



UNIVERSIDAD DE GUAYAQUIL  
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS  
CARRERA DE INGENIERÍA EN NETWORKING Y  
TELECOMUNICACIONES

ELABORACIÓN DEL PLAN DE MEJORAS DE SEGURIDAD DE LA  
INFORMACIÓN, BASADO EN LA APLICACIÓN DE LA NORMA  
ISO 27001 -2013 PARA EL DEPARTAMENTO DE  
INFRAESTRUCTURA DE LA EMPRESA  
RIGHTTEK S.A. DE LA  
CIUDAD DE  
GUAYAQUIL

**PROYECTO DE TITULACIÓN**

Previa a la obtención del Título de:

**INGENIERO EN NETWORKING Y TELECOMUNICACIONES**

AUTORES:

ROBERT EDUARDO SORIA CAJAS

HILDA ELIZABETH VERA BARRERA

TUTOR:

AB. MD BERARDO RODRÍGUEZ GALLEGOS Msc.

GUAYAQUIL - ECUADOR

2017



Presidencia  
de la República  
del Ecuador



Plan Nacional  
de Ciencia, Tecnología,  
Innovación y Saberes



SENESCYT  
Secretaría Nacional de Educación Superior,  
Ciencia, Tecnología e Innovación

## REPOSITORIO NACIONAL EN CIENCIA Y TECNOLOGÍA

### FICHA DE REGISTRO DE TESIS/TRABAJO DE GRADUACIÓN

**TÍTULO Y**

**SUBTÍTULO:**

“ELABORACIÓN DEL PLAN DE MEJORAS DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA APLICACIÓN DE LA NORMA ISO 27001 -2013 PARA EL DEPARTAMENTO DE INFRAESTRUCTURA DE LA EMPRESA RIGHTTEK S.A. DE LA CIUDAD DE GUAYAQUIL”

**AUTOR(ES):**

Robert Eduardo Soria Cajas  
Hilda Elizabeth Vera Barrera

**REVISOR(ES)/TUTOR(ES)**

AB. MD BERARDO RODRÍGUEZ GALLEGOS Msc.

**INSTITUCIÓN:**

Universidad de Guayaquil

**UNIDAD/FACULTAD:**

Facultad de Ciencias Matemáticas y Físicas

**MAESTRÍA/ESPECIALIDAD**

Ingeniería en Networking y Telecomunicaciones

**GRADO OBTENIDO:**

Ingeniero en Networking y Telecomunicaciones

**FECHA DE PUBLICACIÓN:**

**No. DE PÁGINAS:**

129

**ÁREAS TEMÁTICAS:**

Networking, Telecomunicaciones

**PALABRAS CLAVES  
/KEYWORDS:**

Seguridad de la Información, Activos de Información, Auditoría, Magerit, ISO 27001:2013, Políticas de Seguridad, controles.

#### RESUMEN/ABSTRACT

La norma ISO 27001 -2013 Seguridad de la Información, consiste en verificar si existe cumplimiento de los controles y las cláusulas establecidas por el estándar si se identifica el no cumplimiento de dichos controles en general se generan las no conformidades que son redactadas por el auditor mediante un informe. La auditoría se basa en los criterios de la Norma, es evidenciada y posee un proceso sistemático independiente. El trabajo de Investigación que se efectuó en el departamento de Infraestructura de la empresa Righttek S.A., consiste en brindar un plan de mejoras de seguridad de la información basado en la norma ISO 27001 -2013, en el cual asegura los datos a través de la confidencialidad, integridad, y disponibilidad, que garantice un tratamiento adecuado de los problemas de seguridad, teniendo como base las mejores prácticas, valorando los riesgos y procedimientos que producen en esta área.

**ADJUNTO PDF:**

SI ☒

NO

**CONTACTO CON  
AUTOR/ES:**

**Teléfono:** 0930087218  
0959197143

E-mail: [robe.du@hotmail.com](mailto:robe.du@hotmail.com)  
[hildaevb22@gmail.com](mailto:hildaevb22@gmail.com)

**CONTACTO CON  
LA INSTITUCIÓN:**

**Nombre:** Ab. Berardo Rodríguez

**Teléfono:** (04) 2 683227

**E-mail:** berardo.rodriguezg@ug.edu.ec

## **CARTA DE APROBACIÓN DEL TUTOR**

En mi calidad de Tutor del trabajo de titulación, “Elaboración del plan de mejoras de Seguridad de la Información, basado en la aplicación de la Norma ISO 27001 -2013 para el departamento de Infraestructura de la Empresa Righttek S.A. de la ciudad de Guayaquil” elaborado por el Sr. Robert Eduardo Soria Cajas y la Srta. Hilda Elizabeth Vera Barrera alumnos no titulados de la Carrera de Ingeniería en Networking y Telecomunicaciones de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil, previo a la obtención del Título de Ingeniero en Networking y Telecomunicaciones, me permito declarar que luego de haber orientado, estudiado y revisado, la Apruebo en todas sus partes.

**Atentamente**

**AB. MD Berardo Rodríguez Gallegos Msc.**

**TUTOR**

## DEDICATORIA

A Dios primero, que por medio de su inmensa misericordia y a través de su Hijo Amado Jesucristo me ha brindado salud, inteligencia y sabiduría para llegar a ser una persona de bien y crecer intelectualmente, y conseguir mi título profesional.

Dedico el presente a mis queridos Padres Bolívar Vera y Elvia Barrera, gracias por inculcarme el camino del bien. A mis hermanas, hermanos, sobrinos, y demás familiares. A mi Pastor Nelson Hidalgo, en los momentos críticos de mi vida, me guio y me brindó su apoyo incondicional.

Hilda Elizabeth Vera Barrera

## DEDICATORIA

Este proyecto se lo dedico a las tres personas incondicionales que tengo en mi vida, a mi querida madre Carmen Cecilia Cajas y padre José Nepta Soria quienes me han guiado y me han dado todo su apoyo durante mi vida universitaria y a querida amiga Hilda Elizabeth Vera por toda su confianza en cada paso que he dado, gracias por creer en mí.

Robert Eduardo Soria Cajas

## AGRADECIMIENTO

Agradezco primero a Dios, sin Él, no estaría donde estoy, siempre me ha dado las fuerzas y el aliento en los duros momentos, y en los buenos momentos siempre sentí, y siento que está conmigo. Nunca perdí la Fe, y gracias a Él, estoy por cumplir una meta en mi vida.

A mi Madre Elvia Elena Barrera Suárez, que siempre creyó en mí, desde un comienzo, y sé que desde el cielo me cuidas, por siempre te llevaré en mi mente y en mi corazón, mi Ángel.

A mi Padre Bolívar Santiago Vera Cevallos, mi motor para seguir adelante, gracias por los consejos y por estar conmigo siempre.

A mi familia por creer en mí, y darme el apoyo moral en todo momento.

A mi mejor amigo Robert, que desde un comienzo de mi carrera universitaria ha estado conmigo en las buenas y en las malas.

Al Abogado Berardo Rodríguez Msc, nuestro tutor, por la guía y colaboración y sobre todo disponibilidad desde el inicio al término de la tesis.

Hilda Elizabeth Vera Barrera

## **AGRADECIMIENTO**

Agradezco a mis padres por todo el esfuerzo que han puesto en darme todo lo necesario para lograr terminar mi carrera profesional.

A mi mejor amiga Hilda por ser un gran apoyo en todos los momentos más difíciles de mi vida.

A mi tutor Ab. Berardo Rodríguez por toda su ayuda en cada paso de este proyecto.

Robert Eduardo Soria Cajas

## TRIBUNAL PROYECTO DE TITULACIÓN

---

Ing. Eduardo Santos Baquerizo Msc  
DECANO DE LA FACULTAD  
CIENCIAS MATEMÁTICAS Y FÍSICAS

---

Ing. Harry Luna Aveiga Msc  
DIRECTOR  
CINT

---

Ab. MD Berardo Rodríguez Gallegos Msc  
PROFESOR DIRECTOR DEL  
PROYECTO DE TITULACIÓN

---

Lic. Pablo Alarcón  
PROFESOR TUTOR REVISOR  
DEL PROYECTO DE TITULACIÓN

---

Ab. Juan Chávez A.  
SECRETARIO



**DECLARACIÓN EXPRESA**

“La responsabilidad del contenido de este Proyecto de Titulación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la UNIVERSIDAD DE GUAYAQUIL”

ROBERT EDUARDO SORIA CAJAS

HILDA ELIZABETH VERA BARRERA



**UNIVERSIDAD DE GUAYAQUIL**  
**FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS**  
**CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES**

**ELABORACIÓN DEL PLAN DE MEJORAS DE SEGURIDAD DE LA**  
**INFORMACIÓN, BASADO EN LA APLICACIÓN DE LA NORMA**  
**ISO 27001 -2013 PARA EL DEPARTAMENTO DE**  
**INFRAESTRUCTURA DE LA**  
**EMPRESA RIGHTTEK S.A.**  
**DE LA CIUDAD DE**  
**GUAYAQUIL**

Proyecto de Titulación que se presenta como requisito para optar por el  
título de  
INGENIERO EN NETWORKING Y TELECOMUNICACIONES

**Autores:**

Robert Eduardo Soria Cajas  
C.I. 0930087218

Hilda Elizabeth Vera Barrera  
C.I. 0921622908

**Tutor:**

Ab. MD Berardo Rodríguez Gallegos Msc.

**Guayaquil, diciembre del 2017**

## **CERTIFICADO DE ACEPTACIÓN DEL TUTOR**

En mi calidad de Tutor del proyecto de titulación, nombrado por el Consejo Directivo de la Facultad de Ciencias Matemáticas y Físicas de la Universidad de Guayaquil.

### **CERTIFICO:**

Que he analizado el Proyecto de Titulación presentado por los estudiantes ROBERT EDUARDO SORIA CAJAS E HILDA ELIZABETH VERA BARRERA, como requisito previo para optar por el título de Ingeniero en Networking y Telecomunicaciones cuyo tema es:

ELABORACIÓN DEL PLAN DE MEJORAS DE SEGURIDAD DE LA  
INFORMACIÓN, BASADO EN LA APLICACIÓN DE LA NORMA ISO 27001 -2013  
PARA EL DEPARTAMENTO DE INFRAESTRUCTURA DE LA EMPRESA  
RIGHTTEK S.A.  
DE LA CIUDAD DE GUAYAQUIL

Considero aprobado el trabajo en su totalidad.

Presentado por:

Soria Cajas Robert Eduardo    Cédula de ciudadanía N°0930087218  
Vera Barrera Hilda Elizabeth    Cédula de ciudadanía N°0921622908

Tutor: AB. MD Berardo Rodríguez Gallego Msc.  
**Guayaquil, diciembre del 2017**



**UNIVERSIDAD DE GUAYAQUIL**  
**FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS**  
**CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES**

**Autorización para Publicación de Proyecto de Titulación en Formato Digital**

**1. identificación del Proyecto de Titulación**

**2. Autorización de Publicación de Versión Electrónica del Proyecto de**

<b>Nombre Alumno:</b> Robert Eduardo Soria Cajas - Hilda Elizabeth Vera Barrera	
<b>Dirección:</b> Coop. Los Jardines Mz.4 V.8 - Alborada 5ta Etapa	
<b>Teléfono:</b> 0959197143 - 0985893908	<b>E-mail:</b> <a href="mailto:hilda.verab@ug.edu.ec">hilda.verab@ug.edu.ec</a> , <a href="mailto:robert.soriac@ug.edu.ec">robert.soriac@ug.edu.ec</a>

<b>Facultad:</b> CIENCIAS MATEMÁTICAS Y FÍSICAS
<b>Carrera:</b> INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES
<b>Título al que opta:</b> Ingeniería en Networking y Telecomunicaciones
<b>Profesor guía:</b> AB. MD Berardo Rodríguez Gallegos Msc.

<b>Título del Proyecto de titulación:</b> ELABORACIÓN DEL PLAN DE MEJORAS DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA APLICACIÓN DE LA NORMA ISO 27001 - 2013 PARA EL DEPARTAMENTO DE INFRAESTRUCTURA DE LA EMPRESA RIGHTTEK S.A. DE LA CIUDAD DE GUAYAQUIL.
--

<b>Tema del Proyecto de Titulación:</b> Plan de mejoras, Seguridad de la Información, Norma ISO 27001 -2013, Departamento de Infraestructura
---

**Titulación.**

A través de este medio autorizo a la Biblioteca de la Universidad de Guayaquil y a la Facultad de Ciencias Matemáticas y Físicas a publicar la versión electrónica de este Proyecto de titulación.

**Publicación electrónica:**

Inmediata	Después de 1 año
-----------	------------------

Firma Alumno:

**3. Forma de envío:**

El texto del proyecto de titulación debe ser enviado en formato Word, como archivo .Doc. O .RTF y. Puf para PC. Las imágenes que la acompañen pueden ser: .gif, .jpg o .TIFF.

DVDROM ☒

CDROM ☐

## ÍNDICE GENERAL

CARTA DE APROBACIÓN DEL TUTOR.....	II
DEDICATORIA.....	III
DEDICATORIA.....	IV
AGRADECIMIENTO.....	V
AGRADECIMIENTO.....	VI
TRIBUNAL PROYECTO DE TITULACIÓN.....	VII
DECLARACIÓN EXPRESA.....	VIII
CERTIFICADO DE ACEPTACIÓN DEL TUTOR.....	X
ÍNDICE GENERAL.....	XII
ABREVIATURAS.....	XIV
ÍNDICE DE CUADROS.....	XV
RESUMEN.....	XVII
ABSTRACT.....	XVIII
CAPÍTULO I.....	5
EL PROBLEMA.....	5
PLANTEAMIENTO DEL PROBLEMA.....	5
Situación Conflicto. Nudos Críticos.....	7
Causas Y Consecuencias Del Problema.....	8
Delimitación del Problema.....	9
Formulación del Problema.....	10
Evaluación del Problema.....	11
Alcances del Problema.....	13
JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN.....	17
CAPÍTULO II.....	18
MARCO TEÓRICO.....	18
ANTECEDENTES DEL ESTUDIO.....	18
FUNDAMENTACIÓN LEGAL.....	52
FUNDAMENTACIÓN SOCIAL.....	57
Hipótesis.....	58
Variables de la Investigación.....	59
CAPÍTULO III.....	63

METODOLOGÍA.....	63
DISEÑO DE LA INVESTIGACIÓN.....	63
MODALIDAD DE LA INVESTIGACIÓN .....	63
Tipo de investigación.....	63
Población y Muestra .....	65
Recolección de información.....	69
Procesamiento y análisis .....	93
CAPÍTULO IV .....	94
PROPUESTA TECNOLÓGICA.....	94
Factibilidad operacional.....	107
Factibilidad Técnica.....	107
Factibilidad Económica.....	110
Entregables del proyecto .....	120
Criterios de aceptación del producto o servicio.....	127
Conclusiones y Recomendaciones .....	128
Bibliografía.....	130
ANEXOS .....	134

## ABREVIATURAS

<b>ISO</b>	International Standard Organization
<b>SGSI</b>	Sistema de Gestión de la Seguridad de la Información
<b>SI</b>	Seguridad Informática
<b>PHVA</b>	Planificar, Hacer, Verificar, Actuar
<b>TI</b>	TECNOLOGÍA DE LA INFORMACIÓN
<b>BS</b>	British Standards
<b>FTP</b>	File Transfer Protocol
<b>DHCP</b>	Dynamic Host Control Protocol
<b>LAN</b>	Local Área Network
<b>WLAN</b>	Wireless Local Área Network
<b>WAN</b>	Wide Área Network
<b>WIFI</b>	Wireless Fidelity

## ÍNDICE DE CUADROS

CUADRO 1	
Causas Y Consecuencias Del Problema .....	8
CUADRO 2	
Primeras normas ISO de seguridad .....	24
CUADRO 3	
Historia de la norma ISO 27001 .....	28
CUADRO 4	
Descripción de componente de la norma .....	35
CUADRO 5	
Descripción de la metodología PHVA .....	37
CUADRO 6	
Activos físicos .....	47
CUADRO 7	
Activos lógicos .....	47
CUADRO 8	
ISO 27001 & COBIT .....	48
CUADRO 9	
Análisis de Población y Muestra .....	66
CUADRO 10	
Instrumentos de Investigación .....	69
CUADRO 11	
Proceso de Checklist .....	71
CUADRO 12	
Programa de la auditoría .....	99
CUADRO 13	
Plan de la auditoria interna .....	101
CUADRO 14	
Costos de ejecución del proyecto .....	110
CUADRO 15	
Costos de ejecución de la auditoria .....	111
CUADRO 16	
Activos del área de Infraestructura .....	112
CUADRO 17	
Valoración de activos.....	113
CUADRO 18	
Abreviaturas .....	114
CUADRO 19	
Análisis de Amenazas en los activos .....	114
CUADRO 20	
Análisis de activos, vulnerabilidad y riesgo .....	116
CUADRO 21	
Análisis de Aplicabilidad .....	126
CUADRO 22	
Criterios de aceptación .....	127



## ÍNDICE DE GRÁFICOS

GRÁFICO 1	
Norma ISO.....	22
GRÁFICO 2	
Estructura de políticas de seguridad .....	25
GRÁFICO 3	
Familia de la norma ISO 27000 .....	26
GRÁFICO 4	
Número de certificaciones ISO 27001.....	31
GRÁFICO 5	
Número de certificaciones ISO 27001.....	32
GRÁFICO 6	
Componentes de la norma ISO 27001 -2013.....	34
GRÁFICO 7	
Ciclo PHVA.....	39
GRÁFICO 8	
Objetivos de la seguridad de la información.....	42
GRÁFICO 9	
Análisis de los controles Anexo 6 .....	120
GRÁFICO 10	
Expectación de los servidores del área.....	121
GRÁFICO 11	
Revisión del checklist .....	122
GRÁFICO 12	
Anotación de hallazgos.....	122
GRÁFICO 13	
Diseño de red de la Agencia Carchi.....	123
GRÁFICO 14	
Diseño de red de la Agencia Carchi.....	124



**UNIVERSIDAD DE GUAYAQUIL**  
**FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS**  
**CARRERA DE INGENIERÍA EN NETWORKING Y TELECOMUNICACIONES**

ELABORACIÓN DEL PLAN DE MEJORAS DE SEGURIDAD DE LA INFORMACIÓN,  
BASADO EN LA APLICACIÓN DE LA NORMA ISO 27001 -2013 PARA EL  
DEPARTAMENTO DE INFRAESTRUCTURA DE LA EMPRESA RIGHTTEK S.A.  
DE LA CIUDAD DE GUAYAQUIL

Autor: Hilda Elizabeth Vera Barrera

Autores: Robert Eduardo Soria Cajas

Tutor: AB. MD Berardo Rodríguez Gallegos Msc.

## **RESUMEN**

La norma ISO 27001 -2013 Seguridad de la Información, consiste en verificar si existe cumplimiento de los controles y las cláusulas establecidas por el estándar si se identifica el no cumplimiento de dichos controles en general se generan las no conformidades que son redactadas por el auditor mediante un informe. La auditoría se basa en los criterios de la Norma, es evidenciada y posee un proceso sistemático independiente. El trabajo de Investigación que se efectuó en el departamento de Infraestructura de la empresa Righttek S.A., consiste en brindar un plan de mejoras de seguridad de la información basado en la norma ISO 27001 -2013, en el cual asegura los datos a través de la confidencialidad, integridad, y disponibilidad, que garantice un tratamiento adecuado de los problemas de seguridad, teniendo como base las mejores prácticas, valorando los riesgos y procedimientos que producen en esta área.

**Palabras claves:** ISO 27001 -2013, plan de mejoras, evidencias,  
seguridad de la información, activos de información, controles.



**UNIVERSIDAD DE GUAYAQUIL  
FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS  
CARRERA DE INGENIERÍA EN NETWORKING Y  
TELECOMUNICACIONES**

ELABORATION OF INFORMATION SAFETY IMPROVEMENT PLAN,  
BASED ON THE APPLICATION OF ISO 27001-2013 STANDARD FOR  
THE RIGHTTEK S.A.  
COMPANY INFRASTRUCTURE DEPARTMENT OF  
THE CITY OF GUAYAQUIL

Author: Hilda Elizabeth Vera Barrera

Authors: Robert Eduardo Soria Cajas

Tutor: AB. MD Berardo Rodríguez Gallegos Msc.

**ABSTRACT**

The ISO 27001 -2013 Information Security standard consists of verifying whether there is compliance with the controls and the clauses established by the standard if the non-compliance of said controls is identified, in general, the non-conformities that are drafted by the auditor are generated. a report. The audit is based on the criteria of the Standard, is evidenced and has an independent systematic process. The research work carried out in the Infrastructure Department of Righttek SA, is to provide an information security improvement plan based on the ISO 27001-2013 standard, in which it ensures the data through confidentiality, integrity, and availability, which guarantees an adequate treatment of security problems, based on best practices, assessing the risks and procedures they produce in this area.

**Keywords:** ISO 27001 -2013, improvement plan, evidence, information security, information assets, controls.

## INTRODUCCIÓN

En la actualidad las amenazas a la cual afronta la información han ido evolucionando de una manera agresiva que busca en forma directa afectar el buen desempeño de las Organizaciones degradando su rendimiento, de las cuales van desde varias formas de ataques por medio de virus, hasta llegar a ataques recientes como ransomware y amenazas sofisticadas como los ataques día cero, lo cual solicita de forma urgente la implementación de controles que puedan ser gestionado a través de una apropiada visión de seguridad de la información. (Valencia-Duque & Orozco-Alzate, 2017)

Hoy en día establecer un plan de seguridad permite minimizar los riesgos, amenazas y vulnerabilidades de los activos de información, amortiguando un posible daño informático que ocasione pérdidas exuberantes de datos, logrando a que las Empresas entre en una crisis de carácter tecnológico y financiero, la ventaja de tener este plan de contingencia ayuda a las Corporaciones a estar preparados ante incidentes de seguridad que puedan ocurrir en un tiempo determinado cubriendo el aspecto físico y lógico del proceso, sin olvidar el factor humano que incide en técnicas o procedimientos que atentan con la seguridad de los datos.

La observación ha sido la esencia que ha permitido a lo largo de muchos años, permitir a los investigadores llegar a la conclusión científica, ideando

un experimento para ver el funcionamiento de las cosas.

La seguridad de los activos informáticos es un elemento especial para el desarrollo de las empresas, en la era digital que se afronta la información el uso no deseado del hardware, software y la falta de conciencia en el personal de un área, da paso a riesgos y amenazas que incidan en la red o en el entorno físico de un proceso. Identificar las amenazas, riesgos y fallos de seguridad mediante la auditoría en el departamento de Tecnología, ayuda a las entidades de índole pública y privada tener un breve conocimiento sobre el impacto negativo que provoca al no tener en cuenta los debidos procedimientos de técnicas de protección, de tal forma que permita establecer en forma correcta los niveles de seguridad que posee la misma.

Mediante la Metodología Magerit, se gestiona el riesgo, y realiza un análisis en el cual expone a los activos informáticos, con el fin de tener un mejor control sobre ellos, garantizando la seguridad de los sistemas y procesos de la empresa.

**Capítulo I.- EL PROBLEMA,** Se identifica la actual situación frente a la seguridad de la Información de la Empresa Righttek S.A., definiendo el problema que actualmente tienen, además se describen los objetivos generales y específicos para efectuar en conjunto con el tema, y a la vez se redacta la justificación e importancia del proyecto, dando como resultado los beneficios que se obtendrá.

**Capítulo II.- MARCO TEÓRICO,** se relata los antecedentes del estudio, donde se definen breves investigaciones de casos pertinentes a la seguridad de información en entornos de red y equipos de comunicación, profundizando el tema de titulación a desarrollar, fundamentación teórica, fundamentación social, y a su vez se describen las leyes ligadas al proyecto.

**Capítulo III.- METODOLOGÍA DE LA INVESTIGACIÓN,** Se menciona la modalidad, y el tipo de investigación que se ajusta al proyecto de investigación; también se explica las técnicas como la observación y la entrevista para la recolección de datos empleada para realizar el análisis de la información obtenida.

**Capítulo IV.- PROPUESTA TECNOLÓGICA,** En este último capítulo se detalla el análisis de factibilidad, la factibilidad técnica, operacional, económica y legal del proyecto de titulación referente al plan de mejoras utilizando la norma ISO 27001 -2013 seguridad de la información y los criterios de aceptación del producto que determinan la aprobación del mismo en la empresa Righttek S.A en la cual se implementará la propuesta.

## **CAPÍTULO I**

### **EL PROBLEMA**

#### **PLANTEAMIENTO DEL PROBLEMA**

##### **Ubicación del Problema en un Contexto**

La empresa Righttek S.A., ubicada en la ciudad de Guayaquil dio sus inicios desde el año 1998, brindando servicios de consultoría e implementación de aplicaciones administrativas, financieras y de comercio electrónico.

##### **Perfil de la Empresa**

###### **Misión**

Posicionarse entre las empresas que proveen servicios de tecnología y consultoría, con nivel alto de “calidad y eficiencia en la región.”

###### **Visión**

Otorgar soluciones integrales tecnológicas de calidad a todas las empresas y sectores industriales del Ecuador y la región en las áreas de desarrollo de sistemas de información, Telecomunicaciones, Redes y Seguridad.

Mediante el uso de metodologías probadas y con personal certificado en cada una de las ramas que representamos.

### **Fuente: Datos de la Empresa**

En la actualidad el departamento de Infraestructura de la Empresa Righttek S.A., no cuenta con políticas de seguridad y no posee un plan de contingencia que proporcione mecanismos para el tratamiento de eventos inesperados dando lugar a riesgos, amenazas y vulnerabilidades que afecten al funcionamiento de la red. Este lugar asume la responsabilidad de asegurar que la red de datos esté operativa sin ningún inconveniente que afecte a la funcionalidad de la misma, llevando a cabo operaciones de seguridad, servidores, sistemas operativos, mantenimiento de los equipos de computación, cableado estructurado, aplicaciones, configuraciones de redes LAN, WAN, WLAN, WIFI entre otros. El objetivo de esta área es proporcionar servicios de seguridad informática, mantenimiento e implementación de tecnologías de red de la organización. Es notable la carencia de controles en los activos físicos y lógicos que representa este departamento para la empresa, dando paso a la credibilidad de los tres entes fundamentales de la seguridad de la información, como lo son: confidencialidad, integridad y disponibilidad de los datos.

En el departamento de Infraestructura, sólo se encuentra un servidor FTP que cumple varias funciones, una de ellas la más importante es hacer de intermediario entre las computadoras de la Organización, el Firewall aplica mecanismos de control y bloqueo de comunicaciones no



autorizadas.

### **Situación Conflicto. Nudos Críticos**

Dentro del departamento de Infraestructura de la Empresa Righttek S.A., se lleva a cabo información de suma importancia, en la cual el problema surge debido a la falta de inversión y concientización en temas de seguridad por parte de la Organización, sobre una norma de seguridad de la información que facilite al líder del área los controles necesarios que ayuden a satisfacer los requerimientos de la compañía de índole corporativo, aumentando así la credibilidad de la misma.

Debido a los diferentes servicios que ofrece el departamento de Infraestructura a la red interna de la Empresa, el sistema eléctrico que energiza al departamento de Infraestructura no es el adecuado por lo que provocaría un apagado abrupto en los servidores del cual está a cargo el área afectando la productividad de toda la empresa.

**CUADRO 1 Causas Y Consecuencias Del Problema**

<b>Causas</b>	<b>Consecuencias</b>
Fallas en el sistema eléctrico	Cortocircuito en los dispositivos
Inexistencia de Backup	Pérdida de Información
Instalación de Programas crackeados	Infección de malware o código malicioso hacia los sistemas informáticos
Acceso vulnerables a los racks	Fácil manipulación físico de personas no autorizadas.
Fácil Ingreso al área de Infraestructura Tecnológica	Segregación de acciones mal intencionadas
No existe procesos de Sistemas Redundantes	Discontinuidad en el funcionamiento de la red
Falta de Conocimiento por parte del personal de tecnología	Falla de controles o políticas de seguridad que protejan los activos de información de la Empresa

**Fuente: Datos de Investigación**  
**Elaborado por: Robert Soria – Hilda Vera**

### **Delimitación del Problema**

El presente proyecto se desarrollará bajo la norma ISO 27001 -2013, y se limitará a los activos de información que se manejan dentro del departamento de infraestructura de la Empresa Righttek S.A., definir los controles que son aplicables al proceso a auditar, en el plan de mejoras, encontrando hallazgos en los servidores, Firewall, gestión ambiental, conexiones físicas, lógicas y roles del personal encargado del área, con el fin de evitar eventos adversos al buen funcionamiento de la red y operación de la misma.

**CAMPO:** SEGURIDAD DE LA INFORMACIÓN

**ÁREA:** Red Interna del Departamento de Infraestructura Righttek S.A.

**ASPECTO:** PLAN DE MEJORAS

**TEMA:** “ELABORACIÓN DEL PLAN DE MEJORAS DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA APLICACIÓN DE LA NORMA ISO 27001 -2013 PARA EL DEPARTAMENTO DE INFRAESTRUCTURA DE LA EMPRESA RIGHTTEK S.A. DE LA CIUDAD DE GUAYAQUIL”

## **Formulación del Problema**

¿Cómo y por qué elaborar el plan de mejoras de la seguridad de la Información en base a los controles y requerimientos de la norma ISO 27001 -2013, para la debida administración de activos de información y así salvaguardar los procesos que se llevan a cabo en la red interna del departamento de Infraestructura de la Empresa Righttek S.A. de la ciudad de Guayaquil?

