai], [sg]	10
Dirección de Carrera-002	9	[pna], [iat]	8	[dce], [pii], [pis], [ili]	9	[ini]	9
Dirección de Carrera-003	9	[pna]	8	[dce], [ies], [pis], [ili]	7	[plo], [pds], [dcc]	8
Secretaría de Dirección	7	[plo], [pds], [dcc]	6	[spa]	6	[ip1], [ip2]	6
Secretaría Académica	7	[plo], [pds], [dcc]	6	[spa], [del]	4	[ip1], [ip2]	6
Secretaría de Titulación	7	[plo], [pds], [dcc]	8	[ies], [dce], [ili]	7	[psa], [dcc], [sg]	7

**Fuente:** Investigación Directa

**Elaborado por:** Campoverde Pazmiño Rubén Dario

Dentro de la valoración de los activos de la dirección de carrera de Ingeniería en Teleinformática de la Universidad de Guayaquil, podemos apreciar que todos los activos de esta área representan un pilar crucial para el funcionamiento de la misma y a su vez, podemos estandarizar su funcionamiento y capacidad para agilizar o para interrumpir las funciones que se realizan habitualmente dentro del área de trabajo.

La valoración más baja entre los activos es de 6 siendo este un valor porcentual de índice medio de criticidad al momento de la correcta metodología operacional. En caso de una falla en cualquiera de estos activos podría incrementar su valor de criticidad.

**TABLA N°6**  
**AMENAZAS POR ACTIVO**

VALOR	AMENAZA	VULNERABILIDAD
PC / LAPTOP	Incendio.	Falta de protección contra incendios.
	Inundación.	Falta de protección física ante inundaciones
	Otros desastres naturales.	Condiciones dentro del área de trabajo en la que los recursos son afectados fácilmente por desastres.
	Contaminación.	Falta de mantenimiento preventivo.
	Avería física.	Falta de mantenimiento preventivo.
	Cortes eléctricos.	Falta o mal funcionamiento de UPS.
	Malas condiciones de temperatura.	Funcionamiento inadecuado del sistema de aire acondicionado o calefacción.
	Fallo en mantenimiento en hardware.	Falta de supervisión.
	Fallos de mantenimiento en software.	Falta de supervisión en el proceso de actualización o tratamiento inadecuado.
	Robo.	Falencia en la protección de la integridad física.



EQUIPOS DE OFICINA	Incendio.	Falta de protección contra incendios.
	Inundación.	Falta de protección física ante inundaciones
	Otros desastres naturales.	Condiciones dentro del área de trabajo en la que los recursos son afectados fácilmente por desastres.
	Contaminación.	Falta de mantenimiento preventivo.
	Avería física.	Falta de mantenimiento preventivo.
	Cortes eléctricos.	Falta o mal funcionamiento de UPS.
	Malas condiciones de temperatura.	Funcionamiento inadecuado del sistema de aire acondicionado o calefacción.
	Fallo en mantenimiento.	Falta de supervisión.
	Errores en la selección de los equipos necesarios.	Falta de supervisión en el proceso de actualización en el área de trabajo.
	Robo.	Falencia en la protección de la integridad física.

INFRAESTRUCTURA DE RED	Incendio.	Falta de protección contra incendios.
	Inundación.	Falta de protección física ante inundaciones
	Otros desastres naturales.	Condiciones dentro del área de trabajo en la que los recursos son afectados fácilmente por desastres.
	Contaminación.	Falta de mantenimiento preventivo.
	Avería física.	Falta de mantenimiento preventivo.
	Cortes eléctricos.	Falta o mal funcionamiento de UPS.
	Malas condiciones de temperatura.	Funcionamiento inadecuado del sistema de aire acondicionado o calefacción.
	Fallo en mantenimiento en la red.	Falta de supervisión.
	Fallos de mantenimiento en los protocolos.	Falta de supervisión en el proceso de actualización del estándar de protocolos.
	Degradación.	Falencia en la protección de la integridad física.

<b>INFORMACIÓN</b>	Ingreso de archivos maliciosos.	Falta de supervisión.
	Ingreso de información errónea.	Desconocimiento en el manejo del sistema.
	Eliminación de información.	Falta de supervisión.
	Degeneración de la información.	Falta de respaldo.
	Manejo incorrecto de la información.	Falta de un sistema de control.
	Pérdida de información.	Falta de un sistema de archivado.
<b>APLICACIONES</b>	Error del administrador.	Falta de conocimiento del administrador del sistema.
	Error de usuarios.	Falta de capacitación de las aplicaciones para su correcto funcionamiento.
	Error de monitoreo y control(log).	Incapacidad o nulidad de las aplicaciones de monitoreo.
	Ingreso de información errónea.	Desconocimiento en el manejo de la aplicación.

	Fallos de mantenimiento en software.	Falta de supervisión en el proceso de actualización o tratamiento inadecuado.
	Denegación de servicios.	Incapacidad de discernir una solicitud real o una falsa.
	Declive o caída del sistema por ataques.	Falta de protección ante ataques hacia las aplicaciones del sistema.
	Declive del sistema por extenuación de recursos.	Exceso en el uso de las aplicaciones que pueden generar una sobrecarga al sistema.

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

### 3.5 Identificación de impactos por activo

La identificación de los impactos que se pueden generar dentro de un área de trabajo nos permitirá establecer la criticidad del impacto; la medida preventiva y la medida preventiva en el caso de no poder evitar la incidencia. Se debe tomar en consideración como impacto a todo hecho que pueda preceder o no algún tipo de repercusión positiva o negativa en el funcionamiento de los procesos del área de trabajo.

Se consideran 3 grupos de impactos ordenados según las consecuencias que reduzcan el estado de seguridad del activo que haya sido atacado. (ISOTools Excellence, 2015) Dentro de estos tenemos los siguientes:

**TABLA N°7**  
**IDENTIFICACIÓN DE IMPACTOS**

<b>IMPACTO CUANTITATIVO</b>	
<b>L1</b>	Pérdida intangible de fondos patrimoniales.
<b>L2</b>	Responsabilidad penal por incumplimiento de obligaciones legales.
<b>L3</b>	Alteración en la situación administrativa.
<b>L4</b>	Daño a personas.
<b>IMPACTO CUALITATIVO CON PÉRDIDAS ORGÁNICAS</b>	
<b>N1</b>	Pérdida de valor económico.
<b>N2</b>	Pérdida económica indirecta.
<b>N3</b>	Pérdida económica por interrupción operacional.
<b>N4</b>	Pérdidas asociadas a responsabilidad legal.
<b>IMPACTO CUALITATIVO CON PERDIDAS FUNCIONAL</b>	
<b>[A]</b>	Autenticación.
<b>[D]</b>	Disponibilidad.
<b>[C]</b>	Confidencialidad.
<b>[I]</b>	Integridad.

Fuente: <http://www.pmg-ssi.com>

Elaborado por: Campoverde Pazmiño Rubén Dario

### 3.5.1 Auditoría realizada en el área de dirección de carrera de Ingeniería en Teleinformática de la Universidad de Guayaquil

**TABLA N°8**  
**TABLA DE RIESGOS POR ACTIVO**

VALOR	RIESGO	IMPACTO	TIPOS DE CONSECUENCIAS		
			CUANTITATIVAS	CUALITATIVAS	FUNCIONALES
PC / LAPTOP	Incendio.	Reducción de disponibilidad	L1, L2	N3	[D]
	Inundación.	Reducción de disponibilidad	L1, L2	N3	[D]
	Otros desastres naturales.	Reducción de disponibilidad	L1, L2	N3	[D]
	Contaminación.	Reducción de disponibilidad	L1, L2	N3	[D]
	Avería física.	Reducción de disponibilidad	L1, L2	N3	[D]
	Cortes eléctricos.	Reducción de disponibilidad	L1, L2	N3	[D]
	Malas condiciones de temperatura.	Reducción de disponibilidad	L1, L2	N3	[D]
	Fallo en mantenimiento en hardware.	Reducción de disponibilidad e integridad	L1, L2, L3	N1, N4	[D], [I]

EQUIPOS DE OFICINA	Incendio.	Reducción de disponibilidad	L1, L2	N3	[D]
	Inundación.	Reducción de disponibilidad	L1, L2	N3	[D]
	Otros desastres naturales.	Reducción de disponibilidad	L1, L2	N3	[D]
	Contaminación.	Reducción de disponibilidad	L1, L2	N3	[D]
	Avería física.	Reducción de disponibilidad	L1, L2	N3	[D]
	Cortes eléctricos.	Reducción de disponibilidad	L1, L2	N3	[D]
	Malas condiciones de temperatura.	Reducción de disponibilidad	L1, L2	N3	[D]
	Fallo en mantenimiento.	Reducción de disponibilidad e integridad	L1, L2, L3	N1, N4	[D], [I]
INFRAESTRUCTURA DE RED	Incendio.	Reducción de disponibilidad	L1, L3	N1, N3	[D]
	Inundación.	Reducción de disponibilidad	L1, L3	N1, N3	[D]
	Otros desastres naturales.	Reducción de disponibilidad	L1, L3	N1, N3	[D]
	Contaminación.	Reducción de disponibilidad	L1, L2	N3	[D]

	Avería física.	Reducción de disponibilidad	L1, L2	N3	[D]
	Cortes eléctricos.	Reducción de disponibilidad	L1, L2	N3	[D]
	Malas condiciones de temperatura.	Reducción de disponibilidad	-	-	[D]
	Fallo en mantenimiento en la red.	Reducción de disponibilidad e integridad	L2, L3	N3, N4	[D], [I]
	Fallos de mantenimiento en los protocolos.	Reducción de disponibilidad	L2, L3	N3, N4	[D], [I]
	Degradación.	Reducción de disponibilidad	L3	N1, N2	[D]
INFORMACIÓN	Ingreso de archivos maliciosos.	Reducción de autenticación y disponibilidad	L2, L3, L4	N1, N3, N4	[A], [D]
	Ingreso de información errónea.	Reducción de integridad	L1, L2	N3	[I]
	Eliminación de información.	Reducción de disponibilidad	L1, L2	N1	[D]
	Degeneración de la información.	Reducción de integridad	L2	N3	[I]
	Manejo incorrecto de la información.	Reducción de disponibilidad e integridad	L1, L2, L3	N3, N4	[D], [I]
	Pérdida de información.	Reducción de disponibilidad	L1, L2,	N3	[D]




