DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE INFORMÁTICA DE LA COOPERATIVA DEL MAGISTERIO DE TÚQUERRES BAJO LA NORMA ISO 27001:2013

DUBAN OSWALDO PALACIOS PORTILLA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2015

DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA EL ÁREA DE INFORMÁTICA DE LA COOPERATIVA DEL MAGISTERIO DE TÚQUERRES BAJO LA NORMA ISO 27001:2013

DUBAN OSWALDO PALACIOS PORTILLA

Tesis de grado para optar el título de:
Especialista En Seguridad Informática

Director de Proyecto:
Ing. Erika Liliana Villamizar Torres

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SAN JUAN DE PASTO
2015

Nota de Aceptación:

_____
_____
_____
_____
_____
_____

_____
Firma del Presidente del Jurado

_____
Firma del Jurado

_____
Firma del Jurado

Bogotá, 29 de Octubre de 2015

DEDICATORIA

Dedico mi trabajo a todas las personas que siempre han estado conmigo brindándome su apoyo, principalmente a Dios, a mi madre y a mis seres queridos que de una u otra forma han aportado un granito de arena para que esta gran meta se plasme en una realidad.

Dios los bendiga.

DUBAN OSWALDO PALACIOS PORTILLA

AGRADECIMIENTOS

Agradezco a toda la comunidad académica de la UNAD por difundir el conocimiento necesario para el éxito de mi desempeño tanto laboral como profesional.

Muchas gracias a todos…

DUBAN OSWALDO PALACIOS PORTILLA

CONTENIDO

		Página
INTRODUCCIÓN		11
1.	PROBLEMA DE INVESTIGACIÓN	13
1.1	OBJETO O TEMA DE ESTUDIO	13
1.2	ÁREA DE INVESTIGACIÓN	13
1.3	LÍNEA DE INVESTIGACIÓN	13
1.4	DESCRIPCIÓN DEL PROBLEMA	13
1.5	FORMULACIÓN DEL PROBLEMA	15
2.	ALCANCE Y DELIMITACIÓN DEL PROYECTO	16
3.	JUSTIFICACIÓN	17
4.	OBJETIVOS	19
4.1	OBJETIVO GENERAL	19
4.2	OBJETIVOS ESPECÍFICOS	19
5.	MARCO REFERENCIAL	20
5.1	ANTECEDENTES	20
5.2	MARCO TEÓRICO	22
5.2.1	Activo de información	22
5.2.2	Amenazas informáticas	22
5.2.3	Seguridad informática	23

5.2.4 Seguridad de la información 24
5.2.5 Análisis de riesgos 24
5.2.6 Sistema de gestión de seguridad de la información 25
5.2.7 MAGERIT 29
5.2.8 Familia de normas ISO 27000 29
5.2.9 Norma ISO/IEC 27001:2013 31
5.2.10 Políticas de seguridad de la información 32
5.3 MARCO CONCEPTUAL 33
5.3.1 Seguridad 33
5.3.2 Estándares de seguridad 33
5.3.3 Modelo de seguridad 33
5.4 MARCO LEGAL 33
5.4.1 Estatuto Coacremat 35
5.4.2 Acuerdo No. 089 – Coacremat 36
5.5 MARCO CONTEXTUAL 37
5.5.1 Área de sistemas 40
5.5.1.1 Jefe Área de sistemas 40
5.5.1.2 Profesional Área de sistemas 40
5.5.1.3 Infraestructura tecnológica 41
5.5.1.4 Política de manejo de los computadores 41
6. DISEÑO METODOLÓGICO 42
7. NOMBRE INTEGRANTES DEL PROCESO 43

8. RECURSOS 44

8.1 TALENTO HUMANO 44

8.2 RECURSOS FISICOS 44

8.3 PRESUPUESTO 44

9. CRONOGRAMA DE ACTIVIDADES 45

10. DESARROLLO DEL PROYECTO 46

10.1 CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN 46

10.1.1 Activos de información 46

10.1.2 Infraestructura física 49

10.1.3 Infraestructura informática 49

10.2 AMENAZAS A LAS QUE ESTÁN EXPUESTOS LOS ACTIVOS DE INFORMACIÓN DEL ÁREA DE SISTEMAS DE LA COOPERATIVA DEL MAGISTERIO DE TÚQUERRES 58

10.3 ANÁLISIS ANEXO A DE LA NORMA EN LA INFORMACIÓN RECOLECTADA 90

10.3.1 Aplicabilidad en Dominios, Objetivos de control y Controles acorde a la norma ISO 27001:2013 90

10.4 PLAN DE IMPLEMENTACIÓN 111

10.4.1 Liderazgo y compromiso 111

10.4.2 Política 112

10.4.3 Procedimientos de seguridad 114

10.4.4 Roles y responsabilidades 116

10.4.5 Planificación 116

10.4.5.1 Valoración de riesgos de la seguridad de la información 116

10.4.5.2 Plan de tratamiento de riesgos 117
10.4.6 Objetivos de seguridad de la información 117
10.4.7 Soporte 118
10.4.7.1 Recursos 118
10.4.7.2 Competencia 118
10.4.8 Toma de conciencia 118
10.4.9 Comunicación 119
10.4.10 Evaluación del desempeño 119
10.4.10.1 Seguimiento, medición, análisis y evaluación 119
10.4.10.2 Auditoria interna 120
10.4.10.3 Revisión por la dirección 120
10.4.11 Mejora 121
10.4.11.1 No conformidades y acciones correctivas 121
10.4.11.2 Mejora continua 122
11. CONCLUSIONES 123
12. RECOMENDACIONES 124
BIBLIOGRAFÍA 126

LISTA DE TABLAS

Página

Tabla 1. Responsables del proyecto 43

Tabla 2. Clasificaciones de seguridad 46

Tabla 3. Escala de valoración de rango porcentual de impacto en los activos 47

Tabla 4. Clasificación de activos de información 47

Tabla 5. Valoración para los activos 50

Tabla 6. Criterio de valoración de activos 51

Tabla 7. Dimensiones de los riesgos 51

Tabla 8. Dimensiones de valoración del impacto 52

Tabla 9. Amenazas 53

Tabla 10. Escala de rango de frecuencia de amenazas 57

Tabla 11. Amenazas para los activos de información 58

Tabla 12. Controles identificados 90

Tabla 13. Políticas propuestas 112

Tabla 14. Procedimientos de seguridad 115

LISTA DE FIGURAS

	Página
Figura 1. Ciclo PHVA	28
Figura 2. Organigrama	39
Figura 3. Misión y objetivos del área de sistemas	40

INTRODUCCIÓN

Con el avance que en los últimos años ha tenido la computación y los sistemas a nivel global, cada día se hace más intensivo el manejo y la manipulación de la información, lo cual ha generado muchos beneficios para la sociedad, es tal que hoy en día muchas organizaciones han incursionado a las nuevas tecnologías de la información mejorando su operatividad y servicio, permitiendo así un desarrollo integral en la sociedad, brindando manejo de información de forma oportuna, creando procesos más eficientes y productivos entre otros, por lo cual se puede decir que es imprescindible la seguridad de la información en los entornos organizacionales.

Es por esto, que la Cooperativa del Magisterio de Túquerres busca implementar políticas, métodos y mecanismos que permitan salvaguardar el activo más importante que puede tener una organización hoy en día; la información. La cual es de vital importancia para el éxito y cumplimiento de los objetivos propuestos a corto y largo plazo.

Ante esta situación y aprovechando la infraestructura tecnológica disponible, se propone diseñar un sistema de gestión de seguridad de la información que permita conocer, gestionar y minimizar los posibles riesgos que atenten contra la seguridad de la información en la empresa, para lo cual se deberán establecer mecanismos alineados a la norma ISO 27001:2013 que ayuden a mantener controlado el riesgo al que se expone la integridad de la información diariamente no solo desde el exterior de la empresa, sino también desde el interior.

1. PROBLEMA DE INVESTIGACIÓN

1.1 OBJETO O TEMA DE ESTUDIO

Diseñar un sistema de gestión de seguridad de la información para el área de informática de la Cooperativa del Magisterio de Túquerres - Coacremat Ltda., bajo la norma ISO 27001:2013.

1.2 ÁREA DE INVESTIGACIÓN: CADENA DE FORMACIÓN EN SISTEMAS

El presente proyecto se inscribe dentro del área de formación en sistemas, específicamente en la línea de gestión en sistemas.

1.3 LÍNEA DE INVESTIGACIÓN: GESTIÓN EN SISTEMAS

Esta línea de investigación ha sido escogida teniendo en cuenta que el proyecto a realizar comprende políticas, gestión y métodos para la seguridad de la información de la cooperativa, es importante resaltar que la seguridad informática comprende software, bases de datos, metadatos, archivos y todo lo que la organización valore (activo) y signifique un riesgo si ésta llega a perderse o a manos de personas no autorizadas. Garantizando así la confidencialidad, disponibilidad, integridad y autenticidad de la información.

1.4 DESCRIPCIÓN DEL PROBLEMA

La situación actual de la Cooperativa del Magisterio de Túquerres en relación a la seguridad de la información es la siguiente:

En este momento se cuenta con un sistema de información bastante robusto, el cual proporciona diferentes y eficientes servicios a los usuarios del mismo,

desafortunadamente no cuenta con las políticas y mecanismos que ayuden a salvaguardar su integridad, disponibilidad y confidencialidad.