El plan de mejoras, no solo permite ayudar a mitigar y examinar los riesgos, también ayuda a la toma de decisiones que fundamente al conocimiento que parte a través de la recopilación de datos, y concretar el impacto de las amenazas, riesgos, vulnerabilidades, que resguarden las futuras decisiones que se tome con respecto al negocio. (Arana Northia, 2016)

Con respecto, a lo anterior citado es importante realizar el plan de mejoras, porque se identifica los puntos débiles de un proceso o área auditada, y con los controles a aplicar se reduce el impacto que se pueda generar si no se tiene una debida gestión de control de riesgos. Hoy en día una eventual Auditoría para una posterior certificación de Seguridad de Sistemas de Información, cubre una demanda a las Organizaciones, porque al contar con la necesidad de una guía, permitirá a mitigar los riesgos y vulnerabilidades, que se enfrentan a diario y en diferentes escenarios los sistemas frente a los ataques tantos de manera interna y /o externa, una vez identificados. (Arana Northia,

2016)

### **Evaluación del Problema**

Los factores tomados en cuenta en el presente proyecto, se acogen a la investigación y desarrollo a continuación son:

**Delimitado:** Puesto que en la actualidad no se ha establecido un plan de concientización sobre políticas de seguridad de la información, controles, normas, en el personal del departamento de Infraestructura y la Empresa Righttek S.A, para un debido uso de los activos de información. Por lo tanto, se encuentra expuesto los servidores y equipos de computación a las amenazas y riesgos, afectando la integridad de los datos.

**Concreto:** Se refiere a un objetivo común que es el plan de mejoras de la seguridad de la información, para contrarrestar vulnerabilidades en los activos de información del departamento de Infraestructura de la Empresa Righttek de la ciudad de Guayaquil.

**Evidente:** A simple vista es notable la ausencia de controles que brinda en su totalidad la norma ISO 27001 -2013, a los activos de información que posee el departamento de Infraestructura, incitando diversos problemas que llegase afectar la continuidad y operatividad de las actividades del área.

**Factible:** Con la elaboración del plan de mejoras sobre la seguridad de Información en base a los controles de la norma ISO 27001 -2013, se podrá determinar el nivel de seguridad que posee el departamento de Infraestructura, y por medio de la propuesta se podrá sugerir a la Organización un respectivo tratamiento para los riesgos.

**Relevante:** La importancia que tiene la Norma ISO 27001 -2013 en el departamento de Infraestructura de la Empresa Righttek S.A, se halla en los diversos controles que se deben emplear para salvaguardar la información, con ello se pueden tomar decisiones en base a la gestión de los riesgos, la cual si no se aplica podrá destruir la Organización dado que es un activo de información muy valioso.

**Original:** La norma ISO 27001 -2013 es una solución innovadora para el departamento de Infraestructura de la empresa Righttek S.A, enfatizando los controles de seguridad para mitigar los riesgos que amenazan la integridad de la información, siendo la flexibilidad para adaptarse a las PYMES una de las ventajas más notables, brindando respuestas apropiadas frente a distintos acontecimientos en la seguridad de la información.

**Identifica los productos esperados:** activos de información, eficaz, ajustable, control y políticas de seguridad para minimizar vulnerabilidades en los sistemas y entorno físico de la empresa.

### **Alcances del Problema**

El presente proyecto de Investigación tiene como alcance realizar la auditoría a los activos de información, que incluye los componentes de hardware, software y factor ambiental que prevalece actualmente en el departamento de Infraestructura, y según los requisitos del Anexo A de la norma ISO 27001 -2013 y los objetivos de control, entregar un plan de mejoras de seguridad de la información en el cual se refleje el estado actual del área, aplicando los controles adecuados para verificar así los problemas existentes de la Empresa Righttek S.A

El autor Chamba Maleza Jennifer, en su proyecto de investigación recalca lo siguiente:

(Chamba Maleza, 2017) Dice: “El plan Informático no establece políticas de seguridad para los sistemas de información a razón de que estos sistemas actúan en base de sus propias normas y tienen manuales de operación predefinidos.”

En base a lo anterior citado, en el presente proyecto de Investigación, la limitante del plan de seguridad es que no establece políticas de seguridad que obligue a la Organización adaptarlo al departamento de TI, ya que ellos tienen sus propios estándares de ejecución de operaciones y el presente plan tiene como fin que ellos visualicen los puntos a críticos y en un futuro efectúen los controles propuestos.

Cabe recalcar que el proyecto no implica la certificación legítima de la

ISO 27001 -2013. La demostración del plan de mejoras, aplica la norma vigente del país y órganos de control de la ISO 27001:2013, que permitirá conocer la identificación y evaluación de los activos y determinar las prevenciones para que no ocurra alguna insolvencia, pérdida o interrupción de información por un daño que se produzca en los diferentes elementos del área.

El autor Ing. García Araque Javier, en su trabajo de Investigación, relata lo siguiente:

(García Araque, 2017) Dice: “Establecer un diagnóstico inicial de los procesos a auditar, para posteriormente planear como realizar la auditoría, que recursos se van a necesitar y en qué tiempo se llevará a cabo; luego de ejecutar la auditoría.”

Realizar el plan de mejoras en base al Anexo A objetivos de control y controles de referencia de la Norma ISO/IEC Segunda Edición 27001 - 2013 (SGSI, 2014), iniciando como primer paso la auditoría para el departamento de Infraestructura que permite tener un punto de partida para el reconocimiento del área, conociendo sus debilidades y fortalezas.

El plan incluye como punto primordial para la propuesta el documento de confidencialidad a las partes interesadas, en el cual evidencia los recursos y procedimientos realizados en el área auditada.

En el proceso del proyecto incluye la entrevista al Líder responsable del departamento de Infraestructura de la Empresa Righttek S.A., quien



otorgará información acerca del área, procesos y procedimientos en base a la protección y seguridad de la información.

(27001:2013, ISO, 2015) Dice la ISO: “Durante estas entrevistas, las preguntas van dirigidas a la familiarización de las personas con las funciones y los roles que tienen, además de conocer si cumplen con todos los controles que se encuentran implementados.”

## **OBJETIVOS DE LA INVESTIGACIÓN**

### **Objetivo general**

ELABORAR EL PLAN DE MEJORAS DE SEGURIDAD DE LA INFORMACIÓN, BASADO EN LA APLICACIÓN DE LA NORMA ISO 27001 -2013 PARA EL DEPARTAMENTO DE INFRAESTRUCTURA DE LA EMPRESA RIGHTTEK S.A. DE LA CIUDAD DE GUAYAQUIL.

### **Objetivos Específicos**

- Realizar el levantamiento de Información, analizando los activos de Información que posee el Departamento de Infraestructura de la Empresa Righttek S.A.
- Identificar las amenazas, riesgos y vulnerabilidades de los activos y procesos en el departamento de infraestructura Righttek S.A.
- Evaluar las políticas de seguridad que se podría implementar para un debido procesamiento de datos en la red.
- Analizar el plan de mejoras de buenas prácticas sobre la seguridad de la información en base a la Norma ISO 27001 -2013, para el departamento de la Empresa Righttek.

## **JUSTIFICACIÓN E IMPORTANCIA DE LA INVESTIGACIÓN**

La norma ISO 27001 -2013, es uno de los estándares de la seguridad de la información más importante y utilizada por las organizaciones cuyo objetivo principal es satisfacer sus necesidades en base a los problemas presentes en los centros de datos. La Empresa Righttek S.A. en el departamento de infraestructura se tiene como propósito diagnosticar qué medidas de seguridad se deben tomar para una respectiva implementación del estándar que ayude a los especialistas en el área de tecnología estar preparados ante incidentes o anomalías que pueden ocasionar el daño permanente de los activos de carácter confidencial. (García Araque, 2017)

Realizar el análisis al departamento de infraestructura, provee a la Empresa Righttek S.A., los resultados óptimos referente al levantamiento de información, e identificar las vulnerabilidades y amenazas en los activos de información, con el fin de aplicar mejoras en el proceso auditar, además esta auditoría es de gran ayuda a la compañía en mención por la cual se da a conocer a la Organización los riesgos latentes y por medio de los controles de seguridad que se detalla en el plan de mejoras proporciona soluciones en donde exista la remediación de los sitios críticos. Los beneficiarios del proyecto de investigación son las partes interesadas, en este caso el Líder del departamento de Infraestructura, da la aprobación para el establecimiento del plan de mejoras a la cual se le brinda servicios de seguridad en la red.

## **CAPÍTULO II**

### **MARCO TEÓRICO**

#### **ANTECEDENTES DEL ESTUDIO**

En la actualidad las empresas recopilan información de sus clientes, usuarios en sistemas informáticos en donde a través de un correo electrónico, video chat, y otras funciones que los mantienen comunicado.

Según el autor Ing. Javier García Araque, en su Tema de Investigación: (García Araque, 2017) Dice: “Desde finales del siglo XX junto al auge de las tecnologías de la información y su productivo en las empresas se identificaron debilidades en la conformación de sistemas informáticos e infraestructuras tecnológicas.”

Referente a lo anterior expuesto, las organizaciones buscan a diario el modo de llegar a protegerse ante diversas amenazas y lograr garantizar credibilidad a sus clientes, con el cumplimiento de lineamientos apegados a los estándares que le consientan poseer la confianza necesaria y establecer el adecuado negocio.

En Ecuador se consigue descubrir casos que han implantado la norma ISO 27001 -2013, como es el caso de la Empresa CNT (Corporación Nacional de Telecomunicaciones), Empresa Pública en el sector de las Telecomunicaciones, en su sitio web publicaron la noticia el 29 de mayo del año 2015, el Gerente General recibió el reconocimiento conforme a la Norma UNE-ISO/IEC 27001:2007 por parte de la Asociación Española de Normalización y Certificación AENOR (Ecuador), recalcando en ese año, “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 de la información que maneja”. (Sala de Prensa CNT, 2015)

(Doria Corcho, 2015) dice: “El departamento TI, no sólo soporta las estrategias del negocio existentes de una compañía, sino que genera nuevas habilidades, agregando el valor a los productos y servicios que la organización ofrece.”

Lo anterior citado, se argumenta que el área de Infraestructura de toda Empresa juega un papel sumamente importante, y se debe mantener en un ambiente seguro donde tenga controlado los niveles de riesgo informático, evitando así que los usuarios malintencionados puedan cometer fraudes.

En la actualidad se considera que la gestión adecuada de la seguridad de la información no sólo permite a la Empresa dar cumplimiento a sus

obligaciones y regulaciones, sino que garantiza las medidas de protección que son de gran ayuda para salvaguardar los datos, mediante estas normas se han generado confianza en sus trabajadores internos, externos y clientes. (Mina Calderón, 2015) , en el departamento de Infraestructura de Righttek, lugar donde se lleva a cabo las operaciones de Infraestructura y redes, establecer los protocolos necesarios, permite minimizar los riesgos y vulnerabilidades que se puedan producir tanto en componentes físicos, lógicos en la red de información de la Organización. Se puede citar el proyecto de Investigación por Rosales Paúl y Suárez Mery, en una Institución Financiera Ecuatoriana promovieron a un análisis del escenario realizando como punto de partida en donde incluyeron el personal y sus funciones, materiales, servidores que brindan dentro de la Organización, esquemas de redes, infraestructura de la comunicación. (Rosales Bravo, 2015)

La elaboración de una lista de componentes que conforma el área en donde se identifique los activos de información, permite tener en claro lo que se lleva a cabo en la misma. Es considerable tomar en cuenta los factores de seguridad que simbolice una pérdida de confianza a la privacidad de la información, dando como resultado estadísticas que arrojen aspectos negativos, y que a lo largo perjudique el avance de la Empresa.

La investigación realizada por el Autor (Cedeño Tenorio, 2017), fundamenta que los riesgos cumplen con dos características que son la “probabilidad

de que la amenaza explote la vulnerabilidad y que el impacto se materialice formando una amenaza, dando como resultado los niveles de riesgos”. La evaluación y el cálculo se basan en parámetros como el tiempo de recuperación de la Institución, posibilidad real de ocurrencia del riesgo referente al intervalo de cortes en las actividades. En lo citado, se basa en el análisis de riesgo por medio de la evaluación que se hace a través de la auditoría informática de sistemas realizada en un entorno en donde se encuentra comprometida la información siendo necesario segmentar los procesos, para mitigar futuros problemas que se presenten con el transcurso del tiempo.

El autor (Coral Ojeda, 2017), en su investigación “DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD PARA LA RED DE DATOS BAJO LA NORMA ISO 27001 -2013 EN EL CENTRO DE ESTUDIOS EMSSANAR CETEM DE LA CIUDAD DE PASTO” dentro de su estudio redacta las normas, basado en el modelo dirigido al área de seguridades, funcionarios y terceros que intercambian la información, definiendo políticas de seguridad orientadas a la disminución de riesgos para la red de datos, mejorando su operatividad.

Según lo citado, es necesario establecer controles a los diferentes riesgos que se pueda anticipar, concediendo al personal del área de Tecnología optimizar y prevenir futuros ataques, en los procesos que operen dentro del mismo.

## FUNDAMENTACIÓN TEÓRICA

### GRÁFICO 1 Norma ISO



**Fuente:** (Mindiamart, s.f.)  
**Elaborado por:** Robert Soria – Hilda Vera

Se define por sus siglas ISO (Organización Internacional de Normalización), es una federación mundial de organismos nacionales de normalización (organismos miembros de ISO) que colabora en conjunto con la IEC (Comisión Electrotécnica Internacional), para el proceso de normalización electrónica. Es una asociación de estándares alineados a establecer oficialmente los objetivos de una empresa, ubicados en diferentes entornos ambientes. (ISO Online Browsing Platform (OBP))



## **Historia ISO**

La palabra ISO se expresa a raíz griega “igual”, siendo un ente independiente que pretende contribuir calidad, eficiencia, y una mejor seguridad en los sistemas de comunicación de las empresas de los diferentes países. La norma ISO (Organización Internacional de Normalización), se fundó en el año 1946, conformado por 64 delegados procedentes de 25 estados, reunión tuvo lugar en la nación de Londres, Inglaterra en el centro del Instituto de Ingenieros Civiles. En el año 1947, el 27 de febrero empezaron las operaciones y actividades a la creación de la ISO, y desde aquel año se han creado más de 19.500 normas para todas las secciones de producción, tecnológico, el sector salud, la industria, etc. La Organización ISO, tiene sede en Ginebra (Suiza), lugar donde se encuentra la Secretaría General de ISO, se inspeccionan a los demás países. (WeblogBlog Calidad ISO UOS Xtended Studies, 2014)

## **Normas ISO 27000**

Está desarrollada por esquemas contemplados por ISO e IEC, que enseña como una Organización que se orienta a un trascurso metodológico, documentado y encaminado a objetivos de seguridad y gestión de riesgos. (Rosero Proaño, 2015)

El proceso de la Norma, la página web de la ISO 27000, en su apartado indica que desde el año 1901, “BSI (British Standards Institution, la organización británica equivalente a AENOR en España)”. (ISO 27000.es, s.f.) es el ente que se responsabiliza en publicar normas de suma

importancia como:

### **CUADRO 2 Primeras normas ISO de seguridad**

BS 5750	Anunciado en el año 1979	Originado de la ISO 9001
BS 7750	Anunciado en el año 1992	Originado de la ISO 14001
BS 8880	Anunciado en el año 1996	Originado de OHSAS 18001

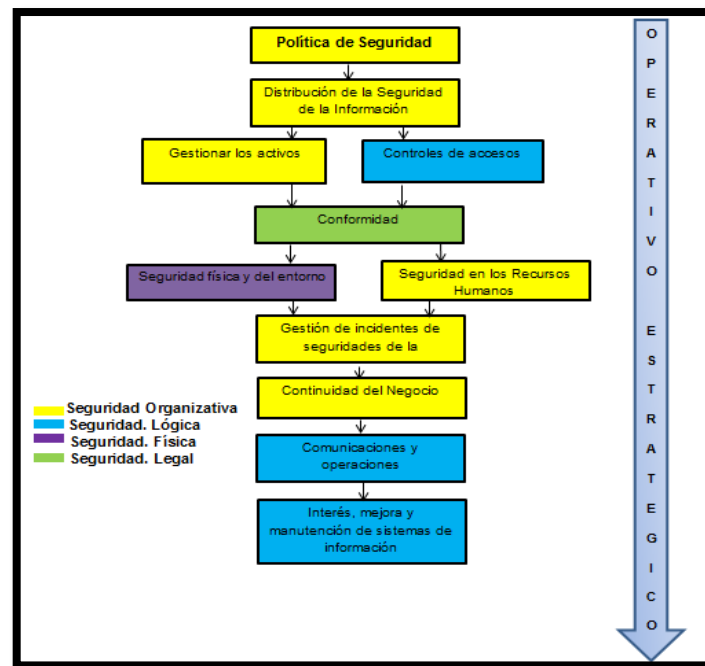
**Fuente: (ISO 27000.es, s.f.)**  
**Elaborado por: Robert Soria – Hilda Vera**

### **ORIGEN**

Según en el portal ISO27000, describe que la Norma ISO/IEC 27000 fue anunciada el “1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012, una tercera edición el 14 de enero de 2014 y una 4ta en febrero de 2016”. (ISO 27000.es, s.f.).

El autor Cedeño Jonathan, en su investigación relata, que la fecha de publicación de la norma ISO 27000, fue en el año 2008 en el mes de noviembre, conteniendo requisitos y conceptos que se implanta en toda la serie 27000. Se ha predicho que sea gratuita, referente a las otras series que sí tienen coste. (Cedeño Tenorio, 2017)

## GRÁFICO 2 Estructura de políticas de seguridad



Fuente: (tcp Dirige tu negocio: Controla tus procesos, s.f.)  
 Elaborado por: Robert Soria – Hilda Vera

GRÁFICO 3 Familia de la norma ISO 27000



**Fuente:** (Rosero Proaño, 2015)  
**Autores:** Robert Soria – Hilda Vera

### **Norma ISO 27001**

La Norma ISO 27001 es un estándar internacional publicado por la Organización Internacional de Normalización (ISO), escrita por expertos en este campo señala Dejan Kosutic, y que se ha convertido en un consenso de las principales prácticas de seguridad de información; por ende, no conlleva un solo autor. (Kosutic, Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios, 2016).

Define la norma el Autor Castro Rojas como “la única norma internacional auditable que define los requisitos para un sistema de gestión de seguridad de la información (SGSI), y se ha concebido para garantizar la selección de controles de seguridad adecuados y a proteger los activos de información dando confianza a las partes interesadas”. (Castro Rojas, Farigua Gutiérrez, & Suárez Cortés, 2016)

En lo citado anteriormente se argumenta que la norma ISO 27001 está encaminada directamente a determinar los controles y hallazgos que arroje la auditoría, con el fin de proteger los activos de la Empresa.

### Origen de la Norma ISO 27001

En la página Oficial del SGSI, en la sección de Blog, relata acerca del Origen e historia de la norma en mención, e indica; International Organization for Standardization y la Comisión International Electrotechnical Commission fueron los encargados de anunciar esta norma en el año 2005, y es el eje principal de la evolución de otras normas sobre la seguridad de la información. (Un blog editado por ISOTools Excellence, 2013)

**CUADRO 3 Historia de la norma ISO 27001**

<b>Año</b>	<b>Breve Reseña</b>
1901	British Standards Institution, anuncia normas con el prefijo “BS” con carácter internacional.
1995- BS 7799-1:1995	Empresas Británicas empleaban mejores prácticas para solventar a la administración de la Seguridad de la información, esta metodología no permitía certificación

1998 – BS 7799-2:1999	Síntesis de la norma anterior, establece requisitos para implementación de un SGSI certificable.
1999 – BS 7799-1:1999:	Sólo se repasa
2000 – ISO/IEC 17799:2000	Sin experimentar inmensos cambios, la ISO tomó a la norma BS 7799-1, que dio lugar a la ISO 17799.
2002 – BS 7799-2:2002	Anuncio de nueva versión con acreditación de empresas por un ente certificador en Reino Unido, y otros
2005 – ISO/IEC 27001:2005 e ISO/IEC17799:2005	Surge la ISO 27001 como norma internacional certificable y se analiza la ISO 17799 proporcionando la ISO 27001:2005.

2007 – ISO 17799:	Se denomina ISO 27002:2005
2007 – ISO/IEC 27001:2007	Anunciada nueva versión
2009	ISO 27001:2007/1M: 2009.  Publicado como documento adicional de reformas
2013	Propagación de la nueva versión de la ISO 27001, consigo trae evaluación y tratamiento de riesgos, adicional significativos cambios en su estructura.

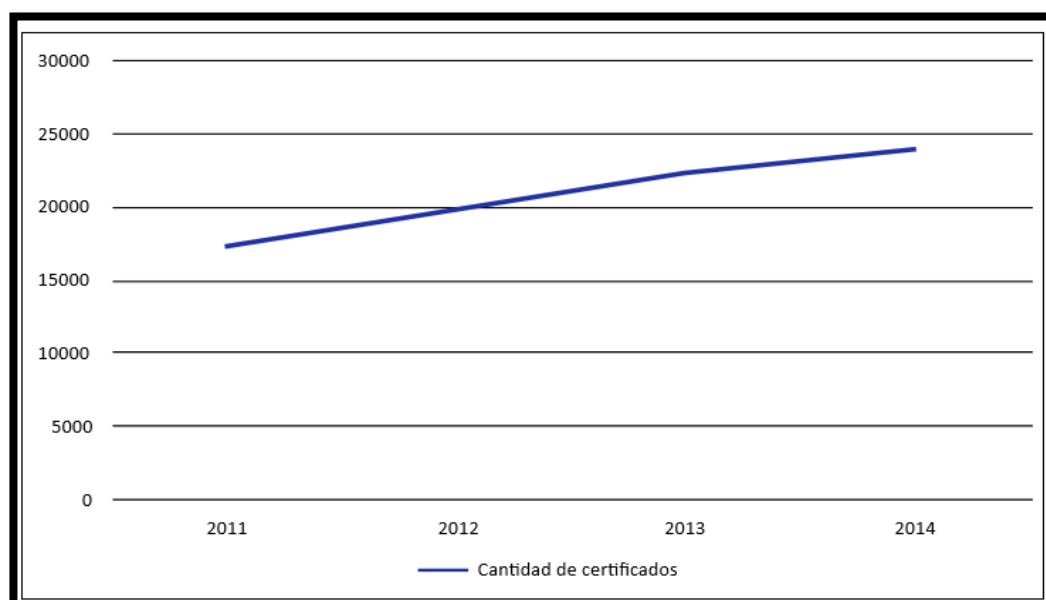
**Fuente:** (Un blog editado por ISOTools Excellence, 2013)

**Elaborado por: Robert Soria – Hilda Vera**



En los últimos años, las organizaciones se han certificado bajo esta norma que, a diferencia de otros modelos de normas de seguridad de la información, la norma ISO 27001 -2013 con la certificación acreditada, se podrá expresar hacia sus usuarios, socios, propietarios y otros comprometidos, en los lineamientos de cumplimientos. A continuación, el autor Dejan Kosutic en su libro primera edición, 2016 muestra una gráfica donde indica el número de certificados en los últimos años. (Kosutic, Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios, 2016)

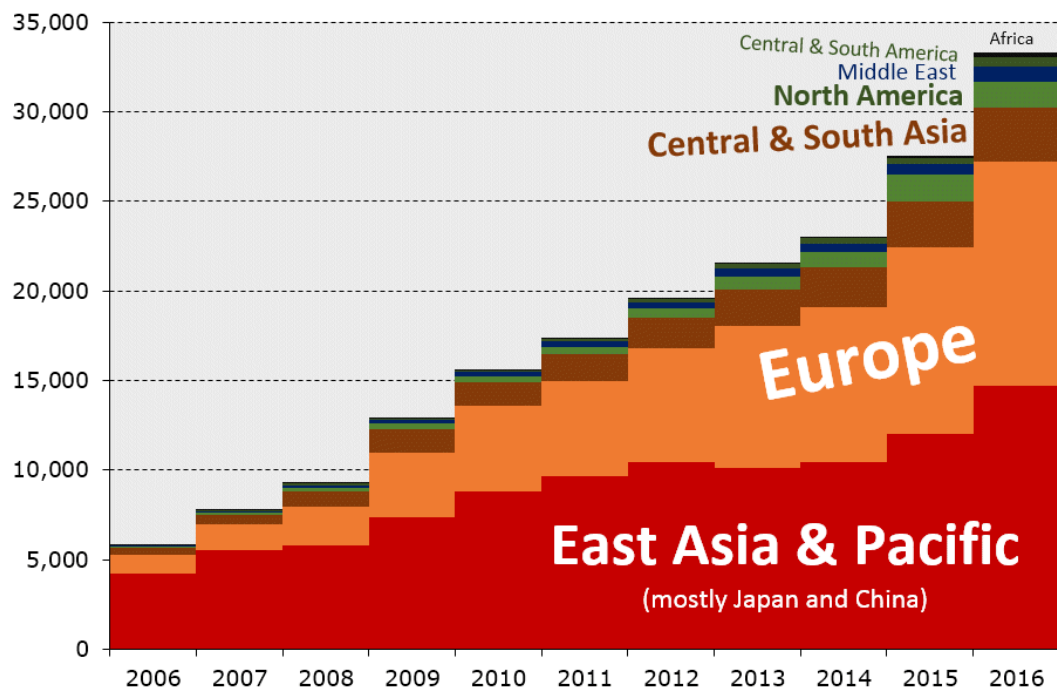
**GRÁFICO 4 Número de certificaciones ISO 27001**



**Fuente:** (Kosutic, Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios, 2016)

**Elaborado por:** Kosutic Dejan

**GRÁFICO 5 Número de certificaciones ISO 27001**



**Fuente:** <http://www.iso27001security.com/html/27001.html>

**Elaborado por:** Universidad de Princeton

### **Norma ISO 27001:2013**

#### **Definición**

El estándar ISO 27001 -2013, facilita métodos que describe los requerimientos para “establecer, implementar, mantener y mejorar continuamente un sistema de gestión de seguridad de la información” enfocándolo a las Empresas.

Es sustancial que los procesos y la estructura de la gestión de seguridad informática, sea considerada dentro del sistema de gestión de seguridad de la información, incluyendo el diseño de los procesos, controles en los sistemas informáticos. (Castro Rojas, Farigua Gutiérrez, & Suárez Cortés, 2016)

Se cita el artículo publicado por Intedya International Dynamic Advisors, en donde indica lo siguiente:

“El propósito de la norma ISO/IEC 27001 es, garantizar que los riesgos de la seguridad de la información sean gestionados adecuadamente por la organización”. (Advisors, Intedya International Dynamic, 2016)

Se justifica en lo citado, que la norma ISO/IEC 270001, tiene como finalidad velar el debido procesamiento de la información de toda Organización, empleando mecanismos y controles que protejan los datos. La ISO 27001-2013 establece de forma ordenada los requerimientos y procesos para tratar los riesgos, en donde la Organización se alinea a un avance fundamentado de un Sistema de Gestión.

En la revisión de la ISO 27001 realizada en el año 2013, muestra cambios importantes que se relaciona con la estructura de la parte esencial de la norma, objetivos, partes interesadas, medición y seguimiento, adicional el Anexo A cuenta con un número reducido de 133 a 114 en lo que implica a controles, con respecto a secciones de 11 a 14. Eliminación de acciones preventivas y documentación de ciertos procedimientos, están dentro de algunos requisitos omitidos y revisados en el 2013.

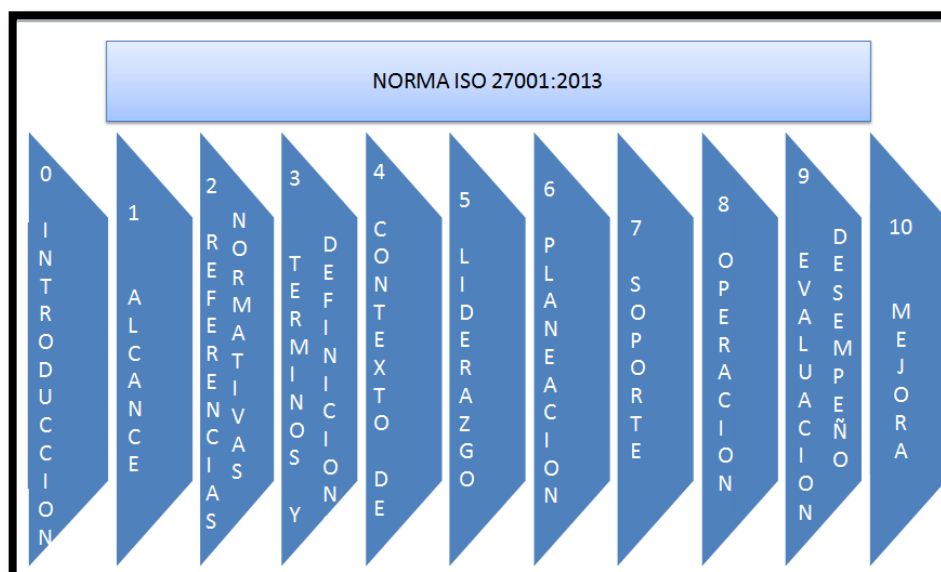
(Kosutic, Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios, 2016)

### Estructura de la ISO 27001 -2013

El tratamiento de la norma ISO 27001 -2013, en la cual ha sido anexado el documento SL, en el cual brinda una especificación, alineado bajo la misma estructura de todos los formatos que se conciernen al Sistema de Gestión de Seguridad de la Información. Con el desarrollo documentado de un Sistema de Gestión, en donde se evite problemas de unión con otros modelos referenciales. (Un blog editado por ISOTools Excellence, 2015)

De acuerdo a los cambios ocurridos, en la norma ISO 27001 -2013, a continuación, se describe cada uno de los siguientes componentes que la conforma:

**GRÁFICO 6 Componentes de la norma ISO 27001 -2013**



**Fuente:** (Un blog editado por ISOTools Excellence, 2015)

**Elaborado:** Robert Soria – Hilda Vera

**CUADRO 4 Descripción de componente de la norma**  
**ISO 27001-2013**

0 Introducción	Enfoque de Proceso
1 Alcance	Requisitos Genéricos de SGSI adaptados para empresas u organizaciones de cualquier índole.
2 Referencias Normativas	La norma ISO 27000 es principalmente para los usuarios de 27001.
3 Términos y Condiciones	Temporales definiciones formales.
4 Contexto de la Organización	Partes interesadas, define alcance del SGSI.
5 Liderazgo	Compromiso y Liderazgo por parte de la alta dirección hacia el SGSI, asigna política de mando, roles y autoridades de seguridad de la Información
6 Planificación	Proceso de identificar, analizar y planificar el tratamiento de los riesgos de información. Objetivos claros de la Seguridad de la Información.
7 Apoyo	Asigna recursos apropiados, aptos

	para control de la documentación.
8 Operación	Detalle de la evaluación y tratamiento de los riesgos de la información, gestión de cambios y documentación.
9 Evaluación del desempeño	Procesos de revisión a controles de seguridad de la información, sistemas de gestión con el fin de realizar mejoras sistemáticas en el momento apropiado,
10 Mejora	Auditorías y revisiones; ej.: no conformidades y acciones correctivas, para mejoras continuas al SGSI.
Anexo A  Objetivos y controles de control de referencia	El anexo A es “normativo”, es decir que se espera que las Empresas Certificadas la usen, sin necesidad de que se implante o aborde riesgos de información.