APLICACIONES	Error del administrador.	Reducción de disponibilidad, confidencialidad e integridad	L2	N4	[D], [C], [I]
	Error de usuarios.	Reducción de disponibilidad e integridad	L1, L3	N3	[D], [I]
	Error de monitoreo y control(log).	Reducción de confidencialidad	L2	N4	[C]
	Ingreso de información errónea.	Reducción de integridad	L2, L4	N3, N4	[I]
	Fallos de mantenimiento en software.	Reducción de disponibilidad e integridad	L2, L3	N3, N4	[D], [I]
	Denegación de servicios.	Reducción de disponibilidad	L3	N3	[D]
	Declive o caída del sistema por ataques.	Reducción de autenticación, disponibilidad, confidencialidad e integridad.	L1, L2, L3, L4	N3, N4	[A], [D], [C], [I]
	Declive del sistema por extenuación de recursos.	Reducción de disponibilidad, confidencialidad e integridad.	L1, L2, L3	N3, N4	[D], [C], [I]

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario


**TABLA N°9**  
**GESTIÓN DE CONTROL DE BASE DE DATOS**

	<b>CUESTIONARIO DE CONTROL AUDITORÍA</b> <b>PLAN DE PROCESOS</b>			
<b>INSTITUCIÓN:</b> Facultad De Ingeniería Industrial – Ingeniería En Teleinformática			<b>APP-BD</b>	
<b>CUESTIONARIO DE CONTROL DE BASE DE DATOS</b>			<b>TI-001</b>	
<b>DOMINIO</b>		BASE DE DATOS		
<b>PROCESO</b>		SEGURIDAD DE LA INFORMACIÓN		
<b>OBJETIVO DE CONTROL</b>		SEGURIDAD DE LA INFORMACIÓN BASE DE DATOS		
<b>CUESTIONARIO</b>				
<b>PREGUNTA</b>		<b>SI</b>	<b>NO</b>	<b>N/A</b>
¿Cuenta con algún archivo de tipo Log donde se guarde información de las operaciones realizadas en la Base de datos?		X		
¿En el caso de manejar archivos de tipo Log, maneja algún servidor que los respalde?		X		
¿Realizan copias de seguridad del BD (diariamente, semanalmente, mensualmente, etc.)?				X
¿Algún otro usuario externo tiene asignado el rol de Administrador de la BD del servidor?		X		
¿Tiene conocimiento alguno de si el administrador de la BD lleva un control de usuarios?				X
¿Los perfiles de usuario son gestionados y asignados por el administrador de la BD?		X		
¿Son gestionados los accesos a las instancias de la BD?		X		
¿Las instalaciones que contienen el repositorio de la BD, tienen acceso restringido?		X		
¿Las claves de los usuarios de la BD son renovadas en un periodo determinado?			X	
¿Existe alguna política para gestionar el cambio de clave?			X	
¿Se encuentra un listado de todos los accesos no satisfactorios o denegados a la BD?			X	
¿Posee la BD un diseño físico y lógico?		X		
¿Existe una instancia con copia temporal de la BD para el entorno de trabajo?		X		
¿Posee algún método de encriptado para el resguardo de la BD?		X		
¿Cuándo se necesita modificar o restablecer la BD, se le comunica al administrador?		X		
¿Se documentan los cambios efectuados en la BD?		X		
¿Hay algún procedimiento para dar de baja a un usuario?			X	
¿Existe un periodo de tiempo determinado para dar de baja un usuario?			X	
<b>TOTAL</b>		<b>11</b>	<b>5</b>	<b>2</b>

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario


**TABLA N°10**  
**GESTIÓN DE CONTROL DE REDES**

	<b>CUESTIONARIO DE CONTROL AUDITORÍA</b> <b>PLAN DE PROCESOS</b>			
<b>INSTITUCIÓN:</b> Facultad De Ingeniería Industrial – Ingeniería En Teleinformática			<b>APP-RC</b>	
<b>CUESTIONARIO DE CONTROL DE REDES DE COMUNICACIÓN</b>			<b>TI-002</b>	
<b>DOMINIO</b>		REDES Y COMUNICACIONES		
<b>PROCESO</b>		INSTALACIÓN Y DISEÑO DE REDES		
<b>OBJETIVO DE CONTROL</b>		EVALUACIÓN DE LAS REDES DE COMUNICACIÓN		
<b>CUESTIONARIO</b>				
<b>PREGUNTA</b>		<b>SI</b>	<b>NO</b>	<b>N/A</b>
¿Se gestiona la infraestructura de la red en base a las necesidades de la carrera?			X	
¿Los enlaces de la red son testeados frecuentemente?			X	
¿Los equipos como patch panel o routers cumplen los requisitos básicos de los estándares 568-A y 568-B?			X	
¿Cuentan con la aplicación de un código de colores para facilitar la identificación de los puntos de red?			X	
¿El cableado estructurado del interior del edificio se encuentra dentro de canaletas o conductos?				X
¿Cuenta con firewall físico para la protección y aseguramiento de la red?			X	
¿Las direcciones IP'S de los equipos son implementados de manera estática?			X	
¿Se cuenta con una conexión a tierra física para la protección de los equipos que puedan ser afectados por posibles descargas eléctricas?			X	
¿Cuenta con dispositivos para la regulación del voltaje?			X	
¿Los dispositivos se encuentran instalados en áreas que cumplen con las temperaturas adecuadas para su correcto funcionamiento?		X		
¿Se encuentra en la red un modelo de balanceo de cargas implementado?				X
¿Dentro de la red, se utilizan protocolos de autenticación, como está establecido en el estándar IEEE 802.11?		X		
¿Posee usted una administración interna de la red? Es decir, ¿Cuenta con VLAN's creadas dentro del servidor para tener una mayor administración en cada área que se dedica a diferentes actividades?			X	
¿Cuenta con un análisis de vulnerabilidades en la implementación y configuración de los dispositivos de red?			X	
¿Posee documentos que acrediten que la red se encuentra estandarizada?			X	
Documentos probatorios presentados:			X	
<b>TOTAL</b>		<b>2</b>	<b>12</b>	<b>2</b>

**Fuente:** Investigación Directa

**Elaborado por:** Campoverde Pazmiño Rubén Dario


**TABLA N°11**  
**GESTIÓN DE CONTROL DE INVENTARIOS**

	<b>CUESTIONARIO DE CONTROL AUDITORÍA</b> <b>PLAN DE PROCESOS</b>			
<b>INSTITUCIÓN:</b> Facultad De Ingeniería Industrial – Ingeniería En Teleinformática			<b>APP-IN</b>	
<b>CUESTIONARIO DE CONTROL DE INVENTARIO</b>			<b>TI-003</b>	
<b>DOMINIO</b>		ADQUISICIÓN E IMPLEMENTACIÓN		
<b>PROCESO</b>		ADQUIRIR Y MANTENER LA ARQUITECTURA TECNOLÓGICA		
<b>OBJETIVO DE CONTROL</b>		EVALUACIÓN DE NUEVO HARDWARE		
<b>CUESTIONARIO</b>				
<b>PREGUNTA</b>		<b>SI</b>	<b>NO</b>	<b>N/A</b>
¿Cuenta con un inventario de todo tipo de dispositivos o recursos que integran el área de trabajo?		X		
¿Se revisa seguido el inventario?		X		
¿Posee una bitácora de fallas detectadas en los recursos adquiridos?				X
¿En el caso de no poseer una bitácora, estaría dispuesto a adquirir una?		X		
<b>CARACTERÍSTICAS DE LA BITÁCORA (SELECCIONE LAS OPCIONES).</b>				
¿Posee un personal especializado para la verificación de la bitácora?		X		
¿Es señalada la fecha de detección de la falla?		X		
¿Señala la fecha de revisión y corrección de la falla de los dispositivos o recursos?			X	
¿Posee un registro individual de los dispositivos y recursos?		X		
¿La bitácora hace referencia a hojas de servicio, donde se detallan las fallas, causas de origen y refacciones utilizadas?				X
¿Existe algún plan o programa de mantenimiento para los equipos del área de trabajo?			X	
¿Cuenta con un equipo de mantenimiento para todos los equipos?			X	
¿Realiza una inspección y mantenimiento preventivo de los equipos frecuentemente?		X		
¿Existe algún tipo de plan para el reciclado de los equipos que terminan su vida útil?			X	
¿Utiliza criterios de evaluación para la adquisición de los recursos y dispositivos?			X	
¿Posee documentos que certifiquen la garantía y correcto funcionamiento de los equipos?			X	
¿El área de trabajo fue diseñada específicamente para la estructura de trabajo actual?				X
¿Se tomó en consideración una distribución del espacio adecuada para la facilitación del trabajo?			X	
¿Existen lugares dentro del área de trabajo con acceso restringido?			X	
¿Se cuenta con un sistema de emergencia como detectores de humo, alarmas u otros sensores?			X	
Documentos probatorios presentados:			X	
<b>TOTAL</b>		<b>7</b>	<b>10</b>	<b>3</b>