La Cooperativa del magisterio de Túquerres opera con un aproximado de 7.000 asociados y continúa en crecimiento, además es una de las cooperativas más importantes del departamento de Nariño, por lo tanto implica que deben tomarse medidas para evitar posibles riesgos que puedan llevar a perder uno de los activos más importantes para la organización, la información. Repercutiendo para la empresa en grandes pérdidas económicas, daño a su reputación y potencial de la misma.

Por tanto, es necesario establecer, priorizar y mantener contramedidas que ayuden a evitar desastres en la infraestructura informática y la información, en relación a lo anterior se evidencia lo siguiente:

- Se encuentra una red de datos obsoleta y desprotegida en algunas áreas.

- No se cuenta con un servidor espejo de restablecimiento en caso de un siniestro.

- La sala de servidores no cuenta con los estándares adecuados para su correcta operación.

- No se cuenta con políticas y métodos para la gestión de copias de seguridad.

- En algunas áreas no se cuenta con la seguridad física necesaria para evitar el posible robo y/o acceso no autorizado a la información.

- No se cuenta con planes de contingencia adecuados a la posible falla o interrupción del sistema.

- Falta de capacitación y concientización a los funcionarios y directivos con respecto a la seguridad informática.

- No se cuenta con planes de mantenimiento y actualización de hardware y software.

En general, la Cooperativa del Magisterio de Túquerres no cuenta con un sistema de gestión de seguridad de la información que le permita optimizar y proteger la integridad de la información que se gestiona diariamente. Por lo tanto el propósito de un sistema de gestión de seguridad de la información, es garantizar que los riesgos sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que puedan presentarse.

Por último se puede percibir que hoy en día la tecnología ha avanzado a pasos agigantados, al igual que las amenazas a la misma, es por eso que es necesario que las medidas preventivas también avancen, se controlen y se mantengan en la Cooperativa del Magisterio de Túquerres.

1.5 FORMULACIÓN DEL PROBLEMA

¿Cómo se pueden proteger los activos de información en el área de informática de la Cooperativa del Magisterio de Túquerres?

¿Cómo se pueden mitigar los riesgos asociados al uso de la información y los servicios informáticos brindados dentro del área de informática de la Cooperativa del Magisterio de Túquerres?

2. ALCANCE Y DELIMITACIÓN DEL PROYECTO

Este proyecto abarca el diseño de un sistema de gestión de seguridad de la información (SGSI) para el área de informática de la cooperativa del magisterio de Túquerres bajo la norma ISO 27001:2013, esto con el propósito de mejorar la confidencialidad, disponibilidad e integridad de la información manejada y procesada en la empresa.

Para diseñar el SGSI en el área de informática, se aplicará mecanismos apropiados que permitan detectar amenazas y riesgos existentes en la seguridad de los activos y la información, de la misma forma se evaluara la infraestructura física, los recursos humanos, la transferencia de información, las políticas de seguridad de la información y el control efectuado a los sistemas.

3. JUSTIFICACIÓN

El desarrollo avanzado de las comunicaciones y la tecnología ha sido fundamental para el progreso de la humanidad, es tanto así, que en estos tiempos es casi inconcebible que una organización (de cualquier índole) no tenga acceso a los servicios informáticos para poder llevar a cabo sus tareas y cumplir de la manera más eficiente sus objetivos. Por esta razón, los datos y la información se han vuelto el activo más importante e imprescindible de cualquier empresa en el mundo.

Toda la incursión de tecnología ha traído a las sociedades muchos beneficios pero de la misma forma también ha traído consigo amenazas y riesgos muy importantes que no se pueden descuidar, como es la manipulación, control, transmisión y demás operaciones que permitan conservar y mantener la integridad, confidencialidad, disponibilidad y no repudio de la información.

Por las razones expuestas anteriormente, se debe tener en cuenta que la protección a los datos y a la información debe ser una necesidad para todas las organizaciones sin importar el modelo o tamaño del negocio, esto debido a que es casi imprescindible contar hoy en día con políticas y mecanismos que protejan este activo, para lo cual es de gran importancia contar con un sistema de gestión de seguridad de la información adecuado a los requisitos y necesidades de la Cooperativa del Magisterio de Túquerres.

Así las cosas, el contexto de la información en la cooperativa debe ser salvaguardada y protegida de cualquier evento o siniestro que amenace o ponga en riesgo la inmediata respuesta a los usuarios internos o externos que requieran de la misma, ello supone que se debe crear políticas, mecanismos, planes y proyectos contingentes que mitiguen el impacto que pueda tener una entidad de esta categoría al presentar un desastre en sus activos de información.

De esta manera este proyecto busca mejorar la efectividad en todos los procesos que incursiona y se utiliza la información, tanto en lo administrativo, contable, operativo e incluso tecnológico que se presenta al interior y exterior de la organización, con el fin de mantener el riesgo para nuestra información por debajo del nivel asumible por la propia organización y así optimizar la calidad de los servicios que se prestan a todos los asociados y la sociedad en general.

4. OBJETIVOS

4.1 OBJETIVO GENERAL

Diseñar un sistema de gestión de la seguridad de la información para la implementación bajo la norma ISO 27001:2013 en el área de informática de la Cooperativa del Magisterio de Túquerres – Coacremat Ltda.

4.2 OBJETIVOS ESPECÍFICOS

- Determinar los activos de información del área informática de la cooperativa del Magisterio de Túquerres y darles la clasificación de seguridad aplicable para cada uno.

- Determinar las amenazas a las que están expuestas los activos de información del área de sistemas de la Cooperativa del Magisterio de Túquerres.

- Realizar un análisis del estado actual de seguridad de la Cooperativa del Magisterio de Túquerres confrontarlo con los controles del anexo A de la norma ISO/IEC 27001:2013 y proponer las recomendaciones de seguridad a implementar para dar cumplimiento a la norma.

- Proponer el plan de implementación del sistema de seguridad de la información para el área informática.

5. MARCO REFERENCIAL

5.1 ANTECEDENTES

Este trabajo de grado ha tomado como referentes los siguientes proyectos a nivel nacional e internacional, con el fin de conocer las experiencias llevadas a cabo en diferentes ámbitos para la adecuada implementación de un sistema de gestión de seguridad de la información.

Título: **Sistema de gestión de seguridad de la información (SGSI) basado en la norma ISO 27001 y 27002 para la unidad de informática y telecomunicaciones de la Universidad de Nariño**

Autores de la investigación:

- YEZID CAMILO GUERRERO ANGULO
- ROBERT MARCELO TABANGO GOYES

Este trabajo busca mejorar la seguridad de la información mediante la aplicación de un proceso de análisis de riesgos y de verificación de los controles de seguridad que permitan estructurar un sistema de gestión de seguridad de la información para la unidad de informática y telecomunicaciones de la Universidad de Nariño, basado en la norma ISO 27001 y 27002.

Este proyecto sirve como guía para evidenciar y aportar el conocimiento necesario para implementar un SGSI, utilizando las técnicas necesarias para el levantamiento de los activos de información y el análisis de riesgos, que permitan la adecuada definición de controles en base a los hallazgos encontrados, basados en la norma ISO 27001:2013.

Título: **Planeación y Diseño de un Sistema de Gestión de la Seguridad de la Información basado en la norma ISO/IEC 27001 - 27002**

Autores de la investigación:

- JOSÉ LUIS BUENAÑO QUINTANA
- MARCELO ALFONSO GRANDA LUCES

Este proyecto busca establecer mecanismos adecuados para mitigar los riesgos asociados al uso de la información, de los sistemas y servicios utilizados por el personal de la sede de Guayaquil de la Universidad Politécnica Salesiana.

El proyecto a desarrollar es hacer algo similar buscando la mejor manera de establecer mecanismos y políticas que permitan tolerar los riesgos referentes al uso constante y permanente de la información en la cooperativa.

Título: **Metodología de implantación de un SGSI en un grupo empresarial jerárquico.**

Autor:

- GUSTAVO PALLAS MEGA

Este proyecto busca dar lineamientos metodológicos, de aplicación sistemática para el diseño, implantación, mantenimiento, gestión, monitoreo y evolución de un SGSI según la norma ISO 27000, para una empresa perteneciente a un grupo empresarial.

El proyecto que se llevara a cabo busca brindar métodos y herramientas que permitan diseñar y mantener a futuro el sistema de gestión de seguridad de la información en la cooperativa.

5.2 MARCO TEÓRICO

Hoy en día la información se ha convertido en el activo más importante para cualquier tipo y tamaño de organización, es por esto que se deben implementar estrategias y mecanismos que permitan salvaguardarla de cualquier riesgo, amenaza o vulnerabilidad que pudieran ocasionar la pérdida de su confidencialidad, disponibilidad e integridad.

5.2.1 Activo de información[1].

Las organizaciones poseen información que deben proteger de amenazas y riesgos, es por ello que todo lo que se considere de valor se considera un activo para la organización y por tanto debe protegerse, tales como; información física y digital, software, hardware, servicios de información, servicios de comunicaciones, servicios de almacenamiento, personas, imagen y reputación.