**Fuente:** (ISO/IEC 27001, s.f.)  
**Elaborado:** Robert Sora – Hilda Vera

### Metodología PHVA

Para estructurar todos los procesos del SGSI, el estándar 27001 acoge la guía “Planifica-Hacer-Verificar-Actuar”, para así establecer una organización de todos los procesos del SGSI.

**CUADRO 5 Descripción de la metodología PHVA**

Planear (Implantar el SGSI)	Para manejar el riesgo y mejora de la seguridad de la información se establece políticas, procesos, procedimientos y objetivos del SGSI, para otorgar resultados anexos a las políticas y objetivos de la Empresa.
Hacer (Efectuar y Aplicar el SGSI)	Realizar las políticas, procesos, procedimientos y controles del SGSI.
Verificar (Monitoreo y Análisis el SGSI)	En relación con los objetivos, políticas y prácticas realizadas del SGSI, se evalúan en donde se puede aplicar y así regular el desempeño del proceso, para reporte de resultados y observación por parte de la Empresa
Actuar (Conservar y optimizar el SGSI)	Para lograr el respectivo mejoramiento continuo del SGSI, las acciones correctivas y preventivas, se basan en los resultados del SGSI.

**Fuente:** (Solarte Solarte, ENRIQUEZ ROSERO, & Benavides Ruano, 2015)

**Elaborado por: Robert Soria – Hilda Vera**

## **Deming**

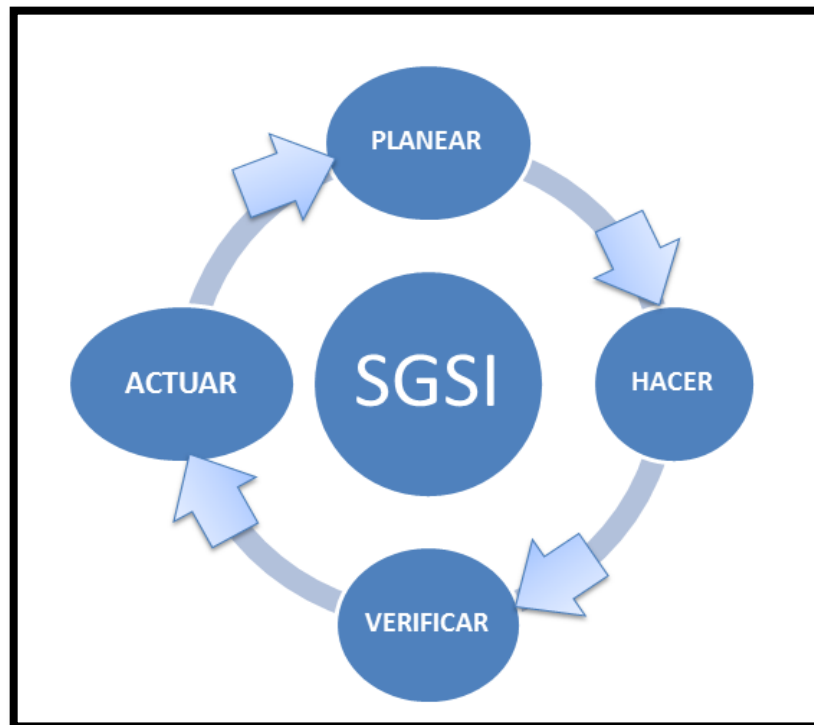
Terminología conocida también como PDCA (Plain-Do-Check-Act), que tiene el objetivo de definir una ciencia en el cual provoque un valor alto a la información y que sea aplicada en grandes y pequeñas empresas, que avale un nivel seguro a la integridad, disponibilidad y confidencialidad para impedir que los datos se vuelvan públicos sin previa autorización. (Bustamante, 2014).

Según Dejan Kosutic en su artículo, indica que el ciclo PDCA, tiene su significado que se desarrolló hace unos 60 años por un reconocido maestro de calidad de gestión, William Edwards Deming, con el fin de conceptualizarlo como gestión de calidad aplicado en todas partes referentes a estándares de gestión ISO. (Kosutic, 27001 Academy, 2014)

## **PHVA (PLAN-HACER-VERIFICAR-ACTUAR)**

Se determina una metodología que se compone y se refiere sobre la calidad de la seguridad de la información y la aplicabilidad de la misma en pequeñas Organizaciones que avale un método seguro de los tres factores que son: Integridad, disponibilidad y confidencialidad para impedir que dicha información se haga pública de forma no permitida, en sí la norma ISO 27001 -2013 en la que adopta el ciclo PHVA como metodología, para poder emplear todos los procesos que emite el SGSI. (Figuerola Pérez & Malagón Sáenz, 2017)



**GRÁFICO 7 Ciclo PHVA**

**Fuente:** (Un blog editado por ISOTools Excellence, 2015)  
**Elaborado por:** Robert Soria e Hilda Vera

Las “Cuatro etapas cíclicas” que compone el “círculo de Deming”, es un ciclo repetitivo es decir que una vez que se acabe una fase se debe retornar a la primera y reanudar de nuevo el ciclo, con el fin de la re-evaluación periódica de las actividades para en un momento dado agregar eventos flexibles de mejoras.

Se describe a continuación las etapas que compone el ciclo PHVA:

-Planear: Fase inicial, donde se evalúa el análisis y estudio del escenario actual de los riesgos de los activos de información de la Organización.

-Hacer: Fase donde se evalúa y analiza los riesgos. Implementa y opera el SGSI.

-Verificar: Fase en donde se implanta el control de todas las operaciones implantadas en el SGSI.

-Actuar: Fase de mantenimiento y mejora del SGSI, se realiza las acciones correctivas y preventivas de la Empresa. (Figueroa Pérez & Malagón Sáenz, 2017)

### **Definición de Seguridad de la Información**

Se define seguridad de la información, a la adopción de todas las prevenciones que toda empresa debe cumplir, siguiendo los objetivos de seguridad informática como son "la disponibilidad, confidencialidad e integridad de los activos". (Giraldo Cepeda, 2016)

Según en su fuente informativa ISOTools Excellence, publicado el 10 de agosto del 2017, señala que el objetivo de la Seguridad de la Información es "establecer la administración de la misma, siendo parte fundamental de los objetivos y las actividades de la empresa". (Un blog editado por ISOTools Excellence, 2017)

Para preservar los registros y archivos es necesario que las empresas adopten y apropien las debidas metodologías, para un debido

funcionamiento en la infraestructura tecnológica adecuada y que sea el responsable para la custodia y vigilancia de la información. (Solarte Solarte, ENRIQUEZ ROSERO, & Benavides Ruano, 2015)

El autor Miguel Ángel Mendoza, en su artículo publicado el 16 de junio de 2015, indica:

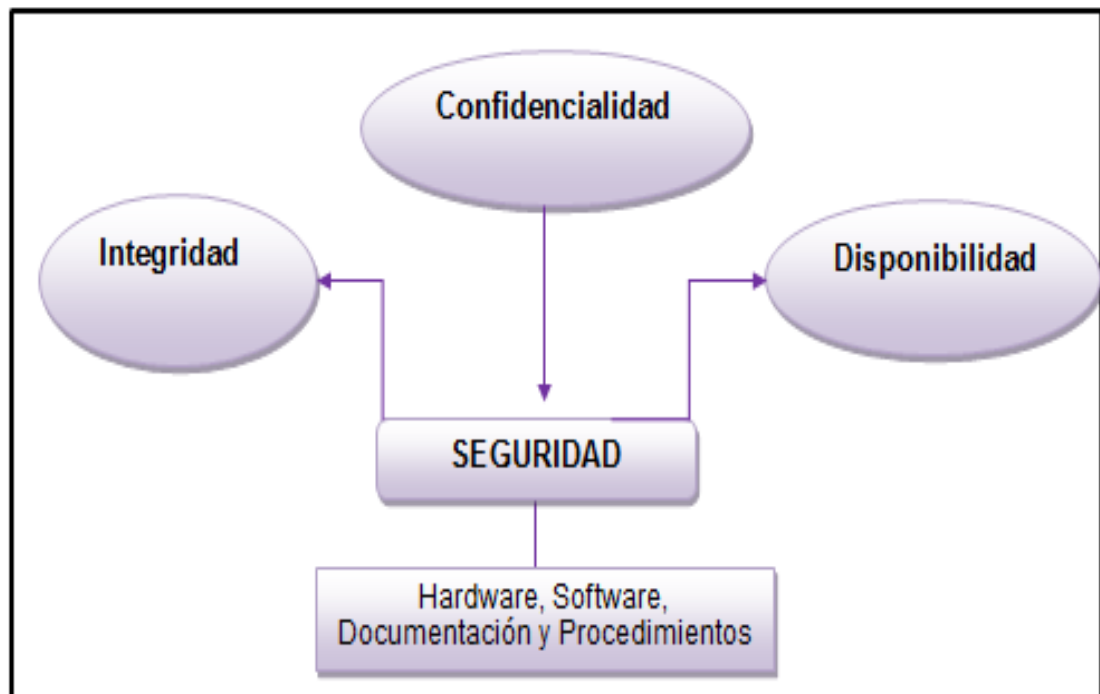
(MENDOZA, 2015) Dice: “Seguridad apunta a una condición ideal, ya que no existe la certeza de que se pueden evitar todos los peligros, su propósito es reducir riesgos hasta un nivel aceptable para los interesados”.

Las medidas que trata de abordar las medidas de Seguridad son;

- Protección de la confidencialidad de información
- Salvaguardar la “integridad de los datos”
- Autorizando el uso de datos, promoviendo la disponibilidad

Los objetivos ante mencionado, forman parte de la tríada que son: “confidencialidad, integridad, y disponibilidad (CIA)”. (Mark S. Merkow, 2014)

**GRÁFICO 8 Objetivos de la seguridad de la información**



**Fuente: Datos de Investigación**  
**Elaborado: Robert Soria – Hilda Vera**

### **Confidencialidad**

Se define a la confidencialidad el asegurar que el personal plenamente autorizado, posea el debido acceso a la información.

Dejan Kosutic, en su libro relata, acerca de la confidencialidad lo siguiente:

(Kosutic, Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios, 2016) En el libro el autor Kosutic, indica: “propiedad que hace que la información no esté disponible o sea revelada a individuos no autorizados, entidades o

procesos”

### **Disponibilidad**

Se define a la disponibilidad como el aseguramiento de la Información, esté al alcance y disponible para el personal autorizado, siempre que lo requiera. El autor Dejan Kosutic, la define como la “propiedad de ser accesible y usable bajo demanda por una entidad autorizada”. (Kosutic, Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios, 2016)

### **Integridad**

El autor Justino Salinas Zully en su trabajo de Investigación define a la integridad, a toda información debe mantenerse persistentemente correcta, compleja y protegida. (Justino Salinas, 2015)

## **Clasificación de la Seguridad**

### **Seguridad Física**

En base al concepto de la seguridad física, (Salamanca, 2016) refiere este término consiste en salvaguardar el lugar donde se encuentra los dispositivos de computación (ordenadores, software, hardware instalados, equipos electrónicos), adicional el control de acceso a salas de computación, que provee un correcto funcionamiento frente a las condiciones ambientales (temperatura, flujo eléctrico y humedad) de forma

que suministre energía eléctrica ininterrumpida. Con lo expuesto anteriormente se considera a la seguridad física la aplicación de herramientas y métodos predestinados a salvaguardar la información en las distintas plataformas informáticas que se lleva a cabo en una empresa.

### **Seguridad Lógica**

La seguridad lógica se define como el ente de protección de la información en el modo de usar aplicaciones y sistemas. Según en el artículo realizado por Salamanca Oscar, indica que la norma ISO/IEC 27002:2013(2015) constituye la seguridad lógica como una limitante al ingreso a la TI (Tecnología de la Información), a las aplicaciones y sus funciones dependiendo de la Organización y las políticas que establece. En sí asiste garantía de seguridad y protección de los medios y/o sistemas de tecnologías en una empresa, mediante parámetros de resguardo de la información. (Salamanca, 2016)

### **Auditor de Seguridad**

Es el agente delegado que tiene la profesión de analizar la seguridad de los distintos sistemas informáticos, equipos de comunicación (Hardware, Software y otros), aplicaciones, tecnologías de redes e informática que se utilizan dentro de una empresa. El auditor de seguridad propone un esquema de descubrimiento de vulnerabilidades (ataques hacia los activos informáticos y/o sistemas informáticos), las reporta para que de alguna forma se solucione con éxito.

### **Consultor de Seguridad**

Es la persona de perfil especializado con conocimientos amplios con respecto a la materia de seguridad de la información, se encarga de especificar el tipo de estrategia adecuada frente a la seguridad en las organizaciones, en diferentes entornos. Su función se basa en sugerir sobre la forma adecuada y eficaz de efectuar alguna acción con criterios técnicos, gestión o ambos en una empresa. (Moratilla, 2017)

## **Magerit**

### **Definición**

Según en el proyecto de investigación del Ing. Giraldo Luis, señala que es una metodología de análisis y gestión de riesgos y se enfoca principalmente en que todas las empresas deben optar por el uso de las tecnologías de la información para su rápido y correcto crecimiento. La Metodología Magerit proporciona procedimientos que permiten saber la medida y el valor de los activos además identifica el perfil de riesgo al que está expuesta la información de carácter confidencial. (Giraldo Cepeda, 2016)

Dentro de la Metodología de Magerit, la valoración de activos, es la fase importante en el Análisis de Riesgo, establece el valor de afectación a un activo frente a la utilidad de los servicios y procesos que abarca el negocio

de la Organización. El costo es la base para la valoración de los activos dentro de un área y que se produce debido a la falla y pérdida de disponibilidad, integridad, y confidencialidad, siendo el resultado de un problema ocasionado. (Mejía Viteri, 2016)

### **Activos de Información**

Según Miguel Ángel Mendoza en su artículo indica que la Norma ISO 27001 define todo activo de información como los conocimientos o datos que tienen valor para una organización, y señala lo siguiente:

(Carvajal Azcona, 2017) Dice: “Protección de activos de información, a través del tratamiento de amenazas que ponen en riesgo la información que es procesada, almacenada y transportada por los sistemas de información que se encuentran interconectados”.



**Los activos de información se clasifican en dos partes:**

**CUADRO 6 Activos físicos**

Hardware	Computador, UPS, dispositivos de networking, servidores, switches, routers, medios de almacenamiento.
Gestión documental	Se refiere a todos los datos de los procesos.

**Fuente: Trabajo de Investigación  
Elaborado por: Soria Robert – Vera Hilda**

**CUADRO 7 Activos lógicos**

Sistemas Informáticos	Sistemas Operativos:  -Windows  -Mac  -Linux
Aplicaciones	Antivirus  Navegadores web  Software de gestión financiero, administrativo, académico, etc.

**Fuente: Trabajo de Investigación  
Elaborado por: Soria Robert – Vera Hilda**

## CUADRO 8 ISO 27001 & COBIT

### DIFERENCIAS

	COBIT	ISO 27001
CARACTERÍSTICAS	<p>Fue publicado por primera vez en 1996, con el objetivo de controlar la función de TI , gestionar riesgos de sobrecarga en los recursos de TI, asegurar que la organización de TI alcance sus objetivos y que estén encaminados con los objetivos de negocio, también los objetivos de eficiencia, evaluación de madurez de proceso y medición del desempeño de la función de TI, la estructura de COBIT cubre 4 dominios la planificación y organización, adquisición e implementación, entrega y soporte, monitoreo y evaluación; estos dominios son procedidos por varios procesos y cada proceso incluye una serie de actividades con</p>	<p>El estándar fue creado y publicado en octubre de 2005 con el fin de formar un sistema para la gestión de la seguridad de la información, esta norma sustituye a la norma británica BS estándar 7799:2 que contenía las pautas y el estándar en sí, el cual hasta ese entonces era el principal estándar referenciando para la aplicación de un sistema de gestión de seguridad de la información. La norma 27001 puede ser adaptada con la norma ISO 27002 para proteger los recursos</p>

	objetivos específicos u objetivos de actividad.	de información, el objetivo de la norma 27001 es proteger los datos de todo tipo de amenazas asegurando su integridad, confidencialidad y disponibilidad, y puede aplicarse en muchos entornos empresariales
FUNCIONES	Orientación empresarial y gobierno de TI en su totalidad	Implementación de controles de seguridad, énfasis en el enfoque de gestión de riesgos
APLICABILIDAD	Planificación de procesos de TI	Sistema de gestión de la seguridad de la información
VENTAJAS	COBIT posee una fuerte vinculación con los objetivos empresariales en conjunto con el marco de TI de la organización, que incluye la aplicación, los datos, la infraestructura y los individuos. COBIT también tiene un gran	Las organizaciones pueden optar por implementar sólo las estrategias de seguridad necesarias para su organización y tener un camino claro para

	<p>enfoque hacia los objetivos de una organización y lo que debe lograrse para lograrlos, lo que incluye operaciones de negocios diarios, fusiones y seguridad de la información. COBIT crea un entorno de gestión de la información persistente que asegura soluciones de TI alineadas a los negocios y garantiza que los objetivos de una organización estén a la vanguardia de todos los empleados.</p>	<p>implementar una estructura adicional si sus necesidades de negocio cambian o se desarrollan. Estas fortalezas ofrecen un modelo flexible que se puede utilizar a la carta y crecer o adaptarse a medida que las necesidades de la organización cambian con el tiempo.</p>
DESVENTAJAS	<p>Las debilidades del marco COBIT son la falta de enfoque en cómo lograr los objetivos necesarios del marco COBIT. Esto deja el esfuerzo de implementar el marco para el equipo de gestión del cuerpo. Además, este marco puede ser difícil de implementar debido a la necesidad de que todos los interesados, participen en la creación y gestión de COBIT. Este</p>	<p>Esta norma tiene una visión amplia de las normas de seguridad para una organización y no desglosa en los requisitos específicos de acción necesarios para cumplir con los marcos sugeridos. La empresa u organización que implemente estas estructuras de seguridad</p>

	marco se debe implementar mientras la organización es bastante pequeña o se necesita reservar un tiempo significativo para identificar y crear todos los pasos necesarios para realizar plenamente el marco COBIT.	necesitará una comprensión profunda de los pasos que deben tomar para proteger su información vulnerable y una amplia capacidad técnica para seguir las directrices establecidas en el marco ISO 27002.
USADO POR LOS AUDITORES	Para proporcionar varios modelos de madurez y métricas que miden el logro, al mismo tiempo que identifica las responsabilidades de negocio asociadas de los procesos de TI	Para demostrar que la empresa sigue las mejores prácticas de seguridad de la información, proporcionando una evaluación independiente y especializada de si sus datos están adecuadamente protegidos.
CERTIFICACIÓN	No es certificable para organizaciones	Si es certificable

**Fuente: Trabajo de Investigación**  
**Elaborado por: Soria Robert – Vera Hilda**

## **FUNDAMENTACIÓN LEGAL**

### **CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR**

#### **TÍTULO II**

#### **DERECHOS**

#### **Capítulo sexto**

#### **Derechos de libertad**

**Art. 66 Numeral 19.-** El derecho a la protección de datos de carácter personal, que incluye el acceso y la decisión sobre información y datos de este carácter, así como su correspondiente protección. La recolección, archivo, procesamiento, distribución o difusión de estos datos o información requerirán la autorización del titular o el mandato de la ley. (Armando Costa & Valencia Vernaza, 2013)

### **CONSTITUCIÓN DE LA REPÚBLICA DEL ECUADOR**

#### **Sección octava**

#### **Ciencia, tecnología, innovación y saberes ancestrales**

**Art. 385.-** El sistema nacional de ciencia, tecnología, Innovación y saberes ancestrales, en el marco del respeto al ambiente, la naturaleza, la vida, las culturas y la soberanía, tendrá como finalidad:

- a) Generar, adaptar y difundir conocimientos científicos y tecnológicos.

- b) Desarrollar tecnologías e innovaciones que impulsen la producción nacional, eleven la eficiencia y productividad, mejoren la calidad de vida y contribuyan a la realización del buen vivir. (Romero Maldonado, 2015)

**Art. 386.-** El sistema comprenderá programas, políticas, recursos, acciones, e incorporará a instituciones del Estado, universidades y escuelas politécnicas, institutos de investigación públicos y privados, empresas públicas y privadas, organismos no gubernamentales y personas naturales o jurídicas, en tanto realizan actividades de investigación, desarrollo tecnológico, innovación y aquellas ligadas a los saberes ancestrales.

El Estado, a través del organismo competente, coordinará el sistema, establecerá los objetivos y políticas, de conformidad con el Plan Nacional de Desarrollo, con la participación de los actores que lo conforman.

**Art. 387.-** Será responsabilidad del Estado:

- a) Facilitar e impulsar la incorporación a la sociedad del conocimiento para alcanzar los objetivos del régimen de desarrollo.
- b) Promover la generación y producción de conocimiento, fomentar la investigación científica y tecnológica...

- c) Asegurar la difusión y el acceso a los conocimientos científicos y tecnológicos, el usufructo de sus descubrimientos y hallazgos en el marco de lo establecido en la Constitución y la Ley.
  - d) Garantizar la libertad de creación e investigación en el marco del respeto a la ética, la naturaleza, el ambiente...
  - e) Reconocer la condición de investigador de acuerdo con la Ley.
- (CONSTITUCIÓN DEL ECUADOR)

## **LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS PÚBLICOS**

### **Capítulo II PRINCIPIO GENERALES DEL REGISTRO DE DATOS PÚBLICOS**

**Art. 4** Responsabilidad de la Información. - Las instituciones del sector público y privado y las personas naturales que actualmente o en el futuro administren bases o registros de datos públicos, son responsables de la integridad, protección y control de los registros y bases de datos a su cargo. Dichas instituciones responderán por la veracidad, autenticidad, custodia y debida conservación de los registros. La responsabilidad sobre la veracidad y autenticidad de los datos registrados, es exclusiva de la o el declarante cuando esta o este provee toda la información.

Las personas afectadas por información falsa o imprecisa, difundida o



certificada por registradores o registradores, tendrán derecho a las indemnizaciones correspondientes, previo el ejercicio de la respectiva acción legal.

La Dirección Nacional de Registro de Datos Públicos establecerá los casos en los que deba rendirse caución. (LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS, 2010)

## **Código Orgánico Integral Penal**

### **CAPÍTULO TERCERO**

#### **DELITOS CONTRA LOS DERECHOS DEL BUEN VIVIR**

##### **SECCIÓN TERCERA**

Art. 229.- **Revelación ilegal de base de datos.** - La persona que, en provecho propio o de un tercero, revele información registrada, contenida en ficheros, archivos, base de datos o medios semejantes, a través o dirigidas a un sistema electrónico, informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Si esta conducta se comete por una o un servidor público, empleadas o empleados bancarios internos o de instituciones de la economía popular y solidaria que realicen intermediación financiera o contratistas, será

sancionada con pena privativa de libertad de tres a cinco años. (informática jurídica.com, 2017)

## **LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y**

### **MENSAJES DE DATOS**

**Ley No. 2002-67**

**CONGRESO NACIONAL**

#### **Título I**

#### **DE LOS MENSAJES DE DATOS**

##### **Capítulo I**

##### **Principios Generales**

**Art. 9.-** Protección de datos. - Para la elaboración, transferencia o utilización de bases de datos, obtenidas directa o indirectamente del uso o transmisión de mensajes de datos, se requerirá el consentimiento expreso del titular de éstos, quien podrá seleccionar la información a compartirse con terceros.

La recopilación y uso de datos personales responderá a los derechos de privacidad, intimidad y confidencialidad garantizados por la Constitución Política de la República y esta ley, los cuales podrán ser utilizados o transferidos únicamente con autorización del titular u orden de autoridad competente.

No será preciso el consentimiento para recopilar datos personales de fuentes accesibles al público, cuando se recojan para el ejercicio de las funciones propias de la administración pública, en el ámbito de su

competencia, y cuando se refieran a personas vinculadas por una relación de negocios, laboral, administrativa o contractual y sean necesarios para el mantenimiento de las relaciones o para el cumplimiento del contrato.

El consentimiento a que se refiere este artículo podrá ser revocado a criterio del titular de los datos; la revocatoria no tendrá en ningún caso efecto retroactivo. (LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS (Ley No. 2002-67))

### **FUNDAMENTACIÓN SOCIAL**

El presente proyecto de investigación se desempeña en mitigar las problemáticas de los procesos de activos de información, como el hardware, software y factor ambiental que existe en el departamento de Infraestructura de la Empresa Righttek S.A., con la elaboración de la actual Norma ISO 27001 -2013, en los controles del Anexo A.

Además, el estudio, alcanza los siguientes efectos;

#### **¿Qué impacto social tendrá la implementación del proyecto?**

El impacto que tendrá la elaboración del plan de mejoras basado en la Norma ISO 27011 -2013, ayudará a salvaguardar la información que se lleva a cabo en el área por medio de los sistemas informáticos, brindando a los usuarios internos, Líder, y al Gerente de la Empresa, disponibilidad, integridad y confidencialidad de los datos.

**¿De qué manera va a intervenir o a resolver la problemática existente?**

Por medio de la Herramienta de análisis de riesgos Magerit, se detecta las vulnerabilidades y amenazas de los activos de información en el departamento de Infraestructura de la Empresa Righttek S.A., donde se determina el nivel de mayor a menor impacto que podría generar si no se tiene una solución inmediata, ofreciendo pautas para que la información que se encuentra en los sistemas informáticos estén protegidas en su totalidad, y así evitar algún evento adverso al buen funcionamiento de la red.

**¿Qué impacto tiene en la comunidad?**

Los usuarios internos que laboran en la Empresa Righttek S.A., quienes facilitan su información a ser almacenada por medio de los sistemas informáticos que son administrados por el personal del departamento de Infraestructura, se sabrá que, por medio del plan de mejoras, la Organización se encuentra preparada para una futura certificación, generando credibilidad y confianza en los procesos de los activos de información.

**Hipótesis**

¿Sera posible que el plan de mejoras basado en la norma ISO 27001 -2013 reduzca los fallos de seguridad de la información en el departamento de Infraestructura de la Empresa Righttek S.A.?

## **Variables de la Investigación**

**Variable independiente:** ISO 27001 -2013

**Variable dependiente:** Plan de Mejoras

## **DEFINICIONES CONCEPTUALES**

### **Plan de Mejoras**

Un plan de mejoras consiste en el agrupamiento de medidas de cambio que se toman en base al problema identificado por el auditor que está realizando la auditoría una vez establecido este plan, las organizaciones tienen la capacidad de tomar decisiones para el tratamiento del riesgo, evitando así causas mayores. **(ISOTools, 2015)**

### **Checklist**

Se define como una lista de apoyo para el auditor, en el cual se revisan los puntos relacionado a una norma, que apoya a contemplar los objetivos de la auditoría, ofreciendo al plan de auditoría las evidencias necesarias para asegurar la continuidad y profundidad del objetivo de la auditoría, facilitando el desarrollo de la norma ISO 27001 -2013. (Castro Rojas, Farigua Gutiérrez, & Suárez Cortés, 2016). En síntesis, es una lista de comprobación o también llamado cuestionario que tiene como alcance lo que se está evaluando o los objetivos que se pretende alcanzar.

## **Entrevista**

Técnica empleada para recolección de datos, y es la más usada en el ámbito de las investigaciones, seguido de la técnica de las encuestas, a diferencia que la entrevista es una técnica cualitativa.

“El éxito de la entrevista, depende de los siguientes factores (repartidos por igual entre el auditor y el entrevistado): la experiencia y los conocimientos del auditor y la predisposición y los conocimientos del entrevistado.” (Barros Marcillo & Cadena Marten, 2012)

## **Auditoría Interna**

Se define la auditoría como la labor y responsabilidad del auditor (latín “audire”, que quiere decir oír.

“La palabra auditoría es el examen crítico y sistemático que realiza una persona o grupo de personas independientes del sistema auditado.” (P Verdezoto, 2015)

## **Evidencia**

Se define la evidencia a cualquier información utilizada por el auditor, para establecer si cumple los criterios u objetivos implantados, la auditoría realizada a la Organización o los datos. (Kosutic, Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios, 2016)

La evidencia es una exigencia que hace que el auditor a través de las

conclusiones que realizó, se apoye en evidencias capaces, justas y relevantes.

### **Políticas de Seguridad**

Las Políticas de Seguridad se interpreta que forma parte de la gestión de protocolos a proseguir por la Organización y su personal, con el fin de sobrepasar las amenazas y vulnerabilidades que se logren mostrar y perturben a los sistemas de información, y para garantizar un buen uso es necesario la documentación, con el objetivo de certificar que el coste para realizar aquellas políticas, no sobresalga la reparación de acontecimientos adversos a la seguridad.