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario


**TABLA N°12**  
**GESTIÓN DE CONTROL DE INVENTARIOS (SEGURIDAD)**

	<b>CUESTIONARIO DE CONTROL AUDITORÍA PLAN DE PROCESOS</b>		
<b>INSTITUCIÓN:</b> Facultad De Ingeniería Industrial – Ingeniería En Teleinformática		<b>APP-IS</b>	
<b>CUESTIONARIO DE CONTROL DE INVENTARIO</b>		<b>TI-004</b>	
<b>DOMINIO</b>	<b>ENTREGA DE SERVICIOS Y SOPORTES</b>		
<b>PROCESO</b>	<b>ADMINISTRACIÓN DE INSTALACIONES</b>		
<b>OBJETIVO DE CONTROL</b>	<b>INSTALACIONES, ADECUACIONES Y SEGURIDAD</b>		
<b>CUESTIONARIO</b>			
<b>PREGUNTA</b>	<b>SI</b>	<b>NO</b>	<b>N/A</b>
¿Se cuenta con un sistema de seguridad que impida el acceso a lugares restringidos a personal no autorizado?		X	
¿Existen señalizaciones adecuadas en las salidas de emergencia y rutas de evacuación?	X		
¿Poseen medios adecuados para la extinción de fuego dentro del área de trabajo?	X		
¿Posee iluminación adecuada e iluminación de emergencia en el caso de que se presente una contingencia?		X	
¿Poseen sistemas de seguridad para evitar la sustracción de los equipos dentro del área de trabajo?		X	
¿Se tiene asignado un lugar para papelería y utensilios de trabajo?		X	
¿Existen prohibiciones de ingesta de bebidas o consumo de alimentos dentro del área de trabajo?	X		
¿Se limpia frecuentemente el área de trabajo?	X		
¿Poseen algún sistema para el control de acceso del personal externo?		X	
¿Poseen un sistema o equipos de control ambiental?		X	
¿Se tiene un contrato de mantenimiento para los equipos de control ambiental?		X	
¿Se tienen instalados y limpian periódicamente los filtros de aire?	X		
¿Existe un plan de contingencia en el caso de que se suscite un fallo en los controles ambientales?		X	
¿Se cuentan con políticas definidas para dar de baja los elementos informáticos que finalizan su vida útil?	X		
¿La instalación eléctrica fue establecida específicamente para el área de trabajo?			X
¿Se cuenta con una instalación eléctrica alterna que permita a los equipos de cómputo seguir funcionando en caso de la red eléctrica principal?		X	
¿Existe un panel de control central donde llegue la acometida eléctrica?	X		
¿Dentro del panel de control se tomó en consideración una futura expansión?			X
¿La instalación eléctrica del área de trabajo es independiente?		X	
¿Se cuenta con protección en caso de un corto circuito?		X	
¿Posee medidas implementadas ante la falla del sistema de seguridad?		X	
¿Se tiene un registro de ingreso de las personas que ingresan al área de trabajo?		X	
<b>TOTAL</b>	<b>7</b>	<b>13</b>	<b>2</b>

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

**TABLA N°13**  
**GESTIÓN DE CONTROL DE SEGURIDAD**

		<b>CUESTIONARIO DE CONTROL AUDITORÍA</b> <b>PLAN DE PROCESOS</b>		
<b>INSTITUCIÓN:</b> Facultad De Ingeniería Industrial – Ingeniería En Teleinformática				<b>APP-IS</b>
<b>CUESTIONARIO DE CONTROL SEGURIDAD LÓGICA E</b> <b>INFORMÁTICA</b>				<b>TI-005</b>
<b>DOMINIO</b>		MANEJO DE INFORMACIÓN Y ELEMENTOS		
<b>PROCESO</b>		SEGURIDAD DE LA INFORMACIÓN		
<b>OBJETIVO DE CONTROL</b>		SEGURIDAD DE LA INFORMACIÓN		
<b>CUESTIONARIO</b>				
<b>PREGUNTA</b>		<b>SI</b>	<b>NO</b>	<b>N/A</b>
¿Existe alguna metodología de respaldo de información?		X		
¿Se realizan periódicamente respaldos de la información?		X		
¿Existe algún estándar o método de encriptado para la creación de contraseñas?			X	
¿Las contraseñas cuentan con números, letras y símbolos?				X
¿Se obliga a los usuarios a cambiar cada cierto tiempo las credenciales de autenticación?			X	
¿Se cuenta con un plan de procesos estratégico para dar un mantenimiento preventivo al software?		X		
¿Poseen un plan de procesos para dar mantenimiento correctivo al software?		X		
¿Posee un software antivirus instalado en los equipos del área de trabajo?		X		
¿Se tiene instalado un anti malware en los equipos del área de trabajo?		X		
¿Los softwares antivirus poseen una licencia original y actualizada?				X
¿Existe algún proceso para mantener las licencias actualizadas?				X
¿Existe un proceso para la adquisición de nuevas licencias?			X	
¿Posee un listado de software y hardware no permitido en el área de trabajo?			X	
¿Se cuenta con una sanción establecida para el integrante del área de trabajo que instale software no permitido?			X	
¿Los equipos de trabajo poseen la capacidad operativa necesaria para el correcto funcionamiento de los distintos sistemas que se utilizan en el área de trabajo?		X		
¿Cuenta con políticas de trabajo que impidan a los encargados de cada sección de trabajo el traslado de información no autorizada?		X		
¿Posee un plan de manejo de información?			X	
¿Cuenta con un proceso de respaldo de la información?			X	
¿Posee usted un plan de contingencia en el caso de filtrado indebido de la información?			X	
¿Existe un sistema para la medición de vulnerabilidades en la información?			X	
¿Considera usted necesaria la aplicación de un plan estratégico de trabajo para la mejora en el manejo de la información en el área de trabajo?			X	
<b>TOTAL</b>		<b>8</b>	<b>10</b>	<b>3</b>

**Fuente:** Investigación Directa

**Elaborado por:** Campoverde Pazmiño Rubén Dario

## **CAPÍTULO IV**

### **DESARROLLO DE LA PROPUESTA**

#### **4.1 Definición del plan de procesos de respaldo**

Un plan de procesos de respaldo (PPR) consiste en la selección y aplicación de las medidas más adecuadas. Con el fin, de poder mitigar las falencias dentro del actual proceso de tratamiento de la información e intensificar la seguridad e integridad de los documentos que se manejan dentro del área de trabajo.

#### **4.2 Compromiso del área de dirección de carrera**

El área de dirección de la carrera de Ingeniería en Teleinformática se encuentra comprometida con el manejo en la seguridad de la información, al adquirir de manera integral los principios y reglamentos que se encuentran enunciados en la Norma ISO 27001:2013; con la finalidad de mejorar su proceso de trabajo y asegurar el mejor uso de los recursos de la información dentro de la carrera. Durante el proceso de capacitación que se iniciaría con el plan de procesos de respaldo, junto a los altos mandos de dirección de carrera, en conjunto a su grupo de trabajo harán referencia a los principios y normas del mismo. Para la correcta adaptación e implementación en cada sub-área dentro del área de trabajo.

Para transmitir el cumplimiento de los procesos de respaldo los jefes encargados del área de la carrera de Ingeniería en Teleinformática se comprometen a transmitir a sus colaboradores los siguientes aspectos:

1. Se destinarán los recursos que sean necesarios para el cumplimiento de la seguridad de la información y su correcto respaldo.

2. Se aplicarán medidas de control mediante la Norma ISO 27001.
3. Orientar los esfuerzos en conjunto para minimizar las ocurrencias de incidentes que puedan generar un impacto o riesgo en la seguridad de la información en los procesos críticos de la dirección de carrera.
4. Es responsabilidad del área administrativa elaborar y establecer las políticas y directrices a tomar en consideración dentro de un futuro Sistema de Gestión de Seguridad de la Información, tomando como directriz principal el inicio de un plan de procesos de respaldo planteado.
5. El tratamiento de la información mediante los procesos de la ISO 27001, serán conversados dentro de un comité de aplicabilidad que permita la correcta gestión del plan de respaldo.
6. Se creará una unidad de riesgo operativo que permita establecer los posibles incidentes a futuro a medida que se genera una evolución en el tratamiento de la información, además, será la encargada de gestionar las capacitaciones correspondientes al personal dentro del área.
7. Se realizarán capacitaciones semestrales o anuales que permitan a las demás áreas tener el conocimiento del tratamiento de información que se llevará a cabo dentro de la dirección de carrera con la finalidad de que se acojan al mismo plan a futuro.

#### **4.2.1 Planificación a futuro para un Sistema de Gestión de Seguridad de la Información (SGSI) en la dirección de carrera**

Se definirán etapas de desarrollo que permitan la implementación de un Sistema de Gestión de Seguridad de la Información completo según los siguientes parámetros:



- Documentar el sistema a ser aplicado.
- Implementar el sistema de gestión.
- Evaluar la eficiencia y eficacia del sistema a través de auditorías.
- Gestionar el sistema y orientarlo a la mejora continua con los datos de evaluación obtenidos.

#### **4.2.2 Criterios de evaluación del tratamiento de la información**

Dentro de la elaboración del SGSI se debe tomar en consideración los siguientes aspectos:

1. Identificación del tipo de información, riesgos de la misma e impacto que podría generar.
2. Elaboración de un sistema de reporte u bitácora de control que le permita a cada área llevar un control de todos los procesos que se realizan para el tratamiento de la información.
3. El Director de carrera será el responsable de la validación, verificación, documentación y firma de los registros de cada uno de los eventos o incidentes de seguridad en la información que ocurran dentro del área de trabajo para luego ser enviados al área de riesgo operativo.

Los criterios de para la valoración de la criticidad de los activos de la información deberá ser elaborada mediante la escala de valoración de activos de la TABLA N°3 y de ser necesario se podrá modificar a criterio del evaluador la escala adecuada para la situación actual en la que se pueda encontrar el tratamiento de la información.

### 4.3 Valoración de los procesos de respaldo según la información

El respaldo de la información considera los siguientes parámetros:

- Tipo de información.
- Impacto de la información.
- Cantidad de información.

Estos parámetros serán el pilar fundamental para la medición del tipo de información que se posee dentro de cada sub-área de trabajo la cual será respaldada dependiendo de las necesidades de la dirección de carrera.

Con la finalidad de poder establecer una medición estandarizada de los tipos de datos e información que se maneja dentro de la dirección de la carrera de Ingeniería en Teleinformática de la Universidad de Guayaquil se considerarán las siguientes tablas de medición:

**TABLA N°14**  
**IMPACTO DE LA INFORMACIÓN**

IMPACTO	
MUY BAJO	1
BAJO	2
MEDIO	3
ALTO	4
MUY ALTO	5

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

**TABLA N°15**  
**CANTIDAD DE LA INFORMACIÓN**

CANTIDAD	
MUY POCA	1
POCA	2
MEDIA	3
ALTA	4
MUY ALTA	5

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

Las tablas de medición de la cantidad y el impacto en la información serán utilizadas para la ponderación y consideración de los datos que se ingresen dentro de la dirección de carrera por medio de la siguiente estala:

**TABLA N°16**  
**MODELO PARA LA PONDERACIÓN DE LA INFORMACIÓN**

PONDERACIÓN DE LA INFORMACIÓN										
TIPO DE INFORMACIÓN	CANTIDAD DE LA INFORMACIÓN					IMPACTO DE LA INFORMACIÓN				
	1	2	3	4	5	1	2	3	4	5
INFORMACIÓN PRIVILEGIADA										
INFORMACIÓN PRIVADA										
INFORMACIÓN PÚBLICA										
INFORMACIÓN INTERNA										
INFORMACIÓN EXTERNA										
INFORMACIÓN DIRECTA										
INFORMACIÓN INDIRECTA										

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

Dentro de los procesos del tratamiento de la información es indispensable una estandarización y una clasificación previa que realizar

un respaldo de la información que se encuentra dentro de área de trabajo. Debido a esto se debe tomar en consideración la siguiente terminología:

#### **4.3.1 Información privilegiada**

Información estrictamente manejada por los jefes del área de trabajo, de carácter restringido para el resto del personal del área y que de hacerse pública podrían afectar a la integridad total del área de trabajo y de otras áreas relacionadas.

