FACULTAD DE CIENCIA Y TECNOLOGÍA

ESCUELA DE INGENIERÍA ELECTRÓNICA

Implementación de la norma ISO/IEC 27001 para seguridad del Data Center del GAD Municipal del Cantón Cuenca.

Trabajo de graduación previo a la obtención del título de:

INGENIERA ELECTRÓNICA

Autora:

MABEL CATHERINE OCHOA QUEZADA

Director:

DANIEL ESTEBAN ITURRALDE PIEDRA

CUENCA, ECUADOR

2016

DEDICATORIA

Con mucho amor dedico el presente trabajo a mis padres Jaime y María, por que sus brazos siempre se abrían cuando necesitaba un abrazo, sus corazones comprendían cuando necesitaba un amigo, sus ojos se endurecían cuando me hacía falta una lección y gracias a su fortaleza y amor hoy puedo alcanzar una meta más en mi vida.

A mis hermanos Juan Carlos, Yadira Cecibel y a mi cuñado Alejandro Xavier, que siempre me brindan su apoyo y amor en cada instante de mi vida. Y de manera especial durante todo el trayecto de la realización de este proyecto.

A mis sobrinas Alejandra y Victoria quienes son mi motivación, inspiración y felicidad. Llenando de alegría cada día de mi vida con sus muestras de valentía y cariño.

A mis familiares por sus consejos y apoyo a lo largo de mi vida universitaria.

A mis amigas y amigos, mis hermanos de corazón, por la amistad sincera e incondicional que me han brindado y el constante apoyo en todas las etapas de mi vida.

A mis maestros quienes nunca desistieron al enseñarme y me orientaron para la culminación de mis estudios profesionales.

Mabel Ochoa

AGRADECIMIENTOS

Agradezco primeramente a Dios y a la Virgen del Cisne por todas las bendiciones recibidas, por haberme dado fortaleza para realizar y culminar feliz y satisfactoriamente con un objetivo más de mi vida profesional.

A mis padres y hermanos porque a través de sus sabios consejos y ejemplo me han enseñado a no desfallecer y siempre perseverar.

De igual forma mi agradecimiento imperecedero a la Ing. Ximena Barrera directora del departamento de informática del GAD Municipal del cantón Cuenca, al Ing. Marco Timbi, promotor del proyecto y al personal que labora en esta institución ya que, sin su muestra de confianza, su apoyo y colaboración durante todo el proceso de ejecución de este proyecto no hubiese sido posible cumplir con esta meta.

De manera muy especial quiero agradecer al Mst. Daniel Iturralde, director del proyecto, por su valiosa guía y asesoramiento en la realización del mismo.

Finalmente hago llegar los más sinceros reconocimientos a mis amigos y a todas aquellas personas, que de una u otra manera colaboraron desinteresadamente durante la realización de este trabajo de investigación

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

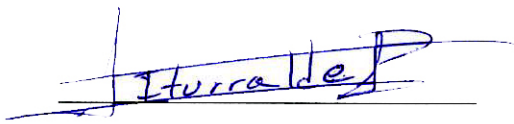
ÍNDICE DE ANEXOS

"IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001 PARA SEGURIDAD DEL DATA CENTER DEL GAD MUNICIPAL DEL CANTÓN CUENCA."

RESUMEN

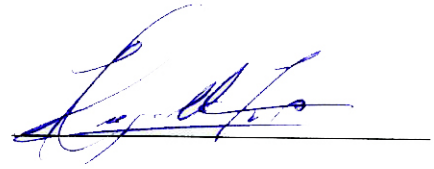
En este trabajo se presenta la implementación de la norma ISO/IEC 27001:2013 en el *Data Center* del GAD Municipal del cantón Cuenca, dicha norma presta un marco para el sistema de gestión de la seguridad de la información útil para implementar mecanismos y procedimientos para salvaguardar los sistemas y la información de las empresas. La metodología se basa en el análisis de la situación actual, la cual muestra deficiencias en la evaluación de las amenazas y vulnerabilidades, luego se identifican y analizan las mismas, se seleccionan los controles y objetivos de control, se fundamenta su uso y por último se presenta una plantilla para el plan de tratamiento de riesgos donde se identifican las acciones apropiadas para minimizar los riesgos.

Palabras claves: Sistema de Gestión de Seguridad de la Información, ISO/IEC 27001:2013.



Daniel Esteban Iturralde Piedra

Director del Trabajo de Titulación



Hugo Marcelo Torres Salamea

Director de Escuela

Mabel Catherine Ochoa Quezada

Autora

IMPLEMENTATION OF ISO / IEC 27001:2013 STANDARD FOR THE SECURITY OF THE MUNICIPAL DATA CENTER OF THE CANTON OF CUENCA

ABSTRACT

This research paper deals with the implementation of the ISO / IEC 27001 2013 standard at the Data Center of the Municipal GAD of the Canton of Cuenca. This standard provides a framework for a useful Information Security Management System in order to implement mechanisms and procedures to safeguard businesses systems and information.

The methodology is based on the analysis of the current situation that shows deficiencies in the assessment of threats and vulnerabilities; which are then identified and analyzed. The controls and control objectives are selected, their use is substantiated; and finally a template for a risk treatment plan which identifies the appropriate actions to minimize the risks, is presented.

Keywords: Information Security Management System, ISO / IEC 27001: 2013.

Daniel Esteban Iturralde Piedra
Thesis Director

Hugo Marcelo Torres Salamea
School Director

Mabel Catherine Ochoa Quezada
Author

UNIVERSIDAD DEL AZUAY
Dpto. Idiomas

Translated by,
Lic. Lourdes Crespo

Ochoa Quezada Mabel Catherine
Trabajo de Titulación
Ing. Daniel Esteban Iturralde Piedra, Mst.
Junio, 2016

IMPLEMENTACIÓN DE LA NORMA ISO/IEC 27001 PARA SEGURIDAD DEL DATA CENTER DEL GAD MUNICIPAL DEL CANTÓN CUENCA.

INTRODUCCIÓN

En la sociedad existe un alto índice de empresas infectadas con *software* malicioso y con presencia de varias vulnerabilidades debido a la falta de atención a los riesgos a los cuales se encuentran expuestos. El GAD Municipal del cantón Cuenca maneja información de alta confidencialidad en su *Data Center*, que se encuentra susceptible a diferentes tipos de ataques por parte de personas externas e internas lo que puede ocasionar fallos en los servicios que brinda y alteraciones en la información, siendo necesario implementar un mecanismo de seguridad de la información que permita aminorar intrusiones graves en la información y la pérdida de datos importantes, garantizando una mayor seguridad en la trasmisión de información.

Por esta razón el siguiente trabajo describe el análisis, desarrollo e implementación de la norma ISO/IEC 27001, que otorga un modelo a seguir para la creación y funcionamiento de un sistema de gestión también destacado como el sistema de gestión de la seguridad de la información (SGSI). para la protección de los activos, datos intelectuales, financieros, de los empleados, o los confiados a ellos por los clientes.

CAPÍTULO 1

GENERALIDADES

1.1. Descripción del problema

La información es un aspecto importante ya que se ha convertido en un recurso económico valioso en las organizaciones, impactando significativamente en la productividad y en la toma de decisiones. Esta se ha transformado en punto clave para el crecimiento, desarrollo o éxito personal, profesional y empresarial, entre mayor sea el conocimiento obtenido por medio de la información mayor será el beneficio alcanzado (Fonseca, 2012).

Dentro de la organización el valor de los datos depende de años de investigación, ideas, creaciones, conceptos y reglamentos, es sustancial identificar la información lucrativa para la organización ya que mucha de esta se obtiene por diferentes medios (Granados, 2015).

Se debe tener presente su importancia, ya que como fuente del conocimiento otorga un bien a quien la posee, en algunas ocasiones puede ser medida imaginariamente, suponiéndose el impacto que tendría al ser expuesta a vulnerabilidades y amenazas. (BVEx España, 2014).

Los ataques, tanto a la información como al uso de recursos que permiten el acceso a ella, es uno de los problemas latentes en las empresas. Entre los principales ataques a los que se encuentran vulnerables tenemos:

- Ataques sobre los servicios generando una negación del servicio, causando la pérdida de la conectividad de la red debido al consumo

del ancho de banda o sobrecarga de los recursos computacionales del sistema de la víctima.

- Ataques sobre la información provocando una revelación de datos, reenvío de datos, manipulación de datos y repudio en envío y/o recepción de datos.

- Ataques a la identidad de las entidades, es decir interceptación de identidades y suplantación de identidad provocando robos, estafas y trayendo consigo graves consecuencias a la entidad como a la persona responsable (Carracedo Gallardo, 2011).

El GAD[1] Municipal del cantón Cuenca maneja información de alta confidencialidad en su *Data Center*, siendo susceptible a diferentes tipos de ataques por parte de personas externas e internas lo que puede ocasionar fallos en los servicios que brinda y alteraciones en los datos.

La ISO[2]/IEC[3] 27001 es una norma internacional emitida por la Organización Internacional de Normalización y describe cómo tratar la seguridad de la información en una empresa.

Además, ISO 27001 es la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento (Kosutic, 2010). La Figura 1.1 muestra el rango en el que se encuentra cada país de acuerdo al número de certificados con los que cuenta.

[1] GAD: Gobiernos Autónomos Descentralizados
[2] ISO: Organización Internacional de Normalización
[3] IEC: Comisión Electrotécnica Internacional

Figura 1.1 Certificados en Latinoamérica

Fuente: (ISO, 2015)

Como se observa en Latinoamérica el rango más alto esta entre 100 y 1000, en la Figura 1.2 y Figura 1.3 se muestra específicamente el número de certificaciones en Ecuador y Perú determinando que existe un bajo índice de empresas que cuentan con una certificación, pero esto irá cambiando con el paso de los años debido a la necesidad que presentan las empresas para garantizar una óptima seguridad a los usuarios. (ISO, 2015)

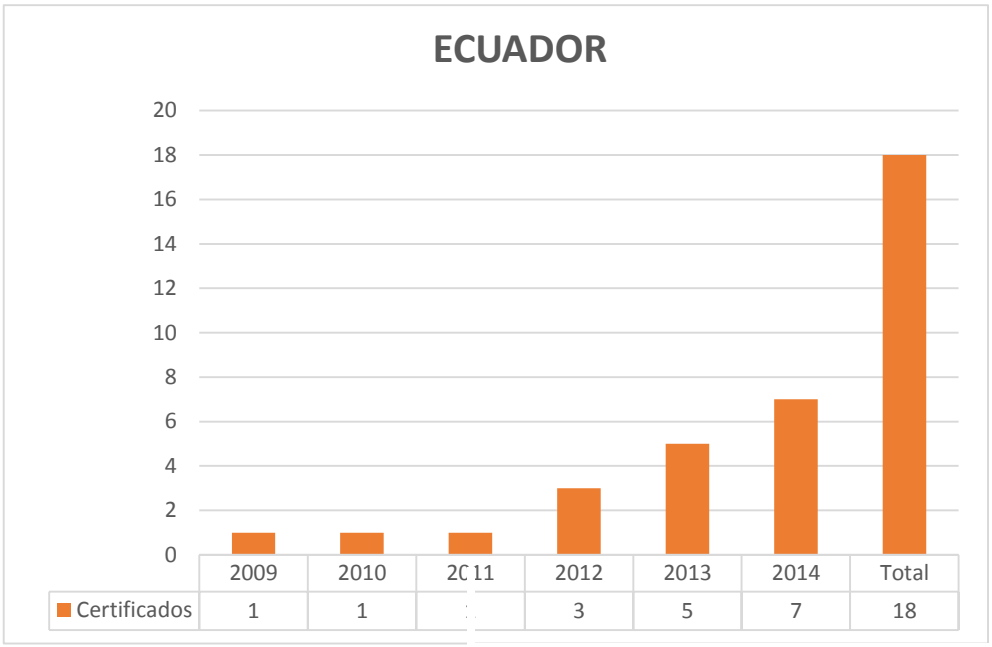


Figura 1.2 Certificados en Ecuador

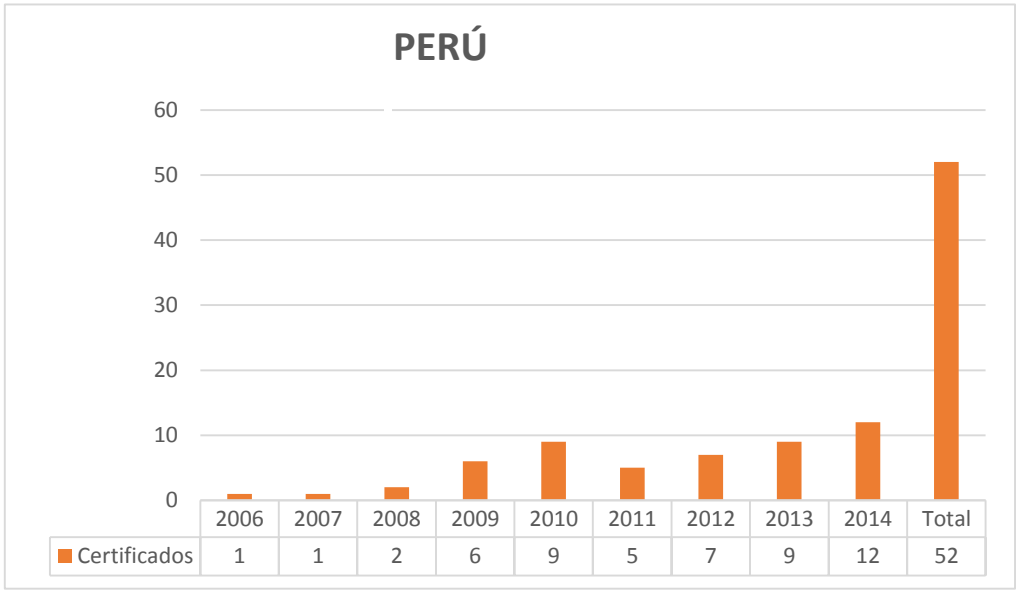


Figura 1.3 Certificados en Perú

A diferencia de Colombia que últimamente ha producido un aumento significativo en el número de certificados obtenidos, como se ve en la Figura 1.4 se tuvo un incremento de 220 certificados en los últimos 3 años. (ISO, 2015)

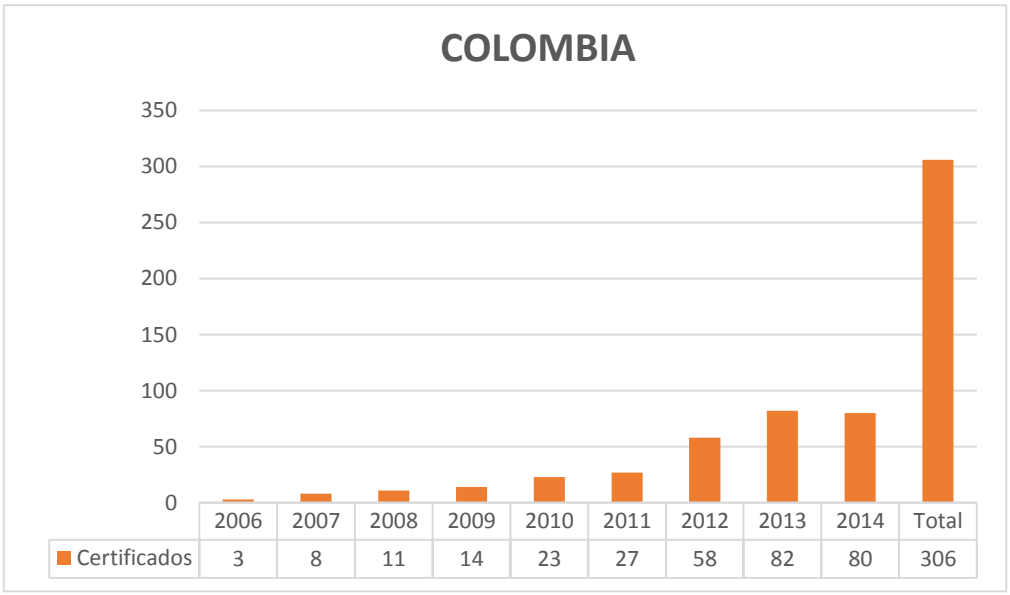


Figura 1.4 Certificados en Colombia

Brasil es uno de los países líderes en certificación a nivel de Latinoamérica, en la Figura 1.5 se puede ver el número de certificados con los que cuenta y el incremento presentado con el paso de los años. (ISO, 2015)

Figura 1.5 Certificados en Brasil

En general, en la sociedad existe un alto índice de empresas infectadas con *software* malicioso y con presencia de varias vulnerabilidades debido a la falta de atención a los riesgos a los cuales se encuentran expuestos.

Durante el 2014, el 70% de las empresas de América Latina presentaron inquietudes para proteger la seguridad informática y enfocar la inversión de recursos, para evitar que estas vulnerabilidades sean blancos de ataques (El Nacional, 2015).

Con el paso del tiempo y el avance de la tecnología en lugar de disminuir los índices de debilidades en los sistemas, está ocurriendo lo opuesto ya que los usuarios no están haciendo uso adecuado de los aplicativos de seguridad (El Nacional, 2015).

Una de las maneras de reducir los riesgos que están afectando a los activos de las empresas es la elaboración de normas, políticas y concientización a los usuarios.

1.2. Alcances y limitaciones

Implementar un Sistema de Gestión de Seguridad de la Información que contenga los mecanismos óptimos de seguridad para el *Data Center* del GAD Municipal del cantón Cuenca basados en la norma ISO/IEC 27001, permitiendo de este modo mejorar la seguridad en la trasmisión y el acceso a los mismos, respaldando la información manejada y la identidad de la persona que la maneja.

El presente proyecto comprende específicamente los mecanismos, políticas y concientización a los usuarios para la seguridad del *Data Center* del área de redes, infraestructura y telecomunicaciones del GAD Municipal.

1.3. Hipótesis

El no tener implementadas normas internacionales de seguridad de la información en el *Data Center* del GAD Municipal, podrá generar riesgos para la información.

La falta de normas de seguridad en el *Data Center* del área de redes, infraestructura y telecomunicaciones trae como resultado pérdida o alteraciones a la información que es el principal activo de una empresa.

Controlar el cumplimiento de las políticas de Seguridad de la Información garantizará una mayor seguridad para la protección de la información en el *Data Center* del GAD Municipal.

1.4. Metodología utilizada

El proyecto se va a alinear y manejar en base a la norma ISO/IEC 27001 a través del método científico, permitiendo conocer más a fondo cómo funciona, los beneficios que brinda, como implementarla y la documentación obligatoria.

Para determinar la situación actual del Data Center del GAD Municipal se desarrollará una investigación formativa, permitiendo conocer los recursos que se encuentran disponibles, que intervenciones se están implementando actualmente y quien lo está haciendo.

La parte de implementación de los mecanismos de seguridad basados en la norma ISO/IEC 27001 se realizará utilizando el método deductivo ya que la norma plantea una guía de controles de seguridad para ser aplicada, teniendo en cuenta las necesidades que presenta el GAD Municipal.

Así mismo se realizará una investigación bibliográfica y deductiva para establecer los mecanismos que de acuerdo a lo investigado se adapten mejor a las necesidades particulares de la empresa y así determinar las políticas precisas de seguridad.

1.5. Organización del trabajo

En el capítulo 2 se establecerán conceptos teóricos necesarios para el entendimiento de la norma, se realizará una recopilación sobre las normas relacionadas explicando los conceptos básicos, como funciona, beneficios, como implementarla y la documentación relacionada.

Luego en el capítulo 3 se hablará de la situación actual del *Data Center* del GAD se establecerá las vulnerabilidades presentes en base a la norma ISO/IEC 27001, los servicios que brinda, tipo de comunicación que maneja y la documentación con la que cuenta.

A continuación, en el capítulo 4 se explicarán los procedimientos necesarios para la implementación de la norma ISO/IEC 27001 se identificarán los mecanismos de seguridad necesarios para disminuir las vulnerabilidades presentes en el *Data Center*, además se establecerán los resultados obtenidos en el presente trabajo.

Por último, se muestran las conclusiones a las que se llegó luego de realizado el trabajo las cuales ayudaran a entender de mejor manera el proyecto elaborado y los beneficios que otorga.

CAPÍTULO 2

MARCO TEÓRICO

En el capítulo 2 se especifica las normas afines, detallando como se relacionan y la documentación acorde, además se establecen conceptos teóricos necesarios para el entendimiento de la norma ISO/IEC 27001, las partes que la forman, los requerimientos que contiene y la correcta interpretación de sus anexos.