5.2.2 Amenazas informáticas[2]

Es la posibilidad de que algún tipo de evento se pueda presentar en cualquier instante de tiempo, en el cual existe un daño material o inmaterial, sobre los sistemas de información, por lo tanto se pueden clasificar en:

- Amenaza criminal: son aquellas acciones en las que intervienen seres humanos violando las normas y las leyes.

[1] POVEDA. José. “Modulo 7: Los activos de seguridad de la información”. {En línea}. {20 de Agosto de 2015}. Disponible en: (http://www.worldvisioncapacitacion.cl/wp-content/uploads/cursos_adjuntos/f52e0bd4c6c2c203413952826f916237.pdf)

[2] GUZMAN, Alexander. Diseño de un sistema de gestión de la seguridad informática – SGSI, para empresas del área textil en la ciudad de Itagüí, Medellín y Bogotá D.C. a través de la auditoría. Colombia, 2015, 176p. Trabajo de grado (Especialización en seguridad informática). UNAD. Escuela de ciencias básicas tecnología e ingeniería.

- Sucesos de origen físico: son los eventos naturales que se pueden presentar, o aquellos eventos en los que el ser humano propicia las condiciones para determinar un hecho físico.

- Negligencia: son las omisiones, decisiones o acciones que pueden presentar algunas personas por desconocimiento, falta de capacitación y/o abuso de autoridad porque tienen influencia sobre los sistemas de información, algunos porque no tienen ética para el desarrollo de la profesión.

Las amenazas a los sistemas de información están latentes cada que se interactúa con los mismos, desde la utilización de dispositivos de almacenamiento externos, hasta el ingreso a sitios web, o la inconformidad de empleados insatisfechos dentro de la misma compañía, por lo tanto los tipos de amenazas según el efecto causado en el sistema.

5.2.3 Seguridad informática[3]

La seguridad informática es una disciplina que se encarga de proteger la integridad y la privacidad de la información almacenada en un sistema informático. De todas formas, no existe ninguna técnica que permita asegurar la inviolabilidad de un sistema.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, o dispositivos de almacenamiento, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (de manera automatizada o a

[3] definicion.de. {En línea}. {10 de Julio de 2015}. Definición de seguridad informática - Qué es, Significado y Concepto. Disponible en (http://definicion.de/seguridad-informatica/#ixzz3YfKiPkQe)

través de delincuentes que se conectan a Internet y acceden sin autorización a distintos sistemas).

5.2.4 Seguridad de la información[4]

Es la protección de la información contra una gran variedad de amenazas con el fin de asegurar la continuidad del negocio, minimizar el riesgo y maximizar el retorno de inversiones y oportunidades de negocio. Los objetivos primordiales de la seguridad de la información se consideran los siguientes:

Confidencialidad: característica que indica que el activo solo sea accedido por el personal, procesos o entidades que se encuentren autorizadas y con los privilegios adecuados.

Integridad: característica que protege la precisión, calidad, veracidad, imparcialidad y completitud del activo.

Disponibilidad: característica que indica que el activo sea oportuno, es decir que pueda ser consultado y usado por la persona, entidad o proceso cuando lo requiera.

5.2.5 Análisis de riesgos[5]

El primer paso en la gestión del riesgo es el análisis de riesgo que tiene como propósito determinar los componentes de un sistema que requieren protección, sus vulnerabilidades que los debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo. Existen varias metodologías para evaluar el riesgo, sin embargo el punto de partida nace de la identificación de activos de información, los cuales son todos los recursos involucrados en la gestión de la

[4] Gestión de riesgo en la seguridad informática. {En línea}. {9 de Agosto de 2015}. Disponible en: (https://protejete.wordpress.com/gdr_principal/seguridad_informacion_proteccion/)
[5] Welivesecurity. {En línea}. {1 de Junio de 2015}. Disponible en: (http://www.welivesecurity.com/la-es/2012/08/16/en-que-consiste-analisis-riesgos)

información. De una adecuada gestión de riesgos depende que una empresa pueda identificar las principales vulnerabilidades de sus activos de información y cuáles son las amenazas que podrían explotar las vulnerabilidades, en la medida que la empresa tenga clara esta identificación de riesgos podrá establecer las medidas preventivas y correctivas viables que garanticen mayores niveles de seguridad en la información.

5.2.6 Sistema de gestión de la seguridad de la información[6]

La seguridad de la información, según ISO 27001:2013, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización. Así pues, estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información:

• Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.

• Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

• Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran.

Para garantizar que la seguridad de la información es gestionada correctamente, se debe hacer uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo empresarial. Este proceso es el que

[6] GUERRERO, Yezid. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO. Pasto, 2014. p56.

constituye un SGSI. El SGSI (sistema de gestión de seguridad de la información) es el concepto central sobre el que se construye ISO 27001.

La gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y conocido por toda la organización. Este modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en un análisis y evaluación de riesgos y en una medición de la eficacia de estos. Por lo tanto el SGSI ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

La aceptación de este estándar debe ser tomada en cuenta como una decisión estratégica para la organización; se pretende que el SGSI se extienda con el tiempo en relación a las necesidades de la organización.

El enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional impulsa que sus usuarios enfaticen 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 de la información.

- Implementar y operar controles para manejar los riesgos de la seguridad de la información.

- Monitorear y revisar el desempeño del Sistema de Seguridad de la Información.

- Mejoramiento continuo en base a la medición del objetivo.

Beneficios de un SGSI

- Involucrar a la Dirección en la seguridad de la información
- Desarrollar políticas formales de cumplimiento obligatorio
- Conocer realmente de qué activos dispone la organización
- Cumplir con la legislación vigente ligada al proyecto
- Realizar análisis de riesgos para el desarrollo del negocio
- Introducción de contratos de niveles de servicio
- Reforzar la seguridad ligada a personal
- Disponer de planes de contingencias ante incidentes
- Disponer planes de continuidad del negocio y recuperación ante desastres
- Desarrollo de indicadores del desempeño del SGSI
- Disminución de riesgos a niveles aceptables, etc.

Para establecer y gestionar un Sistema de Gestión de la Seguridad de la Información basado en ISO 27001, se adopta el ciclo de mejora continua PHVA (Véase Figura 3).

Figura 1. Ciclo PHVA

Fuente: GUERRERO, Yesid. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) BASADO EN LA NORMA ISO 27001 Y 27002 PARA LA UNIDAD DE INFORMÁTICA Y TELECOMUNICACIONES DE LA UNIVERSIDAD DE NARIÑO. Pasto, 2014. p58.

- **Planear**: Establecer el Sistema de Gestión de Seguridad de la Información. Es una fase donde se realiza el análisis y evaluación de riesgos, el Plan de Tratamiento de Riesgos y la definición de las políticas de seguridad.

- **Hacer**: Implementar y operar el Sistema de Gestión de Seguridad de la Información. Es una fase que envuelve la implementación y operación de los controles.

- **Verificar**: Monitorear y revisar el Sistema de Gestión de Seguridad de la Información. Es una fase de medición de resultados, auditoria interna y revisión por parte de la dirección de la organización.

- **Actuar**: Mantener y mejorar el Sistema de Gestión de Seguridad de la Información. Es una fase en la que se llevan a cabo acciones preventivas y correctivas para el Sistema de Gestión de Seguridad de la Información.

Garantizar un nivel de protección total es virtualmente imposible, incluso en el caso de disponer de un presupuesto ilimitado. El propósito de un sistema de gestión de la seguridad de la información es, por tanto, garantizar que los riesgos de la seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización de una forma documentada, sistemática, estructurada, repetible, eficiente y adaptada a los cambios que se produzcan en los riesgos, el entorno y las tecnologías.

5.2.7 MAGERIT[7]

Es la metodología de análisis y gestión de riesgos de los sistemas de información elaborada por el Consejo Superior de Administración Electrónica, como respuesta a la percepción de que en la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión.

5.2.8 Familia de normas ISO 27000[8]

Teniendo en cuenta que en toda organización el propósito fundamental es identificar y satisfacer las necesidades y expectativas de sus clientes empleando normas y estándares que permitan asegurar la información y la calidad de la misma, es importante el empleo de normas y estándares las cuales son un conjunto de mejores prácticas recomendadas para desarrollar, implementar y mantener especificaciones para los diferentes Sistemas de Gestión de la Seguridad de la Información (SGSI).

Dentro de los beneficios con la utilización de estas normas tenemos:

[7] PORTAL ADMINISTRACIÓN ELECTRONICA. {En línea}. {10 de Mayo de 2015}. Disponible en: (http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.Vh_QD_l_Oko)
[8] ISO27000.ES. {En línea}. {12 de Junio de 2015}. Disponible en: (http://www.iso27000.es/).

- ✓ Reducción del impacto de los riesgos, que en caso de materializarse las amenazas, puedan representar pérdidas (de capital, de facturación, de oportunidades de negocio, por reposición de los daños causados, reclamaciones de clientes, sanciones legales, etc), al aumentar la seguridad efectiva de los sistemas de información, con una mejor planificación y gestión de la seguridad.

- ✓ Garantías de continuidad del negocio basándose en un plan de contingencias.

- ✓ Mejora de la imagen de la organización y aumento del valor comercial de la empresa y sus marcas.

- ✓ Incremento de los niveles de confianza de clientes, proveedores, accionistas, entre otros.