#### **4.3.2 Información privada**

Información de carácter sensible que se maneja exclusivamente en el área de trabajo; no es permitida su divulgación ya que podría afectar la seguridad o intimidad del área laboral.

#### **4.3.3 Información pública**

Información de conocimiento público de que todas las personas dentro y fuera del área laboral tienen acceso y pueden utilizar a conveniencia de cada uno.

#### **4.3.4 Información interna**

Información de uso interno, que sea solo utilizada dentro del área para procesos de control de la misma u otra índole que involucre únicamente el área de trabajo.

#### **4.3.5 Información externa**

Información que ingresa al área de la dirección de carrera, ya sean de otras áreas, solicitudes y otra índole, que no posean un carácter urgente, privado o privilegiado.

#### **4.3.6 Información directa**

Información que proporciona datos directos y que deben de ser respaldados directamente sin pasar un proceso previo de revisión.

#### **4.3.7 Información indirecta**

Información obtenida a través de la revisión, análisis o chequeo de otra información y que necesita un análisis previo al respaldo o clasificación.

#### **4.4 Selección de controles para la gestión de la información**

La selección se basará en los planes de proceso de gestión de la información según la norma ISO 27001:2013 para la gestión de los activos de la información.

**TABLA N°17**  
**PLAN DE PROCESOS DE RESPALDO DE INFORMACIÓN**

INFORMACIÓN	RIESGO	VULNERABILIDAD	PPR
PRIVILEGIADA	Ingreso de archivos maliciosos.	Falta de supervisión.	Mitigar
	Ingreso de información errónea.	Desconocimiento en el manejo del sistema.	Mitigar
	Eliminación de información.	Falta de supervisión.	Mitigar
	Degeneración de la información.	Falta de respaldo.	Mitigar
	Manejo incorrecto de la información.	Falta de un sistema de control.	Mitigar
	Pérdida de información.	Falta de un sistema de archivado.	Mitigar
PRIVADA	Ingreso de archivos maliciosos.	Falta de supervisión.	Mitigar
	Ingreso de información errónea.	Desconocimiento en el manejo del sistema.	Mitigar
	Eliminación de información.	Falta de supervisión.	Mitigar
	Degeneración de la información.	Falta de respaldo.	Mitigar
	Manejo incorrecto de la información.	Falta de un sistema de control.	Mitigar
	Pérdida de información.	Falta de un sistema de archivado.	Mitigar

<b>PÚBLICA</b>	Ingreso de archivos maliciosos.	Falta de supervisión.	Mitigar
	Ingreso de información errónea.	Desconocimiento en el manejo del sistema.	Mitigar
	Eliminación de información.	Falta de supervisión.	Mitigar
	Degeneración de la información.	Falta de respaldo.	Mitigar
	Manejo incorrecto de la información.	Falta de un sistema de control.	Mitigar
	Pérdida de información.	Falta de un sistema de archivado.	Mitigar
<b>INTERNA</b>	Ingreso de archivos maliciosos.	Falta de supervisión.	Mitigar
	Ingreso de información errónea.	Desconocimiento en el manejo del sistema.	Mitigar
	Eliminación de información.	Falta de supervisión.	Mitigar
	Degeneración de la información.	Falta de respaldo.	Mitigar
	Manejo incorrecto de la información.	Falta de un sistema de control.	Mitigar
	Pérdida de información.	Falta de un sistema de archivado.	Mitigar
<b>EXTERA</b>	Ingreso de archivos maliciosos.	Falta de supervisión.	Mitigar

	Ingreso de información errónea.	Desconocimiento en el manejo del sistema.	Mitigar
	Eliminación de información.	Falta de supervisión.	Mitigar
	Degeneración de la información.	Falta de respaldo.	Mitigar
	Manejo incorrecto de la información.	Falta de un sistema de control.	Mitigar
	Pérdida de información.	Falta de un sistema de archivado.	Mitigar
DIRECTA	Ingreso de archivos maliciosos.	Falta de supervisión.	Mitigar
	Ingreso de información errónea.	Desconocimiento en el manejo del sistema.	Mitigar
	Eliminación de información.	Falta de supervisión.	Mitigar
	Degeneración de la información.	Falta de respaldo.	Mitigar
	Manejo incorrecto de la información.	Falta de un sistema de control.	Mitigar
	Pérdida de información.	Falta de un sistema de archivado.	Mitigar
INDIRECTA	Ingreso de archivos maliciosos.	Falta de supervisión.	Mitigar
	Ingreso de información errónea.	Desconocimiento en el manejo del sistema.	Mitigar



	Eliminación de información.	Falta de supervisión.	Mitigar
	Degeneración de la información.	Falta de respaldo.	Mitigar
	Manejo incorrecto de la información.	Falta de un sistema de control.	Mitigar
	Pérdida de información.	Falta de un sistema de archivado.	Mitigar

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

Una vez aplicado el PPR sobre el área de trabajo, se deberá tener en claro que, aún después de haberse aplicado el PPR existe un riesgo residual. El mismo, no posee un nivel de ponderación, estandarización o proporción y siempre se encuentra estimado en función del PPR que se lleva dentro de las distintas áreas de trabajo.

#### **4.4.1 Controles para la gestión de los respaldos de la información**

La Norma ISO 27001:2013 ofrece una amplia gama de objetivos de control y controles que se ajustan apropiadamente al manejo estructurado de la información que permiten reducir los riesgos excesivos que se encuentran identificados. Para la selección del control se tomará como base fundamental las amenazas y vulnerabilidades sujetas al PPR.

**TABLA N°18**  
**SELECCIÓN DE OBJETIVOS DE CONTROL ISO 27001**

ACTIVO	AMENAZA	VULNERABILIDAD	PPR
INFORMACIÓN	Ingreso de archivos maliciosos.	Falta de supervisión.	A.5.1.1 Políticas de la seguridad de la información.
			A.5.1.2 Revisión de las políticas de seguridad de la información.
			A.6.2.1 Política de los equipos móviles.
			A.6.2.1 Trabajo a distancia.
			A.10.1.1 Política del uso de controles criptográficos.
			A.12.2.1 Controles contra el malware.
			A.12.6.2 Restricción en la instalación de software.
			A.16.1.1 Responsabilidad y procedimientos.
			A.18.2.1 Revisión independiente de la seguridad de la información.

	Ingreso de información errónea.	Desconocimiento en el manejo del sistema.	A.6.1.2 Segregación de tareas.
			A.7.2.2 Concientización, educación y capacitación sobre seguridad de la información.
			A.7.2.3 Procesos disciplinarios.
			A.8.2.1 Clasificación de la información,
			A.8.2.3 Etiquetado de la información.
			A.8.2.3 Manejo de los activos.
	Eliminación de información.	Falta de supervisión.	A.18.2.3 Revisión del cumplimiento técnico.
			A.5.1.1 Políticas de la seguridad de la información.
			A.5.1.2 Revisión de las políticas de seguridad de la información.
			A.6.2.1 Política de los equipos móviles.

	Degeneración de la información.	Falta de respaldo.	A.6.2.1 Trabajo a distancia.
			A.7.1.1 Filtración
			A.7.1.2 Términos y condiciones del empleo.
			A.7.2.3 Procesos disciplinarios.
			A.5.1.1 Políticas de la seguridad de la información.
			A.5.1.2 Revisión de las políticas de seguridad de la información.
			A.6.2.1 Política de los equipos móviles.
			A.6.2.1 Trabajo a distancia.
			A.7.2.1 Responsabilidad de la gerencia.
			A.7.2.2 Concientización, educación y capacitación sobre la seguridad de la información.

			A.8.1.1 Inventario de activos.
			A.8.1.2 Propiedad de los activos.
			A.8.1.3 Uso aceptable de los activos.
			A.8.1.1 Retorno de los activos.
			A.8.2.1 Clasificación de la información.
			A.12.1.1 Documentación de los procedimientos operacionales.
			A.12.3.1 Backup de la información.
			A.12.4.2 Protección de la información de logueo.
			A.16.1.2 Reporte de los eventos de seguridad de la información.
			A.16.1.7 Recolección de evidencia.

	Manejo incorrecto de la información.	Falta de un sistema de control.	A.8.2.1 Clasificación de la información.
			A.8.2.3 Manejo de los activos.
			A.9.1.1 Política de control de acceso.
			A.9.2.1 Registro y des-registro del usuario.
			A.9.2.3 Gestión de los derechos de acceso privilegiado.
			A.9.2.5 Verificación de los derechos de acceso de los usuarios.
			A.12.1.3 Gestión de la capacidad.
	Pérdida de información.	Falta de un sistema de archivado.	A.8.2.1 Clasificación de la información,
			A.8.2.3 Etiquetado de la información.
			A.8.2.3 Manejo de los activos.
			A.12.3.1 Backup de la información.

Fuente: Investigación Directa

Elaborado por: Campoverde Pazmiño Rubén Dario

## **4.5 Pasos para el tratamiento del respaldo de la información**

Para la correcta gestión de la información y su debido respaldo se plantean las siguientes estrategias:

### **1. Determinación de los archivos a respaldar**

Para el respaldo de la información, se debe elaborar una valorización de la misma por medio de la TABLA N°16 debido a que, no toda la información deberá respaldarse, con la finalidad de priorizar los recursos que se manejen en el sistema dentro del área de trabajo.

Es recomendable, realizar el respaldo de la información con mayor índice de criticidad y luego respaldar el resto de la información en un orden de prioridades de mayor a menor.