2.1. ISO/IEC 2700:2014

ISO/IEC 27000 es un conjunto de estándares desarrollados por ISO e IEC que prestan un marco de gestión de la seguridad de la información útil para cualquier tipo de organización.

Otorga un modelo a seguir para la creación y funcionamiento de un sistema de gestión también destacado como el sistema de gestión de la seguridad de la información (SGSI) las organizaciones pueden desarrollar e implementar un marco para la gestión de la seguridad de sus activos encerrando sus datos: intelectuales, financieros, de los empleados, o los confiados a ellos por los clientes. Básicamente un sistema de gestión exige que cada organización lleve a cabo cuatro grandes actividades como se muestra en la Figura 2.1.

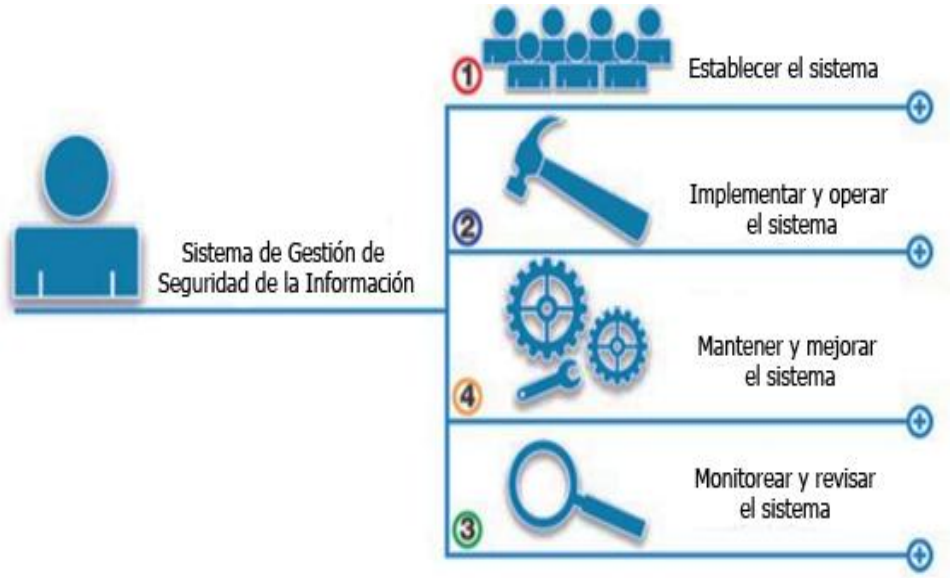


Figura 2.1 Actividades de un sistema de gestión de la seguridad de la información

Fuente: (Juárez, 2011**)**

A continuación, se presenta un resumen de las principales secciones que se establecen en la norma ISO/IEC 27000.

2.1.1. Términos y definiciones

La ISO/IEC 27000 presenta los términos y definiciones más significativos de la familia de normas del SGSI, a continuación, se detallan los más importantes para tener una correcta interpretación de la norma ISO/IEC 27001 (International Organization for Standardization, 2014).

Auditoría

Proceso sistemático, independiente y documentado para obtener evidencia de auditoría y evaluar de manera objetiva el grado en que se cumplen los criterios de auditoría.

Disponibilidad

Propiedad de ser accesibles y utilizables a la demanda por una entidad autorizada.

Competencia

Capacidad de aplicar los conocimientos y habilidades para alcanzar los resultados previstos.

Confidencialidad

Propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos.

Conformidad

Cumplimiento de un requisito.

Mejora continua

Actividad recurrente para mejorar el rendimiento.

Control

Medir el riesgo de modificación.

Corrección

Acción para eliminar una inconformidad detectada.

Acción correctiva

Acción para eliminar la causa de una inconformidad y prevenir la recurrencia.

Información documentada

Información requerida para ser controlado y mantenido en una organización y el medio que la contiene

Efectividad

Grado en que las actividades planificadas se realizan y alcanzan los resultados planificados.

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información.

Integridad

Propiedad de estar completo y exacto.

Parte interesada

Persona u organización que puede afectar, verse afectada, o descubrir que a sí mismos podrían verse afectados por una decisión o actividad.

Sistema de gestión

Conjunto de elementos interrelacionados o que interactúan en una organización para establecer políticas, objetivos y procesos para alcanzar dichos objetivos.

Medición

Proceso para determinar un valor.

Monitoreo

Determinar el estado de un sistema, un proceso o una actividad

Inconformidad

Incumplimiento de un requisito.

Objetivo

Resultado que debe conseguirse.

Organización

Persona o grupo de personas que tiene sus propias funciones con responsabilidades, autoridades y relaciones para alcanzar sus objetivos.

Externalizar (verbo)

Hacer un arreglo donde una organización externa realiza parte de la función o proceso en una organización.

Rendimiento

Es el resultado medible

Política

Ideas e instrucciones de una organización expresadas formalmente por la gerencia.

Proceso

Conjunto de actividades relacionadas mutuamente o que interactúan, las cuales transforman elementos de entrada en resultados.

Requisito

Necesidad o expectativa establecida, generalmente implícita u obligatoria

Opinión

Actividad emprendida para asegurar la conveniencia, adecuación y efectividad de la materia para alcanzar los objetivos establecidos

Riesgo

Efecto de la incertidumbre en los objetivos.

Dueño del riesgo

Persona o entidad con la responsabilidad y la autoridad para administrar el riesgo.

Gerencia

Persona o grupo de personas que dirige y controla una organización el más alto nivel

2.1.2. Sistema de Gestión de Seguridad de la Información

Un Sistema de Gestión de Seguridad de la Información (SGSI) se fundamenta en las políticas, procedimientos, directrices, recursos y actividades gestionadas por una organización para la protección de la información. (International Organization for Standardization, 2014)

Las empresas buscan alternativas para que la información sea actualizada, relevante, oportuna, confiable y explicable garantizando mayor confidencialidad, resguardo y

proporcionando mayor seguridad en el momento que lo requiera tomando en cuenta el creciente ambiente interconectado de negocios. (El Informador, 2015)

La seguridad informática ha tomado gran apogeo debido a la evolución de la tecnología, la capacidad de interconectarse a través de redes ha conseguido nuevos horizontes a las empresas para mejorar su productividad y ha traído consigo grandes preocupaciones a los profesionales en la seguridad del entorno informático.

Esta preocupación debe ser entendida e intervenida por los directivos, considerando a las inversiones en medidas de seguridad informática como un gasto inevitable, que apoya a mantener la operatividad y rentabilidad de la organización. Actualmente, parte del presupuesto de las inversiones en seguridad que realizan las empresas se está destinando a la gestión de la seguridad de la información.

El concepto de seguridad se ha modificado, el de seguridad gestionada ha suplantado al de seguridad informática, y las medidas de seguridad van entorno al concepto de gestión de la seguridad de la información (Gobierno Autonomo Descentralizado Municipal del Canton Portoviejo, 2014).

La seguridad absoluta no existe, la gestión de la seguridad de la información se basa en el planteamiento coherente de directrices, procedimientos y criterios que aseguran la evolución eficiente de la seguridad de los sistemas de información (Degerencia, 2015).

En la Figura 2.2 se describen los principios que contribuyen a la implementación de un SGSI (International Organization for Standardization, 2014)

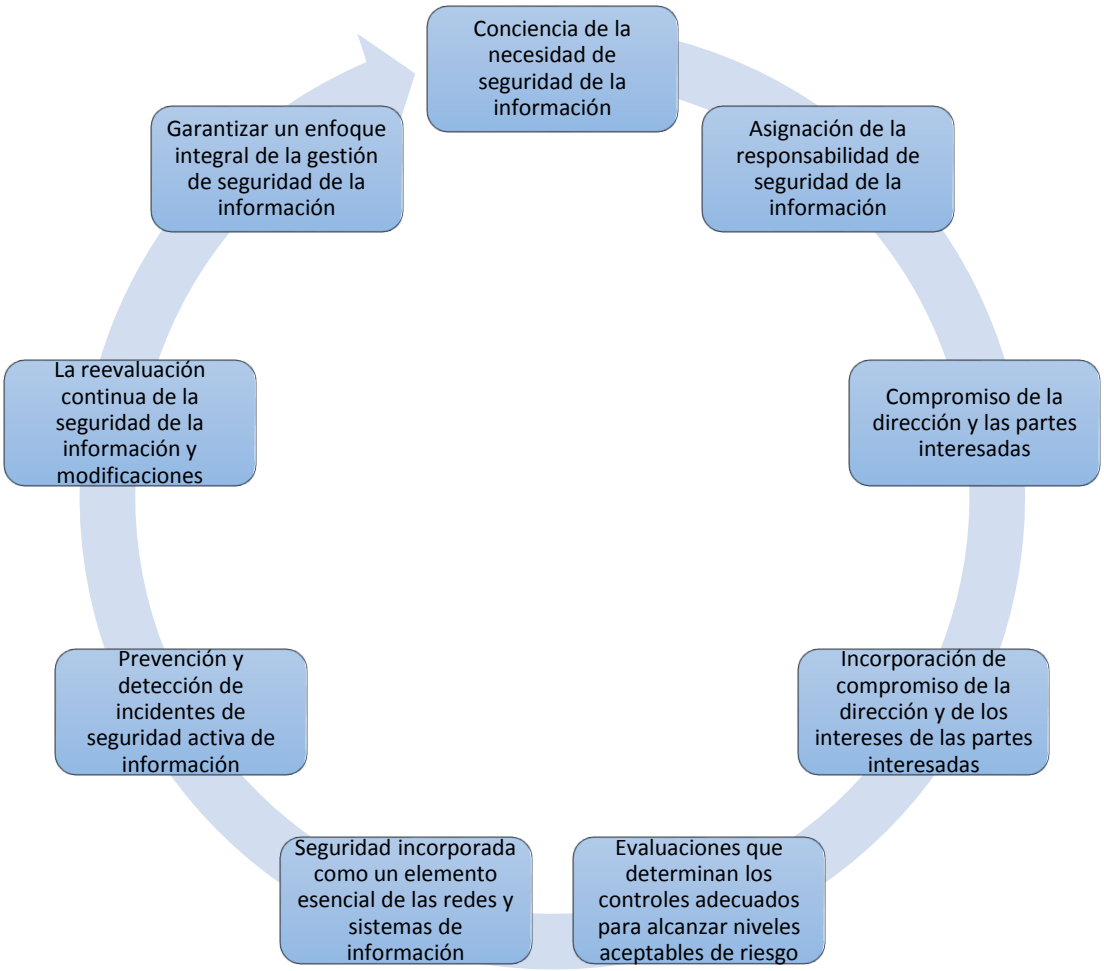


Figura 2.2 Principios para la implementación de un SGSI

2.1.3. Familia de normas del SGSI

La familia de normas del SGSI consta de las siguientes normas interrelacionadas, ya publicadas o bajo desarrollo, que contienen un número de componentes estructurales significativos:

ISO / IEC 27000, Sistemas de gestión de seguridad de la información- Visión general y vocabulario

Contiene términos y definiciones que se emplean en toda la serie 27000, establece un vocabulario claramente definido para evitar distintas interpretaciones de conceptos técnicos y de gestión (López E. L., s.f.).

ISO / IEC 27001, Sistemas de Gestión de Seguridad de la Información-Requisitos

ISO / IEC 27002, Código de buenas Prácticas para la Gestión de Seguridad de la Información

Aporta pautas para la implementación de los controles, anteriormente conocida como ISO/IEC 17799, facilita información sobre cómo implementar los 114 controles establecidos en la norma ISO 27001 (AMAYA, 2013) (Kosutic, 2010).

ISO / IEC 27003, Directrices para la Implementación del Sistema de Gestión de Seguridad de la Información

Establece una guía para la implantación de un Sistema de Gestión de Seguridad de la Información. Se enfoca en los aspectos requeridos para un diseño exitoso y una buena implementación del SGSI desde su inicio hasta la elaboración de los planes del proyecto de ejecución, que incluye las actividades de elaboración y organización antes de la implementación real (ISOTools Excellence, 2014).

ISO / IEC 27004, Gestión de la Seguridad de la Información – Medición

Proporciona normas para la medir, informar y mejorar la eficacia del sistema de seguridad de la información ya que explica cómo determinar si el SGSI ha alcanzado los objetivos en la política, información, procesos de controles y procedimientos para apoyar el proceso de revisión (ISO 27K, s.f.).

ISO / IEC 27005, Gestión del Riesgo de Seguridad de la Información

Surgió de la norma británica BS 7799-3 y brinda más información sobre cómo llevar a cabo la evaluación y el tratamiento de riesgos, está diseñado para ayudar a la implementación de un sistema de seguridad de la información basado en la gestión del riesgo. (Ildapena, 2008).

ISO / IEC 27006, Requisitos para los Organismos que realizan Auditorías y Certificaciones de Sistemas de Gestión de Seguridad de la Información

ISO / IEC 27007, Directrices para Auditar Sistemas de Gestión de Seguridad de la Información.

ISO / IEC TR 27008, Directrices para los Auditores sobre Controles de Seguridad de la información.

ISO / IEC 27010, Gestión de Seguridad de la Información para Comunicaciones inter-sectorial e inter-organizacional.

ISO / IEC 27011 Directrices de Gestión de Seguridad de la Información para las Organizaciones de Telecomunicaciones - basado en la norma ISO / IEC 27002.

ISO / IEC 27013, Guía para la Implementación de la norma ISO / IEC 27001 e ISO / IEC 20000-1

ISO / IEC 27014, Guía de Gobierno Corporativo de la Seguridad de la Información.

ISO / IEC TR 27015, Directrices de Gestión de Seguridad de la Información para Servicios Financieros.

ISO / IEC TR 27016, Gestión de la Seguridad de la Información - Economía Organizacional.

ISO 27799: 2008, Informática de la Salud- Gestión de Seguridad de la Información de la Salud utilizando ISO / IEC 27002

Estas normas permiten definir los requisitos para un SGSI, para aquellos que acrediten dichos sistemas proporcionar apoyo directo, orientación y / o interpretación detallada para el proceso general para establecer, implementar, mantener y mejorar un SGSI, directrices específicas para el sector en el que se desarrolla el SGSI y la evaluación de conformidad para la dirección del SGSI. La Figura 2.3 muestra un resumen de las relaciones que existen entre la familia de normas de Sistema de Gestión de Seguridad de la Información. (International Organization for Standardization, 2014)

Vocabulario	27000 Visión general y vocabulario
Normas de Requerimientos	27001 Requisitos
	27006 Requisitos para los Organismos que Realizan Auditorías y Certificaciones
Normas de Orientación	27002 Código de Buenas Prácticas
	27003 Directrices para la Implementación
	27004 Medición
	27005 Gestión del Riesgo
	27007 Directrices para Auditar Sistemas
	27008 Directrices para los Auditores sobre Controles
	27013 Guía para la Implementación de la norma ISO / IEC 27001
	27014 Guía de Gobierno Corporativo
	27016 Gestión de la Seguridad de la Información - Economía Organizacional
Normas de Orientación a sectores específicos.	27010 Gestión de Seguridad de la Información para Comunicaciones inter-sectorial e inter-organizacional.
	27011 Directrices de Gestión de Seguridad de la Información para las Organizaciones de Telecomunicaciones - basado en la norma ISO / IEC 27002.
	TR 27015 Directrices de Gestión de Seguridad de la Información para Servicios Financieros
	TS 27017 Orientacion de controles de seguridad para servicios de computacion en la nube basados en ISO / IEC 27002.
Normas de Orientación a controles específicos.	2703x
	2704x

Figura 2.3 Relaciones entre la familia de normas de SGSI

Además, la norma ISO / IEC 27000 consta de dos anexos informativos:

2.1.4. Anexo A: Formas verbales para la expresión de las disposiciones

Este Anexo A muestra como debe ser interpretado un documento de la familia SGSI en términos de sus expresiones verbales ya que el usuario debe ser capaz de identificar los requisitos que se deben cumplir de las recomendaciones donde existe elección, en la Tabla 2.1 se da una explicación de cómo debe ser entendido cada término.

Tabla 2.1 Indicación y explicación de términos

Indicación	**Explicación**
Requisito	los términos " deberá " y " no deberán " indica los requisitos estrictamente a seguir afín de ajustarse al documento y de los que no se permite ninguna desviación.
Recomendación	los términos " debe " y " no deben " indica que entre varias posibilidades una está recomendada como adecuada, sin mencionar ni excluir otras, o que se prefiere un determinado curso de acción, pero que no necesariamente se requiere, o que una cierta posibilidad o curso de acción está en desuso, pero no prohibido.
Permiso	el término "podrá" y " no necesita " indica un curso de acción permisible dentro los límites del documento
Posibilidad	el término " puede" y " no puede" indica una posibilidad de que algo ocurra

Fuente: (International Organization for Standardization, 2014)

2.1.5. Anexo B: Términos y propiedades de los términos

En el Anexo B se encuentra una clasificación de los términos empleados en cada una de las normas de la familia del Sistema de Gestión de Seguridad de la Información para lograr una correcta interpretación.

2.2. ISO/IEC 27001:2013

ISO/IEC 27001 ha sido preparada para proporcionar los requisitos para establecer, implementar, mantener y mejorar de manera continua un sistema de gestión de la seguridad de la información conservando confidencialidad, integridad y disponibilidad, teniendo presente que debe ser parte y estar integrado a los procesos de la organización y a la estructura de gestión general.

Sin un adecuado control que integre los esfuerzos y conocimiento humano con las técnicas depuradas de mecanismos automatizados, la gestión de seguridad puede tornarse compleja y difícil de realizar por razones organizativas.

2.2.1. Aspectos Básicos

Este estándar promueve que los usuarios resalten la importancia de entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad, implementar y operar controles para manejar los riesgos de la seguridad de los datos, monitorear y revisar el desempeño y la efectividad del SGSI y mejoramiento continuo en base a la medición del objetivo (Kosutic, 2010).

Además, especifica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o parte de ella.

ISO 27001 puede ser implementada en cualquier tipo de organización, fue elaborada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad permitiendo su certificación (Kosutic, 2010).

2.2.2. Funcionamiento de la norma

La norma ISO 27001 consiste en investigar los problemas que podrían alterar la información para luego establecer lo necesario para evitarlos.

En la Figura 2.4 se observa la filosofía principal de la norma que se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente (Kosutic, 2010). (International Organization for Standardization, 2013)

Figura 2.4 Estructura de ISO 27001

2.2.3. Beneficios de la norma

Las principales ventajas comerciales que ofrece la norma ISO 27001 para una empresa son:

- Efectuar los requerimientos legales
- Conseguir una ventaja comercial
- Bajos costos
- Superior organización

2.2.4. Características de la norma

ISO/IEC 27001 se divide en 11 secciones más el Anexo A; las secciones 0 a 3 son introductorias, mientras que las secciones 4 a 10 son obligatorias. Una organización debe implementar todos sus requerimientos para cumplir con la norma (Neira, 2005).

Los controles del Anexo A deben implementarse sólo si recaen en la declaración de aplicabilidad, conforme se indica en el Anexo 12. (International Organization for Standardization, 2013).En la Figura 2.5 se describe cada una de las secciones de la norma ISO/IEC 27001.

Figura 2.5 Secciones de la norma ISO/IEC 27001

2.2.5. Certificación de la norma

Para obtener la certificación de la norma ISO 27001 en una empresa, se deben seguir varios pasos:

- Obtener el apoyo de la dirección
- Utilizar una metodología para gestión de proyectos
- Definir el alcance del SGSI
- Redactar una política de alto nivel sobre seguridad de la información
- Definir la metodología de evaluación de riesgos
- Realizar la evaluación y el tratamiento de riesgos
- Redactar la Declaración de aplicabilidad
- Redactar el Plan de tratamiento de riesgos
- Definir la forma de medir la efectividad de sus controles y de su SGSI
- Implementar todos los controles y procedimientos necesarios
- Implementar programas de capacitación y concienciación
- Realizar todas las operaciones diarias establecidas en la documentación de su SGSI
- Monitorear y medir su SGSI
- Realizar la auditoría interna
- Realizar la revisión por parte de la dirección
- Implementar medidas correctivas (Kosutic, 2010)

2.2.6. Documentación obligatoria

ISO 27001 requiere que se elabore la siguiente documentación:

- Alcance del SGSI
- Política de seguridad de la información
- Metodología de evaluación y tratamiento de riesgos
- Declaración de aplicabilidad
- Plan de tratamiento de riesgos
- Informe de evaluación de riesgos
- Definición de roles y responsabilidades de seguridad
- Inventario de activos
- Uso aceptable de los activos
- Política de control de acceso
- Procedimientos operativos para gestión de TI
- Principios de ingeniería para sistema seguro
- Política de seguridad para proveedores
- Procedimiento para gestión de incidentes
- Procedimientos para continuidad del negocio
- Requisitos legales, normativos y contractuales

Los registros obligatorios son:

- Registros de capacitación, habilidades, experiencia y calificaciones
- Monitoreo y resultados de medición

- Programa de auditoría interna
- Resultados de auditorías internas
- Resultados de la revisión por parte de la dirección
- Resultados de medidas correctivas
- Registros sobre actividades de los usuarios, excepciones y eventos de seguridad (Neira, 2005).