### **Amenazas**

Se define a las amenazas, a las fallas, virus, uso incorrecto de software, a los ingresos no autorizados, terremotos o inundaciones, factores ambientales, etc. En síntesis, las amenazas son aquellas operaciones que pueden afectar y producir resultados negativos en la operatividad de la Organización.

### **Vulnerabilidad**

Se define a la vulnerabilidad, una debilidad que abarca todo sistema informático, y que logra ser usada para ocasionar un daño, suelen presentarse en diferentes formas en los elementos de un ordenador, que puede ser tanto en componentes de hardware, software, sistemas operativos, aplicaciones, etc.

## **Riesgo**

Los riesgos se refieren a eventos no deseados que pueden tener impacto negativo en la seguridad de la información, y por lo tanto en la empresa, tales como una inundación que pueda destruir información en papel. (Kosutic, Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios, 2016)

## **Hallazgos**

Los hallazgos se denominan como las observaciones vistas por el auditor durante el proceso de auditoría, un hallazgo puede ser evidenciado para la comprobación de la anomalía detectada por el auditor.

Según Kosutic Dejan, define un hallazgo como la columna de todo lo que se ha escrito durante un periodo de auditoría formal, que contiene los nombres de los encargados de las áreas de una organización, lo que dijeron, los contenidos y registros de lo que se inspeccionó, diseño del sitio donde se visitó, los equipos y las observaciones descritas en ellos, etc. (Kosutic, Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios, 2016)



### **CAPÍTULO III**

#### **METODOLOGÍA**

#### **DISEÑO DE LA INVESTIGACIÓN**

##### **MODALIDAD DE LA INVESTIGACIÓN**

Este trabajo de titulación se consideró para su modalidad como proyecto factible, debido a los procesos que se utilizan como el análisis y el estudio de la seguridad de la información en el área de infraestructura, para la elaboración de un modelo que solucione las disconformidades sacadas de la auditoria basada norma ISO 27001.

El presente trabajo de investigación observa un estudio teórico que recaba información y/o propuestas de reconocidos autores y científicos en el tema exponiendo las mejores ideas en base a la Norma ISO 27001 -2013, visualizando caso de estudios en campo, por lo que es importante y necesario obtener información veraz, actualizada y concisa del origen. (Aguila Plaza, 2015)

##### **Tipo de investigación**

El presente proyecto se efectuó como una investigación de proyecto factible, teniendo en cuenta que se contemplan tópicos, como el diagnostico, planteamiento de la propuesta, actividades, procedimientos

metodológicos, análisis y recursos que se enfoca en los objetivos de la presente tesis, el cual permite elaborar la propuesta del manual de buenas prácticas con el fin de dar una solución a los problemas que amenazan la Información del área de infraestructura de la Empresa Righttek S.A.

### **Métodos de Investigación**

#### **Método científico**

En el presente proyecto de investigación en proceso, se utiliza el Método Científico, que es el siguiente: “la adaptación de lineamientos alineados a la seguridad de la información en base a la investigación de las causas y consecuencias que son conllevados al planteamiento del problema, dará como solución la aplicación de una norma que ayude a mejorar la seguridad de los activos de información de la empresa Righttek S.A.

El estándar de seguridad informática ISO 27001 -2013, es aquel estándar que suministra los controles que auxilian a mitigar los niveles de riesgos presentes en la compañía en la que se ejecutará el proyecto mencionado en párrafos anteriores. La definición del método científico es un proceso de transformación consecuente y establecida en los distintos entornos que se enfocan a realizar una operación prolongada de la mente.

## **Método Analítico**

Al aplicar este método de investigación se realiza un análisis profundo en los sistemas de gestión de seguridad de la información descomponiendo y analizando cada una de las partes que lo conforma, logrando observar vulnerabilidades en el entorno de los sistemas y riesgos a los que está expuesto, este análisis es asentado en la observación consiguiendo estudiar cómo se protege los activos, enfocándolo a los resultados de auditoria, conociendo la naturaleza del fenómeno y comprendiendo su esencia.

“Este método permite conocer más del objeto de estudio, con lo cual se puede: explicar, hacer analogías, comprender mejor su comportamiento y establecer nuevas teorías.” (Arias, 2012).

Según se expresa en la cita anterior después de emplear el método analítico se tendrá la explicación del problema y analogías que servirán para analizar el cumplimiento de los controles del anexo A de la norma ISO 27001-2013.

“Analizar significa desintegrar, descomponer un todo en sus partes para estudiar en forma intensiva cada uno de sus elementos, así como las relaciones entre sí y con el todo.” (Arias, 2012).

## **Población y Muestra**

## **Población**

La empresa Righttek está conformado por 157 personas de la cuales nos vamos a enfocar en el Ingeniero que trabajan como líder en el área de Infraestructura de la organización ofreciéndonos toda la información relevante.

**CUADRO 9 Análisis de Población y Muestra**

<b>Población</b>	<b>Muestra</b>
Líder del Área de Infraestructura	1
<b>TOTAL</b>	<b>1</b>

**Fuente: Datos de Investigación**  
**Autores: Robert Soria – Hilda Vera**

Ya que la población a la cual se auditará no sobrepasa los 250 resulta innecesario llevar a cabo un muestreo, considerando el total de nuestra población como muestra

## **Técnicas e instrumentos de Recolección de datos**

Siendo una investigación de campo la que se realizó en la empresa Righttek, contamos con los diversos instrumentos para el levantamiento de información y analizar el estado actual de la organización.

## **Técnica**

## **Observación**

Es la adquisición activa de información de una fuente primaria, en la ciencia, la observación implica el registro de datos mediante el uso de instrumentos refiriéndonos a cualquier dato recogido durante la actividad científica. Se conoce que el método científico requiere de observaciones para formular y probar hipótesis que consiste en los siguientes pasos.

- Hacer una pregunta sobre un fenómeno natural.
- Hacer observaciones del fenómeno.
- Hipotética una explicación del fenómeno.
- Predicción de consecuencias lógicas y observables de la hipótesis que aún no se han investigado.
- Prueba de las predicciones de la hipótesis por un estudio de campo que es lo que realizaremos.
- Formando una conclusión partir de los datos recogidos en el experimento, o haciendo una hipótesis revisada / nueva y repitiendo el proceso.
- Escribir una descripción del método de observación y los resultados o conclusiones alcanzados.
- Revisión de los resultados por pares con experiencia investigando el mismo fenómeno.

Las observaciones juegan un papel muy importante en los pasos segundo y quinto del método científico. Sin embargo, la necesidad requiere que las

observaciones de diferentes observadores puedan ser comparables por eso es recomendable ser realizada por 2 o más personas.

## **Entrevista**

La entrevista periodística es conocida como la acción del intercambio de ideas de dos personas en donde se quiere descubrir un hecho o un pensamiento mediante preguntas abiertas o cerradas.

Durante nuestro proyecto se realizaron entrevistas periodísticas destinadas a recolectar datos relevantes sobre la seguridad de la información que tiene el área, dándonos a conocer la situación en la que se encuentra el área, todas las preguntas fueron hechas para hallar las no conformidades que existen basadas en la norma, que proporciona información, concretando las hipótesis sobre los hitos de la ISO 27001 en el área de infraestructura.

**CUADRO 10 Instrumentos de Investigación**

<b>Técnica</b>	<b>Tipo</b>	<b>Instrumento</b>	<b>Orientación</b>
Observación	Participante	Registro anecdótico, cuaderno de protocolo, diario de campo, cámara de fotos.	Observación natural
Entrevistas	No Estructurada	Libretas de notas, Grabadora/cámara de video	Entrevista Periodística

**Fuente: Datos de Investigación**  
**Autores: Robert Soria – Hilda Vera**

### **Recolección de información**

La recolección de la información se realiza el día en que se inició el proceso de auditoria empezando por la observación de forma generalizada por todo el departamento de infraestructura reconociendo e identificando las vulnerabilidades en la seguridad de la información, después del recorrido por toda el área de infraestructura y los equipos que están bajo su control, se procede con la entrevista realizada al líder del área, para lo cual se realizan preguntas abiertas basándose en un checklist o tablero de notas de la norma ISO 27001 -2013, cumpliendo con todos los controles que son

asociados al proceso a auditar. Para la ejecución de este proceso se cuenta con el tiempo de dos días tomando en consideración a los integrantes y al líder de dicho proceso logrando recabar la mayor cantidad de información posible para el análisis y la procedente elaboración del manual de buenas prácticas.

A continuación, se aprecia una tabla con las preguntas basadas en la norma ISO 27001-2013 y las respuestas que se obtuvieron mediante la entrevista.



CUADRO 11 Proceso de Checklist

ANEXO			ESTADO	RESPUESTA
<b>A5 POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN</b>				
<b>A5.1</b> Orientación de la dirección para la gestión de la seguridad de la información				
<b>Objetivo: Brindar orientación y soporte, por parte de la dirección, para la seguridad de la información de acuerdo con los requisitos del negocio y con las leyes y reglamentos pertinentes</b>				
<b>A5.1.1</b>	Políticas para la seguridad de la información	¿Existen políticas publicadas, aprobadas por la dirección, para apoyar la seguridad de la información?	No cumple	no existen políticas
<b>A5.1.2</b>	Revisión de las políticas para la seguridad de la información.	¿Las políticas de seguridad de la información son revisadas y actualizadas?	No cumple	al no existir políticas no se pueden hacer revisiones de las mismas
<b>A6 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN</b>				
<b>A6.1</b> Organización interna				
<b>Objetivo: Establecer un marco de referencia de gestión para iniciar y controlar la implementación y operación de la seguridad de la información dentro de la organización.</b>				
<b>A6.1.1</b>	Roles y responsabilidades para la seguridad de la información	¿Están definidas todas las responsabilidades de seguridad de la información?	No cumple	no existen definida las responsabilidades de la seguridad de la información
<b>A6.1.2</b>	Separación de deberes	¿Los deberes y las responsabilidades son correctamente segregados teniendo en cuenta las situaciones de conflicto de intereses?	cumple parcialmente	La tareas que se realizan en el área son

				segregadas gracias al personal pero no es algo constante.
<b>A6.1.3</b>	Contacto con las autoridades	¿Existen definidas contactos con las autoridades competentes?	No cumple	No existen tenemos conocimiento de autoridades competentes.
<b>A6.1.4</b>	Contacto con grupos de interés especial	¿Existen definidos contactos con grupos de interés especial o asociaciones profesionales?	Cumple parcialmente	Se tiene contacto con personal especializado pero no para todos los problemas que se pueden presentar en el área.
<b>A6.1.5</b>	Seguridad de la información en la gestión de proyectos.	¿Los proyectos consideran aspectos relacionados con la seguridad de la información?	No cumple	no se han considerando
<b>A6.2</b> Dispositivos móviles y teletrabajo <b>Objetivo: Garantizar la seguridad del teletrabajo y el uso de dispositivos móviles</b>				
<b>A6.2.1</b>	Política para dispositivos móviles	¿Existen definidas reglas para el manejo seguro de los dispositivos móviles?	No cumple	no existen políticas para dispositivos móviles

<b>A6.2.2</b>	Teletrabajo	¿Existen reglas que definen cómo está protegida la información de la organización teniendo en cuenta el teletrabajo?	Cumple parcialmente	Existen reglas pero no han sido estipulado dentro de una SGSI
<b>A7 SEGURIDAD DE LOS RECURSOS HUMANOS</b>				
<b>A7.1</b> Antes de asumir el empleo				
<b>Objetivo: Asegurar que los empleados y contratistas comprenden sus responsabilidades y son idóneos en los roles para los que se consideran.</b>				
<b>A7.1.1</b>	Selección	¿La organización realiza verificaciones de antecedentes de los candidatos para el empleo o para los contratistas?	No aplica	Este proceso se encarga el área de Recursos Humanos
<b>A7.1.2</b>	Términos y condiciones del empleo	¿Existen acuerdos con los empleados y contratistas donde se especifiquen las responsabilidades de seguridad de información?	No aplica	Este proceso se encarga el área de Recursos Humanos
<b>A7.2</b> Durante la ejecución del empleo				
<b>Objetivo: Asegurarse de que los empleados y contratistas tomen conciencia de sus responsabilidades de seguridad de la información y las cumplan.</b>				
<b>A7.2.1</b>	Responsabilidades de la dirección	¿La dirección requiere activamente que todos los empleados y contratistas cumplan con las reglas de seguridad de la información?	No aplica	Este proceso se encarga el área de Recursos Humanos
<b>A7.2.2</b>	Toma de conciencia, educación y formación en la seguridad de la información.	¿Los empleados y contratistas asisten a entrenamientos para realizar mejor sus tareas de seguridad, y existen programas de sensibilización?	No aplica	Este proceso se encarga el área de Recursos Humanos

<b>A7.2.3</b>	Proceso disciplinario	¿La organización tiene un proceso disciplinario?	No aplica	Este proceso se encarga el área de Recursos Humanos
<b>A7.3</b> Terminación y cambio de empleo <b>Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o terminación de empleo</b>				
<b>A7.3.1</b>	Terminación o cambio de responsabilidades de empleo	¿Existen acuerdos que cubren las responsabilidades de seguridad de información que siguen siendo válidas después de la terminación del empleo?	No aplica	Este proceso se encarga el área de Recursos Humanos
<b>A8 GESTIÓN DE ACTIVOS</b> <b>A8.1</b> Responsabilidad por los activos <b>Objetivo: Identificar los activos organizacionales y definir las responsabilidades de protección adecuadas.</b>				
<b>A8.1.1</b>	Inventario de activos	¿Existe un inventario de activos?	cumple parcialmente	se tiene un inventario pero no está actualizado
<b>A8.1.2</b>	Propiedad de los activos	¿Todos los activos en el inventario de activos tienen un dueño designado?	cumple parcialmente	Existen activos etiquetados con personal que ya no labora
<b>A8.1.3</b>	Uso aceptable de los activos	¿Existen definidas reglas para el manejo de activos y de información?	No cumple	no se han identificado y no existe un documento sobre uso

				aceptable de activos
A8.1.4	Devolución de activos	¿Los activos de la organización son devueltos cuando los empleados y contratistas finalizan su contrato?	no aplica	
<b>A8.2</b> Clasificación de la información <b>Objetivo: Asegurar que la información recibe un nivel apropiado de protección, de acuerdo con su importancia para la organización.</b>				
A8.2.1	Clasificación de la información	¿Están definidos los criterios para clasificar la información?	No cumple	la información que se maneja en el área no ha sido clasificada
A8.2.2	Etiquetado de la información	¿Existen procedimientos que definen cómo etiquetar y manejar información clasificada?	No cumple	como la información no ha sido clasificad no se puede etiquetar
A8.2.3	Manejo de activos	¿Existen procedimientos que definen cómo manejar activos?	No cumple	no existen procedimientos para el manejo de los activos
<b>A8.3</b> Manejo de medios <b>Objetivo: Evitar la divulgación, la modificación, el retiro o la destrucción no autorizados de información almacenada en los medios</b>				
A8.3.1	Gestión de medio removibles	¿Existen procedimientos que definen cómo manejar medios extraíbles en consonancia con las reglas de clasificación?	No cumple	no existen políticas para la gestión de

				medios removibles
<b>A8.3.2</b>	Disposición de los medios	¿Existen procedimientos formales para la eliminación de medios?	No cumple	no existen políticas para cumplir con este control
<b>A8.3.3</b>	Transferencia de medios físicos	¿Son protegidos los medios que contienen información sensible durante el transporte?	No cumple	no existen políticas para la transferencia de medios físicos
<b>A9 CONTROL DE ACCESO</b>				
<b>A9.1</b> Requisitos del negocio para el control de acceso				
<b>Objetivo: Limitar el acceso a información y a instalaciones de procesamiento de información.</b>				
<b>A9.1.1</b>	Política de control de acceso	¿Existe una política de control de acceso?	no cumple	no hay políticas para el control de acceso
<b>A9.1.2</b>	Acceso a redes y a servicios en red	¿Los usuarios tienen acceso sólo a los recursos que se les permite?	cumple parcialmente	hay restricciones para los usuarios al acceso de la redes pero no para los servicios una vez dentro de la red
<b>A9.2</b> Gestión de acceso de usuarios				
<b>Objetivo: Asegurar el acceso de los usuarios autorizados y evitar el acceso no autorizado a sistemas y servicios.</b>				

<b>A9.2.1</b>	Registro y cancelación del registro de usuarios	¿Los derechos de acceso son proporcionados mediante un proceso de registro formal?	cumple parcialmente	Se tiene conocimiento de los procesos para cancelar o registrar un usuario pero no está debidamente formalizado
<b>A9.2.2</b>	Suministro de acceso de usuarios	¿Existe un sistema de control de acceso formal para el inicio de sesión en sistemas de información?	cumple parcialmente	Se tiene conocimiento del proceso para suministrar acceso a los usuarios pero no existen un proceso formalizado que satisfaga este control
<b>A9.2.3</b>	Gestión de derechos de acceso privilegiado	¿Los derechos de acceso privilegiado son manejados con especial cuidado?	no cumple	no existe procedimientos para gestionar los accesos privilegiados
<b>A9.2.4</b>	Gestión de información de autenticación secreta de usuarios	¿Las contraseñas, y otra información de autenticación secreta, son proporcionadas de forma segura?	cumple parcialmente	En ciertos activos si aplica pero no en todos

<b>A9.2.5</b>	Revisión de los derechos de acceso de usuarios	¿Los propietarios de activos comprueban periódicamente todos los derechos de acceso privilegiado?	No cumple	las revisiones no son periódicas,
<b>A9.2.6</b>	Retiro o ajuste de los derechos de acceso	¿Los derechos de acceso son actualizados cuando hay un cambio en la situación del usuario (por ejemplo: cambio organizacional o terminación)?	cumple parcialmente	Si se realizan los cambios o se revocan los accesos pero no existe un proceso formalizado
<b>A9.3</b> Responsabilidades de los usuarios <b>Objetivo: Hacer que los usuarios rindan cuentas por la salvaguarda de su información de autenticación.</b>				
<b>A9.3.1</b>	Uso de información de autenticación secreta	¿Existen reglas para los usuarios sobre cómo proteger las contraseñas y otra información de autenticación?	Cumple parcialmente	si existen credenciales pero muchas veces los usuarios suelen compartirla exponiendo al mal uso de la misma
<b>A9.4</b> Control de acceso a sistemas y aplicaciones <b>Objetivo: Evitar el acceso no autorizado a sistemas y aplicaciones.</b>				
<b>A9.4.1</b>	Restricción de acceso a la información	¿El acceso a la información en los sistemas es restringido según la política de control de acceso?	Cumple parcialmente	no existen políticas de control de acceso



<b>A9.4.2</b>	Procedimiento de ingreso seguro	¿Es requerido un sistema de login en los sistemas según la política de control de acceso?	cumple satisfactoriamente	todos los equipos que se manejan en el área poseen un sistema de login
<b>A9.4.3</b>	Sistema de gestión de contraseñas	¿Los sistemas de gestión de contraseñas utilizados por los usuarios de la organización les ayuda a manejar de forma segura su información de autenticación?	no cumple	No existen sistemas que gestionen las contraseñas que usan los usuarios
<b>A9.4.4</b>	Uso de programas utilitarios privilegiados	¿El uso de herramientas de utilidad es controlado y limitado a empleados específicos?	cumple parcialmente	Si es limitada pero no está aplicada a todos los empleados
<b>A9.4.5</b>	Control de acceso a códigos fuente de programas	¿El acceso al código fuente es restringido a personas autorizadas?	no cumple	No existen controles para eso
<b>A10 CRIPTOGRAFÍA</b>				
<b>A10.1 Controles criptográficos</b>				
<b>Objetivo: Asegurar el uso apropiado y eficaz de la criptografía para proteger la confidencialidad, autenticidad y/o la integridad de la información</b>				
<b>A10.1.1</b>	Política sobre el uso de controles criptográficos	¿Existe una política para regular la encriptación y existen otros controles criptográficos?	no cumple	No existen políticas sobre el uso de controles criptográficos

A10.1.2	Gestión de llaves	¿Están debidamente protegidas las claves criptográficas?	no cumple	No existen claves criptográficas
A11	SEGURIDAD FÍSICA Y DEL ENTORNO			
A11.1	Áreas seguras			
Objetivo: Prevenir el acceso físico no autorizado, el daño e la interferencia a la información y a las instalaciones de procesamiento de información de la organización.				
A11.1.1	Perímetro de seguridad física	¿Existen zonas seguras que protegen la información sensible?	no cumple	No se han establecidos perímetros para la seguridad física
A11.1.2	Controles de acceso físicos	¿Es protegida la entrada a las zonas seguras?	no cumple	No existe protección hacia las zonas seguras
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	¿Las zonas seguras están ubicadas en un lugar protegido?	no cumple	No se han realizado planes
A11.1.4	Protección contra amenazas externas y ambientales.	¿Existen instaladas alarmas, sistemas de protección contra incendios y otros sistemas?	no cumple	No hay existencia de alarmas en el área.
A11.1.5	Trabajo en áreas seguras.	¿Existen definidos procedimientos para las zonas seguras?	no cumple	No hay existencia de esos procedimientos

A11.1.6	Áreas de carga, despacho y acceso público	¿Las zonas entrega y carga están protegidas?	no aplica	
<b>A11.2 Equipos</b> <b>Objetivo: Prevenir la pérdida, daño, robo o compromiso de activos, y la interrupción de las operaciones de la organización.</b>				
A11.2.1	Ubicación y protección de los equipos	¿Los equipos son debidamente protegidos?	No cumple	La integridad física de los equipo no es la más optima
A11.2.2	Servicios de suministro	¿Los equipos están protegidos contra las variaciones de energía?	No cumple	Ningún equipo tiene protección contra variaciones de energía
A11.2.3	Seguridad en el cableado.	¿Están adecuadamente protegidos los cables de energía y telecomunicaciones?	cumple parcialmente	Si pero no es todo el cableado
A11.2.4	Mantenimiento de los equipos.	¿Existe mantenimiento de los equipos?	no cumple	No hay un programa de mantenimiento de equipos.
A11.2.5	Retiro de activos	¿La retirada de información y equipos fuera de la organización está controlada?	no cumple	No es controlada
A11.2.6	Seguridad de equipos y activos fuera de las instalaciones	¿Los activos de la organización son debidamente protegidos cuando no están en las instalaciones de la organización?	No aplica	No procesos donde se requiera la utilización de

				equipos fuera del área
<b>A11.2.7</b>	Disposición segura o reutilización de equipos	¿Es correctamente eliminada la información de los equipos que se van a eliminar?	No cumple	No es correctamente eliminada
<b>A11.2.8</b>	Equipos de usuario desatendido	¿Existen reglas para proteger los equipos cuando estos no estén siendo usados por los usuarios?	no cumple	No existen tales reglas
<b>A11.2.9</b>	Política de escritorio limpio y pantalla limpia	¿Hay orientaciones a los usuarios sobre qué hacer cuando estos no están presentes en sus estaciones de trabajo?	no cumple	no se ha realizado capacitaciones al personal sobre eso
<b>A12 SEGURIDAD DE LAS OPERACIONES</b>				
<b>A12.1 Procedimientos operacionales y responsabilidades</b>				
<b>Objetivo: Asegurar las operaciones correctas y seguras de las instalaciones de procesamiento de información.</b>				
<b>A12.1.1</b>	Procedimientos de operación documentados	¿Están documentados los procedimientos del área?	No cumple	No está registrado ningún procedimiento.
<b>A12.1.2</b>	Gestión de cambios	¿Los cambios que podrían afectar a la seguridad de la información son estrictamente controlados?	No cumple	No
<b>A12.1.3</b>	Gestión de capacidad	¿Los recursos son monitoreados y se realizan planes para asegurar su capacidad para cumplir con la demanda de los usuarios?	No cumple	No existen planes para estos procesos
<b>A12.1.4</b>	Separación de los ambientes de desarrollo, pruebas y operación	¿Se separan los entornos de desarrollo, pruebas y producción?	cumple parcialmente	Si pero en algunos casos se realizan cambio

				en los equipos de producción sin antes haber alzado un escenario de prueba
<b>A12.2</b> Protección contra códigos maliciosos <b>Objetivo: Asegurarse de que la información y las instalaciones de procesamiento de información estén protegidas contra códigos maliciosos.</b>				
<b>A12.2.1</b>	Controles contra códigos maliciosos	¿El software antivirus y otros programas para la protección de malware se instalan y utilizan correctamente?	cumple parcialmente	Se han instalado pero no en todos los equipos
<b>A12.3</b> Copias de respaldo <b>Objetivo: Proteger contra la pérdida de datos</b>				
<b>A12.3.1</b>	Respaldo de la información	¿Existe una política de backup definida y se lleva a cabo correctamente?	cumple parcialmente	Se tiene conocimientos de la realización pero no hay políticas específicamente
<b>A12.4</b> Registro y seguimiento <b>Objetivo: Registrar eventos y generar evidencia</b>				
<b>A12.4.1</b>	Registro de eventos	¿Los eventos relevantes de los sistemas son verificando periódicamente?	no cumple	No existe un sistema de eventos
<b>A12.4.2</b>	Protección de la información de registro	¿Los registros están protegidos adecuadamente?	no cumple	no existe una protección

				adecuada para estos
<b>A12.4.3</b>	Registros del administrador y del operador	¿Están adecuadamente protegidos los logs de los administradores?	no cumple	No están protegidos adecuadamente
<b>A12.4.4</b>	Sincronización de relojes	¿Está la hora de todos los sistemas de TI sincronizada?	no cumple	No existe un sistema para hacer eso
<b>A12.5</b> Control de software operacional				
<b>Objetivo: Asegurarse de la integridad de los sistemas operacionales</b>				
<b>A12.5.1</b>	Instalación de software en sistemas operativos	¿La instalación de software es estrictamente controlada?	no cumple	No del todo
<b>A12.6</b> Gestión de la vulnerabilidad técnica				
<b>Objetivo: Prevenir el aprovechamiento de las vulnerabilidades técnicas</b>				
<b>A12.6.1</b>	Gestión de las vulnerabilidades técnicas	¿La información de análisis de vulnerabilidades es correctamente gestionada?	no cumple	No
<b>A12.6.2</b>	Restricciones sobre la instalación de software	¿Existen reglas para definir restricciones de instalación de software a los usuarios?	no cumple	No
<b>A12.7</b> Consideraciones sobre auditorías de sistemas de información				
<b>Objetivo: Minimizar el impacto de las actividades de auditoría sobre los sistemas operativos</b>				
<b>A12.7.1</b>	Controles de auditorías de sistemas de información	¿Están las auditorías de sistemas de producción planeadas y se ejecutan correctamente?	no aplica	No existen auditores internos en la empresa

<b>A13 SEGURIDAD DE LAS COMUNICACIONES</b>				
<b>A13.1</b> Gestión de la seguridad de las redes				
<b>Objetivo: Asegurar la protección de la información en las redes, y sus instalaciones de procesamiento de información de soporte.</b>				
<b>A13.1.1</b>	Controles de redes	¿Las redes son gestionadas para proteger la información de sistemas y aplicaciones?	no cumple	No
<b>A13.1.2</b>	Seguridad de los servicios de red	¿Los requisitos de seguridad para servicios de red están incluidos en los acuerdos?	no cumple	No
<b>A13.1.3</b>	Separación en las redes	¿Existen redes segregadas considerando los riesgos y la clasificación de los activos?	no cumple	No
<b>A13.2</b> Transferencia de información				
<b>Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.</b>				
<b>A13.2.1</b>	Políticas y procedimientos de transferencia de información	¿Las transferencias de información están debidamente protegidas?	no cumple	No
<b>A13.2.2</b>	Acuerdos sobre transferencia de información	¿Los acuerdos con terceras partes consideran la seguridad durante la transferencia de información?	no cumple	no
<b>A13.2.3</b>	Mensajería Electrónica	¿Los mensajes que se intercambian sobre las redes están protegidos correctamente?	no cumple	No están encriptados
<b>A13.2.4</b>	Acuerdos de confidencialidad o de no divulgación	¿La organización posee una lista con todas las cláusulas de confidencialidad que deben ser incluidos en los acuerdos con terceros?	no cumple	No existe algo así
<b>A14 Adquisición, desarrollo y mantenimiento de sistemas</b>				
<b>A14.1</b> Requisitos de seguridad de los sistemas de información				

<b>Objetivo: Asegurar que la seguridad de la información sea una parte integral de los sistemas de información durante todo el ciclo de vida. Esto incluye también los requisitos para sistemas de información que prestan servicios sobre redes.</b>				
<b>A.14.1.1</b>	Análisis y especificación de requisitos de seguridad de la información	¿Se definen requisitos de seguridad para nuevos sistemas de información, o para cualquier cambio sobre ellos?	no cumple	No existen requisitos para los nuevos sistemas de información o para los cambios
<b>A.14.1.2</b>	Seguridad de servicios de las aplicaciones en redes públicas	¿La información de aplicaciones transferida a través de redes públicas es adecuadamente protegida?	no cumple	no
<b>A.14.1.3</b>	Protección de transacciones de los servicios de las aplicaciones.	¿Las transacciones de información a través de redes públicas son adecuadamente protegidas?	No aplica	No existen esa clase de transacciones en la red
<b>A14.2 Seguridad en los procesos de Desarrollo y de Soporte</b>				
<b>Objetivo: Asegurar que la seguridad de la información este diseñada e implementada dentro del ciclo de vida de desarrollo de los sistemas de información.</b>				
<b>A.14.2.1</b>	Política de desarrollo seguro	¿Existen definidas reglas para el desarrollo seguro de software y de los sistemas?	no aplica	El área de infraestructura no desarrolla aplicaciones
<b>A.14.2.2</b>	Procedimientos de control de cambios en sistemas	¿Se controlan los cambios en los sistemas nuevos o existentes?	no aplica	