### **2. Selección del medio de respaldo a utilizar**

En la actualidad, existen muchos sistemas para el respaldo de la información, sin embargo, la mayoría de ellos tienen un costo muy elevado o tienden a perder información. Debido a esto, se generan dos recomendaciones formales para el medio de respaldo.

1. Utilizar el sistema integrado de la Universidad de Guayaquil, el cual permite el respaldo de la información por medio de una cuenta administrativa.
2. Contratar un servicio en una nube (Cloud) que le permita almacenar en paralelo toda la información vital que se maneja dentro de la dirección de carrera.

Tomando en consideración lo estipulado anteriormente, el tratamiento de la información debe de proceder de tal forma, que se puedan

cumplir las tres condiciones primordiales en el resguardo de la información: Disponibilidad, Integridad y Confidencialidad.

Por esta razón, para realizar el correcto respaldo de la información se deben de realizar los siguientes pasos estandarizados:

1. Verificar la validez de la información.
2. Verificar si el documento u oficio es original.
3. Analizar el documento en búsqueda de alguna alteración que pueda afectar a la información en el mismo.
4. Escanear los documentos en formato .pdf y crear un código que permita identificar el grado de criticidad y el tipo de información, seguido de la fecha y nombre correspondiente.
5. Gestionar la validación de la información de forma manual.
6. Gestionar una jerarquía de carpetas que permita la correcta organización de los archivos por categorías.
7. Subir la documentación en el sistema de respaldo elegido.
8. Organizar por grado de criticidad la información.

### **3. Planteamiento de un cronograma periódico de respaldo**

Dentro del plan de trabajo, se debe realizar un estudio que evalúe la cantidad de información que ingresa anual, semestral, mensual, semanal y diariamente a la dirección de carrera y elaborar un plan de trabajo que permita el respaldo de la información el día en que se considere más óptimo



para su respaldo, es decir, se debe de considerar la realización de los respaldos, por fechas y por tipo de información, siempre priorizando la de mayor impacto dentro del área.

#### **4. Realizar el respaldo según el cronograma**

Se debe de realizar el respaldo de la información en los días estipulados y dentro del horario estipulado. Con la finalidad de llevar un mejor control de las tareas que se realicen en el área de trabajo y poder priorizar los distintos procesos ejecutados dentro de las fechas en las que se va a realizar el respaldo.

#### **4.6 Conclusiones**

Dentro de la presente Investigación se pudo analizar la utilidad e importancia de un plan estructurado para el tratamiento de la información. Con el objetivo de obtener un resultado viable y de gran impacto para el beneficio en los procesos de trabajo, dentro del área de la Dirección de carrera de Ingeniería en Teleinformática.

Es importante destacar que, dentro del área de trabajo se realiza por primera vez un plan de procesos de respaldo estructurado, que se basa en un estándar o normativa internacional como es la ISO 27001:2013. Debido a esto, se pueden generar pequeños desajustes por la implementación de una nueva metodología e ideología que se llevará dentro del área de trabajo. El uso de un plan de procesos de respaldo conlleva la continua capacitación o actualización de conocimientos de los reglamentos de control, con el objetivo de realizar socializaciones de manera continua para mantener los conceptos de; cómo se deben de aplicar los procesos de respaldos dentro del área, para que a futuro se vuelva más que una simple norma o política a ejecutar y pase a ser parte de una actividad inherente

dentro del plan de trabajo. Sin embargo, una vez establecida la norma, se demostrará la eficiencia y eficacia de los sistemas de control y manejo de los procesos de trabajo dentro de la utilización de los activos de la información.

#### **4.7 Recomendaciones**

Como se puede apreciar dentro de esta investigación, la dirección de la carrera de Ingeniería en Teleinformática no posee un plan estructural para la gestión de la información como tal, dando su primer paso a la correcta gestión de la información, se crea el plan de procesos de respaldo y su respectivo análisis de vulnerabilidades, para que sea tomado en consideración a futuro por parte de las autoridades respectivas.

Como recomendación formal se sugiere la elaboración de un Sistema de Gestión de la Seguridad de la Información (SGSI) más completo y que incluya todos los procesos de la gestión, no solo de la seguridad en la información, sino también, la seguridad física. La misma que permita a la carrera de Ingeniería en Teleinformática pulir todos sus procesos de trabajo con la finalidad de alcanzar la excelencia académica y de gestión en el área administrativa de toda la carrera.

**ANEXOS**

## ANEXO N°1

### OBJETIVOS DE CONTROL DE LA NORMA ISO/IEC 27001:2013

<b>A.5 Políticas de seguridad de la información</b>		
<b>A.5.1 Gestión de la Gerencia para la seguridad de la información</b>		
A.5.1.1	Políticas de la seguridad de de la información	<i>Control</i> La gerencia debe definir, aprobar, publicar y comunicar a los trabajadores y partes externas involucradas, una serie de políticas para la seguridad de la información.
A.5.1.2	Revisión de las políticas de seguridad de la información	<i>Control</i> Las políticas de seguridad de la información deben ser revisadas en intervalos planificados o si ocurren cambios significativos, para garantizar su idoneidad, adecuación y efectividad continuos.
<b>A.6 Organización de la seguridad de la información</b>		
<b>A.6.1 Organización interna</b>		
A.6.1.1	Funciones y responsabilidades de la seguridad de la información	<i>Control</i> Se debe definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Segregación de tareas	<i>Control</i> Tareas o áreas de responsabilidad en conflicto deben ser segregadas para reducir las oportunidades de modificación no autorizada o involuntaria o el uso inadecuado de los activos de la organización.
A.6.1.3	Contacto con las autoridades	<i>Control</i> Se debe mantener contacto adecuado con las autoridades respectivas
A.6.1.4	Contacto con grupos especiales de interés	<i>Control</i> Se debe mantener contacto con grupos especiales de interés u otros forums y asociaciones de profesionales especializados en seguridad
A.6.1.5	Seguridad de la información en la gestión del proyecto	<i>Control</i> La seguridad de la información debe adaptarse a la gestión del proyecto, independientemente del tipo de proyecto.
<b>A.6.2 Equipos móviles y trabajo a distancia</b>		
<b>Objetivo: Garantizar la seguridad del trabajo a distancia y del uso de los equipos móviles</b>		
A.6.2.1	Política de los equipos móviles	<i>Control</i> Se debe adoptar políticas y medidas de soporte de seguridad para el manejo de los riesgos derivados del uso de equipos móviles.
A.6.2.2	Trabajo a distancia	<i>Control</i> Se debe implementar políticas y medidas de soporte de seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo a distancia.
<b>A.7 Seguridad de los recursos humanos</b>		
<b>A.7.1. Antes de reclutarlo</b>		
A.7.1.1	Filtración	<i>Control</i> Se debe llevar a cabo la verificación de los antecedentes de todos los candidatos al empleo de acuerdo a las leyes y regulaciones vigentes y a la ética; y debe ser proporcional a los requisitos del

		negocio, la clasificación de la información a la que tendrá acceso y los riesgos que se perciban.
A.7.1.2	Términos y condiciones del empleo	<i>Control</i> Los acuerdos contractuales con los trabajadores y contratistas debe fijar sus responsabilidades y las de la organización con respecto a la seguridad de la información.
<b>A.7.2 Durante el trabajo</b>		
<b>Objetivo: Garantizar que los trabajadores y los contratistas sean conscientes y cumplan con las responsabilidades de la seguridad de la información</b>		
A.7.2.1	Responsabilidades de la Gerencia	<i>Control</i> La Gerencia debe instar a todos los trabajadores y contratistas a aplicar la seguridad de la información de acuerdo a las políticas y procedimientos establecidos por la organización.
A.7.2.2	Concientización, educación y capacitación sobre seguridad de la información	<i>Control</i> Todos los trabajadores de la organización y los contratistas, si así lo requiriesen, deben recibir una adecuada educación de concientización y capacitación, así como actualizaciones regulares sobre las políticas y procedimientos organizacionales, de acuerdo a las funciones de trabajo que desempeñen.
A.7.2.3	Procesos disciplinarios	<i>Control</i> Debe haber un proceso disciplinario formal que debe ser comunicado en el lugar, para tomar acción contra los trabajadores que comentan alguna infracción contra la seguridad de la información.
<b>A.7.3 Término y cambio de empleo</b>		
<b>Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o término del empleo</b>		
A.7.3.1	Término o cambio de responsabilidades de empleo	<i>Control</i> Se debe definir, comunicar y reforzar a todos los trabajadores y contratistas, las responsabilidades y tareas de seguridad de la información que permanecerán válidos después del término del empleo.
<b>A.8 Gestión de los Activos</b>		
<b>A.8.1 Responsabilidades sobre los activos</b>		
<b>Objetivo: Identificar los activos de la organización y definir las responsabilidades adecuadas de protección</b>		
A.8.1.1	Inventario de activos	<i>Control</i> Se debe identificar los activos y las instalaciones asociados a la información y al procesamiento de la información y se debe diseñar y mantener un inventario de dichos activos.
A.8.1.2	Propiedad de los activos	<i>Control</i> <b>Assets maintained in the inventory shall be owned.</b> Los activos que se encuentren identificados en el inventario deben de ser asignados a un "propietario".
A.8.1.3	Uso aceptable de los activos	<i>Control</i> Se debe implementar, documentar e implementar las reglas para el uso aceptable de la información y de los activos relacionados a la información y a las instalaciones de procesamiento de la información.
A.8.1.4	Retorno de los activos	<i>Control</i> Todos los trabajadores y usuarios internos y externos deberán devolver todos los activos de la organización que estén en su posesión una vez terminado su empleo, contrato o acuerdo.
<b>A.8.2 Clasificación de la información</b>		
<b>Objetivo: Garantizar que la información reciba un nivel adecuado de protección de acuerdo a su importancia dentro de la organización</b>		
A.8.2.1	Clasificación de la información	<i>Control</i> La información debe ser clasificada en términos de los requisitos y valores legales, siendo crítica y sensible ante la divulgación y modificación no autorizada.
A.8.2.2	Etiquetado de la información	<i>Control</i> Se debe desarrollar e implementar una serie de procedimientos adecuados para el etiquetado de la información, de acuerdo al esquema de clasificación de la información adoptado por la organización.
A.8.2.3	Manejo de los activos	<i>Control</i> Se debe desarrollar e implementar procedimientos de manejo de