CAPÍTULO 3

SITUACIÓN ACTUAL DEL ÁREA DE REDES, INFRAESTRUCTURA Y TELECOMUNICACIONES DEL GAD MUNICIPAL DEL CANTÓN CUENCA

En el presente capítulo se hablará de la situación actual del área de redes, infraestructura y telecomunicaciones del GAD, se determinará la seguridad con la que cuenta en los distintos ámbitos a través de un análisis basado en los controles del Anexo A de la norma ISO/IEC 27001:2013, el cual permitirá definir y determinar el punto de partida para la implementación del Sistema de Gestión de Seguridad.

El Anexo A de la norma, contiene una completa lista de los objetivos y controles que permiten identificar aquellos que son necesarios para implementar el tratamiento de riesgos, en el Anexo 2 se describe cada uno de ellos.

La información de la situación actual se detalla en los puntos posteriores del capítulo y es resultado de los datos recogidos en colaboración de los administradores del área a través de entrevistas realizadas en base al formulario que se observa en el Anexo 3 y Anexo 4 y la revisión de las instalaciones físicas. Se detallará los procesos que actualmente se manejan en el área mas no, todos los procesos del Anexo A de la norma.

Por motivos de privacidad de la empresa se muestra el formulario a llenarse y no el resultado final del proceso.

3.1. Ubicación física del área de redes, infraestructura y telecomunicaciones del GAD Municipal del cantón Cuenca

El área de redes, infraestructura y telecomunicaciones opera en el cuarto piso del Edificio de la Alcaldía de Cuenca, ubicado en las calles Bolívar 7-67 y Borrero. El edificio posee seis pisos, distribuidos en distintas áreas. Con respecto a la disposición física de los servidores estos se encuentran ubicados en el cuarto piso del edificio, en el Departamento de Informática.

3.2. Unidades Organizativas

En la Figura 3.1 se observa la organización presente en el área de redes, infraestructura y telecomunicaciones del GAD Municipal de Cuenca, está conformada por la Dirección del departamento de informática, el jefe informático, el personal del área y tercerizados.

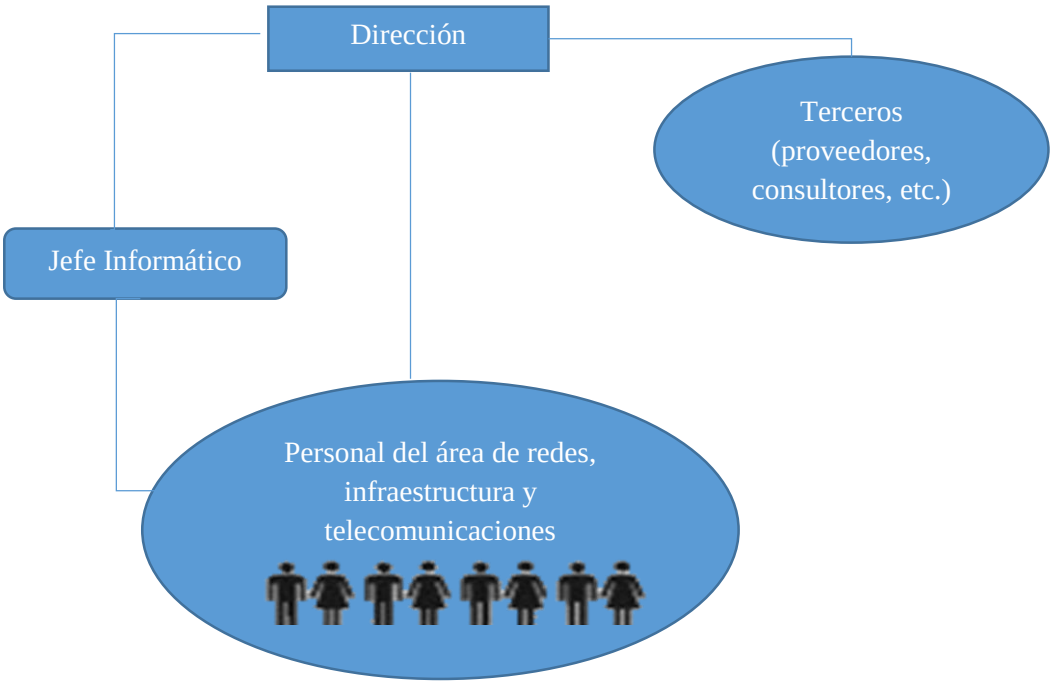


Figura 3.1 Organización del área de redes infraestructura y telecomunicaciones

3.3. Estructura de la red LAN

La red LAN del área de redes, infraestructura y telecomunicaciones, Figura 3.2, cuenta con servidores distribuidos en dos Blade Center IBM, los servidores se encuentran sobre una plataforma de virtualización VMWARE y Power VIOS de IBM para el caso de los servidores de Base de Datos Oracle, y 7 estaciones de trabajo.

El cuarto de servidores cuenta con:

- Chasis Flex System
- 3 Servidores IBM Flex System x240
- 2 Servidores IBM Flex P260
- Chasis IBM H
- 6 Servidores HS23
- 12 switches
- 1 storage IBM Storwize V3700
- 1 Storage IBM DS4700
- Firewall CheckPoint
- Cableado estructurado
- Puesta a Tierra
- Generador Eléctrico
- Aire Acondicionado
- Sensor de Temperatura
- Control de Acceso

La velocidad de transmisión en los servidores es de 10 Gigabits por segundo y la velocidad de acceso a la red es de 1 Gigabit por segundo.

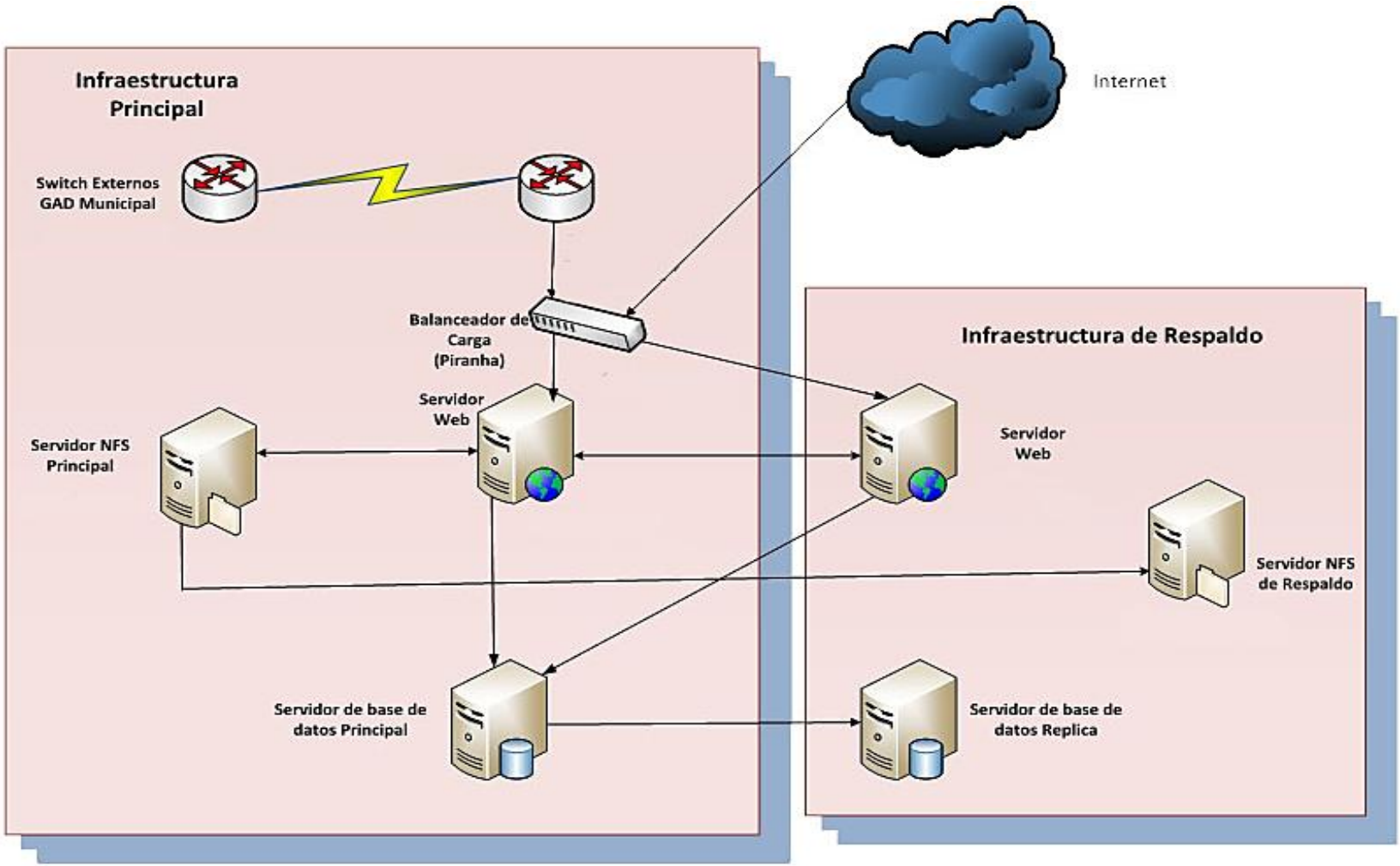


Figura 3.2 Red LAN

Fuente: (Anexo 2)

3.4. Estaciones de tratabajo

Las 7 estaciones de trabajo tienen Windows como sistema operativo, el antivirus Karpesky, Microsoft Office, Netscape para el sistema financiero y como navegador Web utilizan Mozilla Firefox. Además, se encuentra conectada 1 impresora para esta área.

3.5. Documentación

En el área de redes, infraestructura y telecomunicaciones existe documentación sobre:

- Normativa
- Diagramas de red
- Inventario de switches
- Inventario de servidores
- Inventario de impresoras
- IP de las máquinas
- Infraestructura

No hay backups de ninguno de estos datos, ya que son documentos impresos que se van modificando manualmente.

3.6. Seguridad de la información implementada actualmente

Para proporcionar una visión de la situación actual de la seguridad en el área de redes, infraestructura y telecomunicaciones, se realizó un estudio para determinar el grado de seguridad y saber cómo la empresa ha venido protegiendo las ventajas competitivas.

3.6.1. Políticas de seguridad

No se encuentran establecidas normas o procedimientos de seguridad, actualmente las políticas están en trámites de aprobación, los responsables son la directora y el jefe informático. La comunicación de las políticas, normas y procedimientos es por medio telefónico o correo.

Responsabilidad de la seguridad

No hay un encargado específico para la seguridad, existe un responsable general del área.

3.6.2. Administración de activos

Clasificación de datos y hardware: los equipos de la empresa son manejados por una empresa externa la misma que cuenta con un inventario actualizado de los equipos.

Rótulos: el inventario detallado de las características de los equipos de computación con su respectivo rotulo de inventario es manejado por una empresa externa.

Instaladores

Los instaladores de las aplicaciones utilizadas en la empresa se encuentran almacenados de forma digital en un computador.

Licencias

Actualmente cuentan con licencias de Microsoft Office, Server, Windows, Karpesky, Autodesk, InterPro, Firmware, Check Point, Cisco, Vidyo, Oracle.

Cada usuario es responsable de su activo, pero el departamento de activos fijos manejado a nivel del municipio es el responsable de todos los activos, al inventario de estos tienen acceso únicamente los encargados del sistema de gestión financiera.

A nivel del área de informática la encargada de los procesos de los activos es una empresa externa.

3.6.3. Control de accesos

La directora es la persona encargada de autorizar el acceso solicitado de acuerdo a la necesidad de cada funcionario, este procedimiento se lo realiza a través de un formulario.

El registro y cancelación de usuario es operado a través de Talento Humano.

Contraseñas

Las contraseñas son manejadas por el área de soporte ellos son los encargados de crear la cuenta al usuario y asignar una contraseña genérica, la cual debe ser cambiada por cada uno.

3.6.4. Seguridad física y del ambiente

Control de acceso físico al área

En el departamento de Informática existe un perímetro de seguridad física, cada una de las áreas se encuentra separada por una puerta, el acceso al Data Center es a través de una puerta con detección de huella, cuenta con un letrero de señalización de área restringida, además posee un botón de emergencia y uno de alarma contra incendios. Solo el personal de infraestructura tiene permitido el acceso.

Control de acceso a los equipos

El control de acceso a los equipos es responsabilidad exclusiva de cada funcionario.

Dispositivos de Soporte

En el departamento de informática disponen de los siguientes dispositivos para soporte:

- Aire acondicionado: en el Data Center la temperatura se mantiene entre 19ºC y 20ºC solo para esta área, con el fin de mantener esta temperatura todos los días y garantizar la vida de los equipos.

- UPS (Uninterruptible Power Supply): existe un UPS para el Data Center que puede mantener los servidores funcionando por aproximadamente media hora.

- Descarga a tierra: Existe una conexión a tierra propia para el Data Center y otra para el área.

Cableado Estructurado

La instalación del cableado estructurado fue realizada por una empresa externa, resguardo todas las medidas de seguridad necesarias.

Mantenimiento

Solicitud de mantenimiento: cada vez que los usuarios necesitan asesoramiento o servicios del área de informática, se comunican telefónicamente o a través de correos electrónicos con el encargado explicando su situación. Cada requerimiento no se registra en un documento.

Mantenimiento preventivo: Se tiene contratado un servicio de mantenimiento de hardware con una empresa externa, este mantenimiento se realiza cada 3 meses.

3.6.5. Seguridad de las Operaciones

Antivirus

Se adquirió las licencias del antivirus Karpesky, por medio de este se tiene protegido al Servidor y al número de dispositivos finales indicados.

Backup

Backups de datos en los servidores: el backup es realizado a través de VDP (vSphere Data Protection). Cuando se hace un cambio en la configuración del servidor se realizan dos tipos de respaldos, de forma diaria y semanal, dependiendo el servidor al que se le realizó el cambio. Los cambios que se realizan se documentan para datos internos del personal de infraestructura. El procedimiento para la recuperación de los backups es a través del manual técnico de la herramienta.

Backups de datos en las PC's: Los usuarios deben realizar sus propios backups de los datos almacenados en sus máquinas, ya que estos datos son propiedad de cada funcionario. Si realizan un backup deberían hacerlo en sus propias máquinas o en discos de almacenamiento.

Backups en Base de datos: se utiliza Oracle Secure Backup que es una herramienta propia de Oracle.

Eventos

Existe un servidor de logs para los switches y cada servidor tiene su manejador de logs propio del sistema operativo.

Software

La instalación de software se la realiza a través de un formulario de requerimiento.

3.6.6. Seguridad de las Comunicaciones

Correo Electrónico

El correo electrónico en el área de redes, infraestructura y telecomunicaciones es manejado a nivel externo por otra empresa de la ciudad.

Ataques de red

Para prevenir los ataques de red se tienen herramientas de firewall y Check Point que pretende detectar y prevenir la transmisión no autorizada de información confidencial dentro de la organización de una forma eficaz y sin ralentizar las comunicaciones.

3.6.7. Adquisición desarrollo y mantenimiento del sistema

Seguridad de Base de Datos

En la empresa se utiliza Oracle Data Base para el almacenamiento y la administración de los datos, manejando las seguridades propias de la OracleDataBase.

Existe un DBA (administrador de bases de datos) encargado de todos los aspectos técnicos, tecnológicos, legales de la base de datos, él es el responsable de la integridad y disponibilidad de los datos.

Control de Aplicaciones

Actualmente ningún usuario puede instalar aplicaciones en sus equipos, en caso de querer instalar una nueva aplicación se debe dar a conocer la necesidad de la misma al área de Soporte realizando una solicitud con un formato preestablecido justificando la instalación respectiva.

Transacciones en línea

La seguridad para las transacciones en línea se encuentra manejada a través del Firewall Perimetral y el empleo de usuarios y contraseñas, dependiendo el nivel con el que cuenta cada usuario.

3.6.8. Relaciones con el proveedor

Dentro de los contratos establecidos del estado con empresas privadas existen cláusulas de confidencialidad, el encargado de supervisar los servicios del proveedor es el administrador del contrato.

3.6.9. Gestión de incidentes de seguridad de la información

Para el intercambio de información se realizan distintos convenios dependiendo si la empresa es pública o privada. Los eventos de seguridad de la información son comunicados por correo y por el protocolo SNMP (*Simple Network Management Protocol*).

3.6.10. Continuidad del negocio

El área cuenta con alta disponibilidad de Hardware por medio de un servidor principal y un alterno, alta disponibilidad de energía a través del generador.

3.7. Índice actual de debilidades

Luego de efectuado el autodiagnóstico, Anexo 3, se asignó el valor de cero para cada falso y uno para cada verdadero, pudiendo tener un total de 124 verdaderos. El área de redes, infraestructura y telecomunicaciones obtuvo 45 verdaderos determinando un índice general de debilidades del 64%, Figura 3.3, de acuerdo a lo que establece la norma ISO/IEC 27001:2013.

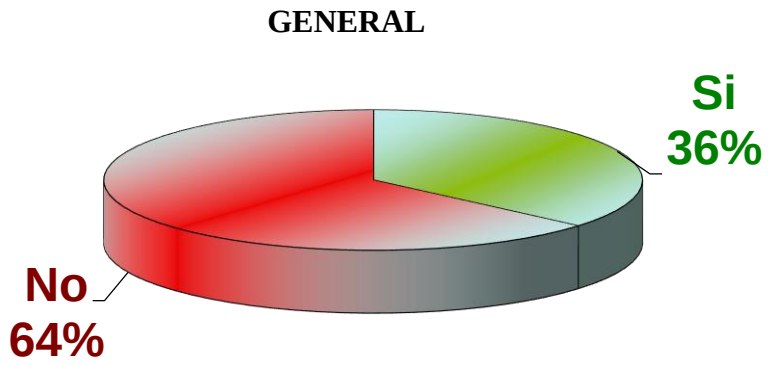


Figura 3.3 Porcentaje general de debilidades

El porcentaje de debilidades existente en cada uno de los dominios que presenta la norma permite identificar los puntos más frágiles en cuanto a seguridad en el área de redes, infraestructura y telecomunicaciones.