<b>A.14.2.3</b>	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	¿Las aplicaciones críticas son debidamente probadas después de los cambios realizados en los sistemas operativos?	no aplica	
<b>A.14.2.4</b>	Restricciones en los cambios a los paquetes de software	¿Se realizan sólo los cambios necesarios a los sistemas de información?	no aplica	
<b>A.14.2.5</b>	Principio de Construcción de los Sistemas Seguros.	¿Los principios de ingeniería de sistemas seguros son aplicados al proceso de desarrollo de sistemas de la organización?	no aplica	
<b>A.14.2.6</b>	Ambiente de desarrollo seguro	¿Es seguro el entorno de desarrollo?	no aplica	
<b>A.14.2.7</b>	Desarrollo contratado externamente	¿Es monitorizado el desarrollo externalizado de sistemas?	no aplica	
<b>A.14.2.8</b>	Pruebas de seguridad de sistemas	¿Existe definido un criterio la seguridad del sistema durante el desarrollo?	no aplica	
<b>A.14.2.9</b>	Prueba de aceptación de sistemas	¿Existe definido un criterio para aceptar los sistemas?	no aplica	
<b>A14.3 Datos de prueba</b>				
<b>Objetivo: Asegurar la protección de los datos usados para pruebas.</b>				
<b>A.14.3.1</b>	Protección de datos de prueba	¿Los datos de prueba son cuidadosamente seleccionados y protegidos?	no aplica	

<b>A15 RELACIONES CON LOS PROVEEDORES</b>				
<b>A15.1</b> Seguridad de la información en las relaciones con los proveedores.				
<b>Objetivo: Asegurar la protección de los activos de la organización que sean accesibles a los proveedores.</b>				
<b>A15.1.1</b>	Política de seguridad de la información para las relaciones con proveedores	¿Existe una política para el tratamiento de los riesgos relacionados con proveedores y socios?	no aplica	El área de Infraestructura no se encarga de estos procesos
<b>A15.1.2</b>	Tratamiento de la seguridad dentro de los acuerdos con proveedores	¿Los requisitos de seguridad son incluidos en los acuerdos con los proveedores y socios?	no aplica	
<b>A15.1.3</b>	Cadena de suministro de tecnología de información y comunicación	¿Los acuerdos con los proveedores incluyen requisitos de seguridad?	no aplica	
<b>A15.2</b> Gestión de la prestación de servicios de proveedores				
<b>Objetivo: Mantener el nivel acordado de seguridad de la información y de prestación del servicio en línea con los acuerdos con los proveedores</b>				
<b>A15.2.1</b>	Seguimiento y revisión de los servicios de los proveedores	¿Son supervisados regularmente los proveedores?	no aplica	
<b>A15.2.2</b>	Gestión del cambio en los servicios de los proveedores	¿Los cambios relacionados con los acuerdos y contratos con proveedores y socios tienen en cuenta los riesgos existentes?	no aplica	
<b>A16 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN</b>				
<b>A16.1</b> Gestión de incidentes y mejoras en la seguridad de la información				

**Objetivo: Asegurar un enfoque coherente y eficaz para la gestión de incidentes de seguridad de la información, incluida la comunicación sobre eventos de seguridad y debilidades.**

<b>A16.1.1</b>	Responsabilidades y procedimientos	¿Los incidentes son gestionados adecuadamente?	no cumple	No pues simplemente se gestionan cuando se muestran.
<b>A16.1.2</b>	Reporte de eventos de seguridad de la información	¿Los eventos de seguridad son reportados adecuadamente?	no cumple	No
<b>A16.1.3</b>	Reporte de debilidades de seguridad de la información	¿Los empleados y contratistas informan sobre las debilidades de seguridad?	no cumple	No
<b>A16.1.4</b>	Evaluación de eventos de seguridad de la información y decisiones sobre ellos	¿Los eventos de seguridad son evaluados y clasificados correctamente?	no cumple	No
<b>A16.1.5</b>	Respuesta a incidentes de seguridad de la información	¿Están documentados los procedimientos para dar respuesta a los incidentes?	no cumple	No existen tales documentos
<b>A16.1.6</b>	Aprendizaje obtenido de los incidentes de seguridad de la información	¿Se analizan los incidentes de seguridad correctamente?	no cumple	No
<b>A16.1.7</b>	Recolección de evidencia	¿Existen procedimientos que definen cómo recopilar evidencias?	no cumple	No

<b>A17 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO</b>				
<b>A17.1</b> Continuidad de Seguridad de la información				
<b>Objetivo: La continuidad de seguridad de la información se debe incluir en los sistemas de gestión de la continuidad de negocio de la organización.</b>				
<b>A17.1.1</b>	Planificación de la continuidad de la seguridad de la información	¿Existen definidos requisitos para la continuidad de la seguridad de la información?	no cumple	No existen tales requisitos
<b>A17.1.2</b>	Implementación de la continuidad de la seguridad de la información	¿Existen procedimientos que aseguren la continuidad de la seguridad de la información durante una crisis o un desastre?	no cumple	No
<b>A17.1.3</b>	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	¿Se realizan test y pruebas de continuidad de seguridad de la información?	no cumple	No
<b>A17.2</b> Redundancias				
<b>Objetivo: Asegurar la disponibilidad de instalaciones de procesamiento de información.</b>				
<b>A17.2.1</b>	Disponibilidad de instalaciones de procesamiento de información	¿La infraestructura del área posee redundancia, incluyendo su planeamiento y operación?	no cumple	No hay redundancia
<b>A18 CUMPLIMIENTO</b>				
<b>A18.1</b> Cumplimiento de requisitos legales y contractuales				

<b>Objetivo: Evitar el incumplimiento de las obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información y de cualquier requisito de seguridad.</b>				
<b>A18.1.1</b>	Identificación de la legislación aplicable.	¿Son conocidos los requisitos legislativos, regulatorios, contractuales y cualquier otro requisito relativo a seguridad?	no cumple	No
<b>A18.1.2</b>	Derechos propiedad intelectual (DPI)	¿Existen procedimientos para proteger los derechos de propiedad intelectual?	no cumple	la gran cantidad de equipos con Windows no tienen licencia así como sus aplicaciones como la suit de Office
<b>A18.1.3</b>	Protección de registros	¿Los registros están protegidos adecuadamente?	no cumple	No
<b>A18.1.4</b>	Privacidad y protección de información de datos personales	¿La información personal está protegida adecuadamente?	cumple parcialmente	No se aplica en todas las personas
<b>A18.1.5</b>	Reglamentación de controles criptográficos.	¿Se utilizan controles criptográficos correctamente?	no cumple	No
<b>A18.2</b> Revisiones de seguridad de la información				
<b>Objetivo: Asegurar que la seguridad de la información se implemente y opere de acuerdo con las políticas y procedimientos organizacionales.</b>				
<b>A18.2.1</b>	Revisión independiente de la seguridad de la información	¿La seguridad de la información es revisada regularmente por un auditor independiente?	no aplica	No aplica Porque esta es la primera auditoría

<b>A18.2.2</b>	Cumplimiento con las políticas y normas de seguridad	¿Los gerentes revisan regularmente si las políticas de seguridad y procedimientos son llevadas a cabo adecuadamente en sus áreas de responsabilidad?	no cumple	
<b>A18.2.3</b>	Revisión del cumplimiento técnico	¿Los sistemas de información son revisados regularmente para comprobar su cumplimiento con los estándares y las políticas de seguridad de la información?	No cumple	no existen tales sistemas

**Fuente: (ISO, 2013)**

**Autores: Robert Soria – Hilda Vera**

### **Procesamiento y análisis**

Mediante la entrevista realizada en la empresa Righttek S.A. los días 7 y 8 de agosto del 2017, se logró identificar la mayor cantidad de vulnerabilidades con sus respectivos riesgos expuestas en el departamento de infraestructura, estos resultados de auditoria dieron a conocer los tipos de amenaza que se pueden cumplir al no aplicar mecanismos de protección a los fallos de seguridad detectados durante el proceso de auditoria en la cual la compañía en mención nos concedió un permiso para implementar un plan de mejoras que sirva de gran ayuda para mantener los riesgos identificados bajo control.

## **CAPÍTULO IV**

### **PROPUESTA TECNOLÓGICA**

Para el desarrollo de este proyecto basado en la norma ISO 27001 -2013 se propone la utilización de herramientas que serán de gran ayuda para realizar el proceso de auditoria en el departamento de tecnología de la empresa Righttek S.A. y con esto poder conocer el estado de la seguridad de la información que posee la compañía en mención, en este proceso se lograra detectar si existe un cumplimiento de los controles que son exigidos por la norma y que se adaptan al procedimiento a auditar al momento de identificar un hallazgo referente a una amenaza que pueda ocasionar perjuicios en la infraestructura, alcanzando la pérdida de información se elabora los respectivos informes de auditoría detallando a la organización los fallos que deben de proceder a corregir.

### **PROPUESTA DEL PROYECTO**

#### **1. Descripción de la propuesta:**

La propuesta que se presentara a la empresa Righttek S.A. enfocándonos en los requerimientos de ella y que esté de acuerdo al proceso de auditoría a realizar con la utilización de las respectivas



herramientas a implementar tales como los checklist, trazas, huellas y demás donde cada una de ellas darán a conocer el tipo de información que está expuesta ante una amenaza presente en la infraestructura tecnológica de la compañía Righttek S.A. se indicara todas las anomalías que deben de ser mitigadas en el momento que finalice la auditoria.

## 2. Planeación del proyecto

El objetivo del proyecto es:

Realizar un plan de mejoras basado en la norma ISO 27001:2013 seguridad de la información, utilizando herramientas aplicadas al proceso de auditoria informática de sistemas y que ayuden a evidenciar los puntos débiles encontrados en el departamento de Infraestructura de la Organización Righttek S.A. y con esto poder elaborar los respectivos informes.

Actividades realizadas:

Fase 1.- Se inició la respectiva reunión con los líderes de la empresa Righttek S.A. a auditar identificando los puntos importantes impartidos por parte de ellos y reuniendo todos los requerimientos del jefe del departamento de infraestructura para poder realizar el proceso de plan de mejoras referente a la auditoria.

Fase 2.- Se procedió con el inicio de la auditoria informática de sistema utilizando herramientas que reúnan la mayor cantidad de información referente al departamento auditado, durante este proceso se recopiló datos que sirven de gran aporte para detectar las no conformidades en la auditoria.

Fase 3.- en esta fase se lleva a cabo una entrevista en la cual es dirigida al jefe del departamento de tecnología de la empresa Righttek S.A. en la cual se puede recolectar la mayor cantidad de información referente al proceso.

**Objetivo específicos del proyecto:**

- Realizar el levantamiento de Información, analizando los activos de Información que posee el Departamento de Infraestructura de la Empresa Righttek S.A.
- Identificar las amenazas, riesgos y vulnerabilidades de los activos y procesos en el departamento de infraestructura Righttek S.A.

- Evaluar las políticas de seguridad que se podría implementar para un debido procesamiento de datos en la red.
- Analizar el plan de mejoras de buenas prácticas sobre la seguridad de la información en base a la Norma ISO 27001 -2013, para el departamento de la Empresa Righttek.

**Resultados propuestos:**

Al momento de utilizar la norma ISO 27001 -2013 con sus respectivas cláusulas y controles que estén asociadas al proceso en el cual se está realizando la auditoria se dará a conocer que la empresa en mención se encuentra expuesta a diferentes riesgos y amenazas que al ser aprovechadas por un atacante puede suceder el filtro de información de carácter confidencial con el objetivo de establecer lucros económicos por medio del uso de los activos lógicos capturados.

**Actividades y metas:**

- Análisis de los riesgos y amenazas a la empresa Righttek S.A. dentro del departamento de infraestructura con el fin de crear un plan de mejoras que ayude a tener todas las amenazas presentes bajo control evitando así accesos ilícitos y danos a la información de carácter confidencial.
- La meta de este presente proyecto es aplicar controles sobre las vulnerabilidades identificadas en el proceso de auditoria enfocado en el

estándar de seguridad de la información ISO 27001:2013 para la reducción de pérdidas de los activos que intenten lograr un mayor declive de índole financiero en la empresa.

CUADRO 12 Programa de la auditoría



RIGHTTEK

Tecnología Apropriada S.A.

PROGRAMA DE LA AUDITORÍA


I. DATOS GENERALES					
1.1. Norma de referencia		ISO/IEC 27001		1.2. Año de vigencia del programa	
1.3. Objetivo		EL PRESENTE DOCUMENTO TIENE COMO OBJETIVO DETERMINAR EL TIEMPO QUE TOMARA EL PROGRAMA DE AUDITORÍA PARA LA EMPRESA "RIGHTTEK".			

II. PROGRAMA DE AUDITORÍA					
Nº	Proceso/Área	Mes/Semana			
		Agosto			
		7	8	9	10
1	INFRAESTRUCTURA				
2					
3					
4					
5					
6					
Nº de Auditorias		1	1		
Total de Auditorias programadas		2			

III. APROBACIÓN DEL PROGRAMA DE AUDITORÍA	
Elaborado por:	Aprobado por:
Robert Soria - Hilda Vera, Auditores	Victor Lemos, Gerente General
Fecha: 10 / Julio / 2017	Fecha: 14 / Julio / 2017

**Fuente:** Trabajo de investigación  
**Autores:** Robert Soria – Hilda Vera

CUADRO 13 Plan de la auditoria interna

 <b>RIGHTTEK</b> <small>Tecnología Apropriada S.A.</small>				<b>PLAN DE AUDITORÍA INTERNA</b>	
<b>I. DATOS DE LA AUDITORÍA INTERNA</b>					
1.1. N° de Auditoria	1	1.2. Norma de referencia		ISO 27001:2013	
<b>II. OBJETIVO DE LA AUDITORÍA INTERNA</b>					
Analizar el estado actual de la empresa Righttek basado a los controles de la Norma ISO 27001					
<b>III. ALCANCE DE LA AUDITORÍA INTERNA</b>					
La Auditoria está limitado al área de Infraestructura de la empresa Righttek					
<b>IV. EQUIPO AUDITOR</b>					
4.1 Auditor Líder	ROBERT SORIA CAJAS (RS)				
4.2 Auditores Internos	HILDA VERA BARRERA(HV)				
<b>V. INVITADOS</b>					
5.1 Expertos Técnicos	N/A				
5.2 Observadores	N/A				

VI. PLAN DE AUDITORÍA						
Fecha	Hora	Auditor	Proceso/Área	Criterios de Auditoria		Auditado
				Cláusula /Control	Documentación	
7/8/2017	9:30	TODOS	Llegada a la organización			
	9:35	TODOS	Reunión de apertura			
	10:00	TODOS	Recorrido por el Área			
	11:00	RS	Infraestructura revisión cláusulas	Cláusulas 4,5	Checklist	Victor Pantoja
	12:00	RS	Infraestructura revisión cláusulas	Cláusulas 7	Checklist	Victor Pantoja
	12:30	TODOS	Recursos varios			
	13:30	RS	Infraestructura revisión cláusulas	Cláusulas 9, 10	Checklist	Victor Pantoja
	15:00	RS	Infraestructura revisión anexos	Anexo A11- A14	Checklist	Victor Pantoja
	16:45	TODOS	Reunión de enlace			
	17:00	TODOS	Reunión de cierre			
	17:30	TODOS	Recursos varios			
8/8/2017	9:30	TODOS	Llegada a la organización			
	9:35	TODOS	Reunión de apertura			
	9:55	RS	Infraestructura revisión cláusulas	Anexo A5 - A7	Checklist	Victor Pantoja
	11:25	RS	Infraestructura revisión anexos	Anexo A8 - A10	Checklist	Victor Pantoja
	12:30	TODOS	Recursos varios			
	13:30	RS	Infraestructura revisión anexos	Anexo A15 - A18	Checklist	Victor Pantoja
	15:30	RS	Infraestructura revisión anexos	Cláusulas 6,8	Checklist	Victor Pantoja
	16:00	TODOS	Reunión de enlace			
	16:30	TODOS	Reunión de cierre			
	17:00	TODOS	Fin proceso auditoria			



7/8/2017	9:30	TODOS	Llegada a la Organización			
	9:35	TODOS	Reunión de Apertura			
	10:00	TODOS	Recorrido por el Área			
	11:00	HV	Infraestructura revisión cláusulas	Cláusulas 4,5	Checklist	Victor Pantoja
	12:00	HV	Infraestructura revisión cláusulas	Cláusulas 7	Checklist	Victor Pantoja
	12:30	TODOS	Recursos varios			
	13:30	HV	Infraestructura revisión cláusulas	Cláusulas 9, 10	Checklist	Victor Pantoja
	15:00	HV	Infraestructura revisión anexos	Anexo A11- A14	Checklist	Victor Pantoja
	16:45	TODOS	Reunión de enlace			
	17:00	TODOS	Reunión de cierre			
	17:30	TODOS	Recursos varios			
8/8/2017	9:30	TODOS	Llegada a la Organización			
	9:35	TODOS	Reunión de Apertura			
	9:55	HV	Infraestructura revisión cláusulas	Anexo A5 - A7	Checklist	Victor Pantoja
	11:25	HV	Infraestructura revisión anexos	Anexo A8 - A10	Checklist	Victor Pantoja
	12:30	TODOS	Recursos varios			
	13:30	HV	Infraestructura revisión anexos	Anexo A15 - A18	Checklist	Victor Pantoja
	15:30	HV	Infraestructura revisión anexos	Cláusulas 6,8	Checklist	Victor Pantoja
	16:00	TODOS	Reunión de enlace			
	16:30	TODOS	Reunión de cierre			
	17:00	TODOS	Fin proceso auditoria			

---

VII. APROBACIÓN DEL PROGRAMA DE AUDITORÍA	
Elaborado por:	Aprobado por:
Robert Soria - Hilda Vera, Auditores	Victor Lemos, Gerente General
Fecha: 10 / Julio / 2017	Fecha: 14 / Julio / 2017

**Fuente:** Trabajo de investigación  
**Autores:** Robert Soria – Hilda Vera

A continuación, se mencionan los aspectos importantes del proceso de checklist que es utilizado para recabar la información mediante entrevistas.

### **Checklist**

Esta herramienta hace mención a todos los controles de la Norma ISO 27001-2013 con lo cual se recaba la siguiente información: la mayoría de los controles aplicables al proyecto y que son brindados por la norma no son cumplidos generando altos índices de riesgos y amenazas de los cuales no se tiene conocimiento hasta que se presenta alguna anomalía o incidente de seguridad. Falta de políticas de seguridad debidamente documentadas la inexistencia de las mismas no permiten cumplir los controles de revisión o actualizaciones, la seguridad física que posee el área no es la apropiada debido a la gran cantidad de equipos que se manipulan en el departamento de infraestructura y los dispositivos que tienen almacenada información sensible son de fácil acceso, no existen restricciones que evite el ingreso de personal no autorizado, la seguridad alrededor de los datos sensibles que maneja el área no son la apropiadas para satisfacer los requerimientos de la norma, la red no está segregada permitiendo a cualquier usuario tener acceso a todos los sistemas que se manejan en la empresa con el fin de que él pueda cometer un fraude informático, la información enviada a través de las redes públicas no son cifradas por la cual no cuentan con un protocolo de criptografía, no tienen

un sistema que gestione los incidentes que se producen dentro del proceso.

### **Análisis de Factibilidad**

Después de realizar la reunión con los líderes de la organización Righttek S.A. es de gran importancia realizar el análisis de factibilidad del proyecto referente al plan de mejoras.

Al realizar el análisis de factibilidad se puede definir la viabilidad del proyecto realizando, la reunión con los líderes de la empresa en mención, la factibilidad técnica, operacional, legal y económica del proyecto sobre el plan de mejoras utilizando la norma ISO 27001:2013, también se podrá la determinar cumpliendo los requerimientos innovadores de la propuesta.

En el presente capítulo se procederá a indicar cada elemento que se detalló anteriormente con sus respectivas conclusiones, también se indica la viabilidad de la propuesta una vez culminada la reunión con los líderes de la compañía mencionada en párrafos anteriores referente al plan propuesto, la ejecución de la entrevista determina que se recopila la mayor cantidad de información y se detecta que no existe cumplimiento en los controles exigidos por la norma, por la cual el plan de mejoras se valida como factible o viable, una vez conocidos los resultados de auditoria en el departamento tecnológico de la corporación, se presenta la factibilidad

adecuada para este proyecto.

### **Factibilidad operacional**

El presente proyecto referente al plan de mejoras se lo desarrollo con la ayuda de la empresa Righttek S.A. dando la facilidad de ingresar al departamento tecnológico para dar el inicio de la auditoria utilizando herramientas para la recopilación de información referente al proceso que se está auditando.

El líder del departamento técnico informático es la persona que proporciono la mayor cantidad de información mediante la entrevista que se elabora para la obtención de los datos y poder dictaminar que controles no se están cumpliendo en el proceso.

### **Factibilidad Técnica**

En esta etapa de la factibilidad técnica se va a detallar los siguientes dispositivos que cuenta la empresa Righttek S.A., se va a realizar la auditoria informática de sistema.

La organización en mención cuenta con lo siguiente: Un Firewall PFSense en su versión 2.3.4-RELEASE-p1 para un procesador (amd64) instalada en un servidor robusto el cual viene integrado con un procesador Intel i7-4770

3.40GHz con 8Gb de memoria RAM 1 TB de disco duro, Este equipo cuenta con 3 tarjetas de RED. Servidor de Base de datos Windows Server 2012 R2 Standard sin licencia, el modelo del equipo es DH87MC con un procesador Intel i7 4770 3.40 GHz con 8 Gb de memoria RAM y 1 TB de disco duro. Un servidor Biométrico con Windows 7 con un procesador Intel(R) Core(TM) i7-3770 CPU @ 3.40GHz, 3392 MHz, 1 procesador principal, 1 procesador lógico con 1 GB de memoria RAM y 100 Gb de disco Duro. Un servidor FTP montado en CentOS 6.4 con un procesador Intel core i5 -4300U CPU 1.90 GHz, 2501 MHz con 8 Gb de memoria RAM y 2 TB de disco duro. Un servidor de aplicación nombrada Odoo instalado en sistema operativo CentOS 7 con un procesador Intel Xeon E 31220 con 8 GB de memoria RAM y con 500 GB de almacenamiento. Central telefónica Elastix 2.5 el cual posee un procesador Intel Pentium G2020 con 4 Gb de memoria RAM, 250 Gb de almacenamiento y con una tarjeta OpenVox A800P35 8 PUERTOS ANÁLOGOS PCI BASE CARD + 3 FXS + 5 FX0, un Servidor Gateway GSM o Base celular modelo VS-GGU-E2M0400 Versión 2.3.1, Servidor de aplicaciones Moodle instalado en un entorno Windows 7 con un procesador Intel Xeon E31220 con 2 Gb y 500 Gb de almacenamiento. Servidor de Correo Groupwise 8 instalado en un SUSE Linux Enterprise 10 con 4 Gb de Memoria RAM y 1 Tb de almacenamiento en disco duro. Servidor de aplicaciones Open Iguana instalado en un Ubuntu 13.10 con un procesador Intel core i7 con 8Gb de memoria RAM y 500 GB de almacenamiento, un servidor de aplicación open RT instalado

en Ubuntu 14.04 con un procesador core i3 con 4 Gb de memoria RAM y 100 Gb de disco duro, un servidor de marcación remota instalado en un Windows 7 con un procesador i3 con 2 GB de memoria RAM y 100 GB de disco duro, todos estos equipos se conectan a la red a través de 1 Switch Cisco modelo DNL14330KQ de 24 puertos 10/100, también cuentan con un Switch RouterBoard Mikrotik modelo CRS226-24C-2S+IN de 24 puertos de capacidad, varios switches de gama baja D-link 10/100 con capacidad de 8 puertos estos son utilizados para hacer cascadas entre las diferentes áreas, dada la gran cantidad de dispositivos con que el área es responsable se considera que Righttek cuenta con una infraestructura técnicamente factible para realizar la auditoría basada en la ISO 27001-2013.

### **Factibilidad Legal**

Durante la elaboración de este proyecto sobre el Plan de Mejoras basado en la norma ISO 27001 -2013 de Seguridad de la Información, no viola las leyes vigentes de la República del Ecuador, debido a que la propuesta solamente se encuentra enfocada a la identificación de riesgos y amenazas presentes en el Departamento de Infraestructura de la Empresa Righttek S.A., en donde el Plan de Mejoras se encargará de aplicar un respectivo tratamiento a los fallos detectados durante el proceso de auditoría, esta planificación es de gran ayuda para dar a conocer todas las falencias que posee la Compañía en mención, por lo explicado anteriormente, este

estudio vincula las leyes que son aplicables a él para un estricto cumplimiento de ellas.

### **Factibilidad Económica**

En la factibilidad económica detallamos los valores generados durante el desarrollo de la propuesta que se requiere para realizar el proyecto de auditoria, dado que la auditoria requiere analizar las vulnerabilidades de la empresa basados en la norma ISO 27001-2013 a continuación indicaremos mediante una tabla los costos invertidos en la elaboración del proyecto.

**CUADRO 14 Costos de ejecución del proyecto**

<b>Tabla de costo del proyecto</b>	
<b>Descripción</b>	<b>Valor</b>
Recursos Varios	\$20,00
costo de equipos informáticos	\$2.400,00
Servicios de internet	\$30,00
<b>Total</b>	<b>\$2.450,00</b>

**Fuente:** Trabajo de investigación

**Autores:** Robert Soria – Hilda Vera

A continuación, se detallará en la siguiente tabla los costos del desarrollo de la auditoria informática de sistemas en la que se realizará en el departamento de infraestructura de la empresa Righttek S.A.



### CUADRO 15 Costos de ejecución de la auditoria

Tabla de costo de auditoria	
Descripción	Valor
Costo de auditoria	\$1.000,00
Costo de la consultoría	\$800,00
Costo de elaboración del Plan de mejora	\$700,00
Recursos varios	\$100,00
<b>Total</b>	<b>\$2.600,00</b>

**Fuente:** Trabajo de investigación

**Autores:** Robert Soria – Hilda Vera

Debido al costo total de la auditoria equivalente a 2600 dólares se determina la viabilidad económica del plan propuesto por la cual dicho valor se encuentra dentro del presupuesto financiero de la compañía a la que se va a realizar la auditoria.

### Etapas de la metodología del proyecto

#### Metodología Magerit

Esta metodología es usada para analizar y gestionar los riesgos en base a los activos que se encontraron

## Inventario de Activos

Se agrupan los activos por grupos en una tabla.

**CUADRO 16 Activos del área de Infraestructura**

Ámbito	Activo	Cantidad
Técnico	Firewall	2
	Base de Datos	1
	Servidor Biométrico	1
	Servidor FTP	1
	Servidor Intranet Odoo	1
	Central Telefónica Elastix	1
	Base Celular	1
	Servidor de Aplicación Moodle	1
	Servidor De Correo Groupwise	1
	Servidor aplicación OPEN Iguana	1
	Servidor aplicación Open RT	1
	Servidor de Marcación Remota	1
Hardware	Switch de gama alta	2
	Switch RouterBoard Mikrotik	1
	Switches de gama Baja	10
	Antenas Nano loco M2	2
Información	Credenciales de todos los servidores de la empresa	1

**Fuente: Trabajo de investigación**  
**Autores: Robert Soria – Hilda Vera**

## Valoración de Activos

La valoración es cuantitativa de los activos se clasifican basado en las siguientes categorías:

- Muy alto
- Alto
- Medio
- Bajo
- Muy bajo

**CUADRO 17 Valoración de activos**

<b>Activo</b>	<b>Cantidad</b>	<b>Valor</b>
Firewall	2	Muy alto
Base de Datos	1	Muy alto
Servidor Biométrico	1	Bajo
Servidor FTP	1	Bajo
Servidor Intranet Odoo	1	Medio
Central Telefónica Elastix	1	Alto
Base Celular	1	Alto
Servidor de Aplicación Moodle	1	Medio
Servidor De Correo Groupwise	1	Medio
Servidor aplicación OPEN Iguana	1	Medio
Servidor aplicación Open RT	1	Medio
Servidor de Marcación Remota	1	Alto
Switch de gama alta	2	Alto
Switch RouterBoard Mikrotik	1	Alto
Switches de gama Baja	10	Medio
Antenas Nano loco M2	2	Medio
Credenciales de todos los servidores de la empresa	1	Muy alto

**Fuente: Trabajo de investigación**

**Autores: Robert Soria – Hilda Vera**

La Metodología MAGERIT puede identificar distintos tipos de amenazas

las cuales se clasifican en:

- Desastres naturales
- De origen industrial
- Errores y fallos no intencionados
- Ataques intencionados

Los Activos son abreviados para obtener un análisis más completo,

presentados en el siguiente cuadro

### CUADRO 18 Abreviaturas

Ámbito	Abreviatura
Técnico	T
Hardware	H
información	I

**Fuente:** Trabajo de investigación  
**Autores:** Robert Soria – Hilda Vera

A continuación, se muestra las amenazas que pueden afectar a los activos del área de infraestructura de Righttek

### CUADRO 19 Análisis de Amenazas en los activos

Tipos	Ref.	Amenaza	T	H	I
Desastres naturales	DN1	Fuego	X	X	
	DN2	Daños por agua	X	X	
	DN3	Otros desastres naturales	X	X	
De origen industrial	OI1	Fuego	X	X	
	OI2	Daños por agua	X	X	
	OI3	Contaminación mecánica	X	X	
	OI4	Contaminación electromagnética	X	X	
	OI5	Avería de origen físico o lógico	X	X	
	OI6	Corte del suministro eléctrico	X	X	
	OI7	Condiciones inadecuadas de temperatura o humedad	X	X	
	OI8	Fallo de servicio de comunicaciones	X	X	
	OI9	Interrupción de otros servicios y suministros esenciales	X	X	
	OI10	Degradación de los soportes de almacenamiento de la información	X		
	OI11	Emanaciones electromagnéticas	X	X	
Errores y fallos no intencionados	EF1	Errores de los usuarios	X		
	EF2	Errores del administrador	X	X	
	EF3	Errores de monitorización (log)	X	X	
	EF4	Errores de configuración	X	X	
	EF5	Deficiencias en la organización			
	EF6	Difusión de software dañino			X
	EF7	Errores de [re-]encaminamiento			
	EF8	Errores de secuencia			

	EF9	Escapes de información			X
	EF10	Alteración accidental de la información			X
	EF11	Destrucción de información			X
	EF12	Fugas de información			X
	EF13	Vulnerabilidades de los programas (software	X	X	
	EF14	Errores de mantenimiento / actualización de programas (software)	X	X	
	EF15	Errores de mantenimiento / actualización de equipos (hardware)	X	X	
	EF16	Caída del sistema por agotamiento de recursos	X	X	
	EF17	Pérdida de equipos	X	X	
	EF18	Indisponibilidad del personal			X
Ataques intencionados	AI1	Manipulación de los registros de actividad (log)	X		
	AI2	Manipulación de la configuración	X		
	AI3	Suplantación de la identidad del usuario	X		
	AI4	Abuso de privilegios de acceso	X		X
	AI5	Uso no previsto		X	
	AI6	Difusión de software dañino		X	
	AI7	[Re-]encaminamiento de mensajes		X	
	AI8	Alteración de secuencia	X	X	
	AI9	Acceso no autorizado	X	X	X
	AI10	Análisis de tráfico		X	
	AI11	Repudio			
	AI12	Interceptación de información (escucha)		X	X
	AI13	Modificación deliberada de la información	X		X
	AI14	Destrucción de información	X		X
	AI15	Divulgación de información	X		X
	AI16	Manipulación de programas	X		
	AI17	Manipulación de los equipos	X	X	
	AI18	Denegación de servicio	X	X	
	AI19	Robo	X	X	X
	AI20	Ataque destructivo	X	X	X
	AI21	Ocupación enemiga			
	AI22	Indisponibilidad del personal			
	AI23	Extorsión			
	AI24	Ingeniería social	X		

**Fuente:** Trabajo de investigación  
**Autores:** Robert Soria – Hilda Vera

A continuación, se detallará las vulnerabilidades y riesgos que se hallaron durante el proceso de auditoria en Righttek S.A.