- ✓ Mejora del retorno de las inversiones, al tener mejor criterio según los riesgos residuales aceptados y ahorro de tiempo y dinero al reducir o eliminar actividades o inversiones de escasa o nula aplicabilidad a los niveles de riesgo identificados en el negocio.

- ✓ Mejora continua a través de la metodología PDCA (Planificar, Hacer, Verificar y Actuar).

- ✓ Mejorar el conocimiento de los sistemas de información, sus problemas y los medios de protección.

- ✓ Mejorar la disponibilidad, integridad y confidencialidad de los datos que existan en la organización.

- ✓ Protección del activo más importante para cualquier organización, la información.

- ✓ La aplicación de estándares puede significar la diferenciación y competitividad de la organización ante el mercado nacional e internacional.

- ✓ Reducción de costos en caso de presentarse pérdida de información.

Una adecuada gestión de la seguridad de la información debe realizarse mediante un proceso sistemático, documentado y basado en objetivos claros de seguridad, este proceso es el que conforma un Sistema de Gestión de Seguridad de la Información (SGSI).

Actualmente existen una serie de normas que proporcionan un marco de gestión para la seguridad de la información, las cuales pueden ser utilizadas por toda organización a nivel nacional sin importar su naturaleza y propósito. Estas normas son las que componen la serie ISO/IEC 27000 por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), donde se indica como estructurar e implantar un Sistema de Gestión de Seguridad de la Información basado en ISO 27001.

5.2.9 Norma ISO/IEC 27001:2013[9]

Es un estándar ISO que proporciona un modelo para establecer, implementar, utilizar, monitorizar, revisar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la información (SGSI). La presente norma incluye también los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información, adaptados a las necesidades de la organización. Los requisitos

[9] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACIÓN ISO/IEC 27001. Primera actualización. Bogotá. ICONTEC, 2013.

establecidos en esta Norma son genéricos y están previstos para ser aplicables a todas las organizaciones, independientemente de su tipo, tamaño o naturaleza.

Es de gran importancia que el SGSI sea parte de los procesos y de la estructura de gestión total de la información de la organización y que esté integrado con ellos, y que la seguridad de la información se considere en el diseño de procesos, sistemas de información y controles. El objetivo principal de la implementación de un SGSI de acuerdo a esta norma, es que sea difundido y asumido conforme con las necesidades de la organización.

5.2.10 Políticas de seguridad de la información[10]

Las políticas de seguridad de la información tienen por objeto establecer las medidas de índole técnica y de organización, necesarias para garantizar la seguridad de las tecnologías de información (equipos de cómputo, sistemas de información, redes (Voz y Datos)) y las personas que interactúan haciendo uso de los servicios asociados a ellos y se aplican a todos los usuarios de cómputo de las empresas.

Este dominio articula los objetivos del negocio y la razón social de la pyme, empresa u organización con las necesidades de la seguridad informática, para salvaguardar los datos, registro y demás información confidencial que se desee proteger, por lo tanto el documento debe contemplar todos los niveles y acciones a seguir en determinado caso:

- Clasificación de la información
- Naturaleza del negocio
- Información de uso interno y externo

[10] Ibíd.

- Necesidades técnicas y operativas

5.3 MARCO CONCEPTUAL

5.3.1 Seguridad

El concepto de seguridad se aplica a los entornos de la vida cotidiana, de manera tal que el hombre siempre ha tenido la necesidad de imaginar mecanismos que le aseguren sus datos, los cuales viajan a través de una red informática o un medio de almacenamiento electrónico de forma segura, los cuales deben llegar sus respectivos receptores.

5.3.2 Estándares de seguridad

"Si bien los estándares nos proporcionan una base importante para llegar a crear un modelo de seguridad, ésta se basa en las políticas de seguridad de la organización, las cuales determinan los procedimientos, los estándares y las herramientas que ayudarán a estas labores"[11].

5.3.3 Modelo de seguridad

Son los mecanismos, protocolos, estándares, procesos, procedimientos y actividades que se enmarcan en un conjunto de pasos para desarrollar y mantener el control frente a los diversos dinamismos que se presentan en una organización frente a los avances tecnológicos.

5.4 MARCO LEGAL

Para la adecuada implementación de un sistema de gestión de seguridad de la información, es necesario y obligatorio que se tengan en cuenta y se cumplan todas las leyes, decretos, normas, resoluciones y demás reglamentaciones que

[11] Gómez, J. (2013). *Seguridad de la Información*. Recuperado el 09 de diciembre del 2013 de: http://www.slideshare.net/hvillas/seguridaddela-informacion-17506228

apliquen durante el desarrollo de las actividades, buscando establecer la manera adecuada de proteger a las organizaciones y sus activos de información, de sus colaboradores, terceros, y demás personas de cualquier delito, infracción, proceso, procedimiento o acto mal ejecutado, que vulnere sus derechos, y ponga en riesgo su integridad, su buen nombre, sus activos y cualquier otro bien al que pertenezca la organización.

Por otra parte se debe tener en cuenta que elementos de infraestructura hardware y software, políticas, sistemas y metodologías de gestión del riesgo, procesos, procedimientos, planes de seguridad, recurso humano y demás elementos serán necesarios para la correcta implementación de SGSI, estos elementos durante su aplicación o implementación son susceptibles a que se pueda omitir el cumplimiento de alguna ley, y tener consecuencias sobre la organización o sobre una o más personas en particular, por eso es necesario conocer algunas leyes, decretos y normas que rigen sobre estos elementos buscando la protección del bien individual o colectivo, algunas de estas leyes, decretos o normas son:

- "Decreto 1360 de 1989, donde se reglamenta el soporte lógico (software) en el registro nacional del derecho de autor, considerando al software como una creación del dominio literario en conformidad a la ley 23 de 1982 sobre derechos de autor"[12].
- "Ley 527 de 1999, que establece y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y las firmas digitales, además de establecer las entidades de certificación y otras disposiciones"[13].

[12] Jaramillo, A. {En línea}. Manual de derecho de autor. {13 de Mayo del 2014}. Disponible en: (http://www.derechodeautor.gov.co/documents/10181/331998/Cartilla+derecho+de+autor+(Alfredo+Vega).pdf/e99b0ea4-5c06-4529-ae7a-152616083d40)

[13] Cuervo, J. {En línea}. Aspectos jurídicos de internet y el comercio electrónico. {13 de Mayo del 2014}. Disponible en: (http://www.informatica-juridica.com/trabajos/Aspectos_juridicos_de_Internet_y_el_comercio_electronico.asp)

- “Decreto 1747 de 2000, que reglamenta parcialmente la ley 527 de 1999, con lo relacionado a las entidades de certificación, los certificados y las firmas digitales”[14].
- “Resolución 26930 de 2000, la cual fija los estándares para la autorización y el funcionamiento de las entidades de certificación y sus auditores”[15].
- “Ley estatutaria 1266 de 2008, que establece las disposiciones generales del habeas data y regula el manejo de la información que se contiene en las bases de datos personales, especialmente la financiera, crediticia, comercial, de servicios y la proveniente de terceros países”[16].
- “Ley 1273 de 2009, con la que se modifica el código penal, se crea u nuevo bien jurídico denominado "de la protección de la información y de los datos", y se preservan integralmente los sistemas que utilicen las tecnologías de información y de comunicaciones”[17].

Por otra parte hay algunas disposiciones internas que maneja la cooperativa, los cuales también deben tenerse en cuenta para la adecuada implementación del SGSI, en el área de informática.

5.4.1 Estatuto Coacremat[18]

Es la normatividad que regula y designa los lineamientos del funcionamiento, características y de la cooperativa. Sirven de guía a los socios para conocer;

[14] Decreto. {En línea}. Artículo 160 del Decreto ley 19 de 2012. {13 de Mayo del 2014}. Disponible en: (http://www.sic.gov.co/documents/10165/2142817/DECRETO+333+DEL+19+DE+FEBRERO+DE+2014+VIG+ENTES+ACREDITAC.pdf/3dcd1c36-533a-48fa-a72c-7fcb2181e771)

[15] Resolución. {En línea}. Por la cual se fijan los estándares para la autorización y funcionamiento de las entidades de certificación y sus auditores. {13 de Mayo del 2014}. Disponible en: (http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=5793)

[16] Concepto. {En línea}. Oficina juridicial nacional. {15 de Mayo del 2014}. Disponible en: (http://www.legal.unal.edu.co/sisjurun/normas/Norma1.jsp?i=42011)

[17] DELTA. {En línea}. Ley de delitos informáticos en Colombia. {13 de mayo del 2014}. Disponible en: (http://www.deltaasesores.com/articulos/autores-invitados/otros/3576-ley-de-delitos-informaticos-en-colombia)

[18] ESTATUTOS – Cooperativa del Magisterio de Túquerres. {En línea}. {12 de Mayo de 2015}. Disponible en: (http://www.coacremat.coop/coacremat/documents/estatuto_coacremat_2014.pdf).

cuales son los objetivos de la Cooperativa, como debe funcionar, cuál debe ser su conducta dentro de ella, cuáles son sus deberes y derechos, como controlar en forma disciplinaria todas las actividades para lograr los objetivos, como puede la Cooperativa utilizar los beneficios obtenidos, entre otros.