		los activos de acuerdo al esquema de clasificación de la información adoptado por la organización.
<b>A.8.3 Manejo de los medios de comunicación</b>		
Objetivo: Prevenir la divulgación, modificación, retiro o destrucción no autorizada de la información almacenada en los medios de comunicación		
A.8.3.1	Gestión de medios de comunicación removibles	<i>Control</i> Se debe implementar procedimientos para la gestión de los medios de comunicación removibles de acuerdo al esquema de clasificación adoptado por la organización
A.8.3.2	Disposición de los medios de comunicación	<i>Control</i> Los medios de comunicación deben ser desechados de manera segura cuando ya no son necesarios, mediante procedimientos formales.
A.8.3.3	Transferencias física de los medios de comunicación	<i>Control</i> Los medios de comunicación que contienen información deben ser protegidos contra el acceso no autorizado, mal uso o corrupción durante su transporte.
<b>A.9 Control de acceso</b>		
<b>A.9.1 Requisitos del negocio sobre control del acceso</b>		
A.9.1.1	Política de control de acceso	<i>Control</i> Se debe establecer, documentar y revisar la política de control del acceso en base a los requisitos del negocio y de la seguridad de la información.
A.9.1.2	Acceso a la red y a los servicios de las redes	<i>Control</i> Los usuarios deben tener acceso únicamente a la red o a los servicios de redes a los que han sido autorizados a usar.
<b>A.9.2 Gestión del acceso al usuario</b>		
Objetivo: Garantizar el acceso al usuario autorizado para evitar el acceso no autorizado a los sistemas y servicios		
A.9.2.1	Registro y des-registro del usuario	<i>Control</i> Se debe implementar un proceso registro y des-registro del usuario para habilitar los derechos de acceso.
A.9.2.2	Provisión de acceso al usuario	<i>Control</i> Se debe implementar un proceso formal de provisión de acceso al usuario, para asignar o revocar los derechos de acceso a todos los tipos de usuarios a todos los sistemas y servicios.
A.9.2.3	Gestión de los derechos de acceso privilegiado	<i>Control</i> Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.
A.9.2.4	Gestión de información de autenticación secreta de usuarios	<i>Control</i> Se debe controlar la asignación de la información de autenticación secreta de usuarios mediante un proceso de gestión formal.
A.9.2.5	Verificación de los derechos de acceso de los usuarios	<i>Control</i> Los propietarios de los activos deben verificar los derechos de acceso de los usuarios a intervalos regulares.
A.9.2.6	Retiro o ajuste de los derechos de acceso	<i>Control</i> Los derechos de acceso a todos los trabajadores y terceros a la información y a las instalaciones de procesamiento de la información deben ser retirados al término del empleo, contrato o acuerdo, o ajustado luego de un cambio.
<b>A.9.3 Responsabilidades del usuario</b>		
Objetivo: Hacer a los usuarios responsables de salvaguardar la autenticación de su información		
A.9.3.1	Uso de información secreta de autenticación	<i>Control</i> Se debe solicitar a los usuarios seguir las prácticas de la organización sobre el uso de la información secreta de autenticación.
<b>A.9.4 Control de acceso a sistemas y aplicaciones</b>		
Objetivo: Evitar el acceso no autorizado a los sistemas y aplicaciones		
A.9.4.1	Restricción del acceso a la información	<i>Control</i> Se debe restringir el acceso a la información y a las funciones de aplicación del sistema de acuerdo a la política de control de acceso.
A.9.4.2	Procedimiento seguro de logeo	<i>Control</i> Si así lo requiere la política de control del acceso, se debe controlar el acceso a los sistemas y a las aplicaciones, mediante un



		procedimiento seguro de logeo.
A.9.4.3	Sistema de gestión de la clave	<i>Control</i> Los sistemas de gestión de la clave deben ser interactivos y deben asegurar la calidad de las claves.
A.9.4.4	Uso de programas utilitarios de privilegio	<i>Control</i> Se debe restringir y controlar severamente el uso de programas utilitarios que puedan controlar manualmente el sistema y los controles de la aplicación.
A.9.4.5	Control del acceso para programar el código fuente	<i>Control</i> Se debe restringir el acceso al programa de código fuente.
<b>A.10 Criptografía</b>		
<b>A.10.1 Controles de la criptografía</b>		
Objetivo: Asegurar el uso adecuado y efectivo de la criptografía para proteger la confidencialidad, autenticidad y/o integridad de la información		
A.10.1.1	Política del uso de controles criptográficos	<i>Control</i> Se debe desarrollar e implementar una política de uso de controles criptográficos para proteger la información.
A.10.1.2	Gestión de las claves	<i>Control</i> Se debe desarrollar e implementar una política para el uso, protección y tiempo de vida de las claves criptográficas a lo largo de todo su ciclo de vida.
<b>A.11 Seguridad física y medioambiental</b>		
<b>A.11.1 Áreas seguras</b>		
Objetivo: Evitar acceso físico no autorizado, daño e interferencia a la información e instalaciones de procesamiento de la información de la organización.		
A.11.1.1	Perímetro de seguridad física	<i>Control</i> Se debe determinar y utilizar los perímetros de seguridad para proteger las áreas que contienen información sensible y crítica y las instalaciones de procesamiento de la información.
A.11.1.2	Controles físicos de los ingresos	<i>Control</i> Se debe proteger las áreas seguras mediante controles adecuados de ingreso para garantizar el ingreso de sólo personal autorizado.
A.11.1.3	Seguridad de las oficinas, salas e instalaciones	<i>Control</i> Se debe diseñar y aplicar mecanismos de seguridad física a las salas, oficinas e instalaciones.
A.11.1.4	Protección contra las amenazas externas y medioambientales	<i>Control</i> Se debe diseñar y aplicar mecanismos de control contra los desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras	<i>Control</i> Se debe diseñar y aplicar procedimientos para el trabajo en áreas seguras.
A.11.1.6	Distribución de las zonas de carga	<i>Control</i> Los puntos de acceso, tales como las zonas de distribución y carga y otros puntos por los que podría ingresar personal no autorizado a las instalaciones deben ser controlados, y en la medida de lo posible, alejados de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.
<b>A.11.2 Equipos</b>		
Objetivo: Evitar la pérdida, daño, robo o actos en los que se comprometan activos y la interrupción de las operaciones de la organización.		
A.11.2.1	Ubicación y protección de los equipos	<i>Control</i> Los equipos deben ser ubicados y protegidos de tal forma que se reduzcan los riesgos como resultado de las amenazas y los peligros del medio ambiente, y las oportunidades de acceso no autorizado.
A.11.2.2	Servicios públicos de soporte	<i>Control</i> Los equipos deben ser protegidos contra las fallas de energía y otras alteraciones causadas por las fallas en los servicios públicos de soporte.
A.11.2.3	Seguridad en el cableado	<i>Control</i> Se debe proteger de cualquier interferencia, interceptación o daño al cableado de energía o telecomunicaciones que transfiere datos o que sirve de apoyo en los servicios de información.
A.11.2.4	Mantenimiento de los	<i>Control</i>

	equipos	Se debe mantener de manera correcta el mantenimiento de los equipos para garantizar su disponibilidad e integridad continuas.
A.11.2.5	Retiro de los activos	<i>Control</i> El equipo, la información o el software no puede ser retirado de su lugar sin una previa autorización
A.11.2.6	Seguridad de los equipos y bienes fuera de las instalaciones	<i>Control</i> Se debe aplicar medidas de seguridad para los activos utilizados fuera de las instalaciones, tomando en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.11.2.7	Disposición o re-uso seguro de los equipos	<i>Control</i> Todos los equipos que contienen medios de comunicación de la información deben ser revisados para garantizar que se haya extraído o que se haya sobre-escrito la información sensible y la licencia del software antes de desechar o re-usar el mismo.
A.11.2.8	Usuario de equipo abandonado	<i>Control</i> Los usuarios deben garantizar una adecuada protección a los equipos abandonados
A.11.2.9	Política de escritorio y pantallas limpias	<i>Control</i> Se debe adoptar la política de escritorio limpio de papeles y de medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de la información.
<b>A.12 Seguridad de las operaciones</b>		
<b>A.12.1 Procedimientos y responsabilidades operaciones</b>		
A.12.1.1	Documentación de los procedimientos operacionales	<i>Control</i> Se debe documentar los procesos operacionales y ponerse a disposición de todos los usuarios que lo necesiten.
A.12.1.2	Cambios en la gerencia	<i>Control</i> Se debe mantener un control sobre los cambios en la organización, el negocio y los sistemas que afectan la seguridad de la información
A.12.1.3	Gestión de la capacidad	<i>Control</i> Debe ser monitoreado y mejorado el uso de recursos, así como las proyecciones hechas sobre los requisitos de capacidad del futuro, para garantizar el desempeño del sistema.
A.12.1.4	Separación de ambientes de desarrollo, prueba y de operaciones	<i>Control</i> Se debe separar los ambientes de desarrollo, prueba y operaciones para reducir los riesgos de acceso o cambios no autorizados dentro de ambiente de operaciones.
<b>A.12.2 Protección contra el malware (programa malicioso)</b>		
Objetivo: Garantizar que la información y las instalaciones de procesamiento de la información estén protegidos contra el malware		
A.12.2.1	Controles contra el malware	<i>Control</i> Se debe implementar mecanismos de control para la detección, prevención y recuperación, para proteger a la información contra el malware, junto con una concientización adecuada al usuario.
<b>A.12.3 Backup</b>		
Objetivo: Proteger la información contra la pérdida		
A.12.3.1	Backup de la información	<i>Control</i> Se debe tomar y poner a prueba de manera regular, el back up de copias de la información, software e imágenes del sistema, de acuerdo a la política de back up de la organización.
<b>A.12.4 Logeo y monitoreo</b>		
Objetivo: Registrar eventos y generar evidencias		
A.12.4.1	Eventos de logeo	<i>Control</i> Se debe llevar a cabo y verificar regularmente eventos de logeo que registren las actividades, excepciones, faltas y cualquier evento de seguridad de la información.
A.12.4.2	Protección de la información del logeo	<i>Control</i> Se debe proteger contra la falsificación y el acceso no autorizado a los medios de logeo y a la información del logeo
A.12.4.3	Logeo del administrador y operador	<i>Control</i> Debe logearse las actividades del sistema del administrador y del operador, y los logs deben ser protegidos y revisados de manera regular.
A.12.4.4	Sincronización de los	<i>Control</i>