Los dominios analizados fueron:

Políticas de seguridad (Figura 3.4)

Organización de la seguridad (Figura 3.5)

Seguridad en RRHH (Figura 3.6)

Administración de activos (Figura 3.7)

Control de acceso (Figura 3.8)

Criptografía (Figura 3.9)

Seguridad física y del ambiente (Figura 3.10)

Seguridad de las operaciones (Figura 3.11)

Seguridad de las comunicaciones (Figura 3.12)

Adquisición, desarrollo y mantenimiento del sistema (Figura 3.3)

Relaciones con el proveedor (Figura 3.14)

Gestión de incidentes de seguridad (Figura 3.15)

Gestión de la continuidad del negocio (Figura 3.16)

Cumplimiento (Figura 3.17)

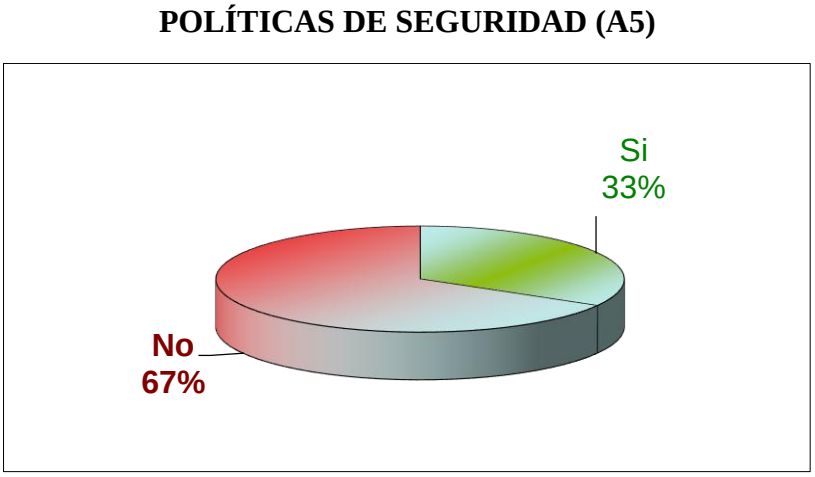


Figura 3.4 Porcentaje de controles para la política de seguridad

ORGANIZACIÓN DE LA SEGURIDAD (A6)

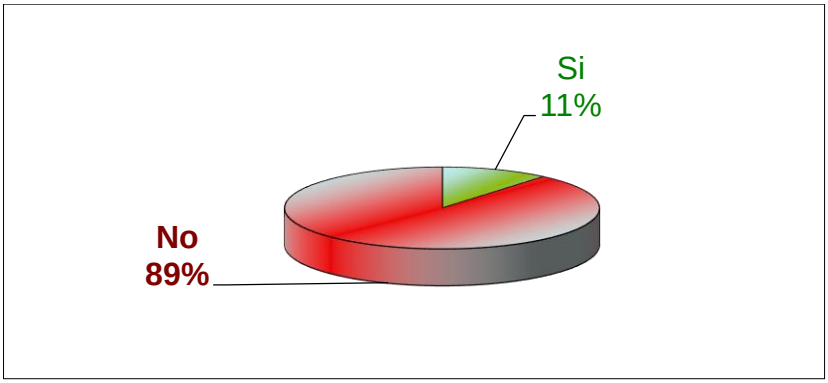


Figura 3.5 Porcentaje de controles para la organización de la seguridad

SEGURIDAD EN RRHH (A7)

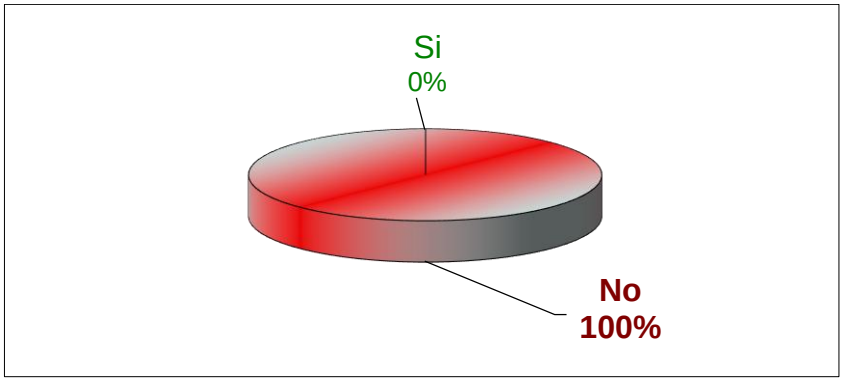


Figura 3.6 Porcentaje de controles para la seguridad en RRHH

ADMINISTRACIÓN DE ACTIVOS (A8)

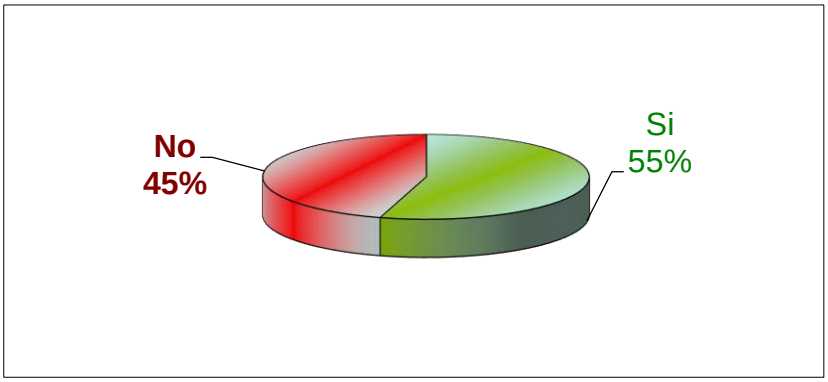


Figura 3.7 Porcentaje de controles para la administración de activos

CONTROL DE ACCESOS (A9)

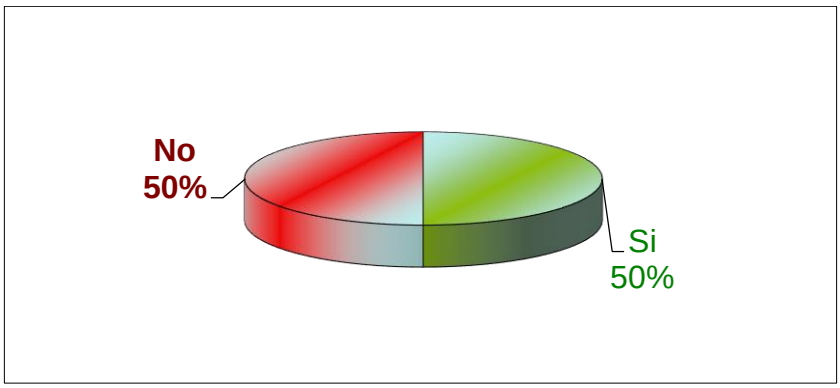


Figura 3.8 Porcentaje de controles para el control de acceso

CRIPTOGRAFÍA (A10)

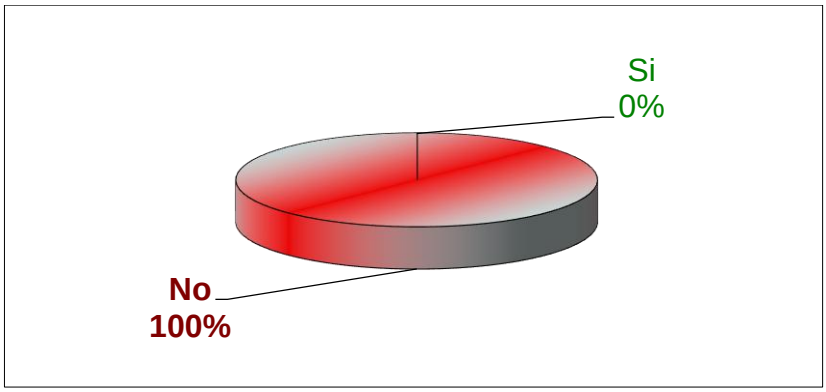


Figura 3.9 Porcentaje de controles en criptografía

SEGURIDAD FÍSICA Y DEL ENTORNO (A11)

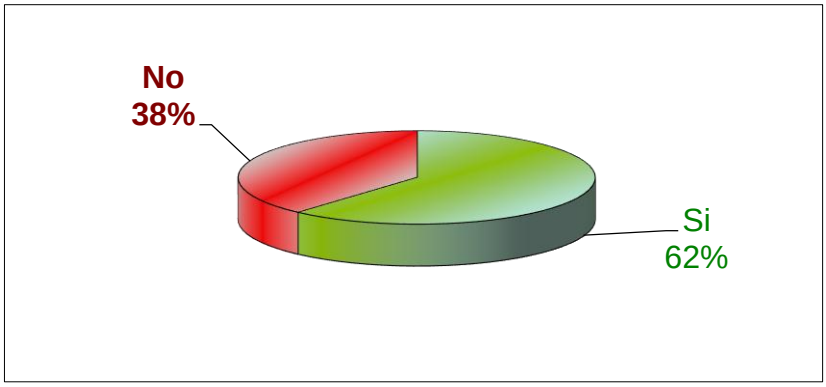


Figura 3.10 Porcentaje de controles en seguridad física y del ambiente

SEGURIDAD DE LAS OPERACIONES (A12)

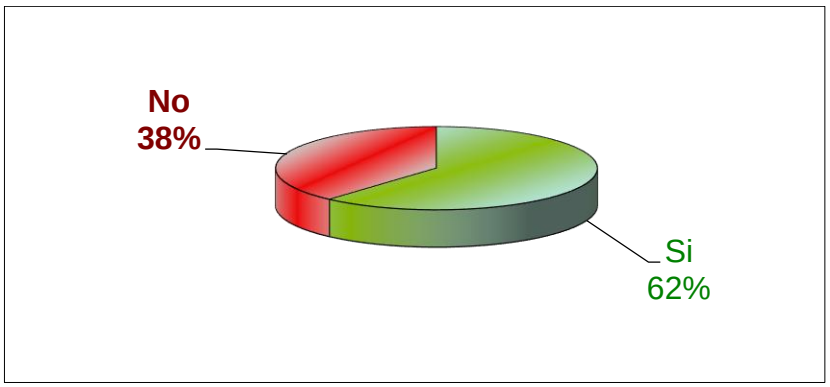


Figura 3.11 Porcentaje de controles en seguridad de las operaciones

SEGURIDAD DE LAS COMUNICACIONES (A13)

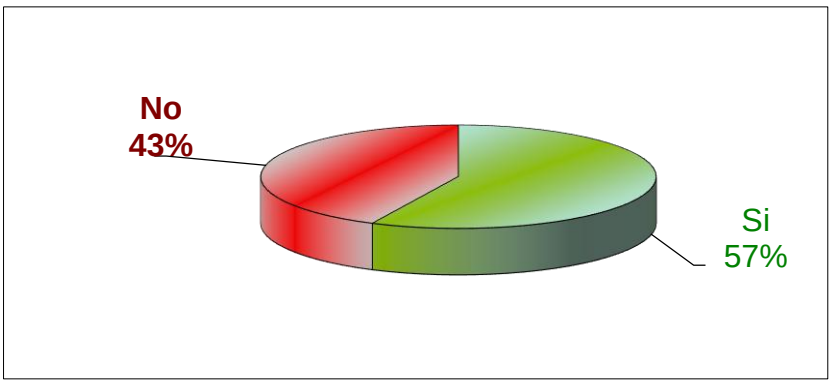


Figura 3.12 Porcentaje de controles en seguridad de las comunicaciones

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA (A14)

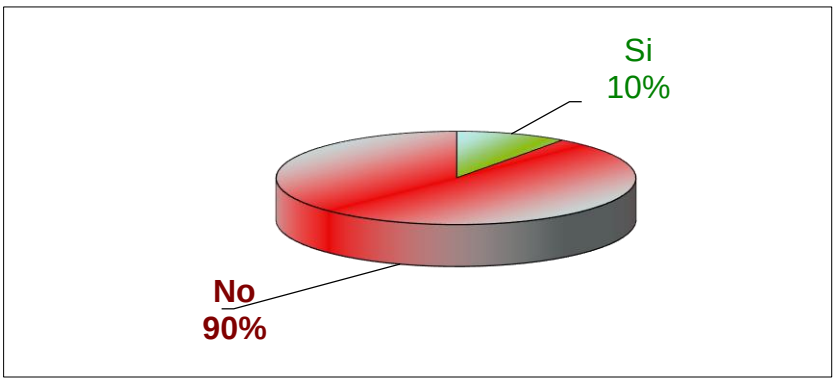


Figura 3.13 Porcentaje de controles en adquisición, desarrollo y mantenimiento del sistema

RELACIONES CON EL PROVEEDOR (A15)

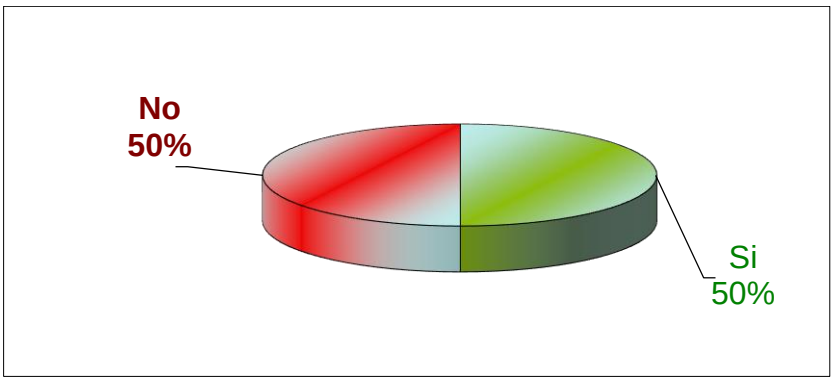


Figura 3.14 Porcentaje de controles en las relaciones con el proveedor

GESTIÓN DE INCIDENTES DE SEGURIDAD (A16)

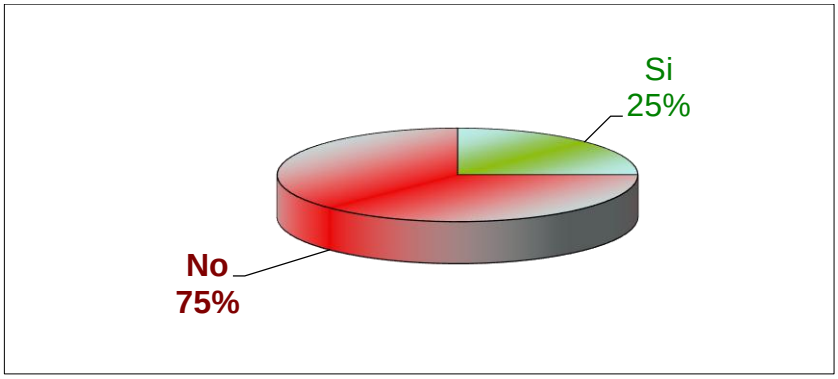


Figura 3.15 Porcentaje de controles en la gestión de incidentes de seguridad

CONTINUIDAD DEL NEGOCIO (A17)

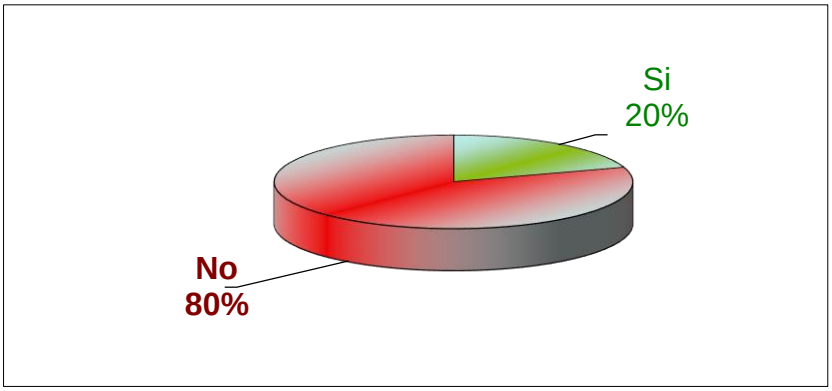


Figura 3.16 Porcentaje de controles en la continuidad del negocio

CUMPLIMIENTO (A18)

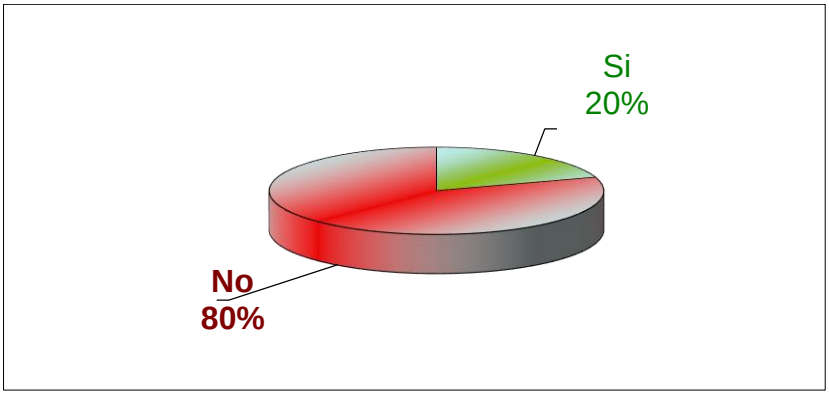


Figura 3.17 Porcentaje de controles en el cumplimiento

CAPÍTULO 4

IMPLEMENTACIÓN DE MECANISMOS DE SEGURIDAD BASADOS EN LA NORMA ISO/IEC 27001

En el capítulo 4 se explicarán los procedimientos y la metodología necesaria para la implementación de la norma ISO/IEC 27001, se identificarán los mecanismos de seguridad precisos para disminuir las vulnerabilidades presentes en el *Data Center* del área de redes, infraestructura y telecomunicaciones sean estos software o hardware. Con el fin de resguardar los datos y presentar las actividades realizadas al GAD Municipal los resultados del presente trabajo se detallan como anexos.

4.1. Proceso de implementación

Normas relacionadas

La serie de normas 27000 contiene normas complementarias para la implementación de la norma ISO/IEC 27001, durante el proceso de ejecución se emplearon las normas que se muestran en la Figura 4.1.

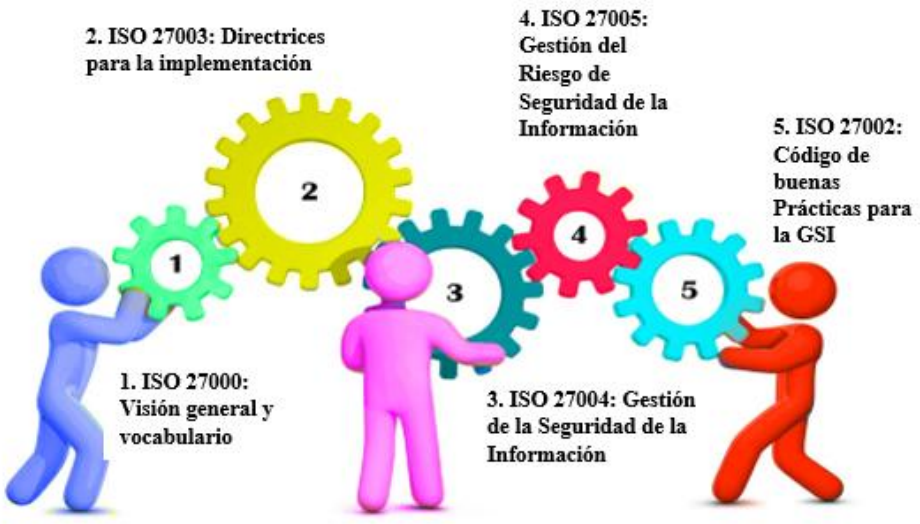


Figura 4.1 Normas usadas en el proceso de implementación de ISO/IEC 27001

Fases para la implementación de un SGSI

Para la implementación del SGSI se deben llevar acabo las fases que se observan en la Figura 4.2 (Normas ISO, 2016).

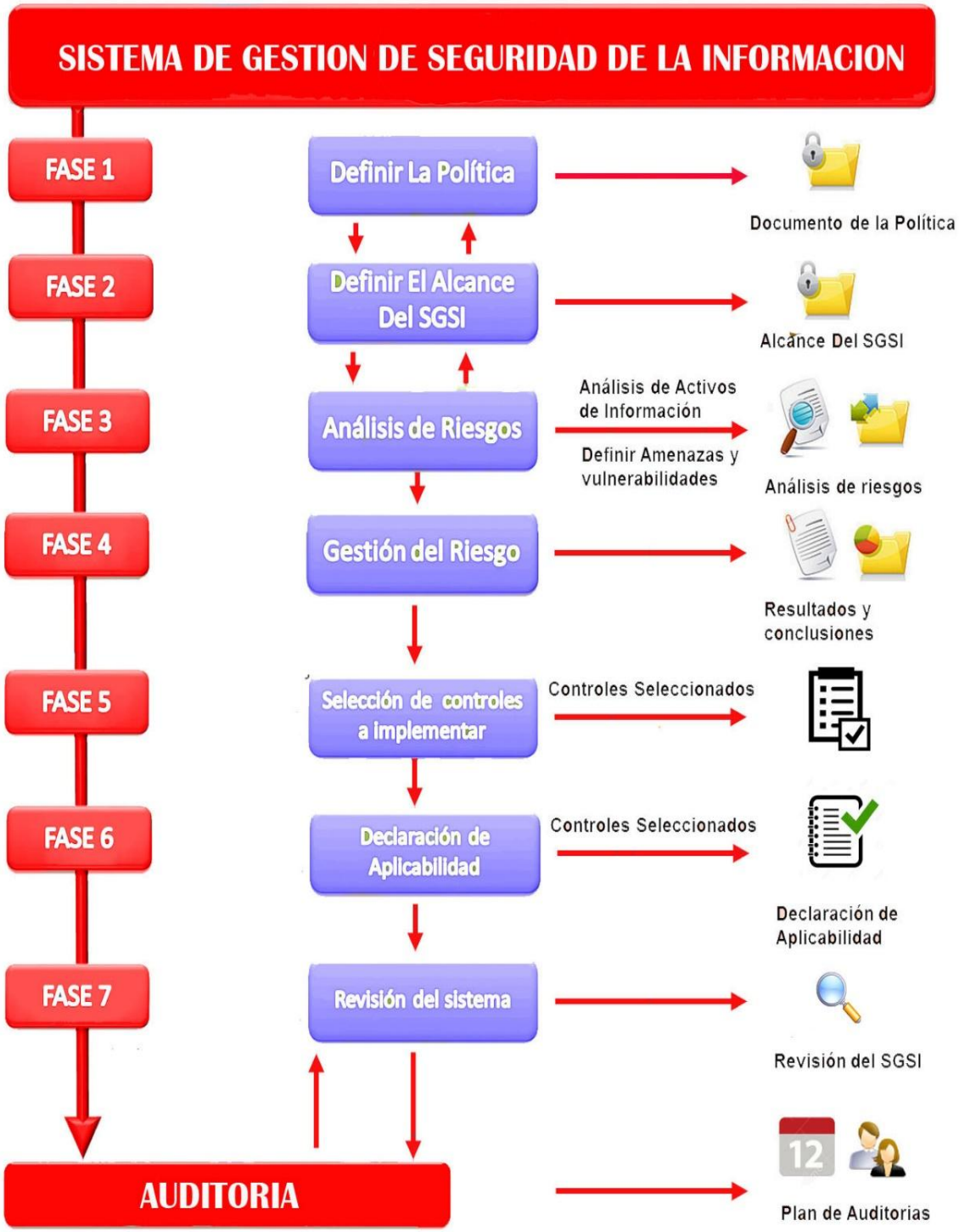


Figura 4.2 Fases de implementación del SGSI

4.2. Plan del Proyecto

Forma parte de la gestión de proyectos, permite informar el progreso dentro del entorno del proyecto de implementación del sistema de gestión de seguridad de la información.