Está compuesto por 158 artículos y 15 capítulos, los más importantes que se pueden resaltar son:

- Capítulo I: del acuerdo cooperativo razón social – domicilio – ámbito territorial de operaciones – duración.

- Capítulo III: de los asociados condiciones de admisión, derechos y deberes exclusión y determinación del órgano competente para su decisión.

- Capítulo VI: administración – vigilancia y control social.

- Capítulo XII: régimen y responsabilidad de la cooperativa y sus asociados.

5.4.2 Acuerdo No. 089 – Coacremat[19]

En el cual se adopta el código de buen gobierno de la Cooperativa del Magisterio de Túquerres. En el cual se constituye el compromiso institucional en el desempeño de la función administrativa que le ha sido encomendada, hacia el logro de una gestión caracterizada por la integridad, transparencia, eficiencia y clara orientación para el cumplimiento de los fines del cooperativismo.

Se hace necesario dotar a los entes de vigilancia y control de un instrumento ágil que oriente el cumplimiento de la respectiva misión, visión, metas y estrategias, dentro de los más elevados principios éticos, de integridad, transparencia,

[19] CONSEJO DE ADMINISTRACIÓN. Acuerdo No. 089. {En línea}. {15 de Julio de 2015}. Disponible en: (http://www.coacremat.coop/coacremat/documents/buen_gobierno.pdf)

eficiencia y eficacia; y por ello la implementación del Código de Buen Gobierno Cooperativo en COACREMAT LTDA. Permitirá consolidar la ética, que en materia de opción y responsabilidad personal, consiste en hacer aquello que es correcto en el momento oportuno.

5.5 MARCO CONTEXTUAL

Este proyecto se aplicara en la oficina principal de la Cooperativa del Magisterio de Túquerres, con domicilio en la ciudad de Túquerres – Nariño, específicamente en el área de informática.

LA COOPERATIVA DEL MAGISTERIO DE TÚQUERRES LTDA., con personería jurídica No. 0452 de Mayo de 1.977, Notaria Primera de Túquerres, presenta las siguientes características jurídicas:

- Es una empresa asociativa, de derecho privado, de responsabilidad limitada, de carácter multiactiva, sin ánimo de lucro, de personal y capital variable e ilimitado.

- El domicilio principal (legal) de la entidad será el municipio de Túquerres, departamento de Nariño.

- El ámbito territorial de operaciones comprenderá la República de Colombia.

- La duración será indefinida, sin embargo podrá disolverse y/o liquidarse en cualquier momento, según los casos previstos en la Ley y en su estatuto.
- Desempeña la calidad de entidad operadora en la realización de operaciones por libranza y ventanilla, destinando para ello los

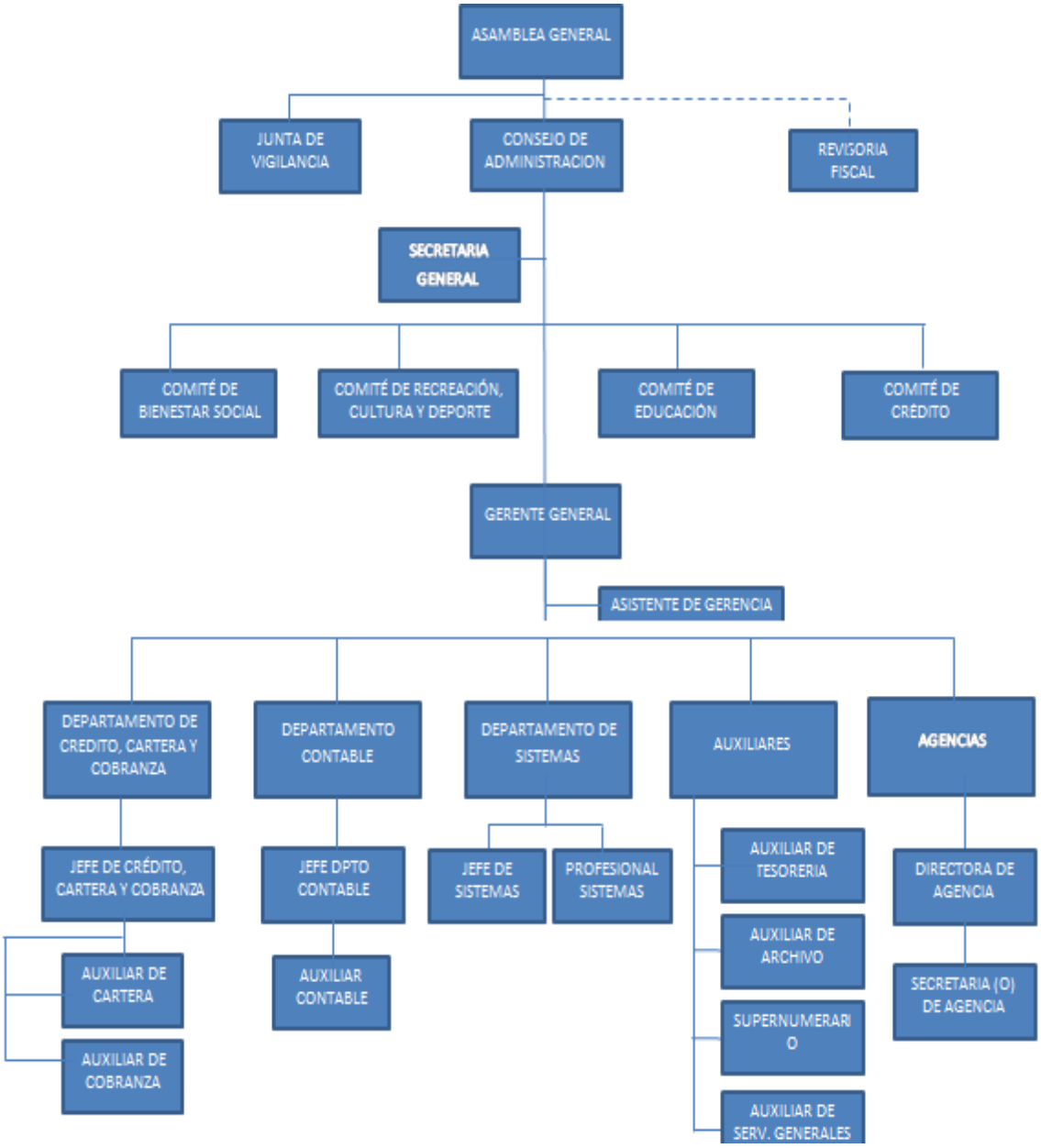
recursos provenientes de los aportes, ahorros, créditos financiados de los asociados que estén legalmente autorizados y que por su procedencia son dineros lícitos y demás recaudos que también sean lícitos.

- Para su dirección, administración y representación la sociedad tiene los siguientes órganos, Asamblea General de Delegados, Consejo de Administración y Gerencia.

Su Misión: es una cooperativa multiactiva, presente en el Departamento de Nariño que presta servicios de asesoría, ahorro, crédito, comercialización y bienestar social para el mejoramiento de la calidad de vida de sus asociados; utilizando talento humano competente comprometido con la organización y con la tecnología adecuada.

Su Visión: para el 2015 será reconocida como la primera opción de servicios solidarios y financieros para la comunidad educativa (docentes y administrativos), profesional e independiente en el sur occidente de Colombia.

Figura 2. Organigrama



Fuente: COACREMAT LTDA. MANUAL DE PROCESOS Y PROCEDIMIENTOS. Pasto, 2013. p42.

5.5.1 Área de Sistemas

Figura 3. Misión y objetivos del área de sistemas

MISIÒN DEL ÀREA
Velar por la Seguridad de la información de COACREMAT Ltda, así como de proveer de las herramientas necesarias para su manipulación, está encargada de satisfacer las necesidades y preparación computacional a todos los miembros de la Cooperativa del Magisterio de Túquerres "COACREMAT Ltda", así como de ofrecer soluciones informáticas y el equipo necesario para su implementación.

OBJETIVOS DEL ÀREA
1. Supervisar el desarrollo del software usado por la Cooperativa del Magisterio de Túquerres "COACREMAT, manteniendo contacto directo con los desarrolladores para asegurar que cumpla con las expectativas del cliente y la misión de la empresa. 2. Proveer soluciones específicas para cada área de la Cooperativa del Magisterio de Túquerres "COACREMAT, implementando estrategias que permitan conocer las dificultades que encuentran los usuarios del software y hardware organizacional. 3. Aprovechar a favor de la Cooperativa "COACREMAT Ltda" las tecnologías de la Información y Comunicación TIC's. 4. Diseñar y gestionar el Sistema de Gestión de Seguridad Informática. 5. Mantener a la Cooperativa "COACREMAT Ltda" a la vanguardia tecnológica. 6. Asesoría y soporte técnico.

Fuente: COACREMAT LTDA. MANUAL DE PROCESOS Y PROCEDIMIENTOS. Pasto, 2013. p85.

5.5.1.1 Jefe Área de Sistemas

Planificar, Coordinar y Controlar actividades dirigidas a la satisfacción de necesidades en Informática y Tecnología de la Cooperativa del Magisterio de Túquerres - COACREMAT Ltda.

5.5.1.2 Profesional Área de Sistemas

Brindar asesoría, soporte y mantenimiento a los equipos necesarios para el adecuado funcionamiento y uso de los paquetes de información de Cooperativa del Magisterio de Túquerres - COACREMAT Ltda.