	relojes	Se debe sincronizar a una sola fuente de tiempo de referencia, los relojes de todos los sistemas de procesamiento de la información correspondientes dentro de la organización o del dominio de seguridad.
<b>A.12.5 Control del software operacional</b>		
Objetivo: Garantizar la integridad de los sistemas operacionales		
A.12.5.1	Instalación del software en los sistemas operacionales	<i>Control</i> Se debe implementar procedimientos para controlar la instalación del software en los sistemas operacionales
<b>A.12.6 Gestión de las vulnerabilidades técnicas</b>		
Objetivo: Evitar la explotación de las vulnerabilidades técnicas		
A.12.6.1	Gestión de las vulnerabilidades técnicas	<i>Control</i> Se debe obtener, de manera oportuna, información sobre las vulnerabilidades técnicas de los sistemas de la información a ser utilizados; evaluar la exposición de la organización a dichas vulnerabilidades y tomar las medidas adecuadas para manejar los riesgos asociados.
A.12.6.2	Restricciones en la instalación de software	<i>Control</i> Se debe establecer e implementar las reglas que gobiernen la instalación de los softwares.
<b>A.12.7 Consideraciones de las auditorías sobre los sistemas de información</b>		
Objetivo: Minimizar el impacto de las actividades de las auditorías en los sistemas operacionales		
A.12.7.1	Controles de la auditoría sobre los sistemas de información	<i>Control</i> Se debe planificar cuidadosamente los requisitos y actividades de la auditoría que involucren la verificación de los sistemas operacionales; y acordar minimizar las alteraciones a los procesos del negocio
<b>A.13 Seguridad de las comunicaciones</b>		
<b>A.13.1 Gestión de la seguridad de las redes</b>		
Objetivo: Garantizar la protección de la información en las redes y de sus instalaciones de procesamiento de la información		
A.13.1.1	Controles en las redes	<i>Control</i> Se debe administrar y controlar las redes para proteger la información de los sistemas y las aplicaciones
A.13.1.2	Seguridad de los servicios de las redes	<i>Control</i> Se debe identificar los mecanismos de seguridad, los niveles del servicio y los requisitos de todos los servicios de redes e incluirlos en los acuerdos de servicios de redes, ya sea que los servicios sean proporcionados por la misma organización o por un tercero.
A.13.1.3	Segregación en las redes	<i>Control</i> Se debe segregar grupos de servicios de información, usuarios y sistemas de información
<b>A.13.2. Transferencia de la información</b>		
Objetivo: Mantener la seguridad de la información transferida dentro de la organización y con cualquier entidad externa		
A.13.2.1	Políticas y procedimientos de la transferencia de la información	<i>Control</i> Se debe dar lugar a las políticas, procedimientos y controles formales de transferencia a través del uso de todo tipo de equipos de comunicación
A.13.2.2	Acuerdos sobre la transferencias de la información	<i>Control</i> Los acuerdos deberán señalar la transferencia segura de la información del negocio entre la organización y terceros.
A.13.2.3	Mensajes electrónicos	<i>Control</i> Se debe proteger adecuadamente la información enviada mediante mensajes electrónicos.
A.13.2.4	Confidencialidad o acuerdos no divulgados	<i>Control</i> Se debe identificar, revisar regularmente y documentar los requisitos para la confidencialidad o acuerdos no divulgados que reflejan las necesidades de la organización sobre la protección de la información.
<b>A.14 Adquisición, desarrollo y mantenimiento del sistema</b>		
<b>A.14.1 Requisitos de seguridad de los sistemas de información</b>		
Objetivo: Garantizar que la seguridad de la información forme parte integral de los sistemas de información a lo largo de todo el ciclo de vida. Esto incluye también los requisitos del sistema de la información que proveen servicios mediante las redes públicas.		

A14.1.1	Análisis y especificaciones de los requisitos de la seguridad de la información	<i>Control</i> Se debe incluir la seguridad de la información relacionada a los requisitos en los requerimientos de nuevos sistemas de información o en el mejoramiento de los sistemas de información existentes.
A14.1.2	Seguridad de los servicios de aplicación en las redes públicas	<i>Control</i> Se debe proteger la información que pasa a través de las redes públicas de las actividades fraudulentas, controversias contractuales y divulgación y modificaciones no autorizadas.
A14.1.3	Protección de las transacciones de los servicios de aplicación	<i>Control</i> Se debe proteger la información que provenga de las transacciones de los servicios de aplicación, para evitar las transmisiones incompletas, desvíos, duplicado o reproducción no autorizados de mensajes.
<b>A14.2 Seguridad en los procesos del programa de desarrollo y soporte</b>		
Objetivo: Garantizar que se diseñe e implemente la seguridad de la información dentro del ciclo del programa de desarrollo de los sistemas de la información		
A14.2.1	Política del programa de desarrollo seguro	<i>Control</i> Se debe establecer y aplicar reglas de desarrollo de software y sistemas a los programas de desarrollo dentro de la organización.
A14.2.2	Procedimiento de control de los cambios de sistemas	<i>Control</i> Se debe controlar los cambios dentro del ciclo de vida de los programas de desarrollo, mediante el uso de procedimientos formales de control de cambios.
A14.2.3	Revisión técnica de las aplicaciones luego de los cambios de la plataforma operacional	<i>Control</i> Luego del cambio de las plataformas operacionales, se debe revisar y verificar las aplicaciones críticas del negocio, para garantizar que no haya un impacto adverso sobre las operaciones o la seguridad organizacional.
A14.2.4	Restricciones a los cambios de los paquetes de software	<i>Control</i> No se facilitará la modificación de los paquetes de sistemas; por el contrario, se les limitará a los cambios necesarios y todos los cambios deberán ser estrictamente controlados.
A14.2.5	Principios del sistema de seguridad para la ingeniería	<i>Control</i> Se debe establecer, documentar, mantener y aplicar los principios de sistemas de seguridad para la ingeniería, a todos los esfuerzos de implementación del sistema.
A14.2.6	Ambiente seguro del programa de desarrollo	<i>Control</i> Las organizaciones deben establecer y proteger adecuadamente los ambientes seguros de desarrollo de los sistemas de desarrollo y la integración de los esfuerzos a lo largo del ciclo de vida del programa de desarrollo del sistema.
A14.2.7	Programa de desarrollo subcontratado	<i>Control</i> La organización debe supervisar y monitorear las actividades de desarrollo del sistema del ente subcontratado.
A14.2.8	Revisión de la seguridad del sistema	<i>Control</i> Se debe llevar a cabo revisiones de la funcionalidad de la seguridad durante el desarrollo.
A14.2.9	Revisión de la aceptación del sistema	<i>Control</i> Se debe establecer programas de verificación de la aceptación y de los criterios relacionados con respecto a los nuevos sistemas de información, renovaciones y nuevas versiones.
<b>A.14.3 Datos de prueba</b>		
Objetivo: garantizar la protección de los datos utilizados para la verificación		
A14.3.1	Protección de los datos de prueba	<i>Control</i> Los datos de prueba deben ser seleccionados, protegidos y controlados cuidadosamente.
<b>A15 Relación con los proveedores</b>		
<b>A15.1 Seguridad de la información en las relaciones con los proveedores</b>		
Objetivo: Garantizar la protección de los activos de la información a los que los proveedores tienen acceso		
A15.1.1	Política de seguridad de la información sobre las relaciones con los proveedores	<i>Control</i> Se debe acordar y documentar los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de los proveedores a los activos de la organización.
A15.1.2	Consideración de la	<i>Control</i>

	seguridad en los acuerdos con los proveedores	Se debe establecer y acordar todos los requisitos relacionados a la seguridad de la información con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proveer con elementos de infraestructura tecnológica, información de la organización.
A15.1.3	Cadena de suministro de tecnología de la información y comunicación	<i>Control</i> Los acuerdos con los proveedores deben incluir los requisitos para el manejo de los riesgos de seguridad de la información relacionados a los servicios de tecnología de la información y la comunicación y a la cadena de suministro del producto.
<b>A15.2 Gestión de la prestación del servicio por parte del proveedor</b>		
Objetivo: Mantener un nivel acordado de seguridad de la información y de la prestación del servicio alineado a los acuerdos del proveedor		
A15.2.1	Monitoreo y revisión del servicio de los proveedores	<i>Control</i> Las organizaciones deben monitorear, revisar y auditar regularmente la prestación de servicios del proveedor.
A15.2.2	Cambios en la gestión del servicio de los proveedores	<i>Control</i> Se debe gestionar los cambios a la provisión de los servicios prestados por los proveedores, incluyendo el mantenimiento y la mejora de políticas, procedimientos y controles de la seguridad de la información, tomando en cuenta la sensibilidad de la información del negocio, los sistemas y los procesos involucrados así como la re-evaluación de los riesgos.
<b>A16 Gestión de los incidentes de seguridad de la información</b>		
<b>A16.1 Gestión de los incidentes de la seguridad de la información y la mejora</b>		
Objetivo: Garantizar una aproximación consistente y efectiva a la gestión de los incidentes de seguridad de la información, incluyendo la comunicación sobre los eventos y debilidades de la seguridad		
A16.1.1	Responsabilidades y procedimientos	<i>Control</i> Se debe establecer responsabilidades de la gerencia y procedimientos para garantizar una respuesta rápida, efectiva y adecuada a los incidentes de seguridad de la información
A16.1.2	Reporte de los eventos de seguridad de la información	<i>Control</i> Se debe reportar los eventos de seguridad de la información a través de canales adecuados lo más pronto posible.
A16.1.3	Reporte de las debilidades de la seguridad de la información	<i>Control</i> Se debe instar a los trabajadores y contratistas que hagan uso de los sistemas de información de la organización, a tomar nota e informar acerca de cualquier debilidad que se observe o sospeche con respecto a los sistemas o servicios del sistema de seguridad de la información.
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	<i>Control</i> Se debe evaluar los eventos de seguridad de la información; y tomar una decisión sobre si deben ser clasificados como incidentes de la seguridad de la información.
A16.1.5	Respuesta a los incidentes de seguridad de la información	<i>Control</i> Se debe responder a los incidentes de seguridad de la información de acuerdo a los procedimientos documentados.
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	<i>Control</i> Se debe usar el conocimiento obtenido del análisis y resolución de los incidentes de la seguridad de la información, con la finalidad de reducir la probabilidad o impacto de futuros incidentes.
A16.1.7	Recolección de evidencia	<i>Control</i> La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y conservación de la información que puede servir como evidencia.
<b>A17 Gestión de los aspectos de la seguridad de la información para la continuidad del negocio</b>		
<b>A17.1 Continuidad de la seguridad de la información</b>		
Objetivo: La continuidad de la seguridad de la información debe estar incrustada en los sistemas de gestión de la continuidad del negocio de la organización		
A17.1.1	Continuidad de los planes de seguridad de la información	<i>Control</i> La organización debe determinar sus requisitos para la seguridad de la información y para la continuidad de la gestión de seguridad de la información en situaciones adversas, e.g. durante una crisis o desastre.
A17.1.2	Implementación de la continuidad de la	<i>Control</i> La organización deberá establecer, documentar, implementar y