En el Anexo 5 se establece el plan de proyecto para el área de redes, infraestructura y telecomunicaciones del GAD Municipal.

4.3. Alcance del Sistema de Gestión de Seguridad de la Información

En el Anexo 6 se determina el alcance del Sistema de Gestión de Seguridad de la Información este es uno de los puntos más críticos en la implementación ya que su correcta definición permitirá que las tareas, el mantenimiento y los responsables estén correctamente determinados de acuerdo a las características del área.

4.4. Política de seguridad de la información

La política de seguridad de la información es el punto de partida para él diseño del SGSI, por medio de esta la dirección establece las líneas de actuación. El Anexo 7 contiene la política de alto nivel la cual define claramente la intención y los objetivos tomando en consideración los requisitos, obligaciones, la realidad del área y los criterios de evaluación.

4.5. Metodología de evaluación y tratamiento de riesgos

Previa la identificación, análisis y evaluación de vulnerabilidades es necesario plantear la metodología de evaluación y tratamiento de riesgos, en la Tabla 4.1 se presenta un resumen de las metodologías analizadas para posteriormente seleccionar la más adecuada acorde la realidad del área.

Tabla 4.1 Metodologías de valoración de riesgos

Metodología de valoración de riesgos			
Método		**Enfoque**	**Características**
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información	En los elementos informáticos, en la información y comunicaciones	Identifica las amenazas
			Determina la vulnerabilidad
			Recomienda medidas apropiadas
EBIOS	Metodología francesa de análisis y gestión de riesgos de seguridad de sistemas de información	Gestores del riesgo de TI	Estudia cuáles son las dependencias de los procesos del negocio
			Determina los puntos de conflicto
			Establece los objetivos de seguridad necesarios y suficientes
OCTAVE	Metodología de Análisis y Gestión de Riesgos desarrollada por el CERT	Garantizar la seguridad de los sistemas informáticos	Estudia de riesgos organizacionales
			Estudia la infraestructura de información
			Estudia el uso de la infraestructura
GMITS	Guías para la administración de seguridad de TI	Acercamiento Básico	La seguridad es manejada sin una valoración de riesgos

			Reduce el tiempo y costo requerido
		Análisis de riesgo detallado	Decide un nivel de seguridad apropiado para cada activo y de esa manera se escoge los controles con precisión
			Necesita más recursos en tiempo, personal y dinero
		Acercamiento combinado	Combina el acercamiento básico y el análisis de riesgo detallado
			Determina cuáles son los activos en los que habrá que invertir más
			Se les aplica un nivel básico de seguridad al resto de los riesgos
			Enfoque más eficaz en cuanto a costes y a adaptabilidad
		Acercamiento informal	Análisis de riesgos basados en la experiencia o en la decisión de la persona responsable
			Se puede pasar por alto áreas de riesgos o amenazas importantes

(Talero, 2016)**,** (La Suma de todos, 2016)**,** (AcronymFinder, 2016)**.**

La metodología elegida para el análisis de riesgo es proporcionada por Academy27001 y se basa en las Guías para la Implementación de Seguridad de TI, con análisis detallado, ya que permite establecer los controles adecuados para los riesgos más críticos ajustándose a los requerimientos de la norma ISO/IEC 27001:2013.

Matriz de riesgo

La matriz de riesgo permite identificar las actividades más importantes, el tipo y nivel de riesgos y los factores de riesgo. En la Figura 4.3 se observa la matriz de riesgo del área de redes, infraestructura y telecomunicaciones del GAD.

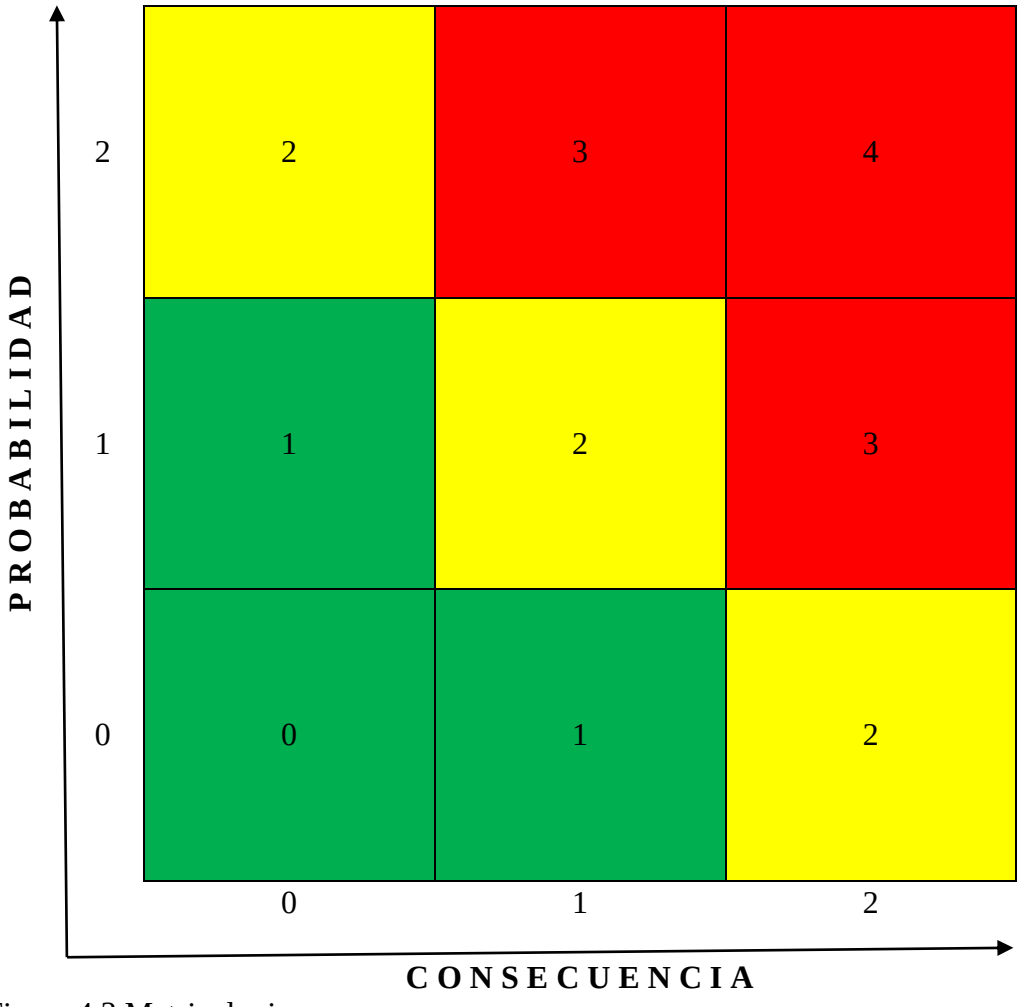


Figura 4.3 Matriz de riesgo

Basados en la matriz de riesgo los valores de 0, 1 y 2 son riesgos aceptables, mientras que los valores 3 y 4 son riesgos no aceptables.

La evaluación de riesgos se implementa a través del Cuadro de evaluación de riesgos. La identificación de amenazas y vulnerabilidades la ejecutan los dueños de los activos, y la evaluación de consecuencias y probabilidad es realizada por los propietarios de los riesgos. Una vez determinados los activos se identifican las amenazas y vulnerabilidades relacionadas con cada uno. En el Anexo 8 se establece la metodología planteada.

4.5.1. Cuadro de evaluación de riesgos

En la evaluación de riesgos se debe identificar todos los activos, es decir, los activos que pueden afectar la confidencialidad, integridad y disponibilidad de la información en el área. Estos pueden ser documentos en papel o en formato electrónico, aplicaciones, personas, equipos de TI, infraestructura y servicios externos o procesos externalizados. Al identificar los activos también es necesario identificar la persona o unidad organizativa responsable de cada activo. En la Figura 4.4 se observa la clasificación realizada para el área, basada en la norma ISO/IEC 27005.

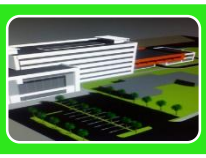
El cuadro de evaluación de riesgos, Anexo 9, contiene una clasificación de los activos, las amenazas y vulnerabilidades que afectan estos activos y el nivel de riesgo que representan de acuerdo al grado de consecuencia y probabilidad. Además, identifica los controles de seguridad empleados actualmente. En la Tabla 4.2 se observa la plantilla utilizada.

Organización

•Autoridades, estructura de la organización, auditores, consultores, instituciones de supervisión

Personal

•Alta dirección, mandos intermedios, empleados, administradores de sistemas, diseñadores, expertos en seguridad, otros empleados, empleados externos a tiempo parcial, personas externas que visitan la organización



Lugar

•Oficinas, archivos, depósitos, gabinetes, instalaciones, suminstro de energía eléctrica

Red

•Medios y soportes, transmision pasiva o activa (enrutamiento, switches,routers, logs), interfaz de comunicación, mantenimiento de equipo de TIC, mantenimiento de sistemas de información, servicios de correo y mensajería

Software

•Software de aplicaciones (con licencia), programas de distribución libre, programas compartidos, software de sistemas, herramientas diversas, bases de datos

Hardware

•Ordenadores de escritorio, ordenadores portátiles, CD de instalación, dispositivos UPS, generadores de electricidad, aire acondicionado, equipamiento de red, cables de alimentación, servidores, teléfonos, centrales telefónicas, teléfonos móviles, dispositivos PDA, impresoras, fotocopiadora, cintas de respaldo, soportes móviles de almacenaje, equipos de medición

Figura 4.4 Clasificación de activos

Tabla 4.2 Cuadro de evaluación de riesgos

No.	Nombre del activo	Propietario del activo	Amenaza	Vulnerabilidad	Propietario del riesgo	Consecuencia	Probabilidad	Riesgo	Controles existentes

4.5.2. Cuadro tratamiento de riesgos

Para los riesgos no aceptables calificados en 3 y 4 se deben seleccionar una o más opciones de tratamiento.

1. Elección de control o controles de seguridad del Anexo A de la norma ISO/IEC 27001 u otros controles de seguridad.
2. Transferencia de los riesgos a terceros.
3. Evitar los riesgos discontinuando una actividad comercial que ocasiona ese riesgo.
4. Aceptación del riesgo: esta opción está permitida solamente si las selecciones de otras opciones de tratamiento del riesgo costarían más que el potencial impacto en el caso de que se materializara dicho riesgo.

La elección de opciones se implementa a través del Cuadro de tratamiento de riesgos. Habitualmente, se escoge la elección de uno o más controles de seguridad. En el Anexo 10 se encuentra el cuadro de tratamiento de riesgos, en este se establece un control o solución para cada riesgo existente y su nivel de efectividad una vez implantado. En la Tabla 4.3 se observa la plantilla utilizada.

4.5.3. Informe sobre evaluación y tratamiento de riesgos

El informe es un resumen del proceso empleado para la evaluación y tratamiento de riesgos y los imprevistos que se presenten durante este proceso. En el Anexo 11 se encuentra redactado el informe de evaluación y tratamiento de riesgos del área de redes, infraestructura y telecomunicaciones.

En base a los resultados obtenidos del análisis, el porcentaje de riesgos presente es del 92% (Figura 4.5) en el ámbito organizacional, en el personal (Figura 4.6) es del 91%, por la infraestructura del lugar es de un 50% (Figura 4.7), en la red (Figura 4.8) existe un 54%, el software (Figura 4.9) presenta un 70% y el hardware un 55% (Figura 4.9).

Tabla 4.3 Cuadro de tratamiento de riesgos

Activos / amenazas / vulnerabilidades					Valor antes del tratamiento				Tratamiento del riesgo		Valor después del tratamiento		
No.	**Nombre del activo**	**Propietario del activo**	**Amenaza**	**Vulnerabilidad**	**Propietario del riesgo**	**Consecuencia**	**Probabilidad**	**Riesgo**	**Elección de opciones**	**Medios de ejecución**	**Consecuencia**	**Probabilidad**	**Riesgo**

Figura 4.5 Riesgo en la organización

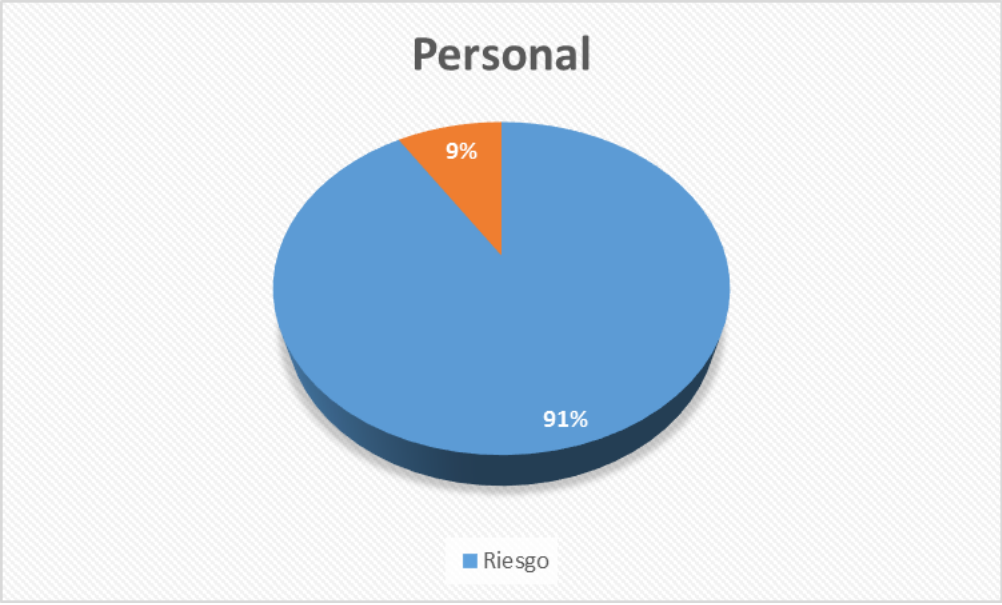


Figura 4.6 Riesgo en el personal

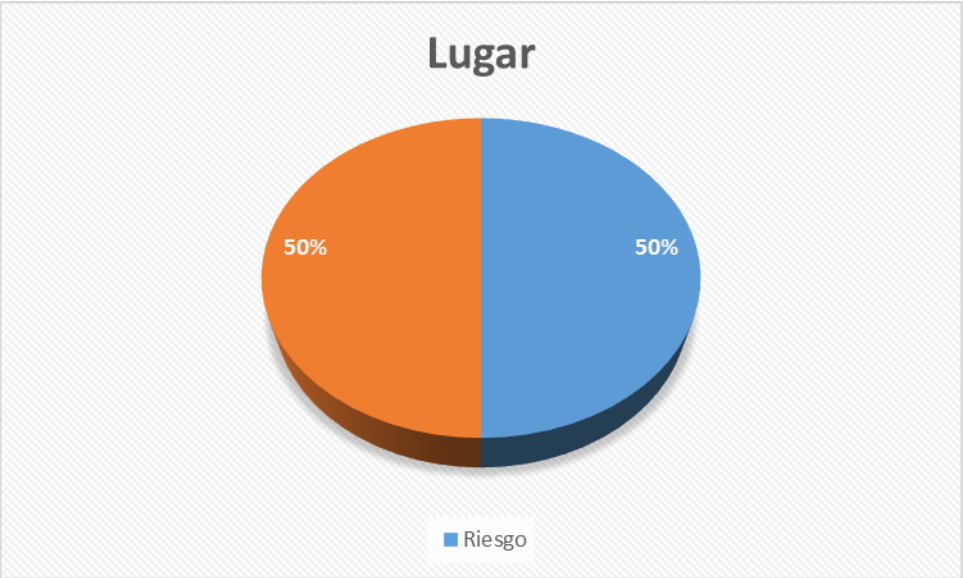


Figura 4.7 Riesgo en el lugar

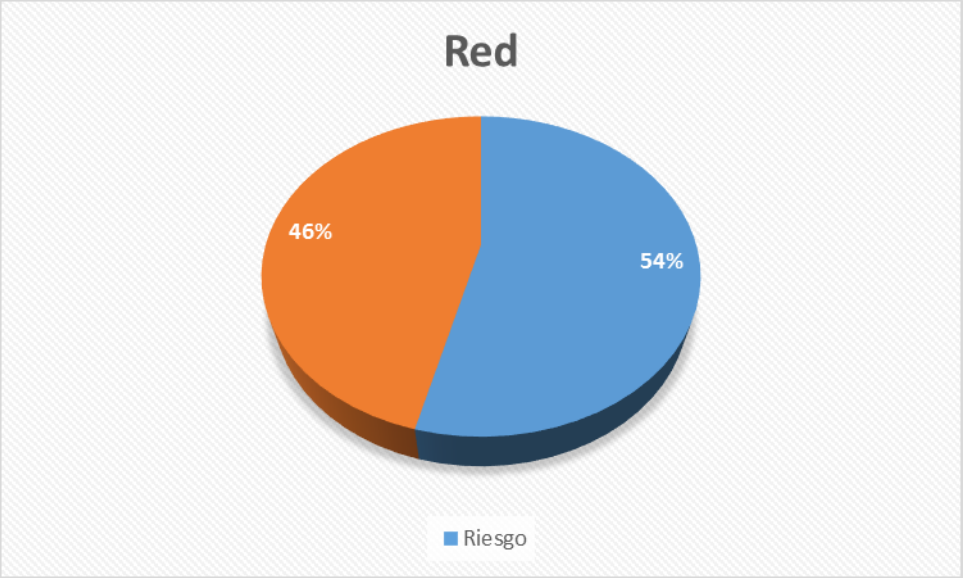


Figura 4.8 Riesgo en la red

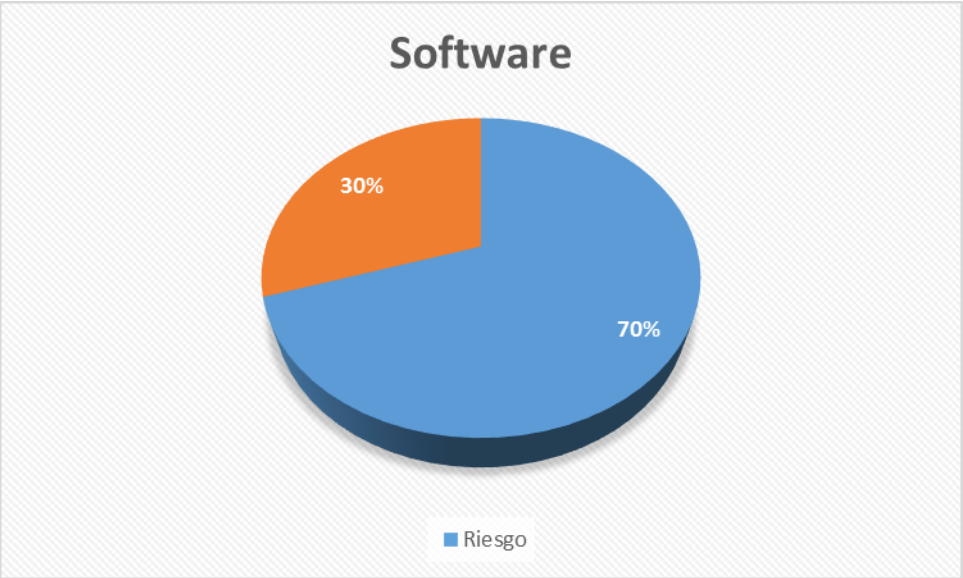


Figura 4.9 Riesgo en el software

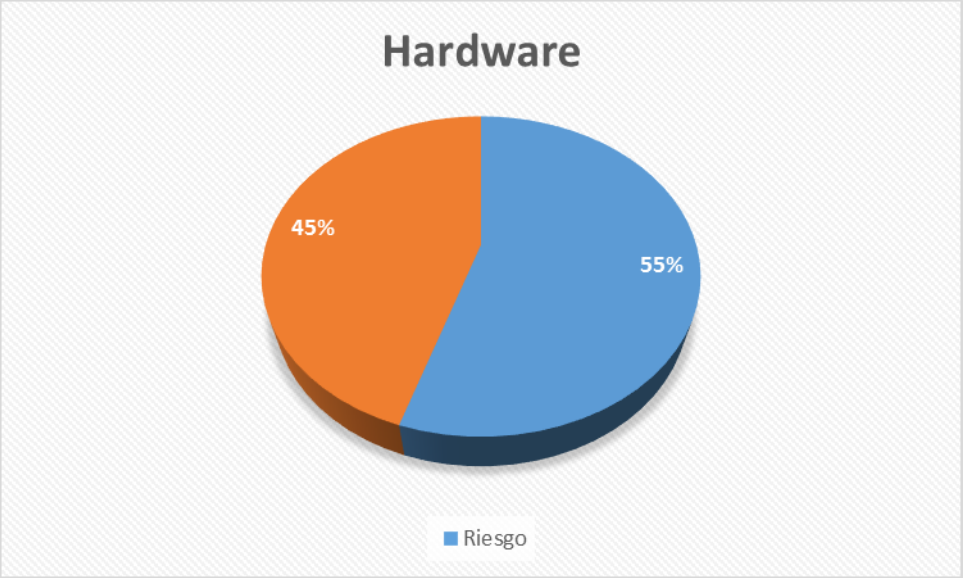


Figura 4.10 Riesgos en el hardware

4.6. Declaración de aplicabilidad

La Declaración de aplicabilidad es una justificación de la elección de uso o no uso de cada uno de los controles que la norma ISO/IEC 27001 presenta en su Anexo A. Esta contiene: qué controles de seguridad son aplicables y cuáles no, la justificación de esa decisión y si están implementados o no. Además, por medio de esta se identifica los riesgos residuales.