5.5.1.3 Infraestructura tecnológica

Gran parte de las actividades que se desarrollan en la cooperativa se apoyan en la tecnología y, por lo tanto, siempre ha sido un punto estratégico el de mantener una infraestructura tecnológica sólida y moderna. Se encuentra conformada por una sala de máquinas con un servidor BLADE, ordenadores y elementos de red de última generación y con sistemas bien posicionados en el mercado. En la gran mayoría se utiliza software propietario, sin embargo también se manejan algunos servicios en software libre.

Por otra parte se cuenta con equipos de autonomía eléctrica (UPS y PLANTA ELECTRICA) que garantizan el funcionamiento del negocio las 24 horas del día los 365 días al año.

Este proyecto será realizado en la oficina principal de la Cooperativa del Magisterio de Túquerres, con domicilio en la ciudad de Túquerres – Nariño, específicamente en el área de informática. Se ha estipulado un tiempo inferior a 12 meses para su ejecución.

5.5.1.4 Política del manejo de los computadores

En la Cooperativa del Magisterio de Túquerres se implementó una política para el manejo de los computadores y demás equipos que componen la infraestructura tecnológica de la organización, dicha política es de obligatorio cumplimiento para todo el talento humano y además contiene los lineamientos que deben seguirse con el fin de salvaguardar la integridad, confidencialidad, disponibilidad y no repudio de los equipos de cómputo con que cuenta la cooperativa.

6. DISEÑO METODOLÓGÍCO

Para este proyecto se trabajara de diversas formas:

Realizar en primer lugar un estudio y análisis de los activos de información con que cuenta el área de informática de la cooperativa, además de investigar sobre la norma ISO/IEC 27001:2013 para realizar las recomendaciones de seguridad que se consideren pertinentes para proteger los activos.

Determinar los activos de información del área de informática de la Cooperativa del Magisterio de Túquerres y asignarle a cada uno su clasificación de seguridad para establecer el estado actual de la seguridad de la información.

Establecer las amenazas a las que se encuentra expuesta la seguridad de la información en el área de informática, tanto en su confidencialidad, integridad y disponibilidad, esto con el fin de identificar las debilidades con que cuenta la información y así tomar las acciones pertinentes.

Por último y de acuerdo a los resultados de la evaluación de las situaciones que generan riesgos, amenazas y procesos implementados en la actualidad, se propondrá el plan de implementación del SGSI acorde a las necesidades del área de informática de la cooperativa, con los procedimientos, mecanismos y controles adecuados para proteger la integridad, disponibilidad y confidencialidad de la información.

7. NOMBRE INTEGRANTES DEL PROCESO

Tabla 1. Responsables del Proyecto

NOMBRE	CARGO
Ing. Duban Oswaldo Palacios Portilla	Ingeniero investigador del proyecto
Ing. Erika Liliana Villamizar Torres	Director investigador del proyecto

8. RECURSOS

8.1 TALENTO HUMANO

El proyecto será desarrollado por Duban Palacios estudiante de la especialización en seguridad informática, con la asesoría de la especialista Erika Villamizar docente de la Universidad Nacional Abierta y a Distancia - UNAD.

8.2 RECURSOS FÍSICOS

Los materiales a utilizar son:
Computadores, impresoras, scanner, papel, lapiceros, lápiz, borrador, libreta de apuntes, cd-rooms, memoria USB y fotocopias.

8.3 PRESUPUESTO

	COSTOS		
DESCRIPCIÓN	**Cant**	**Valor Unit**	**Valor Total**
Dvd´s	10	1.000,00	10.000,00
Resma papel	1	9.000,00	9.000,00
Fotocopias	500	50,00	25.000,00
Memoria Usb	3	60.000,00	180.000,00
Lapiceros	6	600,00	3.600,00
Lápiz	6	600,00	3.600,00
Borrador	3	200,00	600,00
Cuadernos de apuntes	3	1.500,00	4.500,00
Talento humano	12	200.000,00	3.000.000,00
Recarga tonners impresora	5	8.000,00	40.000,00
Computadores	3	2.000.000,00	6.000.000,00
Costo subtotal proyecto			**$9.276.300**
Imprevistos		5%	$463.815
Costo Total del Proyecto			**$9.740.115**

9. CRONOGRAMA DE ACTIVIDADES

ACTIVIDAD	Mes 1	Mes 2	Mes 3	Mes 4	Mes 5	Mes 6	Mes 7	Mes 8	Mes 9	Mes 10	Mes 11	Mes 12
Realizar un análisis del estado actual de seguridad de la información de la Cooperativa del Magisterio de Tuquerres.												
Determinar los activos de información del área informática.												
Determinar las amenazas a los que están expuestos los activos de información del área de sistemas.												
Proponer el plan de implementación del sistema de seguridad de la información.												

10. DESARROLLO DEL PROYECTO

10.1 CLASIFICACIÓN DE ACTIVOS DE INFORMACIÓN

10.1.1 Activos de información

A continuación se presentan las clasificaciones de seguridad que se darán a cada uno de los activos de información:

Tabla 2. Clasificaciones de seguridad

Clasificación Cualitativa	Descripción
Sensitiva	El compromiso de la información podría dañar los intereses de los usuarios y terceros.
En confianza	El compromiso de la información podría perjudicar la privacidad de los usuarios y terceros.
Publica no clasificada	El compromiso de la información afecta la imagen de la entidad.
Top Secret	El compromiso de la información podría dañar los intereses de la organización de manera grave.
Secreta	El compromiso de la información podría dañar los intereses de la organización de manera seria.
Confidencial	El compromiso de la información podría dañar los intereses de la organización de manera significativa.
Restringida	El compromiso de la información podría dañar los intereses de la organización de manera adversa.

Tabla 3. Escala de valoración de rango porcentual de impacto en los activos

Porcentaje	Criterio
90%-100%	Muy alto
75%-89%	Alto
50%-74%	Medio
20%-49%	Bajo
0%-19%	Muy bajo

Para la operación, procesamiento y manejo de la información el área de informática cuenta con los siguientes activos:

Tabla 4. Clasificación de activos de información

INVENTARIO DE ACTIVOS						
Tipos de activos	**Nombre de activos área de informática**	**Clasificación de la información**	**Criticidad**			
			Conf.	**Integ.**	**Disp.**	**Promedio**
Activo de información	Base de datos ORACLE	Confidencial	100%	100%	100%	100%
	Documentos Físicos (Manuales de usuario, correspondencia…	Confidencial	80%	60%	60%	67%

	entre otros)					
Activos de software	LINIX	Restringida	100%	100%	100%	100%
	SAPIENS	Restringida	90%	90%	95%	92%
	WINDOWS 7 PROFESIONAL	Confidencial	100%	100%	100%	100%
	OFFICE 2010 Hogar y empresa	Sensitiva	80%	70%	60%	70%
	KASPERSKY ENDPOINT	Secreta	100%	100%	100%	100%
Activos físicos	Servidor de base de datos	Restringida	100%	100%	100%	100%
	Servidor de aplicaciones	Restringida	100%	100%	100%	100%
	Servidor proxy	Restringida	80%	80%	100%	87%
	Computadores HP	Restringida	100%	100%	100%	100%
	Switches HP	Restringida	90%	100%	100%	97%
	Unidad NAS – Backup		100%	100%	100%	100%
	UPS tripplite	Sensitiva	80%	80%	100%	87%
	Celulares	Sensitiva	70%	100%	100%	90%
Servicios	Conectividad a internet	Confidencial	85%	100%	100%	95%

	Conectividad por MPLS – Movistar	Restringida	90%	100%	100%	97%
	Red de datos	Restringida	100%	100%	100%	100%
Personal	Jefe de sistemas	Restringida	100%	100%	100%	100%
	Profesional área de sistemas	Restringida	100%	100%	100%	100%

10.1.2 Infraestructura física

El área de sistemas de la Cooperativa del Magisterio de Túquerres se encuentra ubicada en el cuarto piso de un edificio ubicado en el municipio de Túquerres – Nariño, en un sector residencial, en el área laboran 2 profesionales en sistemas con los equipos y suministros necesarios para el adecuado desempeño de sus labores.

10.1.3 Infraestructura informática

La infraestructura informática del área de sistemas consta de lo siguiente:

- Canal dedicado de internet de 2Mb.

- Canal de datos MPLS de 2Mb que permite la conexión de manera segura y remota desde el servidor principal a las agencias ubicadas en diferentes lugares del departamento de Nariño.

- Dos equipos de cómputo HP con sistema operativo Windows 7 Profesional.

- Un chasis IBM en Blade, constituido por 6 servidores, de los cuales se encuentran activos y en pleno funcionamiento 3 de ellos (Servidor de aplicaciones, base de datos y proxy).

- Una UPS Tripplite que brinda autonomía en la ausencia del fluido eléctrico.