**CUADRO 20 Análisis de activos, vulnerabilidad y riesgo**

Activos	Vulnerabilidad	Riesgo
2 Firewall	Ausencia de control sobre los datos de entrada y salida, Ausencia de política de control de accesos, Ausencia de política para el uso de la criptografía, Ausencia de redundancia, Inadecuada gestión de contraseñas, Inadecuada concienciación de seguridad	Captura de datos, accesos ilícitos a los sistemas informáticos, identificación de información sensible, caída del sistema afectando el rendimiento de la organización
Base de Datos	Inadecuada clasificación de la información, Inadecuada concienciación de seguridad, Inadecuada gestión de cambios	Mala actualización y eliminación de registros, accesos ilícitos a la base de datos por medio de servidores de aplicaciones.
Servidor Biométrico	Inadecuada protección física, Inadecuado control del acceso físico , Mantenimiento inadecuado, Inadecuada gestión de la red	Danos irreversibles en el equipo, manipulación de las marcaciones de los usuarios mal intencionados, equipos sin servicio
Servidor FTP	Descontrol en las copias de datos, Inadecuada concienciación de seguridad.	Almacenamiento masivo de información irrelevante, sustracción de archivos con contenido sensible

Servidor Intranet Odoo	Inadecuada supervisión de empleados, Inadecuada capacitación de los empleados	mal manejo del sistema informático,
Central Telefónica Elastix	Ausencia de redundancia, Inadecuada capacitación de los empleados	Caída del sistema afectando el rendimiento de la organización, los operadores no poseen la capacidad de proporcionar información requerida por el cliente
Base Celular	Equipamiento sensible a cambios de voltaje, Equipamiento sensible a la humedad y contaminantes	daños permanentes en el equipo
Servidor de Aplicación Moodle	Inadecuada supervisión de empleados, Inadecuada capacitación de los empleados	mal manejo del sistema informático,
Servidor De Correo Groupwise	Inadecuada capacitación de los empleados	abuso de la confianza de los empleados por parte de los atacantes

Servidor aplicación OPEN Iguana	Inadecuada supervisión de empleados, Inadecuada capacitación de los empleados	mal manejo del sistema informático,
Servidor aplicación Open RT	Inadecuada supervisión de empleados, Inadecuada capacitación de los empleados	mal manejo del sistema informático,
Servidor de Marcación Remota	Inadecuada capacitación de los empleados, Inadecuada supervisión de empleados	mal manejo del sistema informático,
2 Switch de gama alta	Inadecuada protección física, Inadecuado control del acceso físico , Mantenimiento inadecuado, Inadecuada gestión de la red	Danos permanentes en los equipos
1 Switch RouterBoard Mikrotik	Inadecuada protección física, Inadecuado control del acceso físico , Mantenimiento inadecuado, Inadecuada gestión de la red	Danos permanentes en los equipos



10 Switches de gama Baja	Inadecuada protección física, Inadecuado control del acceso físico , Mantenimiento inadecuado, Inadecuada gestión de la red	Danos permanentes en los equipos
2Antenas Nano loco M2	Inadecuada protección física, Inadecuado control del acceso físico , Mantenimiento inadecuado, Inadecuada gestión de la red	Danos permanentes en los equipos
Credenciales de todos los servidores de la empresa	Inadecuada concienciación de seguridad	robo de credenciales por parte de los piratas informáticos

**Fuente:** Trabajo de investigación  
**Autores:** Robert Soria – Hilda Vera

## Entregables del proyecto

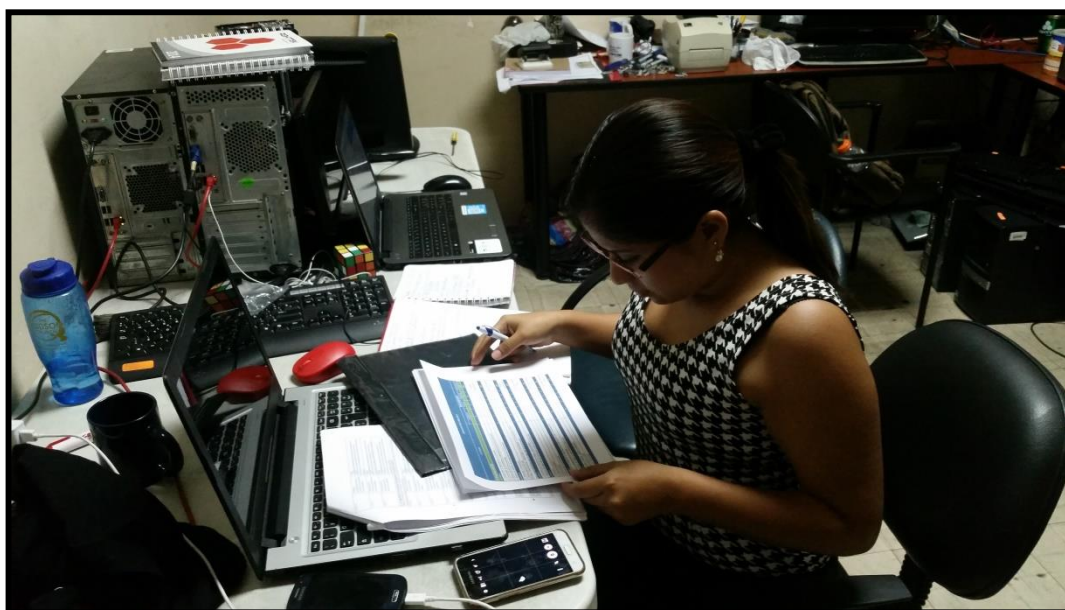
### Informe de los hallazgos encontrados

- **Observaciones**

En este punto se mostrarán todas las observaciones que se realizaron en el proceso de auditoría.

#### Observación 1

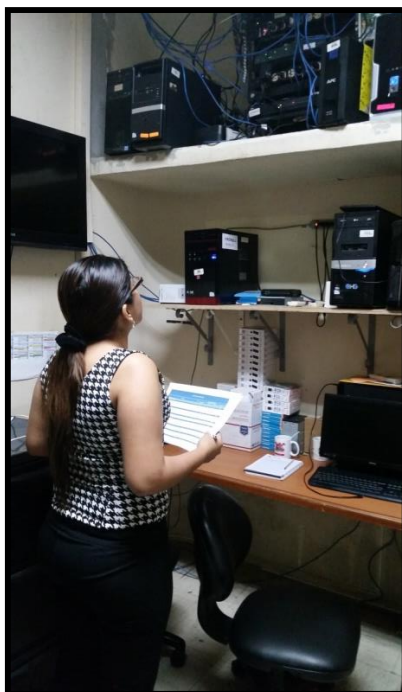
#### GRÁFICO 9 Análisis de los controles Anexo 6



**Fuente:** Trabajo de investigación

**Autores:** Robert Soria – Hilda Vera

**Observación 2**  
**GRÁFICO 10 Expectación de los servidores del área**



**Fuente:** Trabajo de investigación  
**Autores:** Robert Soria – Hilda Vera

**Observación 3**  
**GRÁFICO 11 Revisión del checklist**



**Fuente: Trabajo de investigación**  
**Autores: Robert Soria – Hilda Vera**

**Observación 4**  
**GRÁFICO 12 Anotación de hallazgos**



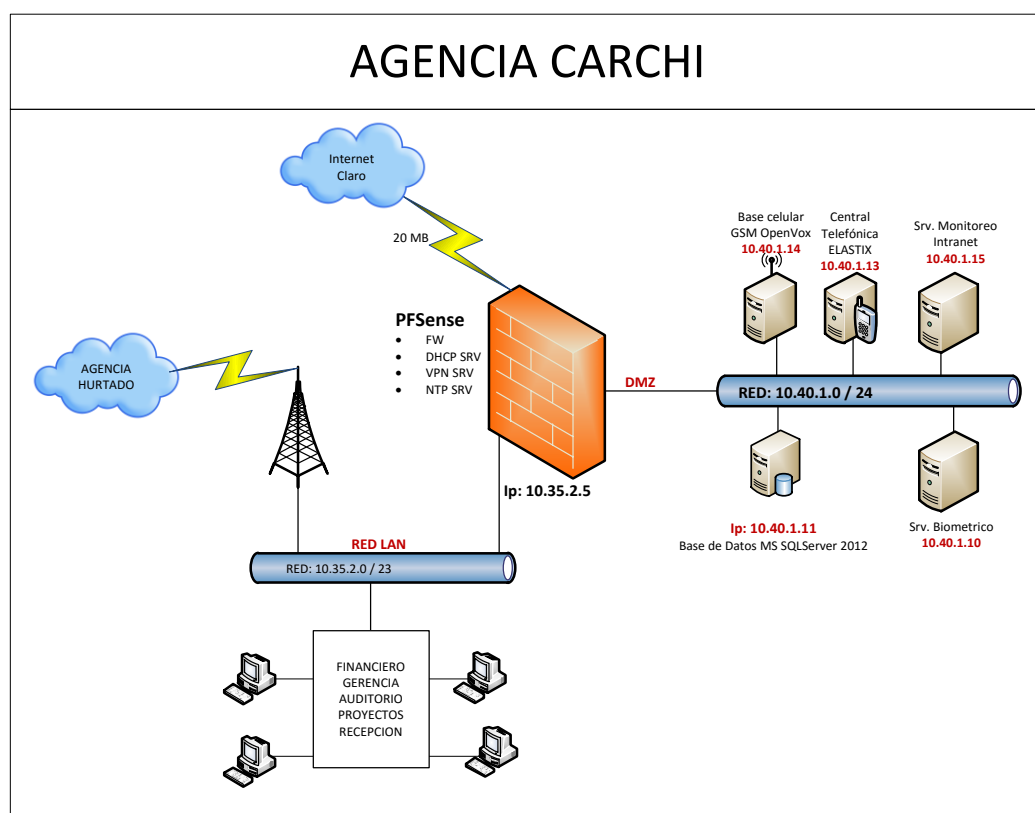
**Fuente: Trabajo de investigación**  
**Autores: Robert Soria – Hilda Vera**

- Anexos de inicio de la Auditoria(permisos)otorgados por la empresa Righttek
- Anexo de Procedimiento para la auditoria
- Anexo Plan de mejora

### Evidencias

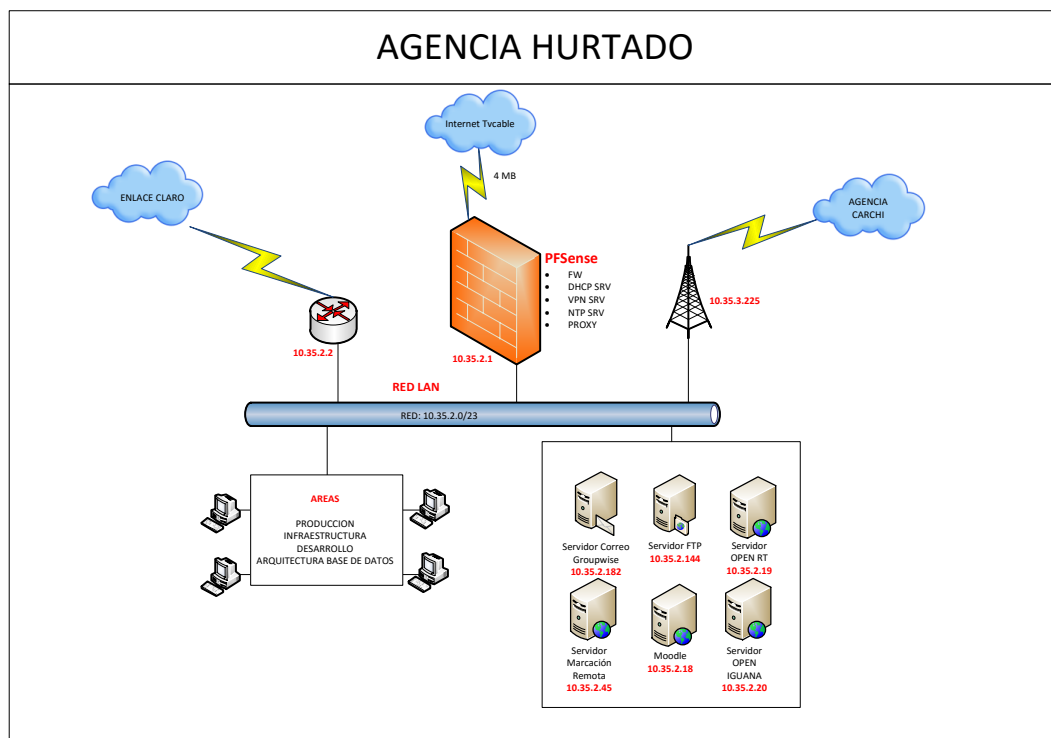
- Diseño de la red

**GRÁFICO 13** Diseño de red de la Agencia Carchi



**Fuente:** Trabajo de investigación  
**Autores:** Robert Soria – Hilda Vera

**GRÁFICO 14 Diseño de red de la Agencia Carchi**



**Fuente:** Trabajo de investigación  
**Autores:** Robert Soria – Hilda Vera

- **Servicios que se ejecutan en la red**

Los servicios que se ejecutan en la red de Righttek son:

**DHCP (Protocolo de Configuración Dinámica de host):**

proporcionado por el firewall de la agencia de Hurtado encargado de asignar Ip a cada equipo de la red de Righttek S.A.

**Servicio de Correo Electrónico:** este servicio es proporcionado por el servidor de correo Groupwise que se encarga de Gestionar el correo local de la empresa Righttek S.A.

**Servicio de transferencia de archivo (Ftp):** Permite la transferencia de archivos entre los ordenadores.

**Servicio de Acceso Remoto:** los servicios de acceso remoto son muy utilizados para acceder a otro equipo por medio de protocolo SSH o telnet.

**Servicio de Telefonía IP:** el servidor Elastix proporciona los servicios para la comunicación de telefonía ip usada por todos los usuarios de Righttek

### Criterios de validación de la propuesta

Mediante una tabla se marcará con una X las políticas que son aplicables al proyecto referente al plan de mejoras validando la propuesta planteada en el inicio de la investigación

### CUADRO 21 Análisis de Aplicabilidad

DESCRIPCIÓN	MUY APLICABLE	APLICABLE	POCO APLICABLE	NADA APLICABLE
POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN	X			
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	X			
SEGURIDAD DE LOS RECURSOS HUMANOS				X
GESTIÓN DE ACTIVOS		X		
CONTROL DE ACCESO	X			
CRİPTOGRAFÍA	X			
SEGURIDAD FÍSICA Y DEL ENTORNO		X		
SEGURIDAD DE LAS OPERACIONES			X	
SEGURIDAD DE LAS COMUNICACIONES	X			
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS		X		
RELACIÓN CON LOS PROVEEDORES			X	
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	X			
ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO	X			
CUMPLIMIENTOS	X			



### Criterios de aceptación del producto o servicio

**CUADRO 22 Criterios de aceptación**

CRITERIO ALCANCE	Positiva	Indiferente	Negativa
los resultados de la auditoria se los comunicara al líder del departamento de infraestructura para llevar a cabo la ejecución del plan de mejoras	X		
Se dictara capacitaciones sobre el buen uso de la información para disminuir los niveles de riesgos y amenazas.	X		
todos los informes de la auditoria se los evidenciara con sus respectivos hallazgos	X		
Indicar los puntos donde se encuentran presentes los riesgos y amenazas en el departamento de infraestructura	X		

## **Conclusiones y Recomendaciones**

### **Conclusiones**

Finalizado el proyecto de titulación concluimos con lo siguiente:

- Mediante el levantamiento de información que se realizó en el departamento de infraestructura de la empresa Righttek S.A. se verifico un total de 26 activos informáticos incluyendo servidores dispositivos de networking y aplicaciones de software, con esta identificación se procedió a realizar la auditoria en la cual mostro amenazas y riesgos en cada uno de los activos.
- Con la identificación de amenazas, riesgos y vulnerabilidades se determinó el ligamiento de cada uno de ellos, este proceso se lo realizo mediante técnicas de observación en la cual se pudo detectar la falta de inversión en TI que lleven a una mejor gestión operacional en toda la red corporativa.
- Mediante la evaluación de las políticas de seguridad de la información se detectó cuáles de ellas son aplicables a la propuesta desarrollada con el fin de que la empresa Righttek S.A. mantenga un buen nivel de seguridad gestionado.
- Al analizar el plan de mejora la empresa Righttek S.A. se podrá enfocar en dicho plan, la evolución de los procesos actualizando

todas las aplicaciones que se ejecutan dentro de la red evitando el cumplimiento de las amenazas que tiene la finalidad de atentar a la información de carácter confidencial.

### **Recomendaciones**

- Se recomienda que se apliquen métodos de protección basados en la norma ISO 27001-2013 con la finalidad de disminuir los riesgos latentes en la red corporativa en la organización.
- Se debe realizar auditorías informáticas de sistema de una forma periódica para que la organización logre conocer sus riesgos, amenazas y vulnerabilidades detectadas tomando en consideración los respectivos planes de acción que ayuden a verificar que controles pueden ser adaptados al proceso para poder tener todos los riesgos bajo control
- Actualizar y cumplir con todas las políticas de seguridad planteadas para el departamento de infraestructura de la organización con el fin de disminuir los índices de amenazas.
- Implementar planes de mejora que sirvan como modelo a seguir para tener un mejor control en la organización.

## Bibliografía

- 27001:2013, ISO. (24 de noviembre de 2015). *SGSI*. Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Información: <http://www.pmg-ssi.com/2015/11/auditoria-certificacion-norma-iso-27001-2013/>
- Advisors, Intedya International Dynamic. (julio de 2016). *Nuestra estrategia, EL DESARROLLO COMPETITIVO*. Obtenido de ISO 27001:2013 Gestión de la Seguridad de la Información: [http://www.intedya.com/productos/seguridad%20en%20la%20informacion%20y%20tecnologia%20C3%ADa/ISO%2027001/07%202016%20ISO%2027001\\_%20PIC\\_%20ed00.pdf](http://www.intedya.com/productos/seguridad%20en%20la%20informacion%20y%20tecnologia%20C3%ADa/ISO%2027001/07%202016%20ISO%2027001_%20PIC_%20ed00.pdf)
- Aguila Plaza, X. A. (Marzo de 2015). *UNIVERSIDAD POLITÉCNICA SALESIANA*. Obtenido de Repositorio Digital: <http://dspace.ups.edu.ec/handle/123456789/10283>
- Arana Northia, A. J. (19 de Julio de 2016). *Repositorio Dspace*. Obtenido de <http://www.dspace.espol.edu.ec/xmlui/handle/123456789/34978>
- Arias, F. G. (2012). *El Proyecto de investigación Introducción a la metodología científica*. Caracas: EDITORIAL EPISTEME, C.A.
- Armando Costa, M., & Valencia Vernaza, C. A. (2013). *Universidad Nacional de Loja*. Obtenido de Repositorio Digital: <http://dspace.unl.edu.ec/jspui/handle/123456789/5228>
- Barros Marcillo, G. F., & Cadena Marten, A. E. (ene de 2012). *Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE*. Obtenido de <http://repositorio.espe.edu.ec/handle/21000/5197>
- Bustamante, G. &. (2014). Metodología de la seguridad de la información como medida de protección en pequeñas empresas. *Cuaderno Activa*, 71-77.
- Castro Rojas, J. E., Farigua Gutiérrez, J. A., & Suárez Cortés, L. E. (9 de jul de 2016). *UNIVERSIDAD CATÓLICA de Colombia Vigilada Mineducación*. Obtenido de Repositorio Institucional: <http://hdl.handle.net/10983/7847>
- Cedeño Tenorio, J. O. (18 de Enero de 2017). *REPOSITORIO DIGITAL PUCESE*. Obtenido de Pontificia Universidad Católica del Ecuador: <https://repositorio.pucese.edu.ec/123456789/1007>
- Chamba Maleza, J. T. (agosto de 2017). *Repositorio Institucional UNIANDES*. Obtenido de <http://dspace.uniandes.edu.ec/handle/123456789/6411>
- CONSTITUCIÓN DEL ECUADOR. (s.f.). Obtenido de [http://www.asambleanacional.gov.ec/documentos/constitucion\\_de\\_bolsillo.pdf](http://www.asambleanacional.gov.ec/documentos/constitucion_de_bolsillo.pdf)
- Coral Ojeda, J. A. (07 de Abril de 2017). *UNAD*. Obtenido de Universidad Nacional Abierta y a Distancia: <http://hdl.handle.net/10596/11875>
- Doria Corcho, A. F. (2015). *UNAD*. Obtenido de Universidad Nacional Abierta y a Distancia: <http://hdl.handle.net/10596/3624>
- Figueroa Pérez, O., & Malagón Sáenz, N. E. (17 de abril de 2017). *UNAD*

- Universidad Nacional Abierta y a Distancia*. Obtenido de <http://hdl.handle.net/10596/11881>
- García Araque, J. O. (07 de abril de 2017). *UNAD*. Obtenido de Universidad Nacional Abierta y a Distancia: <http://hdl.handle.net/10596/11944>
- Giraldo Cepeda, L. E. (16 de abril de 2016). *UNAD Universidad Nacional Abierta y a Distancia*. Obtenido de Repositorio Institucional UNAD: <http://hdl.handle.net/10596/6341>
- informática jurídica.com. (2 de Abril de 2017). *Código Orgánico Integral Penal*. Obtenido de CÓDIGO ORGÁNICO INTEGRAL PENAL REPÚBLICA DEL ECUADOR ASAMBLEA NACIONAL: <http://www.informatica-juridica.com/codigo/codigo-organico-integral-penal/>
- ISO 27000.es. (s.f.). *El portal de ISO 27001 en Español*. Obtenido de <http://www.iso27000.es/iso27000.html>
- ISO Online Browsing Platform (OBP). (s.f.). *ISO/IEC 17021-2:2012(es)*. Obtenido de Prólogo: <https://www.iso.org/obp/ui#iso:std:iso-iec:ts:17021:-2:ed-1:v1:es>
- ISO/IEC 27001. (s.f.). *NOTICEBORED*. Obtenido de ISO/IEC 27001:2013 Information technology — Security techniques — Information security management systems — Requirements (second edition): <http://www.iso27001security.com/html/27001.html>
- ISOTools*. (7 de Mayo de 2015). Obtenido de Blog Calidad y Excelencia: <https://www.isotools.org/2015/05/07/como-elaborar-un-plan-de-mejora-continua/>
- Justino Salinas, Z. I. (04 de Junio de 2015). *PUCP*. Obtenido de <http://tesis.pucp.edu.pe/repositorio/handle/123456789/6045>
- Kosutic, D. (13 de abril de 2014). *27001 Academy*. Obtenido de El blog ISO 27001 & ISO 22301: <https://advisera.com/27001academy/blog/2014/04/13/has-the-pdca-cycle-been-removed-from-the-new-iso-standards/>
- Kosutic, D. (2016). *Seguro & Simple: Una guía para la pequeña empresa para la implementación de la ISO 27001 con medios propios*. Zagreb: Advisera Expert Solutions Ltd.
- LEY DE COMERCIO ELECTRÓNICO, FIRMAS ELECTRÓNICAS Y MENSAJES DE DATOS (Ley No. 2002-67)**. (s.f.). Obtenido de CONGRESO NACIONAL: [http://www.redipd.org/legislacion/common/legislacion/ecuador/ecuador\\_ley\\_2002-67\\_17042002\\_comelectronico.pdf](http://www.redipd.org/legislacion/common/legislacion/ecuador/ecuador_ley_2002-67_17042002_comelectronico.pdf)
- LEY DEL SISTEMA NACIONAL DE REGISTRO DE DATOS**. (24 de Marzo de 2010). Obtenido de LEXIS: <http://www.wipo.int/edocs/lexdocs/laws/es/ec/ec090es.pdf>
- Mark S. Merkow, J. B. (2014). *Seguridad de la Información: Principios y Prácticas, 2ª Edición*. Indianapolis: Pearson IT Certification. Obtenido de <http://www.pearsonitcertification.com/articles/article.aspx?p=2218577&seqNum=3>

- Mejía Viteri, J. G. (2016). Análisis y Evaluación del Riesgo de la Información: Caso de Estudio Universidad Técnica de Babahoyo. *Revista de Ciencia, Tecnología e Innovación*.
- MENDOZA, M. Á. (16 de Junio de 2015). *welivesecurity en español*. Obtenido de ¿Ciberseguridad o seguridad de la información? Aclarando la diferencia: <https://www.welivesecurity.com/la-es/2015/06/16/ciberseguridad-seguridad-informacion-diferencia/>
- Mina Calderón, L. M. (18 de Noviembre de 2015). *Repositorio Institucional*. Obtenido de <http://repository.ucc.edu.co/handle/ucc/304>
- Mindiamart. (s.f.). *ISO Certification Consultancy in Faridabad*. Obtenido de ISO IEC 27001 Certification: <http://valdezaudidores.com/certificacion-iso/>
- Moratilla, J. C. (29 de Mayo de 2017). *Cursos.com*. Obtenido de Seguridad de la Información: Una profesión multidisciplinar y con futuro: <https://cursos.com/seguridad-informacion-profesion-futuro/>
- P Verdezoto, J. R. (2015). Sistema de gestión de la seguridad de la información basado en la norma certificable ISO 27001: 2005 para una empresa proveedora de servicios de Telecomunicaciones e internet (Master's thesis, Espol). GUAYAQUIL.
- Romero Maldonado, J. V. (20 de Noviembre de 2015). *Utmach*. Obtenido de Repositorio Digital de la UTMACH: <http://repositorio.utmachala.edu.ec/handle/48000/3378>
- Rosales Bravo, P. F. (18 de nov de 2015). Obtenido de <http://bibdigital.epn.edu.ec/handle/15000/11952>
- Rosero Proaño, P. V. (30 de Abril de 2015). *ESCUELA POLITECNICA NACIONAL*. Obtenido de Repositorio Digital DSpace JSPUI: <http://bibdigital.epn.edu.ec/handle/15000/10488>
- Sala de Prensa CNT. (29 de mayo de 2015). *Noticias, Noticias Sala Prensa*. Obtenido de CNT ÚNICA EMPRESA PÚBLICA EN EL ECUADOR QUE OBTIENE CERTIFICACIÓN ISO 27001: <http://corporativo.cnt.gob.ec/cnt-unica-empresa-publica-en-el-ecuador-que-obtiene-certificacion-iso-27001/>
- Salamanca, O. (2016). Sistema de gestión de seguridad para redes de área local para empresas desarrolladoras de software. *Revista Venezolana de Información, Tecnología y Conocimiento*, 114-130.
- SGSI. (24 de Noviembre de 2014). Obtenido de Blog especializado en Sistemas de Gestión de Seguridad de la Información: <http://www.pmg-ssi.com/2014/11/iso-270012015-un-cambio-en-la-integracion-de-los-sistemas-de-gestion/>
- Solarte Solarte, F. N., ENRIQUEZ ROSERO, E. R., & Benavides Ruano, M. d. (2015). Metodología de análisis y evaluación de riesgos aplicados a. *Revista Tecnológica ESPOL – RTE*, 492-507. Obtenido de <http://www.rte.espol.edu.ec/index.php/tecnologica/article/viewFile/456/321>
- tcp Dirige tu negocio: Controla tus procesos. (s.f.). *Normativa: ISO 27001*. Obtenido de Servicio de Consultoría: Implantación de la ISO/IEC

27001: [http://www.tcpsi.com/vermas/ISO\\_27001.htm](http://www.tcpsi.com/vermas/ISO_27001.htm)

Un blog editado por ISOTools Excellence. (10 de diciembre de 2013). *SGS/ Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Obtenido de ISO 27001. Origen e historia.: <http://www.pmg-ssi.com/2013/12/iso27001-origen/>

Un blog editado por ISOTools Excellence. (18 de agosto de 2015). *SGS/ Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Obtenido de La norma ISO 27001:2013 ¿Cuál es su estructura?: <http://www.pmg-ssi.com/2015/08/norma-iso-27001-2013-estructura/>

Un blog editado por ISOTools Excellence. (28 de enero de 2015). *SGS/ Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Obtenido de ISO 27001: La implementación de un Sistema de Gestión de Seguridad de la Información: <http://www.pmg-ssi.com/2015/01/iso-27001-la-implementacion-de-un-sistema-de-gestion-de-seguridad-de-la-informacion/>

Un blog editado por ISOTools Excellence. (10 de agosto de 2017). *SGS/ Blog especializado en Sistemas de Gestión de Seguridad de la Información*. Obtenido de ¿Qué objetivo persigue la seguridad de la información?: <http://www.pmg-ssi.com/2017/08/que-objetivo-persigue-la-seguridad-de-la-informacion/>

WeblogBlog Calidad ISO UOS Xtended Studies. (30 de diciembre de 2014). *Historia de la ISO*. Obtenido de <http://blogdecalidadiso.es/historia-de-la-iso/>

## ANEXOS



**Guayaquil 5 de Julio del 2017**

**Señor Gerente General de RIGHTTEK S.A. -**

**VICTOR STALIN LEMOS PONCE. -**

Por medio de la presente solicito a usted señor Gerente que se conceda un permiso para realizar la auditoría de seguridad información en el área de infraestructura basado en la norma ISO 27001:2013 para diagnosticar las falencias de seguridad que poseen y brindarle a usted señor Gerente las posibles soluciones de seguridad para salvaguardar los activos de su empresa de carácter confidencial.