	seguridad de la información	mantener los procesos, procedimientos y controles para garantizar el nivel requerido de continuidad de la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	<i>Control</i> La organización debe verificar los controles de la continuidad de la seguridad de la información establecidos e implementados, a intervalos regulares con la finalidad de asegurar la su validez y efectividad durante situaciones adversa.
<b>A.17.2 Redundancias</b>		
Objetivo: Garantizar la disponibilidad de las instalaciones de procesamiento de la información		
A.17.2.1	Disponibilidad de instalaciones de procesamiento de la información	<i>Control</i> Se debe implementar las instalaciones de procesamiento de la información con una capacidad adicional suficiente para cumplir con los requisitos de disponibilidad.
<b>A.18 Cumplimiento</b>		
<b>A.18.1 Cumplimiento de los requisitos legales y contractuales</b>		
Objetivo: Evitar el incumplimiento de las obligaciones legales, regulatorias o contractuales relacionadas a la seguridad de la información y al cualquier requisito de seguridad		
A.18.1.1	Identificación de la ley aplicable y de los requisitos contractuales	<i>Control</i> Se debe identificar de manera explícita, documentar y mantener actualizados todos los requisitos legislativos regulatorios y contractuales así como el enfoque de la organización para cumplir con estos requisitos, con respecto a cada sistema de información y a la organización.
A.18.1.2	Derechos de propiedad intelectuales	<i>Control</i> Se debe implementar procedimientos adecuados para garantizar el cumplimiento de los requisitos legislativos, regulatorios y contractuales relacionados a los derecho de propiedad intelectuales y al uso de productos registrados de software.
A.18.1.3	Protección de los registros	<i>Control</i> Los registros deben ser protegidos contra la pérdida, destrucción, falsificación, acceso no autorizado y lanzamiento no autorizado, de acuerdo a los requisitos legales, regulatorios, contractuales y del mismo negocio.
A.18.1.4	Privacidad y protección de la información que permite identificar a las personas	<i>Control</i> Se debe garantizar la privacidad y la protección de la información que permita identificar a las personas de acuerdo a lo requerido en la legislación y las regulaciones pertinentes, si fuera aplicable.
A.18.1.5	Regulación de los controles criptográficos	<i>Control</i> Se debe hacer uso de controles criptográficos en cumplimiento con los acuerdos, las leyes y las regulaciones correspondientes.
<b>A.18.2 Revisiones de la seguridad de la información</b>		
Objetivo: Garantizar que la seguridad de a información sea implementada y operada de acuerdo a las políticas y procedimientos organizacionales		
A.18.2.1	Revisión independiente de la seguridad de la información	<i>Control</i> Se debe revisar, a intervalos planificados o cuando ocurre algún cambio significativo, el enfoque de la organización para gestionar la seguridad de la información y su implementación (i.e. objetivos de control, controles, políticas, procesos y procedimientos de la seguridad de la información).
A.18.2.2	Cumplimiento de las políticas y normas de seguridad de la información	<i>Control</i> Los gerentes deben revisar regularmente el cumplimiento de los procedimientos y del procesamiento de la información dentro de su área de responsabilidad, de acuerdo a las políticas, normas de seguridad adecuadas y a los otros requisitos de seguridad.
A.18.2.3	Revisión del cumplimiento técnico	<i>Control</i> Se debe revisar regularmente los sistemas de la información con respecto al cumplimiento de las políticas y normas de seguridad de la información de la organización.

Fuente: ISO/IEC 27001:2013 (E)

Elaborado por: Campoverde Pazmiño Rubén Dario

## BIBLIOGRAFÍA

**Acevedo, J. (02 de 11 de 2015).** Art. ¿Qué expone a una empresa a las amenazas informáticas?. Seguridad de la Información. de <http://www.pcworldenespanol.com/2015/11/02/que-expone-a-una-empresa-a-las-amenazas-informaticas/>

**Aldegani, G. M. (1997).** Libro. Seguridad Informática. Seguridad de la Información. Análisis de Seguridades de la Información. de Seguridad Informática MP Ediciones: Argentina. Pág 22.

**Cardona, A. (13 de 01 de 2015).** Art. ISO 27001: Pilares fundamentales de un SGSI. de <https://www.isotools.org/2015/01/13/iso-27001-pilares-fundamentales-sgsi/>

**Consultores, S. (21 de 11 de 2017).** Art. Top 10 de certificados en Normas ISO a nivel mundial. La Norma ISO 27001 aumenta en relevancia. de <https://www.s bqconsultores.es/top-10-certificados-normas-iso-nivel-mundial/>

**D'Antonio, G. (2007-2016).** Art. Registro de Empresas Certificadas ISO 27001. de <https://www.ismsforum.es/iso27001>. Pág 1.

**Disterer G. (15 de Marzo de 2013).** Art. ISO/IEC 27000, 27001 and 27002 for Information Security Management. de [http://file.scirp.org/pdf/JIS\\_2013042311130103.pdf](http://file.scirp.org/pdf/JIS_2013042311130103.pdf). Pág 1. de PDF.

**Hernández, R., Fernández, C., & Baptista, M. d. (2010).** Art. Metodología de la investigación. Conceptos Generales de la Investigación. de

<https://metodologiasdelainvestigacion.files.wordpress.com/2017/01/metodologia-investigacion-hernandez-sampieri.pdf>. Pág 26 PDF.

**ISO 27002. (2015).** Doc. Tecnologías de la información. Sistemas de gestión de Seguridad de la Información. de [http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/EXTRACTO\\_2014/GAN/nte\\_inen\\_iso\\_iec\\_27002extracto.pdf](http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/EXTRACTO_2014/GAN/nte_inen_iso_iec_27002extracto.pdf). Pág 7 PDF.

**ISO/IEC 27001. (13 de 01 de 2015).** Art. International Organization for Standardization. ISO/IEC 2740:2015. de <https://www.iso.org/standard/44404.html>.

**ISOTools. (11 de 09 de 2015).** Art. ¿En qué consiste la Norma ISO 27001?. La Norma ISO 27001 ayuda a preservar la seguridad informática. de <https://www.isotools.org/2015/09/11/en-que-consiste-la-norma-iso-27001>.

**ISOTools Excellence. (04 de 2015).** Art. ISO 27001: El impacto en los Sistemas de Gestión de Seguridad de la Información. Tipos de impacto. de <http://www.pmg-ssi.com/2015/04/iso-27001-el-impacto-en-los-sistemas-de-gestion-de-seguridad-de-la-informacion>.

**Jara, H., & Pacheco, F. (2012).** Art. Implementación de un Sistema para la Gestión de la Seguridad. de Libro de Ethical Hacking 2.0 Buenos Aires: Fox Andina. Pág 45 PDF.

**Mañero, I. (14 de 03 de 2017).** Art. Mozilla: No sabemos proteger nuestra seguridad en Internet. Seguridad de la Información. de <http://computerhoy.com/noticias/software/mozilla-no-sabemos-proteger-nuestra-seguridad-internet-59684>.

**Mejía, C. (07 de 2012).** Tesis. Propuesta de un Modelo de Sistema de Gestión de Seguridad de la Información para Institutos Superiores Tecnológicos de Educación Aeronáutica. de <http://bibdigital.epn.edu.ec/bitstream/15000/7807/1/CD-4189.pdf>. Pág 13 PDF.

**Mendoza, M. (16 de 06 de 2015).** Art. ¿Ciberseguridad o seguridad de la Información? Aclarando la diferencia. Seguridad de la información; distintas formas y estados de los datos. de <https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia>.

**Mifsud, E. (26 de 03 de 20102).** Art. Introducción a la Seguridad de la Información: Seguridad de la Información/ Seguridad Informática. Seguridad de la Información: Modelo PDCA. de <http://recursostic.educacion.es/observatorio/web/ca/software/softwaregeneral/1040-introduccion-a-la-seguridad-informatica?start=1>. Pág 2.

**Morgan, J. (2014).** Art. Gestión del Riesgo Operacional. Objetivos y política de gestión del riesgo operacional. de <https://www.jpmorgan.com/jpmpdf/1320694344011.pdf>. Pág 2 PDF.

**NTE INEN-ISO/IEC 27003:2012. (2012).** Art. Tecnología de la Información - Técnicas de Seguridad. Guía de Implementación del Sistema de Gestión de la Seguridad de la Información. de [http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/EXTRACTO\\_2014/GAN/nte\\_inen\\_iso\\_iec\\_27003extracto.pdf](http://www.normalizacion.gob.ec/wp-content/uploads/downloads/2014/EXTRACTO_2014/GAN/nte_inen_iso_iec_27003extracto.pdf). Pág 6 PDF.

**Roberto Almeida. (29 de 05 de 2015).** Art. CNT única Empresa Pública en el Ecuador que obtiene Certificación ISO 27001. de <http://corporativo.cnt.gob.ec/cnt-unica-empresa-publica-en-el-ecuador-que-obtiene-certificacion-iso-27001>.

**Seguridad Informática. (12 de 03 de 2012).** Art. Los pilares de la seguridad informática. de <http://seguridaddeinformacion.bligoo.com/los-pilares-de-la-seguridad-informatica#>.

**SGSI, ISOTools. (28 de 09 de 2017).** Art. ¿Cuál es la situación de la Norma ISO 27001 en Sudamérica. ISO 27001. de <http://www.pmg-ssi.com/2017/09/situacion-norma-iso-27001-sudamerica>.