Tabla 5. Valoración para los activos

Escala de valoración cualitativa y cuantitativa para los activos		
Valoración Cualitativa	**Escala de valor cuantitativo**	**Valor cuantitativo**
Muy Alto (MA)	> $ 100.000.000	$ 101.000.000
Alto (A)	$ 100.000.000 <valor> $ 50.000.000	$ 75.000.000
Medio (M)	$ 50.000.000 <valor> $ 20.000.000	$ 35.000.000
Bajo (B)	$ 20.000.000 <valor> $ 10.000.000	$ 15.000.000
Muy Bajo (MB)	$ 10.000.000 <valor> $ 1.000.000	$ 5.500.000

Tabla 6. Criterio de valoración de activos

Valor	Criterio
10	Daño muy grave
7-9	Daño grave
4-6	Daño importante
1-3	Daño menor
0	Irrelevante

Valoración de activos de acuerdo a la dimensiones de seguridad y criterio:

Tabla 7. Dimensiones de los riesgos

Tipos de activos	**Nombre de activos área de informática**	**Dimensiones**				
		Confidencialidad	**Integridad**	**Disponibilidad**	**Autenticidad**	**Trazabilidad**
Activo de información	Base de datos ORACLE	[10][MA]	[10][MA]	[10][MA]	[10][MA]	[10][MA]
	Documentos Físicos (Manuales de usuario,	[10][MA]	[6][M]	[3][B]	[6][B]	[3][B]

	correspondencia… entre otros)					
Activos de software	LINIX	[10][MA]	[10][MA]	[10][MA]	[9][A]	[9][A]
	SAPIENS	[9][MA]	[10][A]	[9][A]	[9][M]	[6][M]
	WINDOWS 7 PROFESIONAL	[6][M]	[9][A]	[9][A]	[6][M]	[6][M]
	OFFICE 2010 Hogar y empresa	[6][M]	[9][A]	[7][M]	[6][M]	[6][M]
	KASPERSKY ENDPOINT	[6][M]	[9][A]	[7][M]	[6][M]	[6][M]
Activos físicos	Servidor de base de datos	[10][MA]	[10][MA]	[10][MA]	[9][A]	[9][A]
	Servidor de aplicaciones	[10][MA]	[10][MA]	[10][MA]	[9][A]	[7][A]
	Servidor proxy	[9][M]	[9][M]	[9][A]	[6][B]	[6][B]
	Computadores HP	[9][A]	[10][MA]	[7][M]	[3][MB]	[3][MB]
	Switches HP	[6][M]	[9][A]	[10][MA]	[6][B]	[6][B]
	Unidad NAS – Backup	[6][M]	[9][A]	[6][M]	[6][B]	[6][B]
	UPS tripplite			[9][A]		
	Celulares	[3][MB]	[3][MB]	[6][B]		
Servicios	Conectividad a	[9][A]	[6][M]	[9][A]	[3][M]	[3][B]

	internet					
	Conectividad por MPLS – Movistar	[9][A]	[9][M]	[9][A]	[3][MB]	[3][B]
	Red de datos	[6][A]	[6][A]	[10][MA]	[3][MB]	[3][B]
Personal	Jefe de sistemas	[10][MA]		[9][A]		
	Profesional área de sistemas	[10][MA]		[9][A]		

Tabla 8. Dimensiones de valoración del impacto

Cod.	**Nombre Dimensiones de valoración**
[D]	Disponibilidad
[I]	Integridad de los datos
[C]	Confidencialidad de la información
[A]	Autenticidad
[T]	Trazabilidad

Tabla 9. Amenazas

Cod.	Amenazas	Impacto
[N] Desastres Naturales		
[N.1]	Fuego	[D]
[N.2]	Daño por agua	[D]
[N.*]	Otros desastres	[D]
[I] De origen industrial		
[I.1]	Fuego	[D]
[I.2]	Daños por agua	[D]
[I.*]	Desastres industriales	[D]
[I.3]	Contaminación mecánica	[D]
[I.4]	Contaminación electromagnética	[D]
[I.5]	Avería de origen físico o lógico	[D]
[I.6]	Corte del suministro eléctrico	[D]
[I.7]	Condiciones inadecuadas de temperatura o humedad	[D]
[I.8]	Fallo de servicios de comunicación	[D]
[I.9]	Interrupción de otros servicios o suministros esenciales	[D]

[I.10]	Degradación de los soportes de almacenamiento	[D]
[I.11]	Emanaciones electromagnéticas	[C]
[E] Errores y fallos no intencionados		
[E.1]	Errores de los usuarios	[D][I][C]
[E.2]	Errores del administrador	[D][I][C]
[E.3]	Errores de monitorización	[I]
[E.4]	Errores de configuración	[I]
[E.7]	Deficiencias en la organización	[D]
[E.8]	Difusión de software dañino	[D][I][C]
[E.9]	Errores de re-encaminamiento	[C]
[E.10]	Errores de secuencia	[I]
[E.14]	Escapes de información	[C]
[E.15]	Alteración accidental de la información	[I]
[E.18]	Destrucción de la información	[D]
[E.19]	Fugas de información	[C]
[E.20]	Vulnerabilidades de los programas (software)	[D][I][C]
[E.21]	Errores de mantenimiento o actualización (software)	[D][I]
[E.23]	Errores de mantenimiento o actualización (hardware)	[D]

[E.24]	Caiga del sistema por agotamiento de recursos	[D]
[E.25]	Perdida de equipos	[D] [C]
[E.28]	Indisponibilidad del personal	[D]
[A] Ataques intencionados		
[A.3]	Manipulación de los registros de actividad	[I]
[A.4]	Manipulación de la configuración	[D][I][C]
[A.5]	Suplantación de la identidad del usuario	[C][A][I]
[A.6]	Abuso de privilegios de acceso	[D][I][C]
[A.7]	Uso no previsto	[D][I][C]
[A.8]	Difusión de software dañino	[D][I][C]
[A.9]	Re-encaminamiento de mensajes	[C]
[A.10]	Alteración de secuencia	[I]
[A.11]	Acceso no autorizado	[C][I]
[A.12]	Análisis de tráfico	[C]
[A.13]	Repudio	[I]
[A.14]	Interceptación de información	[C]
[A.15]	Modificación deliberada de la información	[I]
[A.18]	Destrucción de la información	[D]

[A.19]	Divulgación de información	[C]
[A.22]	Manipulación de programas	[D][I][C]
[A.23]	Manipulación de los equipos	[C][D]
[A.24]	Denegación de servicio	[D]
[A.25]	Robo	[C][D]
[A.26]	Ataque destructivo	[D]
[A.27]	Ocupación enemiga	[D][C]
[A.28]	Indisponibilidad del personal	[D]
[A.29]	Extorsión	[D][I][C]
[A.30]	Ingeniería social	[D][I][C]

Tabla 10. Escala de rango de frecuencia de amenazas

Valoración Cualitativa	Vulnerabilidad	Rango	Valor
MA	Frecuencia muy alta	1 vez al día	100
A	Frecuencia alta	1 vez cada semana	10
M	Frecuencia media	1 vez cada 2 meses	1
B	Frecuencia baja	1 vez cada 6 meses	1/10

MB	Frecuencia muy baja	1 vez al año	1/100

10.2 AMENAZAS A LAS QUE ESTÁN EXPUESTOS LOS ACTIVOS DE INFORMACIÓN DEL ÁREA DE SISTEMAS DE LA COOPERATIVA DEL MAGISTERIO DE TÚQUERRES.

A continuación se dan a conocer las amenazas definidas para los activos de información del área de sistemas:

Tabla 11. Amenazas para los activos de información

Activo TI		**Base de datos ORACLE**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de información**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/10

	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I11	Emanaciones electromagnéticas	1/100
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1
	E2	Errores del administrador	1/10
	E4	Errores de configuración	1
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/10
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización de equipos	1/100
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A5	Suplantación de la identidad del usuario	1/100
	A6	Abuso de privilegios de acceso	1/10
	A7	Uso no previsto	1/100
	A11	Acceso no autorizado	1/100
	A15	Modificación deliberada de la información	1/10
	A18	Destrucción de información	1/100
	A19	Divulgación de información	1/100
	A26	Ataque destructivo	1/100
Activo TI		**Documentos físicos**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de información**	
Tipo	**ID**	**Amenaza**	**Frecuencia**

Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/10
	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I10	Degradación de los soportes de almacenamiento de la información	1/10
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1
	E2	Errores del administrador	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/10
	E19	Fugas de información	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A5	Suplantación de la identidad del usuario	1/100
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/100
	A11	Acceso no autorizado	1/10
	A15	Modificación deliberada de la información	1/100
	A18	Destrucción de información	1/10
	A19	Divulgación de información	1

	A26	Ataque destructivo	1/100

Activo TI		**LINIX**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de software**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/100
	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10
	I11	Emanaciones electromagnéticas	1
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1
	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1
	E4	Errores de configuración	1
	E8	Difusión de software dañino	1/10

	E9	Errores de re-encaminamiento	1/10
	E10	Errores de secuencia	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización de equipos	1/100
	E20	Vulnerabilidades de los programas	1/10
	E21	Errores de mantenimiento/actualización	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1
	A8	Difusión de software dañino	1
	A9	Re-encaminamiento de mensajes	1/10
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/10
	A15	Modificación deliberada de la información	1/100
	A18	Destrucción de información	1/10
	A19	Divulgación de información	1/10
	A22	Manipulación de programas	1/10
	A23	Manipulación de programas	1/10