**Atentamente,**

**Robert Soria Cajas**

**Hilda Vera Barrera**



**UNIVERSIDAD DE GUAYAQUIL**  
**FACULTAD DE CIENCIAS MATEMÁTICAS Y FÍSICAS**  
**CARRERA DE INGENIERÍA EN NETWORKING Y**  
**TELECOMUNICACIONES**

**MANUAL DE BUENAS PRACTICAS**  
**BASADO EN LA NORMA ISO 27001:2013 PARA**  
**EL ÁREA DE INFRAESTRUCTURA RIGHTTEK S.A.**

**AUTORES:**

ROBERT EDUARDO SORIA CAJAS  
HILDA ELIZABETH VERA BARRERA

**GUAYAQUIL – ECUADOR**

**2017**

# Índice

<b>INTRODUCCIÓN.....</b>	<b>5</b>
<b>MANUAL DE BUENAS PRACTICAS .....</b>	<b>6</b>
<b>Política de seguridad de información .....</b>	<b>6</b>
<b>Políticas de Seguridad de información .....</b>	<b>6</b>
<b>Revisión de la Política de Seguridad de Información.....</b>	<b>7</b>
<b>Gestión De La Seguridad De La Información .....</b>	<b>8</b>
<b>Organización Interna .....</b>	<b>8</b>
<b>Roles Y Responsabilidades Sobre Seguridad De La Información.....</b>	<b>8</b>
<b>Segregación De Tareas .....</b>	<b>8</b>
<b>Contacto Con Las Autoridades .....</b>	<b>8</b>
<b>Seguridad De Información En La Gestión De Proyectos .....</b>	<b>8</b>
<b>Dispositivos Móviles Y Teletrabajo.....</b>	<b>8</b>
<b>Política de Dispositivos Móviles .....</b>	<b>8</b>
<b>Teletrabajo .....</b>	<b>9</b>
<b>Gestión De Activos .....</b>	<b>9</b>
<b>Responsabilidad sobre Activos .....</b>	<b>9</b>
<b>Inventario de Activos.....</b>	<b>9</b>
<b>Dueños de Activos.....</b>	<b>9</b>
<b>Uso Aceptable de Activos.....</b>	<b>10</b>
<b>Clasificación de Activos.....</b>	<b>10</b>
<b>Etiquetamiento y Manejo de la Información .....</b>	<b>10</b>
<b>Manejo de Activos de Información .....</b>	<b>10</b>
<b>Manejo de Medios .....</b>	<b>10</b>
<b>Manejo de Medios Removibles.....</b>	<b>10</b>
<b>Desecho de Medios.....</b>	<b>11</b>
<b>Transferencia de medio físico .....</b>	<b>11</b>
<b>Control De Acceso.....</b>	<b>11</b>
<b>Política de control de accesos .....</b>	<b>11</b>
<b>Acceso a Redes y servicios de Redes .....</b>	<b>11</b>
<b>Política de Utilización de los Servicios de Red .....</b>	<b>11</b>
<b>Política De Uso Adecuado De Internet .....</b>	<b>12</b>
<b>Gestión de acceso a usuarios .....</b>	<b>12</b>
<b>Registro de usuario y des-registro .....</b>	<b>12</b>
<b>Aprovisionamiento de acceso a usuarios.....</b>	<b>12</b>
<b>Administración de privilegios de acceso.....</b>	<b>12</b>
<b>Gestión de información de autenticación de usuarios secreta.....</b>	<b>13</b>

Revisión de derechos de acceso .....	13
Remoción o ajuste de derechos de acceso .....	13
Responsabilidades de usuarios .....	13
Uso de información de autenticación secreta .....	13
Control de acceso a sistemas y aplicaciones .....	13
Restricción de acceso a la información .....	13
Procedimiento de registros seguros .....	14
Sistemas de gestión de contraseñas .....	14
Uso de utilerías privilegiadas en los sistemas .....	14
Criptografía.....	15
Controles de criptografía .....	15
Seguridad Física Y Ambiental .....	15
Perímetro de Seguridad Física .....	15
Controles Físicos de Entrada .....	15
Protección contra Amenazas externas y Ambientales.....	15
Trabajo en Áreas Seguras.....	16
Seguridad del Equipo .....	16
Ubicación y protección del Equipo.....	16
Suministros de Apoyo (Energía u Otros) .....	16
Seguridad del Cableado .....	16
Mantenimiento de Equipo .....	17
Remoción de Activos.....	17
Desecho o re utilización Segura de equipo .....	17
Equipo de Usuario Desatendido .....	17
Política de Pantalla y Escritorio Limpio .....	17
Seguridad De Las Operaciones .....	18
Gestión de Capacidades .....	18
Separación de Sitios de Desarrollo, Pruebas y Operación.....	18
Protección de Malware .....	18
Respaldos .....	18
Registro y Monitoreo .....	19
Registros de Eventos .....	19
Protección de la Información de Registros .....	19
Registros de Operadores y Administradores.....	19
Sincronización de Relojes .....	19
Instalación de Software en Sistemas Operativos .....	19
Gestión de Vulnerabilidades Técnicas.....	19
Restricción en Instalación de Software.....	20

<b>Seguridad En Las Comunicaciones .....</b>	<b>20</b>
<b>Gestión de la Seguridad en Redes.....</b>	<b>20</b>
<b>Controles en Redes .....</b>	<b>20</b>
<b>Seguridad en Servicios de Redes .....</b>	<b>20</b>
<b>Segregación de Redes.....</b>	<b>21</b>
<b>Gestión de la Seguridad en Redes.....</b>	<b>21</b>
<b>Mensajería Electrónica .....</b>	<b>21</b>
<b>Adquisición, desarrollo y mantenimiento del sistema.....</b>	<b>21</b>
<b>Requerimientos de Seguridad para Sistemas de Información.....</b>	<b>21</b>
<b>Seguridad en la Aplicación de Servicios en Redes Públicas .....</b>	<b>22</b>
<b>Gestión De Incidentes De Seguridad De La Información .....</b>	<b>22</b>
<b>Gestión de Eventos de Seguridad de Información y Mejoras .....</b>	<b>22</b>
<b>Responsabilidades y Procedimientos .....</b>	<b>22</b>
<b>Reporte de Eventos de Seguridad de la Información .....</b>	<b>22</b>
<b>Reporte de las Debilidades de Seguridad de la Información .....</b>	<b>22</b>
<b>Análisis y Decisiones sobre Incidentes de Seguridad de la Información.....</b>	<b>23</b>
<b>Respuesta a Incidentes de Seguridad de la Información.....</b>	<b>23</b>
<b>Aprendiendo de los Incidentes de Seguridad de la Información .....</b>	<b>23</b>
<b>Colección de Pruebas.....</b>	<b>23</b>
<b>Seguridad De La Información En La Continuidad De La Organización .....</b>	<b>23</b>
<b>Planeando la Continuidad de la Seguridad de la Información .....</b>	<b>24</b>
<b>Implantando la Continuidad de la Seguridad de la Información .....</b>	<b>24</b>
<b>Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información .....</b>	<b>24</b>
<b>Redundancias.....</b>	<b>24</b>
<b>Cumplimiento .....</b>	<b>25</b>
<b>Cumplimiento de Requerimientos Legales.....</b>	<b>25</b>
<b>Identificación de Legislación Aplicable .....</b>	<b>25</b>
<b>Derechos de Propiedad Intelectual (IPR) .....</b>	<b>25</b>
<b>Protección de Registros Organizacionales .....</b>	<b>25</b>
<b>Protección de Datos y Privacidad de Información Personal .....</b>	<b>25</b>
<b>Cumplimiento con Políticas de Seguridad y Estándares.....</b>	<b>26</b>
<b>Revisión del Cumplimiento Técnico .....</b>	<b>26</b>

## **INTRODUCCIÓN**

En RIGHTTEK S.A. el área de Infraestructura Tecnológica considera la información como un elemento indispensable de uso diario y de carácter sensible razón por la cual se elaboró este manual de buenas prácticas, garantizando que se protegerá la información de forma adecuada, sin importar la forma en que se maneje, procese, transporte o almacenen los datos

Este manual contempla controles y recomendaciones basados en la norma ISO 27001:2013.

### **Objetivo**

Establecer las recomendaciones dadas por este manual con el fin de regular la seguridad de la información en el área.

### **Alcance**

El manual de buenas prácticas basado en la seguridad de la información del área de infraestructura de Righttek cubre todos los aspectos ajustados a la misma basada en la norma ISO 27001:2013 el cual deben ser cumplidos por todo el personal del área y las personas que se benefician de los procesos que se brindan en el área, logrando mejorar el estatus de protección de seguridad de la información.

## **MANUAL DE BUENAS PRACTICAS**

### **Política de seguridad de información**

En el área de Infraestructura de Righttek la información es un activo fundamental para la producción de sus procesos cotidianos, servicios y la toma de decisiones eficientes razón por lo cual se recomienda que exista un compromiso expreso para la protección de las propiedades más significativas como parte de una estrategia orientada a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad.

Se debe realizar la elaboración de un modelo de gestión de seguridad de la información que permita identificar y minimizar los riesgos a los cuales se expone la información, lo que ayudaría a reducir costos operativos y financieros, establecer una cultura de seguridad que garantice el cumplimiento de los requerimientos legales, contractuales y regulatorios de Righttek.

El Personal del área de infraestructura tecnología y todos aquellos que tengan responsabilidades sobre repositorios y recursos de procesamiento de la información del área de infraestructura, deben regirse a las políticas de seguridad que se elaboren dentro de la entidad y a los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

El presente documento es un Manual de buenas prácticas sobre la seguridad de la Información fundamentada en los objetivos de control del Anexo A de la Norma Internacional ISO 27001:2013.

### **Políticas de Seguridad de información**

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

Se recomienda que el Comité Integral este compuesto por el representante departamento de infraestructura de Righttek y el representante de la Alta Dirección. Este Comité debería encargarse de elaborar y actualizar las políticas, normas, pautas y procedimientos relativos a seguridad de la Información. También sería responsable de coordinar el análisis de riesgos, planes de contingencia y prevención de desastres. Durante sus reuniones programadas, el Comité efectuará la evaluación y revisión de la situación del área de infraestructura en cuanto a la Seguridad de la Información, incluyendo el análisis de incidentes ocurridos y que afecten la seguridad.

El Área infraestructura debería ser responsable de implantar y velar por el cumplimiento de las políticas, normas, pautas, y procedimientos de seguridad de la información en toda la organización, todo esto en coordinación con la Alta Dirección. También es responsable de evaluar e implantar productos de seguridad de la información, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además, debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad de la información y en particular en los casos de infección de virus, penetración de hackers, fraudes y otros percances.

El Administrador infraestructura debería ser responsable de establecer los controles de acceso apropiados para cada usuario, supervisar el uso de los recursos informáticos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administración como, por ejemplo, aplicar inmediatamente los parches correctivos cuando le llegue la notificación del fabricante del producto. El Administrador de infraestructura debería también ser responsable de informar al Comité Integral sobre toda actividad sospechosa o evento insólito.

Los usuarios deberían ser responsables de acatar con todas las políticas de Righttek relativas a la seguridad de la información.

### **Revisión de la Política de Seguridad de Información**

La Alta Dirección de Righttek debería aprobar un Manual de Políticas de Seguridad de la Información como muestra del compromiso y apoyo en el diseño e implementación de políticas que garanticen la seguridad de la información del área de infraestructura.

Cuando aprueben un manual de Políticas de seguridad de la Información la Alta Dirección de la Organización deberá demostrar su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad de la Información por lo menos una vez al año.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación del Manual de Políticas de Seguridad de la información a todos los empleados de la Organización.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad de la información.
- La verificación del cumplimiento de las políticas.



## **Gestión De La Seguridad De La Información**

### **Organización Interna**

Righttek debe establecer un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información para el área.

### **Roles Y Responsabilidades Sobre Seguridad De La Información**

Las violaciones a las Políticas de Seguridad de la Información deberían ser reportadas, registradas y monitoreadas a través un proceso de Acciones correctivas.

### **Segregación De Tareas**

Se debe contar con una definición clara de los roles y responsabilidades, así como del nivel de acceso y los privilegios correspondientes para todas las tareas en la cual los Usuarios tengan acceso a la infraestructura tecnológica y a los sistemas de información, con el fin de reducir y evitar el uso no autorizado o modificación sobre los activos de información del área, estos deberían ser definidos en un documento de “designación de Responsabilidades”.

### **Contacto Con Las Autoridades**

El Área infraestructura deberá tener actualizado el Directorio de las Autoridades y Grupos de Interés especial de la Organización.

### **Seguridad De Información En La Gestión De Proyectos**

Para todos los nuevos proyectos del área de infraestructura se debería firmar un Convenio de Confidencialidad.

### **Dispositivos Móviles Y Teletrabajo**

#### **Política de Dispositivos Móviles**

Righttek debería proveer las condiciones para el manejo de los dispositivos móviles (teléfonos Inteligentes, laptops) institucionales que se utilizan en el Área de Infraestructura. Así mismo deberá velar porque los usuarios hagan un uso responsable de los servicios y equipos proporcionados por la Organización, se debería hacer una revisión por lo menos 1 vez al mes vía remota o en sitio.

## **Teletrabajo**

Righttek debería especificar las circunstancias y requisitos para el establecimiento de conexiones remotas a la red de la Organización; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

## **Gestión De Activos**

### **Responsabilidad sobre Activos**

Righttek como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su red, otorgará responsabilidad a las áreas sobre sus activos de información con base en la Carta de Designación de Responsabilidades, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) propiedad de Righttek, son activos de la Organización y se proporcionan a los empleados, para cumplir con los propósitos del negocio, mediante Carta de Designación de Responsabilidades.

Toda la información sensible de Righttek, así como los activos donde ésta se almacena y se procesa deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios establecidos en la Matriz de Facultades. El área de compras debe llevar a cabo el levantamiento y la actualización permanente del inventario de activos de la Organización.

### **Inventario de Activos**

El Director General de Righttek, actúa como propietario de la información física y electrónica de la Organización, ejerciendo así la facultad de aprobar o revocar el acceso a su información con los perfiles adecuados para tal fin.

El área de compras debe generar un inventario de activos de información para las áreas o procesos de la Organización, acogiendo las indicaciones de las guías de clasificación de la información; así mismo, deben mantener actualizado el inventario de sus activos de información.

### **Dueños de Activos**

Los propietarios de los activos de información deben monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la

información.

Los propietarios de los activos de información deben ser conscientes que los recursos de procesamiento de información de la Organización, se encuentran sujetos a auditorías.

### **Uso Aceptable de Activos**

Los empleados no deben consumir alimentos y bebidas en los lugares de trabajo, para evitar derrames de líquidos sobre los activos de información.

Los empleados no deben utilizar sus equipos de cómputo y dispositivos móviles personales para desempeñar las actividades laborales.

### **Clasificación de Activos**

Righttek definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una guía de Clasificación de la Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

### **Etiquetamiento y Manejo de la Información**

Se debe definir el procedimiento de control de documentos y registros el rotulado y manejo de información, de acuerdo a la Tabla de Clasificación de la Información. Los mismos contemplarán los recursos de información tanto en formatos físicos como electrónicos, toda la información de la Organización tendrá que ser clasificada y etiquetada con base en la Tabla de Clasificación de la Información.

### **Manejo de Activos de Información**

Sólo el Propietario de la Información puede asignar o cambiar la clasificación de la información asignada.

Cada que la Información sea re clasificada se deberá definir una fecha de efectividad.

### **Manejo de Medios**

Se debe evitar la divulgación no-autorizada; modificación, eliminación o destrucción de activos; y la interrupción de las actividades comerciales.

### **Manejo de Medios Removibles**

Establecer el uso adecuado de los medios removibles durante la vida útil del Equipo en la Organización.

Asegurar el uso, reutilización y eliminación de medios removibles, con el fin de garantizar que la información se salvaguarde adecuadamente.

### **Desecho de Medios**

Righttek se encargará de conservar y resguardar los activos de información por periodos que cumplan las necesidades de los clientes internos y externos de la Organización, asegurando la disponibilidad de los diferentes activos de información cuando así sea necesario

### **Transferencia de medio físico**

Los medios que contienen información deben ser protegidos contra accesos no-autorizados, mal uso o corrupción durante el transporte más allá de los límites físicos de la Organización.

### **Control De Acceso**

#### **Política de control de accesos**

En Righttek se debe elaborar Políticas de control de acceso que restricciones y registros para la gestión de acceso a los usuarios con el fin de asegurar la disponibilidad e integridad de los activos de información de la Organización.

#### **Acceso a Redes y servicios de Redes**

#### **Política de Utilización de los Servicios de Red**

Se deberá controlar el acceso a los servicios de red tanto internos como externos. Para ello, se deberán desarrollar procedimientos para la activación y desactivación de derechos de acceso a las redes, los cuales comprenderían:

- Identificar las redes y servicios de red a los cuales se permite el acceso.
- Realizar normas y procedimientos de autorización para determinar las personas y las redes y servicios de red a los cuales se les otorgará el acceso.
- Establecer controles y procedimientos de gestión para proteger el acceso a las conexiones y servicios de red.
- Se debe limitar las opciones de elección de la ruta entre la terminal de usuario y los servicios a los cuales el mismo se encuentra autorizado a

acceder, mediante la implementación de controles en diferentes puntos de la misma.

### **Política De Uso Adecuado De Internet**

- Righttek consciente de la importancia de Internet como una herramienta para el desempeño de labores, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la Organización.

### **Gestión de acceso a usuarios**

- Se debe definir un procedimiento formal de registro de usuarios para otorgar y revocar el acceso a todos los sistemas, bases de datos y servicios de información multiusuario.
- Se deben utilizar identificadores de usuario únicos, de manera que se pueda identificar a los usuarios por sus acciones evitando la existencia de múltiples perfiles de acceso para un mismo empleado. El uso de identificadores grupales sólo debe ser permitido cuando sean convenientes para el trabajo a desarrollar debido a razones operativas.

### **Registro de usuario y des-registro**

- Registrar, revisar eventos y actividades críticas llevadas a cabo por los usuarios en los sistemas

### **Aprovisionamiento de acceso a usuarios**

- Se deberá llenar el formato para los nuevos accesos a todos los sistemas de información de la Organización con base en la política de control de accesos y el Procedimiento ABC para cuentas de Usuario de Righttek.

### **Administración de privilegios de acceso**

- El Área de Infraestructura deberá gestionar los Accesos a los sistemas de información de todos los usuarios de la Organización con base en la Matriz de Facultades y la Carta de Designación de Responsabilidades.
- El Área de Infraestructura deberá controlar los Accesos a los sistemas de procesamiento

**Gestión de información de autenticación de usuarios secreta**

- Todos los usuarios de la Organización deberán realizar el cambio de las contraseñas de los diferentes sistemas de información a los que tengan acceso, con base en la Matriz de Facultades y la Carta de Designación de Responsabilidades, cada 30 días o cuando se hayan realizado cambios en su perfil de puesto.

**Revisión de derechos de acceso**

- El área de Infraestructura deberá revisar y actualizar la lista de usuarios de Righttek de manera mensual.

**Remoción o ajuste de derechos de acceso**

- Debería haber un formato para la baja de accesos a todos los sistemas de información de la Organización de los usuarios desvinculados con base en la política de control de accesos, política de terminación o cambio de empleo para cuentas de Usuario de Righttek.

**Responsabilidades de usuarios**

- Se deben implementar directivas, con el fin de poner en conocimiento a los usuarios para su cumplimiento, donde debería constituir un medio de validación y autenticación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones o servicios de procesamiento de información.

**Uso de información de autenticación secreta**

- Se deben imponer cambios en las contraseñas en aquellos casos en que los usuarios mantengan sus propias contraseñas.
- Se debe Obligar a los usuarios a cambiar las contraseñas provisionales en su primer procedimiento de identificación, en los casos en que ellos seleccionen sus contraseñas.

**Control de acceso a sistemas y aplicaciones**

- Se debe realizar una evaluación de riesgos a fin de determinar el método de protección adecuado para el acceso al Sistema Operativo.
- Se debe definir un proceso de conexión seguro, este será diseñado para minimizar la oportunidad de acceso no autorizado.

**Restricción de acceso a la información**

- Los usuarios autorizados contarán únicamente con acceso a los puertos (USB, unidad de DVD-RW y elementos afines) que sean necesarios para desarrollar sus actividades.

### **Procedimiento de registros seguros**

- Se debe establecer normas para registrar a los usuarios de forma segura, una de ellas sería el crear cuentas basado a una plantilla, por ejemplo: Primera Letra del primer y segundo Nombre + . + Apellido Paterno; Ejemplo: Robert Eduardo Soria → RE.soria

### **Sistemas de gestión de contraseñas**

Se debe establecer un sistema de gestión de contraseñas en donde puedan tener un control sobre el uso de las mismas en los usuarios, las políticas podrían ser:

- La cuenta debe quedar bloqueada si la contraseña es introducida erróneamente 3 veces consecutivas.
- El sistema le indicará al usuario el momento de renovar su contraseña. Si el usuario no la actualiza, la cuenta quedará bloqueada.

### **Uso de utilerías privilegiadas en los sistemas**

Righttek deberá proveer normas para el correcto uso de herramientas de utilidad pueden anular los controles de seguridad de aplicaciones y sistemas y deberán ser estrictamente controladas, incluyendo limitar su acceso a un estrecho círculo de los empleados.

## **Criptografía**

En Righttek se deberá utilizar sistemas y técnicas criptográficas para la protección de la información con base en un análisis de riesgo efectuado, con el fin de asegurar una adecuada protección de su confidencialidad e integridad.

### **Controles de criptografía**

Se deben utilizar controles criptográficos para la protección de claves de acceso a sistemas, datos y servicios.

## **Seguridad Física Y Ambiental**

Righttek proveerá la implantación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en el área de infraestructura. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

### **Perímetro de Seguridad Física**

- Los sitios escogidos para colocar los sistemas de información, equipos de cómputo y comunicaciones, deben estar protegidos por barreras y controles físicos, para evitar intrusión física, inundaciones, y otro tipo de amenazas que afecten su normal operación.

### **Controles Físicos de Entrada**

- Todos los sitios en donde se encuentren sistemas de procesamiento informático o de almacenamiento, deben ser protegidos de accesos no autorizados, utilizando tecnologías de autenticación, monitoreo y registro de entradas y salidas.

### **Protección contra Amenazas externas y Ambientales**

- Se debe asignar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, manifestaciones y otras formas de desastres naturales o causados por el hombre.
- Se deberá prestar consideración a cualquier amenaza contra la seguridad presentada por vecinos locales; por ejemplo, un fuego en un edificio vecino, escape de agua en el techo o pisos en sótano o una explosión en la calle.



## **Trabajo en Áreas Seguras**

- Se debe diseñar y aplicar la protección física y los lineamientos para trabajar en áreas aseguradas.
- El personal debe estar al tanto de la existencia o las actividades dentro del área asegurada sólo conforme las necesite conocer.

## **Seguridad del Equipo**

- Para evitar pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades del área, se deberá proteger el equipo de amenazas físicas y ambientales.

## **Ubicación y protección del Equipo**

Righttek para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la Organización que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

## **Suministros de Apoyo (Energía u Otros)**

Se debe proteger el equipo de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos de soporte. Todos los servicios públicos de soporte; como electricidad, suministro de agua, desagüe, calefacción/ventilación y aire acondicionado; deberán ser adecuados para los sistemas que soportan. Los servicios públicos de soporte deben ser inspeccionados regularmente y, conforme sea apropiado, probados para asegurar su adecuado funcionamiento y para reducir cualquier riesgo por un mal funcionamiento o falla.

## **Seguridad del Cableado**

El cableado de la energía y las telecomunicaciones que llevan datos o dan soporte a los servicios de información deben protegerse contra la interceptación o daño. Se debe considerar los siguientes lineamientos para la seguridad del cableado.

- Cuando sea posible, las líneas de energía y telecomunicaciones que van a los medios de procesamiento de información debieran ser subterráneas o deben estar sujetas a una alternativa de protección adecuada.
- El cableado de la red debe estar protegido contra interceptaciones no autorizadas o daños, por ejemplo, utilizando un tubo o evitando las rutas a través de áreas públicas.

- Los cables de energía deben estar separados de los cables de comunicaciones para evitar la interferencia.
- Se debe utilizar marcadores de cables y equipos claramente identificables para minimizar errores en el manipuleo, como un empalme accidental de los cables de red equivocados.

### **Mantenimiento de Equipo**

Se debe mantener correctamente el equipo para asegurar su continua disponibilidad e integridad. Se debe considerar los siguientes lineamientos para el mantenimiento de equipo.

- realizar mantenimientos preventivos y correctivos de los recursos de la plataforma tecnológica
- realizar un Plan Anual de mantenimiento de Cómputo y Comunicación llevada a cabo por la verificación aleatoria a los equipos de cómputo.

### **Remoción de Activos**

- Se debe establecer límites de tiempo para el retiro del equipo y se debe realizar un chequeo de la devolución.

### **Desecho o re utilización Segura de equipo**

- Se deben checar los componentes del equipo que contiene medios de almacenamiento para asegurar que se haya retirado o sobre-escrito cualquier dato confidencial o licencia de software antes de su eliminación.
- Los dispositivos que contienen datos confidenciales pueden requerir una evaluación del riesgo para determinar si los componentes deben ser físicamente destruidos en lugar de enviarlos a reparar o descartar.

### **Equipo de Usuario Desatendido**

- El personal de infraestructura debe bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

### **Política de Pantalla y Escritorio Limpio**

Preservar la seguridad de la información de Righttek por medio de buenas prácticas en el manejo de documentos, medios de almacenamiento removibles y pantalla de los dispositivos de procesamiento de información.

Para el aseguramiento de la información sensible del área, los empleados deberán adoptar buenas prácticas al momento de manejar y administrar la información, teniendo en cuenta los niveles de clasificación de la información, los riesgos identificados.

### **Seguridad De Las Operaciones**

- Se debe asegurar la operación correcta y segura de los medios de procesamiento de la información.
- Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información. Esto incluye el desarrollo de los procedimientos de operación apropiados.
- Se deben controlar estrictamente todos los cambios realizados en los sistemas de información.

### **Gestión de Capacidades**

- Se deben monitorear, afinar el uso de los recursos y se deben realizar proyecciones de los requerimientos de capacidad futura para asegurar el desempeño requerido del sistema.

### **Separación de Sitios de Desarrollo, Pruebas y Operación**

Los medios de desarrollo, prueba y operación deben estar separados para reducir los riesgos de acceso no-autorizado o cambios en el sistema operacional. Se debe identificar el nivel de separación necesario entre los ambientes de desarrollo, prueba y operación para evitar los problemas operacionales y se debe implementar los controles apropiados.

### **Protección de Malware**

El software y los medios de procesamiento de la información son vulnerables a la introducción de códigos maliciosos; como virus de cómputo, virus de red, caballos Troyanos y bombas lógicas. Los usuarios deberán estar al tanto de los peligros de los códigos maliciosos. Cuando sea apropiado, se debe introducir controles para evitar, detectar y eliminar los códigos maliciosos.

### **Respaldos**

Mantener la integridad y disponibilidad de la información y los medios de procesamiento de información.

- Se deben establecer los procedimientos de rutina para implementar la política de respaldo acordada y la estrategia para tomar copias de respaldo de los datos y practicar su restauración oportuna.

### **Registro y Monitoreo**

- Se deben establecer procedimientos para el monitoreo del uso de los medios de procesamiento de la información y se deben revisar regularmente los resultados de las actividades de monitoreo.

### **Registros de Eventos**

- Se deben producir y mantener registros de auditoría de las actividades, excepciones y eventos de seguridad de la información durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.

### **Protección de la Información de Registros**

- Se deben proteger los medios de registro y la información del registro para evitar la alteración y el acceso no autorizado.

### **Registros de Operadores y Administradores**

- Se deben registrar las actividades del administrador del sistema y el operador del sistema.
- Los registros de administrador y operador del sistema deben ser revisados de manera regular.

### **Sincronización de Relojes**

- Los relojes de todos los sistemas de procesamiento de información relevantes dentro del área de infraestructura se deben sincronizar con una fuente que proporcione la hora exacta acordada.

### **Control de Software Operativo**

#### **Instalación de Software en Sistemas Operativos**

- El Área deberá realizar todas las pruebas necesarias de cualquier Software nuevo adquirido por la Organización, antes de su instalación.
- El Área deberá asegurarse que todo el Software nuevo adquirido por la Organización cuente con su licencia correspondiente.