En el Anexo 12 se encuentra redactada la declaración de aplicabilidad del área de redes, infraestructura y telecomunicaciones, en la Tabla 4.4 se establece el código empleado en la justificación del uso o no uso, en la Tabla 4.5 se encuentra el código establecido para determinar el estado del control y en la Tabla 4.6 se presenta plantilla usada para la declaración de Aplicabilidad.

Tabla 4.4 Código de justificación de uso y no uso

Código	Significado
L	Requerimiento Legal
C	Obligación contractual
N	Requerimiento del negocio
R	Análisis de riesgos

Tabla 4.5 Código de estado del control

Código	Significado
P	El control está planificado.
PI	El control se lleva acabo, pero el proceso debe ser documentado.
I	El control se documentó e implementó.
NI	No implementado.
NA	El control no es aplicable para la empresa.

Ya que no se consigue reducir todos los riesgos en el proceso de gestión de riesgos, se establece todos los siguientes como riesgos residuales:

1. Todos los riesgos con valor 0, 1 o 2.
2. Los riesgos que no pudieron ser reducidos a los niveles mencionados en el punto anterior luego de la aplicación de los controles.

4.7. Plan de tratamiento de riesgos

Luego de identificar los riesgos y determinar el control que permita mitigar este riesgo se debe especificar quien es el responsable de cumplir con la ejecución del control, cual es el tiempo que tomará, el costo que esto conlleva entre otras características importantes para su ejecución. En la Tabla 4.8 se observa la plantilla, Anexo 13, utilizada para el plan de tratamiento de riesgos.

Para la implementación de los controles del Anexo A de la norma ISO/IEC 27001 se debe seguir el lineamiento otorgado por la norma ISO/IEC 27002 Código de buenas Prácticas, el resumen de lineamiento de los controles que se van a implementar se observa en el Anexo 14.

Tabla 4.6 Declaración de Aplicabilidad

ID	Controles según la norma ISO/IEC 27001	Aplicabilidad (SÍ/NO)	Justificación de elección/ no elección				Objetivos del control	Método de implementación	Estado
			L	C	N	R			

Tabla 4.1 Riesgos residuales

Activos / amenazas / vulnerabilidades					Valor antes del tratamiento				Tratamiento del riesgo		Valor después del tratamiento		
No.	**Nombre del activo**	**Propietario del activo**	**Amenaza**	**Vulnerabilidad**	**Propietario del riesgo**	**Consecuencia**	**Probabilidad**	**Riesgo**	**Elección de opciones**	**Medios de ejecución**	**Consecuencia**	**Probabilidad**	**Riesgo**

Tabla 4.8 Plan de tratamiento de riesgos

Control	Descripción de actividades	Recursos generales y financieros necesarios	Persona Responsable	Método de avaluación de resultados	Programas de capacitación y concienciación	Plazo	Estado

CONCLUSIONES Y RECOMENDACIONES

Conclusiones:

- La seguridad de la información en una empresa se debe tratar por medio de un Sistema de Gestión de Seguridad de la Información, ya que, a pesar del avance de la tecnología, en lugar de disminuir los índices de debilidades en los sistemas de las empresas, está ocurriendo lo opuesto porque los usuarios no están haciendo uso adecuado de los aplicativos de seguridad.

- La implementación de la norma ISO/IEC 27001:2013 además de proteger la empresa permite conseguir una ventaja comercial, ya que permite obtener una certificación que avale la seguridad con la que cuenta el área de redes, infraestructura y telecomunicaciones del GAD Municipal del cantón Cuenca.

- Es de gran ayuda poseer conocimiento de la serie de normas ISO/IEC 27000 ya que ofrecen información de apoyo para la implementación y mantenimiento del Sistema de Gestión de Seguridad de la Información.

- Luego de efectuado el autodiagnóstico, Anexo 3 y Anexo 4, se determinó que el área de redes, infraestructura y telecomunicaciones del GAD Municipal de Cuenca posee un índice de debilidades del 64% de acuerdo a lo que establece la norma ISO/IEC 27001:2013.

- El alcance del SGSI se estableció para el área de redes, infraestructura y telecomunicaciones ya que no fue preciso desarrollar un SGSI para toda la organización porque lo importante es enfocarse donde se encuentren la mayoría de las actividades relacionadas con la gestión de información.

- La parte decisiva para una adecuada implementación del SGSI fue la correcta determinación de los activos para posteriormente identificar las amenazas y vulnerabilidades que pueden afectar a dichos activos.

- En base a los resultados obtenidos del análisis, el porcentaje de riesgos presente es del 92% en el ámbito organizacional, en el personal es del 91%,

por la infraestructura del lugar es de un 50%, en la red existe un 54%, el software presenta un 70% y el hardware un 55%.

- El cumplimiento de las políticas de seguridad, así como la implementación de todos los controles definidos en el plan de tratamiento de riesgos y los recomendados para los riesgos residuales permitirá al área de redes, infraestructura y telecomunicaciones disminuir el nivel de riesgo presente.

- Luego de aplicar los controles se tendrá un porcentaje de riesgo organizacional del 46%, por parte del personal un 45% y para la infraestructura del lugar, la red, el software y el hardware se logrará un porcentaje del 25%.

- El efectuar la ejecución de los controles de seguridad definidos luego de realizada la evaluación de riesgos, no garantiza que en un futuro no ocurra inconvenientes de seguridad, ya que no existe la seguridad total ante cualquier blindaje de protección siempre se podrá encontrar un elemento capaz de romperla, pero la aplicación de los controles permite disminuir la probabilidad de que se materialice un riesgo, reduciendo los impactos y la pérdida de información.

- Se ha contado con el aval de la empresa para corroborar la información obtenida en el transcurso del desarrollo de la tesis, para lo cual se anexa el documento que así lo valida, Anexo 1.

Recomendaciones:

- La seguridad de la información debe ser manejada como un proceso de mejoramiento continuo acorde a los cambios que se realizan en el área de redes, infraestructura y telecomunicaciones.

- Se debe realizar difusiones de las políticas de seguridad de la información y campañas de concientización de la importancia de la seguridad de la información a todo el personal del GAD Municipal.

- Una vez implementados todos los controles propuestos, se recomienda realizar un nuevo análisis para verificar si el índice de debilidades ha disminuido o aumentado y con ello poder tomar medidas en el asunto.

- Se recomienda contar con un responsable de seguridad que cumpla a cabalidad con el Sistema de Gestión de Seguridad implantado y su mejoramiento. La ausencia de un responsable de seguridad provoca que no exista personal idóneo para elaborar una estrategia de seguridad robusta que garantice la disponibilidad, integridad y confiabilidad de los datos, los procesos efectivos y eficientes para preservar los intereses de la organización, y la explicación de las insuficiencias a la alta gerencia pues al implementar un Sistema de Gestión de Seguridad de la Información se incrementan las responsabilidades y al recaer en el personal del área se vuelve complicada la ejecución de las diferentes tareas.

BIBLIOGRAFÍA

AcronymFinder. (2016). *GMITS - Guidelines for the Management of Information Technology Security* . Obtenido de Acronymfinder.com: http://www.acronymfinder.com

AMAYA, C. G. (12 de diciembre de 2013). *welivesecurity*. Obtenido de ISO/IEC 27002:2013 y los cambioc en los dominios de control.

BVEx España. (2014). (La información como activo estratégico de la empresa - BVEx España) Recuperado el 13 de Noviembre de 2015, de http://businessvalueexchange.com

Carracedo Gallardo, J. (Enero de 2011). *intypedia.* Recuperado el Noviembre de 2015, de Introducción a la seguridad en redes Telemáticas: http://www.criptored.upm.es

Degerencia. (2015). (Gestion de la seguridad de la informacion) Recuperado el 13 de Noviembre de 2015, de http://www.degerencia.com

El Informador. (2015). (La información es el principal activo de las empresas) Recuperado el 13 de Noviembre de 2015, de http://www.informador.com

El Nacional. (16 de Junio de 2015). Seguridad informática es un tema que preocupa a las empresas. *El Nacional*.

Fonseca, G. (18 de Abril de 2012). *Guillermo Fonseca*. Obtenido de La información el activo mas importante de cualquier organización: https://guillermofonseca.wordpress.com

Gobierno Autonomo Descentralizado Municipal del Canton Portoviejo. (Enero de 2014). *PLAN DE CONTINGENCIAS INFORMÁTICO*. Obtenido de http://intranet.portoviejo.gob.ec

Granados, G. A. (2015). *Visionindustrial.com.mx*. (INFORMACIÓN Activo valioso para las empresas) Recuperado el 13 de Noviembre de 2015, de http://www.visionindustrial.com

Ildapena. (20 de octubre de 2008). *XperimentoS*. Obtenido de Publicada la norma ISO 27005: Gestión del riesgo: http://www.xperimentos.com

International Organization for Standardization. (2013). *ISO/IEC 27001*. Obtenido de ISO/IEC 27001:2013 Information technology -- Security techniques -- Information security management systems -- Requirements: http://www.iso.org

International Organization for Standardization. (15 de 01 de 2014). *ISO/IEC 27000.* Obtenido de ISO: www.iso.org

ISO. (2015). *Iso.org*. (The ISO Survey) Recuperado el 10 de Noviembre de 2015, de http://www.iso.org

ISO 27K. (s.f.). *ISO/IEC 27004*. Obtenido de ISO/IEC 27004:2009 Information technology — Security techniques — Information security management — Measurement: http://www.iso27001security.com

ISOTools Excellence. (17 de Enero de 2014). *Blog especializado en Sistemas de Gestión* . Obtenido de ISO/IEC 27003 – Guía para la implementación de un Sistema de Gestión de Seguridad de la Información.: http://www.pmg-ssi.com

Juárez, H. A. (08 de noviembre de 2011). *Magazcitum*. Obtenido de ISO-27001: ¿Qué es y para qué sirve? : http://www.magazcitum.com

Kosutic, D. (Septiembre de 2010). *27001Academy*. (¿Qué es norma ISO 27001?) Recuperado el 10 de Noviembre de 2015, de http://advisera.com/27001academy/es/que-es-iso-27001/

La Suma de todos. (2016). *Análisis y cuantificación del Riesgo.* Obtenido de http://www.madrid.org/

López, E. L. (s.f.). *Universidad Nacional Autónoma de México*. Recuperado el 7 de Diciembre de 2015, de Fundamentos de Seguridad Informática: http://redyseguridad.fi-p.unam.mx

López, E. (s.f.). *Universidad Nacional Autónoma de México*. Obtenido de Fundamentos de Seguridad Informática: http://redyseguridad.fi-p.unam.mx

Neira, A. L. (Octubre de 2005). *ISO 27000.es*. Obtenido de El portal de ISO 27001 en Español: http://www.iso27000.es

Normas ISO. (2016). Obtenido de ISO 27001 Presupuesto On Line Sin Compromiso: http://www.normas-iso.com

Talero, F. (2016). *Metodologia de Analisis de Riesgo OCTAVE*. Obtenido de prezi.com: https://prezi.com

ANEXOS

Anexo 1: Certificado de apoyo y validación de datos del área de redes, infraestructura y telecomunicaciones del departamento de Informática del GAD Municipal del cantón Cuenca.

Anexo 2: Anexo A de la norma ISO/IEC 27001:2013

El Anexo A de la norma, contiene una completa lista de los objetivos y controles que permiten identificar aquellos que son necesarios para implementar el tratamiento de riesgos.

A.5 Política de seguridad de la información		
A.5.1 Orientación de la dirección para la seguridad de la información		
Objetivo: Proporcionar orientación y apoyo de la dirección para seguridad de la información, de acuerdo con los requerimientos del negocio y con las regulaciones y leyes pertinentes.		
A.5.1.1	Documentar política de seguridad de información	Control: La dirección debe definir, aprobar, publicar y comunicar a todos los empleados y a las partes externas pertinentes un grupo de política para la seguridad de la información.
A.5.1.2	Revisión de la política de seguridad de la información	Control: Se deben revisar las políticas de seguridad de la información a intervalos planeados o si ocurren cambios significativos para asegurar su conveniencia, suficiencia y eficacia continúas.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna		
Objetivo: Establecer un marco de trabajo de la dirección para comenzar y controlar la implementación y funcionamiento de la seguridad de la información dentro de la organización.		
A.6.1.1	Roles y responsabilidades de la seguridad de la información	Control: Todas las responsabilidades de la seguridad de la información deben ser definidas y asignadas.
A.6.1.2	Segregación de funciones	Control: Se deben segregar las funcione y las áreas de responsabilidad para reducir las oportunidades de modificaciones no autorizadas o no intencionales o el uso inadecuado de los

		activos de la organización.
A.6.1.3	Contacto con autoridades	Control: Se deben mantener los contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos especiales de interés	Control Se deben mantener los contactos apropiados con los grupos especiales de interés u otros foros especializados en seguridad, así como asociaciones de profesionales.
A.6.1.5	Seguridad de la información en la gestión de proyecto	Control: Se debe abordar la seguridad de la información en la gestión de proyecto, sin importar el tipo de proyecto.
A.6.2 Dispositivos móviles y trabajo remoto		
Objetivo: garantizar la seguridad del trabajo remoto y el uso de dispositivos móviles.		
A.6.2.1	Política de dispositivos móviles	Control: Se debe adoptar una política y medidas de apoyo a la seguridad para gestionar los riesgos presentados al usar dispositivos móviles.
A.6.2.2	Trabajo remoto	Control: Se debe implementar una política y medidas de apoyo a la seguridad para proteger la información a la que se accede, procesa o almacena en los lugares de trabajo remoto.
A.7 Seguridad ligada a los recursos humanos		
A.7.1 Previo al empleo		
Objetivo: Asegurar que los empleados y contratistas entiendan sus responsabilidades, y que sea aptos para los roles para los cuales están siendo considerados.		
A.7.1.1	Selección	Control: Se debe realizar la verificación de antecedentes en todos los candidatos al empleo, de acuerdo con las leyes, regulaciones y normas éticas relevantes y en proporción a los requisitos del negocio, la clasificación de la información a ser accedida, y los riesgos percibidos.

A.7.1.2	Términos y condiciones de la relación laboral	Control: Los acuerdos contractuales con los empleados y contratistas deben indicar sus responsabilidades y las de la organización en cuanto a seguridad de la información.
A.7.2 Durante el empleo		
Objetivo: Asegurar que los empleados y contratistas estén en conocimiento y cumplan con sus responsabilidades de seguridad de la información.		
A.7.2.1	Gestión de responsabilidades	Control: La dirección debe solicitar a todos los empleados y contratistas que apliquen la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Concientización, educación y capacitación en seguridad de la información	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas deben recibir formación adecuada en concientización y actualizaciones regulares en políticas y procedimientos organizacionales pertinentes para su función laboral.
A.7.2.3	Proceso disciplinario	Control: Debe existir un proceso disciplinario formal y sabido por los empleados para tomar acciones en contra de los empleados que hayan cometido una infracción a la seguridad de la información.
A.7.3 Desvinculación y cambio de empleo		
Objetivo: Proteger los intereses de la organización como parte del proceso de cambio o desvinculación del empleo.		
A.7.3.1	Responsabilidades en la desvinculación o cambio de empleo	Control: Se deben definir y comunicar las responsabilidades y funciones de la seguridad de la información que siguen en vigor después de la desvinculación o cambio de relación laboral.
A.8 Administración de activos		
A.8.1 Responsabilidad por los activos		

Objetivo: Identificar los activos de la organización y definir las responsabilidades de protección pertinentes.		
A.8.1.1	Inventario de activos	Control: Deberá identificarse los activos asociados a las instalaciones de procesamiento de la información y a la información y se debe realizar y mantener un inventario de dichos activos.
A.8.1.2	Propiedad de los activos	Control: Los activos que se mantienen en inventario deben pertenecer a un dueño.
A.8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con la información y las instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	Control: Todos los empleados y usuarios de terceras partes deben devolver todos los activos pertenecientes a la organización que estén en su poder como consecuencia de la finalización de su relación laboral contrato o acuerdo.
A.8.2 Clasificación de la información		
Objetivo: Asegurar que la información recibe el nivel de protección adecuado, según su importancia para la organización.		
A.8.2.1	Clasificación de la información	Control: La información debe ser clasificada en términos de requisitos legales, valor, criticidad y sensibilidad para la divulgación o modificación sin autorización.
A.8.2.2	Etiquetado de la información	Control: Se debe desarrollar e implementar un conjunto apropiado de procedimientos para el etiquetado de la información, de acuerdo al esquema de clasificación de información adoptado por la organización.
A.8.2.3	Manejo de activos	Control: Se deben desarrollar e implementar los procedimientos para el manejo de activos, de

		acuerdo al esquema de clasificación de información adoptado por la organización.
A.8.3 Manejo de los medios		
Objetivo: Prevenir la divulgación no autorizada, modificación, eliminación o destrucción de la información almacenada en los medios.		
A.8.3.1	Gestión de los medios removibles	Control: Se deben implementar los procedimientos para la gestión de los medios removibles, de acuerdo al esquema de clasificación adoptado por la organización.
A.8.3.2	Eliminación de los medios	Control: Se deben eliminar los medios de forma segura y sin peligro cuando no se necesiten más, usando procedimientos formales.
A.8.3.3	Transferencia física de medios	Control: Los medios que contengan información se deben proteger contra acceso no autorizado, uso inadecuado o corrupción durante el transporte.
A.9 Control de acceso		
A.9.1 Requisitos de negocio para el control de acceso		
Objetivo: Restringir el acceso a la información y a las instalaciones de procesamiento de información.		
A.9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso basadas en los requisitos del negocio y de seguridad de la información.
A.9.1.2	Acceso a las redes y a los servicios de la red	Control: Los usuarios solo deben tener acceso directo a la red y a los servicios de la red para los que han sido autorizados específicamente.
A.9.2 Gestión de acceso del usuario		
Objetivo: Asegurar el acceso de usuarios autorizados y evitar el acceso sin autorización a los sistemas y servicios.		
A.9.2.1	Registro y cancelación de registro de usuario	Control: Se debe implementar un proceso de registro y cancelación de registro de usuario para habilitar la asignación de derechos de

		acceso.
A.9.2.2	Asignación de acceso de usuario	Control: Debe existir un procedimiento formal de asignación de usuario para asignar o revocar los derechos de acceso para todos los típicos de usuarios, a todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiados	Control: Se debe restringir y controlar la asignación y uso de los derechos de acceso privilegiado.
A.9.2.4	Gestión de información secreta de autenticación de usuarios	Control: Se debe controlar la asignación de información de autenticación secreta mediante un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuario	Control: Los propietarios de activos deben revisar los derechos de acceso de los usuarios de manera periódica.
A.9.2.6	Eliminación o ajuste de los derechos de acceso	Control: Se deben retirar los derechos de acceso de todos los empleados y usuarios externos a la información y a las instalaciones de procesamiento de información, una vez que termine su relación laboral, contrato o acuerdo o se ajuste según el cambio.
A.9.3 Responsabilidades del usuario		
Objetivo: Responsabilizar a los usuarios del cuidado de su información de autenticación.		
A.9.3.1	Uso de información de autenticación secreta	Control: Se debe exigir a los usuarios el cumplimiento de las prácticas de la organización en el uso de la información de autenticación secreta.
A.9.4 Control de acceso al sistema y aplicaciones		
Objetivo: Evitar el acceso sin autorización a los sistemas y aplicaciones.		
A.9.4.1	Restricción de acceso a la información	Control: Se debe restringir el acceso a la información y a las funciones del sistema de aplicaciones, de acuerdo con la política de control de acceso.

A.9.4.2	Procedimiento de inicio de sesión seguro	Control: Cuando lo exija la política de control de acceso, el acceso a los sistemas y aplicaciones debe ser controlado por un procedimiento de inicio de sesión seguro.
A.9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar contraseñas de calidad.
A.9.4.4	Uso de programas utilitarios privilegiados	Control: Se debe restringir y controlar estrictamente el uso de programas utilitarios que pueden estar en capacidad de anular el sistema y los controles de aplicación.
A.9.4.5	Control de acceso al código fuente de los programas	Control: Se debe restringir el acceso al código fuente de los programas.
A.10 Criptografía		
A.10.1 Controles criptográficos		
Objetivo: Asegurar el uso adecuado y eficaz de la criptografía para proteger la confidencialidad, autenticidad o integridad de la información.		
A.10.1.1	Política sobre el uso de controles criptográficos	Control: Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información
A.10.1.2	Gestión de claves	Control: Se debe desarrollar e implementar una política sobre el uso, protección y vida útil de las claves criptográficas durante toda su vida útil.
A.11 Seguridad física y del ambiente		
A.11.1 Áreas seguras		
Objetivo: Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de la información y la información de la organización.		
A.11.1.1	Perímetro de seguridad	Control: Se deben definir y utilizar perímetros de seguridad para proteger las áreas que contienen ya sea información sensible o crítica y las instalaciones de procesamiento de

		información.
A.11.1.2	Controles de acceso físico	Control: Las áreas seguras deben estar protegidas por controles de entrada apropiados que aseguren que solo se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, salas e instalaciones	Control: Se debe diseñar y aplicar la seguridad física en oficinas, salas e instalaciones.
A.11.1.4	Protección contra amenazas externas y del ambiente	Control: Se debe diseñar y aplicar la protección física contra daños por desastre natural ataque malicioso o accidentes.
A.11.1.5	Trabajo de áreas seguras	Control: Se deben diseñar y aplicar procedimientos para trabajar en áreas seguras.
A.11.1.6	Áreas de entrega y carga	Control: Se debe controlar los puntos de acceso tales como áreas de entrega y de carga y otros puntos donde las personas no autorizadas puedan acceder a las instalaciones, y si es posible, aislarlas de las instalaciones de procesamiento de la información para evitar el acceso no autorizado.
A.11.2 Equipamiento		
Objetivo: Prevenir pérdidas, daños, hurtos o el compromiso de los activos, así como la interrupción de las actividades de la organización.		
A.11.2.1	Ubicación y protección del equipamiento	Control: El equipamiento se debe ubicar y proteger para reducir los riesgos ocasionados por amenazas y peligros ambientales, y oportunidades de acceso no autorizado.
A.11.2.2	Elementos de soporte	Control: Se debe proteger el equipamiento contra fallas en el suministro de energía y otras interrupciones causadas por fallas en elementos de soporte.
A.11.2.3	Seguridad en el cableado	Control: Se debe proteger el cableado de energía y de telecomunicaciones que transporta datos o brinda soporte a servicios de

		información contra interceptación, interferencia o daños.
A.11.2.4	Mantenimiento del equipamiento	Control: El equipamiento debe recibir el mantenimiento correcto para asegurar su permanente disponibilidad e integridad.
A.11.2.5	Retiro de activos	Control: El equipamiento, la información o el software no se deben retirar del local de la organización sin previa autorización.
A.11.2.6	Seguridad del equipamiento y los activos fuera de las instalaciones	Control: Se deben asegurar todos los activos fuera de las instalaciones, teniendo en cuenta los diferentes riesgos de trabajar fuera de las instalaciones de la organización.
A.11.2.7	Seguridad en la reutilización o descarte de equipos	Control: Todos los elementos del equipamiento que contenga medios de almacenamiento deben ser revisados para asegurar que todos los datos sensibles y software licenciado se hayan removido o se haya sobrescrito con seguridad antes de su descarte o reutilización.
A.11.2.8	Equipo de usuario desatendido	Control: Los usuarios se deben asegurar de que a los equipos desatendidos se les da protección apropiada.
A.11.2.9	Política de escritorio y pantalla limpios	Control: Se debe adoptar una política de escritorio limpio para papeles y medios de almacenamiento removibles y una política de pantalla limpia para las instalaciones de procesamiento de información.
A.12 Seguridad de las operaciones		
A.12.1 Procedimientos operacionales y responsabilidades.		
Objetivo: Asegurar la operación correcta y segura de las instalaciones de procesamiento de información.		
A.12.1.1	Procedimientos de operación documentados	Control: Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesiten.

A.12.1.2	Gestión de cambios	Control: Se deben controlar los cambios a la organización, procesos de negocio, instalaciones de procesamiento de información y los sistemas que afecten la seguridad de la información.
A.12.1.3	Gestión de la capacidad	Control: Se debe supervisar y adaptar el uso de los recursos, y se deben hacer proyecciones de los futuros requisitos de capacidad para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los ambientes de desarrollo, prueba y operacionales	Control: Los ambientes para desarrollo, prueba y operación se deben separar para reducir los riesgos de acceso no autorizado o cambios al ambiente de operación.
A.12.2 Protección contra código malicioso		
Objetivo: Asegurar que la información y las instalaciones de procesamiento de información están protegidas contra el código malicioso.		
A.12.2.1	Controles contra código malicioso.	Control: Se deben implantar controles de detección, prevención y recuperación para protegerse contra códigos maliciosos, junto con los procedimientos adecuados para concientizar a los usuarios.
A.12.3 Respaldo		
Objetivo: Proteger en contra de la pérdida de datos.		
A.12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo y pruebas de la información, del software y de las imágenes del sistema con regularidad, de acuerdo con la política de respaldo acordad.
A.12.4 Registro y monitoreo		
Objetivo: Registrar eventos y generar evidencia.		
A.12.4.1	Registro de evento	Control: Se deben generar, mantener y revisar con regularidad los registros de eventos de las actividades del usuario, excepciones, faltas y eventos de seguridad de la información.

A.12.4.2	Protección de la información de registros	Control: Las instalaciones de registro y la información de registro se deben proteger contra alteraciones y accesos no autorizados.
A.12.4.3	Registros del administrador y el operador	Control: Se deben registrar las actividades de operador y del administrador del sistema, los registros se deben proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	Control: Los relojes de todos los sistemas de procesamiento de información pertinente dentro de una organización o dominio de seguridad deben estar sincronizados a una sola fuente horaria de referencia. (NTP).
A.12.5 Control de software de operación		
Objetivo: Asegurar la integridad de los sistemas operacionales		
A.12.5.1	Instalación del software en sistemas operacionales	Control: Se deben implementar los procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.6 Gestión de vulnerabilidad técnica		
Objetivo: Evitar la explotación de las vulnerabilidades técnicas.		
A.12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener la información acerca de las vulnerabilidades técnicas de los sistemas de información usados se debe obtener de manera oportuna, evaluar la exposición de la organización a estas vulnerabilidades y se deben tomar las medidas apropiadas para abordar el riesgo asociado.
A.12.4.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas que rigen la instalación de software por parte de los usuarios.
A.12.7 Consideraciones de la auditoria de los sistemas de información		
Objetivo: Minimizar el impacto de las actividades de auditoria en los sistemas operacionales.		
A.12.7.1	Controles de auditoria de	Control: Los requisitos y las actividades de

	sistemas de información	auditoria que involucran verificaciones de los sistemas operacionales se deben planificar y acordar cuidadosamente para minimizar el riesgo de interrupciones en los procesos del negocio.
A.13 Seguridad de las comunicaciones		
A.13.1 Gestión de la seguridad de red		
Objetivo: Asegurar la protección de la información en las redes y sus instalaciones de procesamiento de información de apoyo.		
A.13.1.1	Controles de red	Control: Las redes se deben gestionar y controlar para proteger la información en los sistemas y aplicaciones.
A.13.1.2	Seguridad de los servicios de red	Control: Los mecanismos de seguridad, los niveles del servicio y los requisitos de la gestión de todos los servicios de red se deben identificar e incluir en los acuerdos de servicios de red, ya sea que estos servicios son prestados dentro de la organización o por terceros.
A.13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en redes.
A.13.2 Transferencia de información		
Objetivo: Mantener la seguridad de la información transferida dentro de una organización y con cualquier entidad externa.		
A.13.2.1	Políticas y procedimientos de transferencia de información	Control: Las políticas, procedimientos y controles de transferencia formal deben estar en efecto para proteger la transferencia de la información mediante el uso de todos los tipos de instalaciones de comunicación.
A.13.2.2	Acuerdos sobre transferencia de información	Control: Los acuerdos deben abarcar la transferencia segura de la información de negocio entre la organización y terceros.
A.13.2.3	Mensajería electrónica	Control: La información involucrada en la

		mensajería electrónica debe ser debidamente protegida.
A.13.2.4	Acuerdos de confidencialidad o no divulgación	Control: Se deben identificar y revisar regularmente los requisitos de confidencialidad o acuerdos de no divulgación que reflejan las necesidades de protección de la información de la organización.
A.14 Adquisición, desarrollo y mantenimiento del sistema		
A.14.1 Requisitos de seguridad de los sistemas de información.		
Objetivo: Asegurar que la seguridad de la información es parte integral de los sistemas de información en todo el ciclo. Esto también incluye los requisitos para los sistemas de información que proporcionan servicio en las redes públicas.		
A.14.1.1	Análisis y especificaciones de requisitos de seguridad de la información	Control: Los requisitos relacionados a la seguridad de la información deben ser incluidos en los requisitos para los sistemas de información nuevos o las mejoras para los sistemas de información existentes.
A.14.1.2	Aseguramiento de servicios de aplicación en redes públicas	Control: La información relacionada a servicios de aplicación que pasan por redes públicas debe ser protegida de la actividad fraudulenta, disputas contractuales y su divulgación y modificación no autorizada.
A.14.1.3	Protección de las transacciones de servicios de aplicación	Control: La información implicada en transacciones de servicio de aplicación se debe proteger para evitar la transmisión incompleta, la omisión de envió, la alteración no autorizada del mensaje, la divulgación no autorizada, la duplicación o repetición no autorizada del mensaje.
A.14.2 Seguridad en procesos de desarrollo y soporte		
Objetivo: Asegurar que la seguridad de la información está diseñada e implementada dentro del ciclo de desarrollo de los sistemas de información.		

A.14.2.1	Política de desarrollo seguro	Control: Las reglas para el desarrollo de software y de sistemas deben ser establecidas y aplicadas a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios del sistema	Control: Los cambios a los sistemas dentro del ciclo de desarrollo deben ser controlados mediante el uso de procedimientos formales de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de los cambios en la plataforma de operación	Control: Cuando se cambien las plataformas de operación, se deben revisar y poner a prueba las aplicaciones críticas del negocio para asegurar que no hay impacto adverso en las operaciones o en la seguridad de la organización.
A.14.2.4	Restricciones en los cambios a los paquetes de software	Control: Se debe desalentar la realización de modificaciones a los paquetes de software, que se deben limitar a los cambios necesarios, los que deben ser controlados de manera estricta.
A.14.2.5	Principios de ingeniería de sistema seguro	Control: Se deben establecer, documentar, mantener y aplicar los principios para los sistemas seguros de ingeniería para todos los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema.
A.14.2.6	Entorno de desarrollo seguro	Control: Las organizaciones deben establecer y proteger los entornos de desarrollo seguro, de manera apropiada, para el desarrollo del sistema y los esfuerzos de integración que cubren todo el ciclo de desarrollo del sistema.
A.14.2.7	Desarrollo externalizado	Control: La organización debe supervisar y monitorear la actividad del desarrollo del sistema externalizado.
A.14.2.8	Prueba de seguridad del sistema	Control: Durante el desarrollo se debe realizar la prueba de funcionalidad de seguridad.

A.14.2.9	Prueba de aprobación del sistema	Control: Se deben definir los programas de prueba de aceptación y los criterios pertinentes para los nuevos sistemas de información, actualizaciones y versiones nuevas.
A.14.3 Datos de prueba		
Objetivo: Asegurar la protección de los datos usados para prueba		
A.14.3.1	Protección de datos de prueba	Control: Los datos de prueba se deben seleccionar, proteger y controlar de manera muy rigurosa.
A.15 Relaciones con el proveedor		
A.15.1 Seguridad de la información en las relaciones con el proveedor.		
Objetivo: Asegurar la protección de los activos de la organización a los que tienen acceso los proveedores		
A.15.1.1	Política de seguridad de la información para las relaciones con el proveedor	Control: Se deben acordar y documentar, junto con el proveedor, los requisitos de seguridad de la información para mitigar los riesgos asociados al acceso de proveedor a los activos de la organización.
A.15.1.2	Abordar la seguridad dentro de los acuerdos del proveedor	Control: Todos los requisitos de seguridad de la información pertinente, deben ser definidos y acordados con cada proveedor que pueda acceder, procesar, almacenar, comunicar o proporcionar componentes de infraestructura de TI para la información de la organización.
A.15.1.3	Cadena de suministro de tecnologías de la información y comunicaciones	Control: Los acuerdos con los proveedores deben incluir los requisitos para abordar los riesgos de seguridad de la información y las comunicaciones y la cadena de suministro del producto.
A.15.2 Gestión de entrega del servicio del proveedor		
Objetivo: mantener un nivel acordado de seguridad de la información y entrega del servicio, en línea con acuerdos del proveedor.		
A.15.2.1	Supervisión de revisión	Control: Las organizaciones deben supervisar,

	de los servicios del proveedor	revisar y auditar la entrega del servicio del proveedor.
A.15.2.2	Gestión de cambios a los servicios del proveedor	Control: Se deben gestionar los cambios al suministro de los servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas de seguridad de la información existentes, procedimientos y controles al considerar la criticidad de la información del negocio, los sistemas y procesos involucrados y la reevaluación de los riesgos.
A.16 Gestión de incidentes de seguridad de la información		
A.16.1 Gestión de incidentes de seguridad de la información y mejoras		
Objetivo: Asegurar un enfoque consistente y eficaz sobre la gestión de los incidentes de seguridad de la información incluida la comunicación sobre eventos de seguridad y debilidades.		
A.16.1.1	Responsabilidades y procedimientos	Control: Se deben establecer responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y metódica a los incidentes de seguridad de la información.
A.16.1.2	Informe de eventos de seguridad de la información	Control: Se deben informar, lo antes posible, los eventos de seguridad de la información mediante canales de gestión apropiados.
A.16.1.3	Informe de las debilidades de seguridad de la información	Control: Se debe requerir que los empleados y contratistas que usen los sistemas y servicios de información de la organización, observen e informen cualquier debilidad de la seguridad de la información en los sistemas o servicios, observada o que se sospeche.
A.16.1.4	Evaluación y decisión sobre los eventos de seguridad de la información	Control: Los eventos de seguridad de la información se deben evaluar y decidir si van a ser clasificados como incidentes de seguridad de la información.

A.16.1.5	Respuesta ante incidentes de seguridad de la información	Control: Los incidentes de seguridad de la información deben ser atendidos de acuerdo a los procedimientos documentados.
A.16.1.6	Aprendizaje de los incidentes de seguridad de la información	Control: Se debe utilizar el conocimiento adquirido al analizar y resolver incidentes de seguridad de la información para reducir la probabilidad o el impacto de incidentes futuros.
A.16.1.7	Recolección de evidencia	Control: La organización debe definir y aplicar los procedimientos para la identificación, recolección, adquisición y conservación de información, que pueda servir de evidencia.
A.17 Aspectos de seguridad de la información en la gestión de la continuidad del negocio		
A.17.1 Continuidad de la seguridad de la información		
Objetivo: Incorporar la continuidad de la seguridad de la información en los sistemas de gestión de continuidad de negocio de la organización.		
A.17.1.1	Planificación de la continuidad de la seguridad de la información.	Control: La organización debe determinar sus requerimientos de seguridad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, por ejemplo, durante una crisis o desastre.
A.17.1.2	Implementación de la continuidad de la seguridad de la información	Control: La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel necesario de continuidad para la seguridad de la información durante una situación adversa.
A.17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Control: La organización debe verificar, de manera periódica, los controles continuidad de la seguridad de la información definida e implementada para asegurar que son válidos y eficaces durante situaciones adversas.
A.17.2 Redundancias		

Objetivo: Asegurar la disponibilidad de las instalaciones de procesamiento de la información.		
A.17.2.1	Disponibilidad de las instalaciones de procesamiento de la información	Control: Las instalaciones de procesamiento de la información deben ser implementadas con la redundancia para suficiente para cumplir con los requisitos de disponibilidad.
A.18 Cumplimiento		
A.18.1 Cumplimiento con los requisitos legales y contractuales		
Objetivo: Evitar incumplimientos de las obligaciones legales, estatutarias, regulatorias o contractuales relacionadas con la seguridad de la información y todos los requisitos de seguridad.		
A.18.1.1	Identificación de la legislación vigente y los requisitos contractuales	Control: Todos los requisitos estatutarios, regulatorios y contractuales pertinentes y el enfoque de la organización para cumplirlos, se deben definir y documentar explícitamente y mantenerlos actualizados para cada sistema de información y para la organización.
A.18.1.2	Derechos de propiedad intelectual	Control: Se deben implementar procedimientos apropiados para asegurar el cumplimiento del os requisitos legislativos, regulatorios y contractuales relacionados a los derechos de propiedad intelectual y al uso de productos de software patentados.
A.18.1.3	Protección de los registros	Control: Los registros se deben proteger contra perdida, destrucción, falsificación, acceso sin autorización y emisión sin autorización, de acuerdo con los requisitos legislativos, regulatorios, contractuales y del negocio.
A.18.1.4	Privacidad y protección de la información de identificación personal	Control: Se debe asegurar la privacidad y protección de la información de identificación personal, como se exige en la legislación y regulaciones pertinentes, donde corresponda.
A.18.1.5	Regulación de los	Control: Se deben utilizar controles

Anexo 3: Autodiagnóstico del área de redes, infraestructura y telecomunicaciones

El autodiagnóstico de seguridad del área de redes, infraestructura y telecomunicaciones se realizó en base a los mecanismos de seguridad que establece la norma ISO/IEC 27001:2013.

En este autodiagnóstico participo el personal del área de redes, infraestructura y telecomunicaciones del GAD Municipal.

	controles criptográficos	criptográficos que cumplan con todos los acuerdos, leyes y regulaciones pertinentes.
A.18.2 Revisiones de seguridad de la información		
Objetivo: Asegurar que la seguridad de la información se implemente y funcione de acuerdo a las políticas y procedimientos de la organización.		
A.18.2.1	Revisión independiente de la seguridad de la información	Control: El enfoque de la organización para la gestión de la seguridad de la información y su implementación, es decir, objetivos de control, controles, políticas, procesos y procedimientos para seguridad de la información) se debe revisar en forma independiente, a intervalos planificados, o cuando ocurran cambios significativos.
A.18.2.2	Cumplimiento con las políticas y normas de seguridad.	Control: Los gerentes deben revisar con regularidad el cumplimento del procedimiento y los procedimientos de seguridad que están dentro de su área de responsabilidad, de acuerdo con las políticas de seguridad, normas y otros requisitos de seguridad pertinentes.
A.18.2.3	Verificación del cumplimiento técnico	Control: Se deben verificar regularmente los sistemas de información en cuanto a su cumplimiento con las políticas y normas de seguridad de la información de la organización.