### **Gestión de Vulnerabilidades Técnicas**

El área debe revisar periódicamente la aparición de vulnerabilidades

técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Esta encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

### **Restricción en Instalación de Software**

- El Área debe validar que la capacidad del equipo cumpla con los requisitos mínimos para la instalación del software.

## **Seguridad En Las Comunicaciones**

### **Gestión de la Seguridad en Redes**

El área debe establecer, los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la Organización.

### **Controles en Redes**

- Las redes deben ser adecuadamente manejadas y controladas para poder proteger la información y mantener la seguridad de los sistemas y aplicaciones, incluyendo la información en tránsito.
- El Área de Infraestructura debe implementar controles para asegurar la seguridad de la información en las redes, y proteger los servicios conectados de accesos no-autorizados.

### **Seguridad en Servicios de Redes**

- En todo contrato de redes se deben identificar e incluir las características de seguridad, niveles de servicio y requerimientos de gestión de todos los servicios de red, ya sea que estos servicios sean provistos interna o externamente.
- Se debe determinar y monitorear regularmente la capacidad del proveedor del servicio de red para manejar los servicios contratados de una manera segura, y se debe acordar el derecho de auditoría.

### **Segregación de Redes**

- El Área de Infraestructura deberá gestionar las direcciones Ip de los equipos de toda la Organización en grupos de acuerdo a las diferentes Áreas con base en la Matriz de Facultades.

### **Gestión de la Seguridad en Redes**

- Se debe asegurar la protección de la información en redes y la protección de la infraestructura de soporte.
- La gestión segura de las redes, la cual puede abarcar los límites organizacionales, requiere de la cuidadosa consideración del flujo de datos, implicancias legales, monitoreo y protección.

### **Mensajería Electrónica**

Righttek, entendiendo la importancia del correo electrónico como herramienta para facilitar la comunicación entre empleados y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

### **Adquisición, desarrollo y mantenimiento del sistema**

#### **Requerimientos de Seguridad para Sistemas de Información**

- Se debe definir un procedimiento para que, durante las etapas de análisis y diseño del sistema, se incorporen a los requerimientos, los correspondientes controles de seguridad. Este procedimiento debería incluir una etapa de evaluación de riesgos previa al diseño, para definir los requerimientos de seguridad e identificar los controles apropiados. En esta tarea deben participar las áreas usuarias, de Sistemas y Comité Integral, especificando y aprobando los controles automáticos a incorporar al sistema y las necesidades de controles manuales complementarios. Las áreas involucradas podrán solicitar certificaciones y evaluaciones independientes para los productos a utilizar.

## **Seguridad en la Aplicación de Servicios en Redes Públicas**

- El Área deberá asegurarse del correcto funcionamiento del certificado de seguridad, para los sistemas de información de la Organización que cuentan con acceso a través de internet, para brindar el envío y recepción de información de manera segura.

## **Gestión De Incidentes De Seguridad De La Información**

### **Gestión de Eventos de Seguridad de Información y Mejoras**

Righttek promoverá entre los empleados y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

### **Responsabilidades y Procedimientos**

- Righttek asignará responsables para el tratamiento de los incidentes de seguridad de la información, quienes tendrán la responsabilidad de investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad.

### **Reporte de Eventos de Seguridad de la Información**

- Los propietarios de los activos de información deben informar a Área de Infraestructura, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

### **Reporte de las Debilidades de Seguridad de la Información**

- Los usuarios de servicios de información, al momento de tomar conocimiento directa o indirectamente acerca de una debilidad de seguridad, son responsables de registrar y comunicar las mismas al Área de Infraestructura y/o a su Coordinador de Área correspondiente.

### **Análisis y Decisiones sobre Incidentes de Seguridad de la Información**

- El Comité Integral debe analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con la Alta Dirección cuando lo estime necesario.
- Es responsabilidad de los empleados de Righttek y del personal provisto por terceras partes reportar cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos con la mayor prontitud posible.

### **Respuesta a Incidentes de Seguridad de la Información**

- El Área de Infraestructura deberá dar respuesta a los incidentes de seguridad de la información de acuerdo con el Procedimiento de Incidencia de Sistemas.

### **Aprendiendo de los Incidentes de Seguridad de la Información**

- El Área de Infraestructura deberá definir un proceso que permita documentar, cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías. Esta información se utilizará para identificar aquellos que sean recurrentes o de alto impacto. Esto será evaluado a efectos de establecer la necesidad de mejorar o agregar controles para limitar la frecuencia, daño y costo de casos futuros, con base en el Procedimiento de Incidencia de Sistemas y el Procedimiento de Requisiciones de Servicio de Sistemas.

### **Colección de Pruebas**

- El Área de Infraestructura deberá documentar todos los incidentes de seguridad de la información de la Organización con base en el Procedimiento de Incidencias de Sistemas y cuando aplique deberá elaborar una Acción Correctiva o preventiva, para tener actualizada la base de conocimiento y prevenir y/o atender de forma más oportuna los futuros incidentes de seguridad.

### **Seguridad De La Información En La Continuidad De La Organización**

Righttek proporcionará los recursos suficientes para contar con una respuesta efectiva de los empleados y procesos en caso de contingencia o eventos catastróficos que se presenten en la Organización y que afecten la continuidad de su operación. Además, responderá de manera efectiva ante



eventos catastróficos según la magnitud y el grado de afectación de los mismos; se restablecerán las operaciones con el menor costo y pérdidas posibles, manteniendo la seguridad de la información durante dichos eventos. Righttek mantendrá canales de comunicación adecuados hacia los empleados, proveedores y terceras partes interesadas.

### **Planeando la Continuidad de la Seguridad de la Información**

- Se debe contar con un Plan de Continuidad de las Actividades de la Organización.
- El Comité Integral debe tener a cargo la coordinación del proceso de administración de la continuidad de la operación de los sistemas de tratamiento de información de la Organización frente a interrupciones imprevistas.

### **Implantando la Continuidad de la Seguridad de la Información**

- Se deben identificar y acordar respecto a todas las funciones y procedimientos de emergencia.
- Se deben analizar los posibles escenarios de contingencia y definir las acciones correctivas a implementar en cada caso.

### **Verificación, Revisión y Evaluación de la Continuidad de la Seguridad de la Información**

- El Comité Integral debe liderar los temas relacionados con la continuidad del negocio y la recuperación ante desastres.
- El Comité Integral debe realizar los análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad de la información a que haya lugar.

### **Redundancias**

- El Área de Infraestructura deberá asegurar la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la Organización.

## **Cumplimiento**

### **Cumplimiento de Requerimientos Legales**

- Cumplir con las disposiciones normativas y contractuales a fin de evitar sanciones administrativas a la Organización y/o al empleado o que incurran en responsabilidad civil o penal como resultado de su incumplimiento.
- Garantizar que los sistemas cumplan con la política, normas y procedimientos de seguridad de la Organización.

### **Identificación de Legislación Aplicable**

- Se definirán y documentarán claramente todos los requisitos normativos y contractuales pertinentes para cada sistema de información. Del mismo modo se definirán y documentarán los controles específicos y las responsabilidades y funciones individuales para cumplir con dichos requisitos.

### **Derechos de Propiedad Intelectual (IPR)**

Se implementarán procedimientos adecuados para garantizar el cumplimiento de las restricciones legales al uso del material protegido por normas de propiedad intelectual.

### **Protección de Registros Organizacionales**

- Los registros críticos de la Organización se protegerán contra pérdida, destrucción y falsificación. Algunos registros pueden requerir una retención segura para cumplir requisitos legales o normativos, así como para respaldar actividades esenciales de la Organización.

### **Protección de Datos y Privacidad de Información Personal**

- Todos los empleados deberán conocer las restricciones al tratamiento de los datos y de la información respecto a la cual tengan conocimiento con motivo del ejercicio de sus funciones. La Organización redactará una “Carta de Confidencialidad”, el cual deberá ser suscrito por todos los empleados. La copia firmada del compromiso será retenida en forma segura por la Organización.

**Cumplimiento con Políticas de Seguridad y Estándares**

- El Área, realizará revisiones periódicas de todas las áreas de la Organización a efectos de garantizar el cumplimiento de la política, normas y procedimientos de seguridad.

**Revisión del Cumplimiento Técnico**

- El Área verificará periódicamente que los sistemas de información cumplan con la política, normas y procedimientos de seguridad, las que incluirán la revisión de los sistemas en producción a fin de garantizar que los controles de hardware y software hayan sido correctamente implementados.

Título: <b>PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK</b>	Código: <b>RGT-SDI-0001</b>	Versión: <b>01</b>	Página: <b>1/13</b>
--	--------------------------------	-----------------------	------------------------



# **RIGHTTEK**

**Tecnología Apropriada S.A.**

## **PROCEDIMIENTO PARA AUDITORIA INTERNA A LOS SISTEMAS DE GESTION DE LA SEGURIDAD DE LA INFORMACION DE RIGHTTEK**

Concepto	Nombre, Apellido – Puesto	Firma	Fecha de Firma
Elaborado Por:	ROBERT SORIA – AUDITOROR		10-Jul-17
	HILDA VERA - AUDITORA		10-Jul-17
Revisado Por:	VICTOR PANTOJA – LIDER AREA INFRAESTRUCTURA		11-Jul-17

Título: PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK	Código: RGT-SDI-0001	Versión: 01	Página: <b>2/13</b>
--	-------------------------	----------------	------------------------

Aprobado Por:	VICTOR LEMOS – GERENTE GENERAL		14-Jul-17
---------------	--------------------------------	--	-----------

## 1. OBJETIVO

Establecer los lineamientos y el procedimiento a seguir para la planificación, realización y cierre de auditorías internas al SGSI de RIGHTTEK, bajo la norma ISO/IEC 27001:2013, respectivamente.

## 2. ALCANCE

El presente procedimiento es administrado por GR y es fuente de consulta y aplicación para AIT en el alcance del SGSI de RIGHTTEK. El procedimiento se inicia con la realización de la auditoría interna al SGSI a cargo del AI de RIGHTTEK S.A. y finaliza cuando el AIT dispone el tratamiento de los hallazgos de auditoría del SGSI respectivamente.

Este procedimiento es aplicable a los procesos comprendidos dentro del alcance del SGSI, bajo las normas ISO/IEC 27001:2013, respectivamente.

## 3. DOCUMENTOS A CONSULTAR

- 3.1. Norma ISO/IEC 27001:2013. Tecnología de la información. Técnicas de seguridad. Sistemas de gestión de seguridad de la información. Requisitos.

## 4. SIGLAS Y ACRÓNIMOS

- 4.1. AI: Auditor Interno.
- 4.2. GR: Gerente de Righttek
- 4.3. AIT: Áreas de Infraestructura Tecnológica
- 4.4. RED: Representante de la dirección
- 4.5. SGSI: Sistema de Gestión de Seguridad de la Información.

## 5. DEFINICIONES

Para efectos del presente procedimiento se consideran las siguientes definiciones, las mismas que se encuentran señaladas en la norma ISO 19011:2011:

- 5.1. Alcance de la Auditoría: Extensión y límites de una auditoría.  
Nota: El alcance de la auditoría incluye generalmente una descripción de las ubicaciones, las unidades de la organización, las actividades y los procesos, así como el período de tiempo cubierto.
- 5.2. Auditado: Organización que es auditada.
- 5.3. Auditor: Persona que lleva a cabo una auditoría.
- 5.4. Auditoría: Proceso sistemático, independiente y documentado para obtener evidencias de la auditoría y

<b>Título:</b> <b>PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK</b>	<b>Código:</b> <b>RGT-SDI-0001</b>	<b>Versión:</b> <b>01</b>	<b>Página:</b> <b>3/13</b>
---	---------------------------------------	------------------------------	-------------------------------

evaluarlas de manera objetiva con el fin de determinar el grado en que se cumplen los criterios de auditoría.

Nota 1: Las auditorías internas, denominados en algunos casos auditorías de primera parte, se realizan por la organización, o en nombre, para la revisión por la Dirección y para otros propósitos internos. Pueden formar la base para una auto declaración de conformidad de una organización. En muchos casos, particularmente en organizaciones pequeñas, la independencia puede demostrarse al estar libre el auditor de responsabilidades en la actividad que se audita o al estar libre del sesgo o conflicto de intereses.

Nota 2: Las auditorías externas incluyen auditorías de segunda y tercera parte. Las auditorías de segunda parte se llevan a cabo por partes que tienen un interés en la organización, tal como los clientes, o por otras personas en su nombre. Las auditorías de tercera parte se llevan a cabo por organizaciones auditoras independientes y externas, tales como las autoridades reglamentarias o aquellas que proporcionan la certificación.

- 5.5. Cliente de la Auditoría: Organización o persona que solicita una auditoría.

Nota 1: En el caso de auditoría interna, el cliente de la auditoría también puede ser el auditado o la persona que gestiona el programa de auditoría. Las solicitudes de una auditoría externa pueden provenir de fuentes como autoridades reglamentarias, partes contratantes o clientes potenciales.

- 5.6. Competencia: Capacidad para aplicar conocimientos y habilidades para alcanzar los resultados pretendidos.

- 5.7. Conclusiones de la Auditoría: Resultado de una auditoría, tras considerar los objetivos de la auditoría y todos los hallazgos de la auditoría.

- 5.8. Criterios de Auditoría: Conjunto de políticas, procedimientos o requisitos usados como referencia frente a la cual se compara la evidencia de la auditoría.

- 5.9. Equipo Auditor: Uno o más auditores que llevan a cabo una auditoría, con el apoyo si es necesario, de expertos técnicos.

Nota 1: A un auditor del equipo se le designa como

líder del mismo. Nota 2: El equipo auditor puede

incluir auditores en formación.

- 5.10. Evidencia de la Auditoría: Registros, declaraciones de hechos o cualquier otra información que son pertinentes para los criterios de auditoría y que son verificables.

Nota: La evidencia de la auditoría puede ser cualitativa o cuantitativa.

- 5.11. Experto Técnico: Persona que aporta conocimientos o experiencia específicos al equipo auditor.

Nota 1: El conocimiento o experiencia específicos son los relacionados con la organización, el proceso o la actividad a auditar, el idioma o la orientación cultural.

Nota 2: Un experto técnico no actúa como un auditor en el equipo auditor.

- 5.12. Hallazgos de la Auditoría: Resultados de la evaluación de la evidencia de la auditoría recopilada frente a los criterios de auditoría.

- 5.13. No Conformidad: Incumplimiento de un requisito.

- 5.14. Observador: Persona que acompaña al equipo auditor pero que no audita.

Nota 1: Un observador no es parte del equipo auditor y no influye ni interfiere en la realización de la auditoría.

Nota 2: Un observador puede designarse por el auditado, una autoridad reglamentaria u otra parte interesada que testifica la auditoría.

<b>Título:</b> <b>PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK</b>	<b>Código:</b> <b>RGT-SDI-0001</b>	<b>Versión:</b> <b>01</b>	<b>Página:</b> <b>4/13</b>
---	---------------------------------------	------------------------------	-------------------------------

- 5.15. Plan de Auditoría: Descripción de las actividades y de los detalles acordados de una auditoría.
- 5.16. Programa de la Auditoría: Detalles acordados para un conjunto de una o más auditorías planificadas para un periodo de tiempo determinado y dirigidas hacia un propósito específico.

Además, se consideran las siguientes definiciones, las mismas que se encuentran señaladas en la norma ISO 9000:2005:

- 5.17. Acción Correctiva: Acción tomada para eliminar la causa de una No Conformidad detectada u otra situación no deseable.
- 5.18. Acción Preventiva: Acción tomada para eliminar la causa de una No Conformidad potencial u otra situación potencial no deseable.
- 5.19. Corrección: Acción tomada para eliminar una no conformidad detectada.
- Nota 1: Una corrección puede realizarse junto con una acción correctiva.

Asimismo, para el caso específico del presente procedimiento se consideran las siguientes definiciones:

- 5.20. Auditor en Formación: Auditor en proceso de entrenamiento, que realiza sus labores de auditoría bajo la dirección y orientación de un auditor competente.
- 5.21. Auditor Líder: Miembro del equipo auditor designado para dirigir la auditoría.
- 5.22. Auditoría Extraordinaria: Auditoría realizada fuera del Programa Anual de Auditoría.
- 5.23. Observación: No conformidad potencial u otra situación potencial no deseable.
- 5.24. Oportunidad de Mejora: Falla aislada o esporádica en el contenido o implementación del sistema de gestión, o cualquier situación en la que pueda mejorarse algún aspecto del sistema.
- 5.25. Reunión de Enlace: Reunión del equipo auditor en la cual se analiza e informa los hallazgos de la Auditoría con el fin de llegar a un consenso en los resultados de la misma.

## 6. CONDICIONES BÁSICAS

- 6.1. Las auditorías internas se realizarán a fin de determinar el grado en que el SGSI está implementado y mantenido de manera eficaz, si cumple con los requisitos de las normas ISO/IEC 27001:2013 y con los requisitos propios de la organización. Esta formará parte del Programa Anual de Auditoría, el cual deberá ser elaborado según Anexo N° 1 del presente, y aprobado por la alta Gerencia dentro del primer trimestre de cada año. Dicho programa podrá ser modificado en caso de ser necesario, las modificaciones deberán ser aprobadas del mismo modo como se aprobó el programa original.
- 6.2. Para la elaboración del Programa Anual de Auditoría se debe tener en cuenta lo siguiente:
- Las auditorías internas deben realizarse a intervalos planificados (por lo menos una vez al año).
  - El alcance de las auditorías internas puede ser parcial o integral. El programa anual debe comprender la evaluación integral del SGSI, según corresponda.
  - El alcance y la frecuencia de las auditorías internas serán determinados en función de la importancia y el estado de los procesos o áreas a auditar, y los resultados de auditorías previas.
  - Las auditorías externas, de seguimiento o de recertificación, según corresponda.
- 6.3. El Equipo Auditor puede estar conformado por uno o varios Auditores Internos dependiendo de la

<b>Título:</b> <b>PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK</b>	<b>Código:</b> <b>RGT-SDI-0001</b>	<b>Versión:</b> <b>01</b>	<b>Página:</b> <b>5/13</b>
---	---------------------------------------	------------------------------	-------------------------------

complejidad y características de la auditoría interna; y en caso de ser necesario, podrán participar auditores en formación, expertos técnicos y observadores. En el caso de los auditores en formación, estos deberán haber llevado previamente el curso de auditor interno en la Norma ISO/IEC 27001, en el caso de los observadores, estos deberán haber llevado previamente el curso de Interpretación de la Norma ISO/IEC 27001, según corresponda.

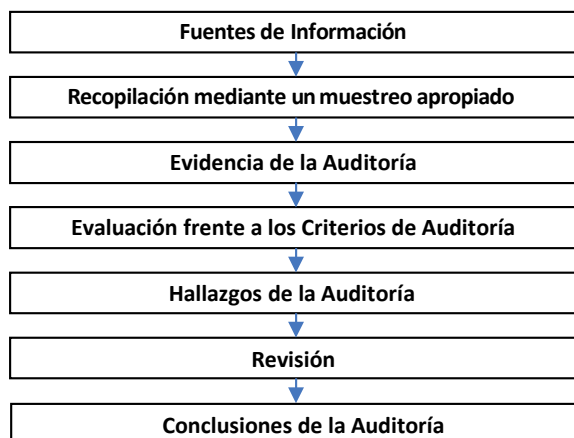
- 6.4. Los auditores internos, podrán ser personal de la entidad o terceros; en ambos casos deben cumplir con las competencias de educación, formación y experiencia establecida en el Perfil del Auditor Interno (Ver Anexo N° 4). Deben guardarse los registros que evidencien el cumplimiento del perfil precitado por parte de cada uno los auditores internos.
- 6.5. Los auditores internos deben mantener imparcialidad durante la realización de la auditoría.
- 6.6. Las recomendaciones producto de la realización de las auditorías internas no tienen carácter vinculante.

## 7. CONDICIONES ESPECÍFICAS

- 7.1. El Líder del área auditada, según corresponda, es el responsable de velar por el cumplimiento de lo dispuesto en este procedimiento.
- 7.2. El Líder del área , es el responsable de gestionar el Programa Anual de Auditoría para el SGSI, dicha gestión incluye entre otros aspectos:
  - a. Elaborar, modificar y obtener de la Alta Gerencia la aprobación del Programa Anual de Auditoría.
  - b. Comunicar a las partes pertinentes la aprobación, modificación, avance y resultados del Programa Anual de Auditoría.
  - c. Asegurarse de la implementación del Programa de Anual de Auditoria, incluyendo el establecimiento de los objetivos, el alcance y los criterios de auditoría de las auditorías individuales y la selección del Equipo Auditor y del Auditor Líder, cuando corresponda.
  - d. Seguimiento, revisión y mejora del Programa Anual de Auditoría.
  - e. Asegurarse de que se gestionan y mantienen los registros apropiados del Programa Anual de Auditoria.
  - f. Determinar y gestionar los recursos necesarios para la implementación del Programa de Anual de Auditoría.
  - g. Solicitar auditorías extraordinarias cuando lo considere necesario; debiendo actualizar el Programa Anual de Auditoria, si los cambios se justifican
- 7.3. La presente figura representa de manera esquemática la metodología para llevar a cabo las auditorías interna



<b>Título:</b> PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK	<b>Código:</b> RGT-SDI-0001	<b>Versión:</b> 01	<b>Página:</b> 6/13
--	--------------------------------	-----------------------	------------------------



7.4. El Jefe

del órgano o unidad orgánica, o el Coordinador del Departamento,

responsable del proceso o área objeto de la auditoría, debe:

- Poner a disposición del equipo auditor los medios necesarios para la auditoría.
- Facilitar el acceso a las instalaciones y documentos relevantes para la auditoría.
- Cooperar con los auditores para asegurar el éxito de la auditoría.
- Tomar las acciones correctivas necesarias sin demora injustificada para eliminar las no conformidades detectadas durante la auditoría y sus causas.

7.5. Los hallazgos de la auditoría se clasifican y tratan de acuerdo con lo siguiente:

Tipo de Hallazgo	Acción para su tratamiento
No Conformidad	Acción Correctiva
Observación	Gestión del Riesgo (SGSI)

7.6. Luego de la reunión de cierre, la Alta Dirección debe analizar las fortalezas, debilidades, observaciones y oportunidades de mejora del SGSI señaladas en el informe de auditoría. Asimismo, debe tomar las acciones y decisiones necesarias para el tratamiento de los hallazgos de la auditoría, de acuerdo con la normativa vigente.

7.7. Se pueden realizar Auditorías Extraordinarias, siempre que se considere necesario, previa comunicación a las áreas involucradas. Estas Auditorías Extraordinarias pueden llevarse a cabo entre otras causas debido a:

- Introducción de cambios en la organización.
- Se sospeche o se tenga certeza de la pérdida de eficacia del Sistema de Gestión.
- Se considere oportuno para la verificación de acciones correctivas o correctivas que requieran control y seguimiento de su implantación y efectividad.

## 8. REGISTROS

Descripción	Código	Nº de ejemplares	Lugar de archivo
Plan de Auditoría Interna	RGT-SI-0003	1	Servidor FTP Righttek

<b>Título:</b> <b>PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK</b>	<b>Código:</b> <b>RGT-SDI-0001</b>	<b>Versión:</b> <b>01</b>	<b>Página:</b> <b>7/13</b>
---	---------------------------------------	------------------------------	-------------------------------

Correo Electrónico de difusión de Plan de Auditoría Interna	No aplica	1	Servidor FTP Righttek
Informe de Auditoría Interna	RGT-SI-0004	1	Servidor FTP Righttek
Evidencia de cumplimiento del Perfil del Auditor Interno	No aplica	1	Servidor FTP Righttek

## 9. HOJA DE CONTROL DE CAMBIOS

Nº de versión	Nº de capítulo/ Ítem	Párrafo/ Figura/ Tabla/ Nota	Modificaciones
N/A	N/A	N/A	N/A

## 10. ANEXOS

Descripción	Anexo
Formato Programa Anual de Auditoría	1
Formato Plan de Auditoría Interna	2
Formato Informe de Auditoria Interna	3
Perfil del Auditor Interno	4

<b>Título:</b> <b>PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK</b>	<b>Código:</b> <b>RGT-SDI-0001</b>	<b>Versión:</b> <b>01</b>	<b>Página:</b> <b>8/13</b>
---	---------------------------------------	------------------------------	-------------------------------

## **ANEXO**

### **Nº 1**

Título: PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK	Código: RGT-SDI-0001	Versión: 01	Página: 9/13
--	-------------------------	----------------	-----------------

 <b>RIGHTTEK</b> <small>Tecnología Apropriada S.A.</small>				<b>PROGRAMA DE AUDITORIA</b>			
<b>I. DATOS GENERALES</b>							
1.1. Norma de referencia				1.2. Año de vigencia del programa			
1.3. Objetivo							
<b>II. PROGRAMA DE AUDITORIA</b>							
Nº	Proceso/Area	Mes/Semana					
		MES					
		Días		Días		Días	
1							
2							
3							
4							
5							
6							
Nº de Auditorias							
Total de Auditorias programadas							
<b>III. APROBACION DEL PROGRAMA DE AUDITORIA</b>							
Elaborado por:				Aprobado por:			
Nombres, cargo y firma Fecha: ____/____/____				Nombres, cargo y firma Fecha: ____/____/____			



Título: PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK	Código: RGT-SDI-0001	Versión: 01	Página: <b>11/13</b>
--	-------------------------	----------------	-------------------------

### ANEXO Nº 3



**RIGHTTEK**  
Tecnología Apropiable S.A.

## INFORME DE AUDITORIA INTERNA

Fecha: dd/mm/aaaa

I. DATOS DE LA AUDITORIA INTERNA			
1.1. N° de Auditoria		1.2. Norma de referencia	
1.3. Fecha de Auditoria	Del dd/mm/aaaa al dd/mm/aaaa		
1.4. Lugar de Auditoria			

II. OBJETIVO DE LA AUDITORIA INTERNA

III. ALCANCE DE LA AUDITORIA INTERNA(señalar exclusiones de ser el caso)

IV. EQUIPO AUDITOR	
4.1. Auditor Lider	
4.2. Auditores Internos	
4.3. Auditores en formacion	

V. INVITADOS	
5.1. Expertos Tecnicos	
5.2. Observadores	

VI. RESULTADO DE LA AUDITORIA INTERNA
no conformidades:_____ Observaciones:_____

No Conformidades				
N°	Area/Proceso	Descripcion	norma	Auditor

Observaciones				
N°	Area/Proceso	Descripcion	norma	Auditor

VII. CONCLUSIONES DE LA AUDITORIA INTERNA

RGT-SDI-0004

<b>Título:</b> <b>PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK</b>	<b>Código:</b> <b>RGT-SDI-0001</b>	<b>Versión:</b> <b>01</b>	<b>Página:</b> <b>12/13</b>
---	---------------------------------------	------------------------------	--------------------------------

#### ANEXO Nº 4

PERFIL DEL AUDITOR INTERNO		
<b>Reporta a:</b>	Auditor Líder y/o Representante de la Dirección para el SGC u Oficial de Seguridad de la Información.	
<b>Misión</b>	Realizar auditorías internas al Sistema de Gestión de Seguridad de la Información (SGSI), según corresponda, de acuerdo con los criterios de auditoría establecidos.	
<b>Funciones</b>	<ol style="list-style-type: none"> <li>1. Revisar la documentación del SGSI, elaborar el Plan de Auditoría Interna; y coordinar con Alta Gerencia, según corresponda, y los demás miembros del equipo auditor la ejecución de la auditoría interna, en caso haya sido designado como Auditor Líder.</li> <li>2. Preparar los documentos de trabajo y realizar las entrevistas a los dueños y personal involucrado en los procesos asignados por el Auditor Líder, de acuerdo con el Plan de Auditoría Interna aprobado.</li> <li>3. Clasificar los hallazgos obtenidos en la auditoría interna y elaborar el reporte correspondiente.</li> <li>4. Elaborar en colaboración con los demás miembros del equipo auditor, el informe de auditoría interna correspondiente, en caso haya sido designado como Auditor Líder.</li> <li>5. Realizar (Auditor Líder) o participar (Auditor Interno) en las reuniones de apertura, retroalimentación y cierre de la auditoría interna.</li> </ol>	
<b>Coordinaciones Principales</b>	<b>Internas</b> <ul style="list-style-type: none"> <li>• Dueños y personal de los procesos involucrados en el SGSI, según corresponda.</li> </ul>	
<b>Requisitos Mínimos del Auditor Interno</b>	<b>Educación, Formación y Experiencia</b> <ul style="list-style-type: none"> <li>• Título Profesional Universitario o Grado Académico de Bachiller en Administración, Ingeniería o carreras vinculadas a la actividad o especialidad.</li> <li>• Curso de Auditor Interno para Sistemas de Gestión de Seguridad de la Información - ISO 27001, según corresponda.</li> <li>• Deseable formación como Auditor ISO 27001</li> <li>• Experiencia general mínima de tres (3) años.</li> <li>• Participación en un mínimo de dos (2) auditorías internas al SGSI según corresponda en calidad de auditor líder, auditor interno o auditor interno en entrenamiento, realizadas en los últimos tres (3) años y con una duración total mínima de 8 horas.</li> </ul>	
	<b>Competencias Deseables</b>	
	<b>Específicas</b>	<b>Institucionales</b>
	• Orientación a los resultados	• Excelencia e innovación
	• Atención al detalle	• Integridad y comportamiento ético
	• Organización y planificación	• Respeto y trabajo en equipo
	• Comunicación efectiva	
	• Relaciones interpersonales	

<b>Título:</b> <b>PROCEDIMIENTO PARA AUDITORÍA INTERNA A LOS SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN DE RIGHTTEK</b>	<b>Código:</b> <b>RGT-SDI-0001</b>	<b>Versión:</b> <b>01</b>	<b>Página:</b> <b>13/13</b>
---	---------------------------------------	------------------------------	--------------------------------