POLÍTICAS DE SEGURIDAD (A5)

- Existen documento(s) de políticas de seguridad de la información ☐
- Existe normativa relativa a la seguridad de la información ☐
- Existen procedimientos relativos a la seguridad de la información ☐
- Existe un responsable de las políticas, normas y procedimientos ☐
- Existen mecanismos para la comunicación a los usuarios de las normas. ☐
- Existen controles regulares para verificar la efectividad de las políticas ☐

ORGANIZACIÓN DE LA SEGURIDAD (A6)

- Existen roles y responsabilidades definidos para las personas implicadas en la seguridad ☐
- Existe un responsable encargado de evaluar la adquisición y cambios de seguridad de la información ☐
- La Dirección y las áreas de la Organización participa en temas de seguridad ☐
- Existen condiciones contractuales de seguridad con terceros y subcontratación (outsourcing) ☐
- Existen criterios de seguridad para la gestión de proyectos ☐
- Existen programas de formación en seguridad para los empleados, clientes y terceros ☐
- Existe un acuerdo de confidencialidad de la información que se accesa. ☐
- Se revisa la organización de la seguridad periódicamente por una empresa externa ☐

- Existen políticas de seguridad para el uso de dispositivos móviles ☐

SEGURIDAD DE LOS RRHH (A7)

- Se tienen definidas responsabilidades y roles de seguridad ☐
- Se tiene en cuenta la seguridad en la selección y baja del personal ☐
- Se plasman las condiciones de confidencialidad y responsabilidades en los contratos ☐
- Se imparte la formación adecuada de seguridad y tratamiento de activos ☐
- Existe un canal y procedimientos claros a seguir en caso de incidente de seguridad ☐
- Se recogen los datos de los incidentes de forma detallada ☐
- Informan los usuarios de las vulnerabilidades observadas o sospechadas ☐
- Se informa a los usuarios de que no deben, bajo ninguna circunstancia, probar las vulnerabilidades ☐
- Existe un proceso disciplinario de la seguridad de la información ☐

ADMINISTRACIÓN DE ACTIVOS (A8)

- Existen un inventario de activos actualizado ☐
- El Inventario contiene activos de datos, software, equipos y servicios ☐
- Se dispone de una clasificación de la información según la criticidad de la misma ☐
- Existe un responsable de los activos ☐

- Existe un proceso para la devolución de los activos ☐
- Existen procedimientos para clasificar la información ☐
- Existen procedimientos de etiquetado de la información ☐
- Existen procedimientos de manejo de activos ☐
- Existen procedimientos para la gestión de los medios removibles ☐
- Existe un proceso para la eliminación de los medios ☐
- Existe un proceso para la transferencia física de los medios ☐

CONTROL DE ACCESOS (A9)

- Existe una política de control de accesos ☐
- Existe una revisión de acceso a la red y a sus servicios ☐
- Existe un procedimiento formal de registro y cancelación de usuarios ☐
- Existe un procedimiento de asignación de acceso de usuario ☐
- Existe una gestión de acceso privilegiado ☐
- Existe una gestión formal de la asignación de información de autenticación secreta ☐
- Existen políticas de revisión de los derechos de acceso ☐
- Existen políticas de ajuste o eliminación de los derechos de acceso ☐
- Existe una política de uso de información de autenticación secreta ☐
- Existe un procedimiento de inicio de sesión seguro ☐
- Existe un sistema de gestión de contraseñas ☐
- Se está controlando el uso de programas utilitarios ☐
- Está controlado el acceso al código fuente de los programas ☐

- Existe una autenticación de usuarios en conexiones externas ☐

CRIPTOGRAFÍA (A10)

- Existen controles criptográficos. ☐
- Existe políticas sobre las claves criptográficas ☐

SEGURIDAD FÍSICA Y DEL AMBIENTE (A11)

- Existe perímetro de seguridad física (una pared, puerta con llave). ☐
- Existen controles de entrada para protegerse frente al acceso de personal no autorizado ☐
- Un área segura ha de estar cerrada, aislada y protegida de eventos naturales ☐
- En las áreas seguras existen controles adicionales al personal propio y ajeno ☐
- Las áreas de carga y expedición están aisladas de las áreas de SI ☐
- La ubicación de los equipos está de tal manera para minimizar accesos innecesarios. ☐
- Existen protecciones frente a fallos en la alimentación eléctrica ☐
- Existe seguridad en el cableado frente a daños e intercepciones ☐
- Se asegura la disponibilidad e integridad de todos los equipos ☐
- Existe algún tipo de seguridad para los equipos retirados o ubicados exteriormente ☐
- Se incluye la seguridad en equipos móviles ☐
- Existe políticas de escritorio limpio ☐
- Existe políticas de pantalla limpia ☐

SEGURIDAD DE LAS OPERACIONES (A12)

- Todos los procedimientos operativos identificados en la política de seguridad han de estar documentados ☐
- Están establecidas responsabilidades para controlar los cambios en equipos ☐
- Están establecidas responsabilidades para supervisar y adaptar el uso de los recursos ☐
- Existen separación entre los ambientes de desarrollo, prueba y operación ☐
- Existen controles contra software maligno ☐
- Realizar copias de backup de la información esencial para el negocio ☐
- Existe registro de eventos ☐
- Se registra las actividades del operador y administrador ☐
- Se controla que los sistemas de procesamiento estén sincronizados a una sola fuente horaria ☐
- Existen procedimientos para controlar la instalación de software en los sistemas operacionales ☐
- Se controlan las vulnerabilidades de los equipos ☐
- Existen políticas para la instalación de software ☐
- Existen consideraciones sobre las auditorías de los sistemas ☐

SEGURIDAD DE LAS COMUNICACIONES (A13)

- Existe seguridad en las aplicaciones ☐
- Existe algún control en las redes ☐
- Existe una separación entre los servicios de información, usuarios y sistemas de información ☐

- Existen políticas de seguridad en la transferencia de información ☐
- Existen acuerdos para intercambio de información ☐
- Existen medidas de seguridad en la mensajería electrónica ☐
- Existen acuerdos de confidencialidad o no divulgación de la información ☐

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DEL SISTEMA (A14)

- Existen requisitos relacionados a la seguridad de la información ☐
- Existen seguridad para los servicios de aplicación en redes públicas ☐
- Existen medidas de seguridad en las transacciones en línea ☐
- Existen políticas de desarrollo de software ☐
- Existen procedimientos de control de cambios del sistema ☐
- Existen revisión técnica después de cambios en las plataformas de operación ☐
- Existen políticas de restricción para los cambios a los paquetes de software ☐
- Existe supervisión del desarrollo por parte de terceros ☐
- Existe seguridad en los ficheros de los sistemas ☐
- Existen políticas para la protección de datos ☐

RELACIONES CON EL PROVEEDOR (A15)

- Existen políticas de seguridad con el/los proveedores/es ☐
- Se han establecido los requisitos para abordar riesgos con los proveedores ☐

- Existen encargados de la supervisión de los servicios por parte de los proveedores ☐
- Existe una gestión para el cambio de proveedor ☐

SEGURIDAD DE LA INFORMACIÓN (A16)

- Están establecidas responsabilidades para asegurar una respuesta rápida, ordenada y efectiva frente a incidentes de seguridad ☐
- Existe algún método para reducir el mal uso accidental o deliberado de los sistemas ☐
- Existen contratistas externos para la gestión de los Sistemas de Información ☐
- Existe un Plan de Capacidad para asegurar la adecuada capacidad de proceso y de almacenamiento ☐
- Existen criterios de aceptación de nuevos SI, incluyendo actualizaciones y nuevas versiones ☐
- Existen los para las actividades realizadas por los operadores y administradores ☐
- Existen los de los fallos detectados ☐
- Hay establecidos controles para realizar la gestión de los medios informáticos. (cintas, discos, removibles, informes impresos) ☐
- Eliminación de los medios informáticos. Pueden disponer de información sensible ☐
- Existe seguridad de la documentación de los sistemas ☐
- Se han establecido e implantado medidas para proteger la confidencialidad e integridad de información publicada ☐

GESTIÓN DE INCIDENTES (A17)

- Se comunican los eventos de seguridad ☐
- Se comunican las debilidades de seguridad ☐
- Existe definidas las responsabilidades antes un incidente. ☐
- Existe un procedimiento formal de respuesta ☐
- Existe la gestión de incidentes ☐

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

- Existen procesos para la gestión de la continuidad. ☐
- Existe un plan de continuidad del negocio y análisis de impacto ☐
- Existe un diseño, redacción e implantación de planes de continuidad ☐
- Existe un marco de planificación para la continuidad del negocio ☐
- Existen prueba, mantenimiento y reevaluación de los planes de continuidad del negocio. ☐

CUMPLIMIENTO (A18)

- Se tiene en cuenta el cumplimiento con la legislación por parte de los sistemas ☐
- Existe el resguardo de la propiedad intelectual ☐
- Existe el resguardo de los registros de la organización ☐
- Existe una revisión de la política de seguridad y de la conformidad técnica ☐
- Existe una revisión de la política de conformidad técnica ☐

Fuente: (International Organization for Standardization, 2013)

Anexo 4: Entrevista al personal del área de redes, infraestructura y telecomunicaciones

Una vez establecidas las medidas de seguridad con las que se cuenta por medio del autodiagnóstico (Anexo 2), se realizó la entrevista para determinar de qué manera se están efectuando. Esta fue ejecutada a diferentes personas del área de redes, infraestructura y telecomunicaciones dependiendo de la información requerida.

1. ¿Cuál es la estructura de la red LAN?

2. ¿Cuál es la velocidad de trasmisión de los servidores?

3. ¿Cómo está formado el Data Center?

4. ¿Dónde se encuentra ubicado el Data Center?

5. ¿Quién tiene acceso al Data Center?

6. ¿Qué medidas de seguridad existen para el Data Center?

7. ¿Se documentan los cambios realizados en el Data Center?

   ☐ SI
   ☐ NO

8. ¿Existe un procedimiento formal para la recuperación de respaldos?

   ☐ SI
   ☐ NO

9. ¿Cuántas estaciones de trabajo existen en el área de redes, infraestructura y telecomunicaciones?

   _____
   _____
   _____
   _____
   _____

10. ¿Cuáles son las características de cada estación de trabajo?

    _____
    _____
    _____
    _____
    _____

11. ¿Existen impresoras conectadas, cuantas?

    _____
    _____
    _____
    _____
    _____

12. ¿Cómo se maneja el correo electrónico?

    _____
    _____
    _____
    _____
    _____

13. ¿Qué tipo de antivirus se utiliza?

    _____
    _____
    _____
    _____
    _____

14. ¿Cuál es el control presente en la red?

    _____
    _____

15. ¿Qué herramientas existen para contrarrestar el ataque a la red?

16. ¿Cómo se manejan y almacenan las contraseñas?

17. ¿Cómo se maneja la seguridad en la base de datos?

18. ¿Cuál es el procedimiento para la instalación de aplicaciones?

19. ¿Cómo se maneja el control de acceso a los equipos?

20. ¿Existe aire acondicionado en el Data Center? ¿A qué temperatura?

21. ¿Existe un UPS, cual es el tiempo de duración?

_____
_____
_____
_____
_____

22. ¿Existe descarga a tierra?

- ☐ SI
- ☐ NO

23. ¿Cómo se realizó el cableado estructurado?

_____
_____
_____
_____
_____

24. ¿Quién es responsable de los equipos?

_____
_____
_____
_____
_____

25. ¿Cómo se realiza el mantenimiento a los equipos?

_____
_____
_____
_____
_____

26. ¿Existe rotulación en los equipos?

- ☐ SI
- ☐ NO

27. ¿Cómo se encuentran los instaladores?

_____
_____
_____
_____
_____

28. ¿Con que licencias cuentan?

_____
_____
_____

29. ¿Cómo se realiza el respaldo en los servidores?

30. ¿Se realiza respaldo a la información de los equipos?

31. ¿Cuál es la documentación con la que cuentan actualmente?

32. ¿Quién es el responsable de las políticas, normas y procedimientos?

33. ¿Cuál es el mecanismo para la comunicación a los usuarios?

34. ¿Quién tiene acceso al inventario de activos?

35. ¿Cuál es la persona responsable de los activos?

36. ¿Cómo se maneja el proceso de devolución de los activos?

37. ¿Cuáles son los procedimientos para el manejo de activos?

38. ¿Cuál es la política para el control de acceso a la información?

39. ¿Cuál es el procedimiento de registro y cancelación de usuario?

40. ¿Cuál es el control contra software maligno?

41. ¿Cómo se realiza el registro de eventos?

42. ¿Cuál es la política para la instalación de software?

43. ¿Cómo se determinan los acuerdos de intercambio de información?

44. ¿Cuál es la medida de seguridad para las transacciones en línea?

45. ¿Cuál es la política de seguridad para los proveedores?

46. ¿Cuáles son los encargados de la supervisión a los proveedores?

47. ¿Cómo se maneja los logs para las actividades realizadas por os operadores?

48. ¿Cómo se maneja los logs para fallos detectados?

49. ¿Cómo se comunican los eventos de seguridad?

_____
_____
_____
_____
_____

50. ¿Qué proceso existe para la gestión de la continuidad?

_____
_____
_____
_____
_____

Anexo 5: Plan del proyecto

ÁREA DE REDES, INFRAESTRUCTURA Y TELECOMUNICACIONES DEL GAD MUNICIPAL

PLAN DEL PROYECTO
PARA LA IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Código	
Versión:	001
Fecha de la versión:	09 de noviembre de 2015
Creado por:	Mabel Ochoa
Aprobado por:	
Nivel de confidencialidad:	Bajo

Historial de modificaciones

Fecha	Versión	Creado por	Descripción de la modificación

Tabla de contenido

1. Objetivo, alcance y usuarios

El objetivo del Plan del proyecto es definir claramente el propósito del proyecto de implementación del Sistema de Gestión de Seguridad de la Información (SGSI), las funciones y responsabilidades del proyecto y los documentos que se redactarán.

El Plan del proyecto se aplica a todas las actividades realizadas en el proyecto de implementación del SGSI.

Los usuarios de este documento son la dirección del departamento de Informática, los miembros del área de redes, infraestructura y telecomunicaciones del GAD Municipal y los miembros del equipo del proyecto que implementa el SGSI.

2. Documentos de referencia

- Norma ISO/IEC 27001
- Norma ISO 22301
- Norma BS 25999-2

3. Abreviaturas

ISO: International Standarization Organization (Organización Internacional de Estandarización)

SGSI: Sistema de Gestión de Seguridad de la Información

IEC: International Electrotechnical Commission (Comisión Electrotécnica Internacional)

4. Proyecto de implementación del SGSI

4.1 Objetivo del proyecto

Determinar los requisitos necesarios para implementar un Sistema de Gestión de Seguridad de la Información en conformidad con la norma ISO 27001:2013.

4.2 Resultados del proyecto

Durante el proyecto de implementación del SGSI, se debe redactar algunos documentos de gran importancia para cumplir con la norma ISO/IEC 27001:2013.
Los documentos de carácter obligatorio para la certificación son:

Documentos	**Capítulo de ISO 27001:2013**
Alcance del SGSI	4.3
Políticas y objetivos de seguridad de la información	5.2, 6.2
Metodología de evaluación y tratamiento	6.1.2

de riesgos	
Declaración de aplicabilidad	6.1.3 d)
Plan de tratamiento del riesgo	6.1.3 e), 6.2
Informe de evaluación de riesgos	8.2
Definición de funciones y responsabilidades de seguridad	A.7.1.2, A.13.2.4
Inventario de activos	A.8.1.1
Uso aceptable de los activos	A.8.1.3
Política de control de acceso	A.9.1.1
Procedimientos operativos para gestión de TI	A.12.1.1
Principios de ingeniería para sistema seguro	A.14.2.5
Política de seguridad para proveedores	A.15.1.1
Procedimiento para gestión de incidentes	A.16.1.5
Procedimientos de la continuidad del negocio	A.17.1.2
Requisitos legales, normativos y contractuales	A.18.1.1
Registros de capacitación, habilidades, experiencia y calificaciones	7.2
Resultados de supervisión y medición	9.1
Programa de auditoría interna	9.2

Dentro de este proyecto se redactarán los siguientes documentos, algunos de los cuales contienen apéndices mencionados a continuación:

Documento sobre el alcance del SGSI: Define el alcance del SGSI considerando los procesos, funciones, activos, ubicaciones físicas, tecnología, partes interesadas y la determinación de los aspectos internos y externos al área.

Política de Seguridad de la Información: define la forma en la que la dirección controla la gestión de la seguridad de la información.

Metodología de evaluación y tratamiento de riesgos: Describe en un documento la metodología para gestionar los riesgos de la información.

Anexo 7: Cuadro de evaluación de riesgos

Anexo 8: Cuadro de tratamiento de riesgos

Anexo 9: Informe sobre evaluación y tratamiento de riesgos

Declaración de aplicabilidad: Es un documento que determina los objetivos y la aplicabilidad de cada control establecido en el Anexo A de la norma ISO 27001:2013.

Plan de tratamiento del riesgo: Es un documento donde se detallan los controles de seguridad adecuados para cada riesgo inaceptable de tal forma que se evidencia su tratamiento.

Se pueden excluir los controles del Anexo A si se determina que no existen riesgos ni otros requisitos que podrían demandar la implementación de un control.

Anexo 12: Lineamiento de implementación

4.3 Plazos

El plazo para la entrega será determinado de acuerdo a las condiciones del área.

4.4 Organización del proyecto

4.4.1 Promotor:

El gerente del proyecto debe comunicar al promotor el estado del proyecto. El promotor no participa activamente en el proyecto, pero debe actuar si este se encuentra detenido.

Promotor: Ing. Marco Paul Timbi

4.4.2 Gerente:

El gerente es el encargado de llevar a cabo el proyecto garantizando los recursos necesarios para llevar acabo la implementación, informando al promotor sobre el avance del proyecto.

Gerente del Proyecto: Mabel Ochoa

4.4.3 Equipo:

El equipo es el encargado de participar en la implementación del proyecto tanto en la toma de decisiones del SGSI como en la ejecución de las tareas planificadas.

Equipo del Proyecto: Personal del área de redes, infraestructura y telecomunicaciones.

4.5 Principales Riesgos del Plan

- Ampliación de los plazos en los entregables
- Cambios en los miembros del equipo del proyecto

- Inoportuna definición del alcance
- Selección de excesivos controles
- Falta de compromiso del equipo del proyecto
- Falta de recursos asignados al proyecto
- Luego de trascurrido el tiempo de validez del proyecto, no se tome la decisión para su implantación.

4.6 Herramientas para implementación del proyecto y generación de informes

- Se debe crear un contenedor de los documentos del SGSI que permita establecer una carpeta compartida con todos los documentos generados durante el proyecto.
- Sólo el gerente del proyecto y miembros del equipo del proyecto estarán autorizados a realizar modificaciones y a borrar archivos.
- Checklist
- Documentos existentes en la organización.

5. Gestión de registros guardados en base a este documento

Nombre del registro	Ubicación de archivo	Persona responsable del archivo	Controles para la protección del registro	Tiempo de retención
Informes parciales de la Implementación del proyecto	Archivos SGSI 27001 GAD Municipal	El gerente del proyecto	El gerente del proyecto y miembros del equipo del proyecto estarán autorizados a realizar modificaciones y a borrar archivos.	Los datos son archivados por un plazo determinado
Incidencias de cambios o mejoras al proyecto	Archivos SGSI 27001 GAD Municipal	El gerente del proyecto	El gerente del proyecto y miembros del equipo del proyecto estarán autorizados a realizar modificaciones y a borrar archivos.	Los datos son archivados por un plazo determinado

6. Validez y gestión de documentos

Este documento es válido mientras no exista una actualización de la normativa.

El propietario de este documento es la Directora del departamento de informática, que debe verificar y si es necesario actualizar el documento por lo menos una vez al año, antes de la revisión del SGSI.

Al evaluar la efectividad y adecuación de este documento, es necesario tener en cuenta los siguientes criterios:

- Viabilidad
- Aplicabilidad
- Resultados

7. Firmas

Elaborado por:

Mabel Catherine Ochoa Quezada
Gerente Proyecto

Aprobado por:

Ing. Ximena Barrera
Directora del Departamento de Informática

Ing. Marco Paul Timbi
Promotor