	A24	Denegación de servicio	1/10
	A25	Robo	1/10
	A26	Ataque destructivo	1/10

Activo TI		**SAPIENS**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de software**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/100
	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10
	I11	Emanaciones electromagnéticas	1
Errores y	E1	Errores de los usuarios	1/10
	E2	Errores del administrador	1/10

	E3	Errores de monitorización	1
	E4	Errores de configuración	1
	E8	Difusión de software dañino	1/10
	E9	Errores de re-encaminamiento	1/10
	E10	Errores de secuencia	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización de equipos	1/100
	E20	Vulnerabilidades de los programas	1/10
	E21	Errores de mantenimiento/actualización	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/100
	A8	Difusión de software dañino	1/100
	A9	Re-encaminamiento de mensajes	1/10
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/10
	A15	Modificación deliberada de la información	1/100
	A18	Destrucción de información	1/10
	A19	Divulgación de información	1/10

	A22	Manipulación de programas	1/100
	A23	Manipulación de programas	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**WINDOWS 7 PROFESIONAL**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de software**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/100
	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10

	I11	Emanaciones electromagnéticas	1/10
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1/10
	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1
	E4	Errores de configuración	1
	E8	Difusión de software dañino	1/10
	E9	Errores de re-encaminamiento	1/10
	E10	Errores de secuencia	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización de equipos	1/100
	E20	Vulnerabilidades de los programas	1/10
	E21	Errores de mantenimiento/actualización	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100

	A7	Uso no previsto	1/100
	A8	Difusión de software dañino	1/100
	A9	Re-encaminamiento de mensajes	1/10
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/10
	A15	Modificación deliberada de la información	1/100
	A18	Destrucción de información	1/10
	A19	Divulgación de información	1/10
	A22	Manipulación de programas	1/100
	A23	Manipulación de programas	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**OFFICE 2010**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de software**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10

	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/100
	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10
	I11	Emanaciones electromagnéticas	1/100
Errores y/o fallos no intencionados	E1	Errores de los usuarios	10
	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/10
	E8	Difusión de software dañino	1/10
	E9	Errores de re-encaminamiento	1/10
	E10	Errores de secuencia	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización de equipos	1/100
	E20	Vulnerabilidades de los programas	1/10
	E21	Errores de mantenimiento/actualización	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100

Ataques intencionados	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/100
	A8	Difusión de software dañino	1/100
	A9	Re-encaminamiento de mensajes	1/10
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/10
	A15	Modificación deliberada de la información	1/100
	A18	Destrucción de información	1/10
	A19	Divulgación de información	1/10
	A22	Manipulación de programas	1/100
	A23	Manipulación de programas	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**KASPERSKY ENDPOINT**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de software**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen	I1	Fuego	1/10
	I2	Daños por agua	1/10

	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/100
	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10
	I11	Emanaciones electromagnéticas	1/100
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1/10
	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/10
	E8	Difusión de software dañino	1/10
	E9	Errores de re-encaminamiento	1/10
	E10	Errores de secuencia	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización de equipos	1/100
	E20	Vulnerabilidades de los programas	1/10
	E21	Errores de mantenimiento/actualización	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10

	E25	Perdida de equipos	1/100
Ataques intencionados	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/100
	A8	Difusión de software dañino	1/100
	A9	Re-encaminamiento de mensajes	1/10
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/10
	A15	Modificación deliberada de la información	1/100
	A18	Destrucción de información	1/10
	A19	Divulgación de información	1/10
	A22	Manipulación de programas	1/100
	A23	Manipulación de programas	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**Servidor de base de datos**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de software**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10

	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/10
	I6	Corte del suministro eléctrico	1
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10
	I10	Degradación de los soportes de almacenamiento de información	1/10
	I11	Emanaciones electromagnéticas	1/100
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1/10
	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques inten	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100

	A7	Uso no previsto	1/100
	A11	Acceso no autorizado	1/100
	A15	Modificación deliberada de la información	1/100
	A18	Destrucción de información	1/10
	A19	Divulgación de información	1/10
	A23	Manipulación de programas	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**Servidor de proxy**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de software**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/10

	I6	Corte del suministro eléctrico	1
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10
	I10	Degradación de los soportes de almacenamiento de información	1/10
	I11	Emanaciones electromagnéticas	1/100
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1/10
	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/100
	A11	Acceso no autorizado	1/100
	A15	Modificación deliberada de la información	1/100

	A18	Destrucción de información	1/100
	A19	Divulgación de información	1/100
	A23	Manipulación de programas	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**Computadores HP**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de software**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/10
	I6	Corte del suministro eléctrico	1
	I7	Condiciones inadecuadas de temperatura o humedad	1/10

	I8	Fallo de servicios de comunicaciones	1/10
	I10	Degradación de los soportes de almacenamiento de información	1/10
	I11	Emanaciones electromagnéticas	1/100
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1/10
	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/100
	A11	Acceso no autorizado	1/100
	A15	Modificación deliberada de la información	1/100
	A18	Destrucción de información	1/100

	A19	Divulgación de información	1/100
	A23	Manipulación de programas	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**Switches HP**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo de software**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/10
	I6	Corte del suministro eléctrico	1
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10

Errores y/o fallos no intencionados	E1	Errores de los usuarios	1/10
	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/10
	E9	Errores de re-encaminamiento	1/10
	E10	Errores de secuencia	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/100
	A9	Re-encaminamiento de mensajes	1/100
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/100
	A12	Análisis de tráfico	1/10
	A14	Interceptación de información	1/100
	A15	Modificación deliberada de la información	1/100
	A19	Divulgación de información	1/100
	A24	Denegación de servicio	1/100

	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**Unidad NAS**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo físicos**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/10
	I4	Contaminación electromagnética	1/10
	I5	Avería de origen físico o lógico	1/10
	I6	Corte del suministro eléctrico	1
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10
	I10	Degradación de los soportes de almacenamiento	1/10
	I11	Emanaciones electromagnéticas	1/100
Er ro r	E1	Errores de los usuarios	1/10

	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/10
	E8	Difusión de software dañino	1/10
	E9	Errores de re-encaminamiento	1/10
	E10	Errores de secuencia	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E20	Vulnerabilidades de los programas (SW)	1/100
	E21	Errores de mantenimiento/actualización	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A3	Manipulación de los registros de actividad	1/100
	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/10
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/100
	A8	Difusión de software dañino	1/10
	A9	Re-encaminamiento de mensajes	1/100
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/100
	A12	Análisis de tráfico	1/10
	A14	Interceptación de información	1/100
	A15	Modificación deliberada de la información	1/100
	A18	Destrucción de información	1/10
	A19	Divulgación de información	1/100

	A22	Manipulación de programas	1/100
	A23	Manipulación de los equipos	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**Celulares**	
Responsable		**Área de Sistemas**	
Tipo activo		**Activo físicos**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1
	N2	Daños por agua	1
	N*	Desastres naturales	1
De origen industrial	I1	Fuego	1
	I2	Daños por agua	1
	I*	Desastres industriales	1
	I3	Contaminación mecánica	1
	I4	Contaminación electromagnética	1
	I5	Avería de origen físico o lógico	1
	I6	Corte del suministro eléctrico	1
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/10
	I10	Degradación de los soportes de almacenamiento	1/10

	I11	Emanaciones electromagnéticas	1/100
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1/10
	E2	Errores del administrador	1/10
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/10
	E8	Difusión de software dañino	1/10
	E9	Errores de re-encaminamiento	1/10
	E10	Errores de secuencia	1/10
	E15	Alteración accidental de la información	1/10
	E18	Destrucción de información	1/100
	E19	Fugas de información	1/10
	E20	Vulnerabilidades de los programas (SW)	1/100
	E21	Errores de mantenimiento/actualización	1/10
	E23	Errores de mantenimiento/actualización (HW)	1/10
	E24	Caída del sistema por agotamiento de recursos	1/10
	E25	Perdida de equipos	1/100
Ataques intencionados	A3	Manipulación de los registros de actividad	1/100
	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/100
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/100
	A8	Difusión de software dañino	1/10
	A9	Re-encaminamiento de mensajes	1/100
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/100
	A12	Análisis de tráfico	1
	A14	Interceptación de información	1
	A15	Modificación deliberada de la información	1/100

	A18	Destrucción de información	1/10
	A19	Divulgación de información	1/100
	A22	Manipulación de programas	1/10
	A23	Manipulación de los equipos	1/10
	A24	Denegación de servicio	1/10
	A25	Robo	1
	A26	Ataque destructivo	1

Activo TI		**Conectividad Internet**	
Responsable		**Área de Sistemas**	
Tipo activo		**Servicios**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/100
	I4	Contaminación electromagnética	1/100
	I5	Avería de origen físico o lógico	1/100
	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/100

	I9	Interrupción de otros servicios	1/10
	I11	Emanaciones electromagnéticas	1/100
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1/100
	E2	Errores del administrador	1/100
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/100
	E9	Errores de re-encaminamiento	1/100
	E10	Errores de secuencia	1/100
	E15	Alteración accidental de la información	1/100
	E18	Destrucción de información	1/10
	E19	Fugas de información	1/100
	E23	Errores de mantenimiento/actualización (HW)	1/100
	E24	Caída del sistema por agotamiento de recursos	1/100
	E25	Perdida de equipos	1/100
Ataques intencionados	A3	Manipulación de los registros de actividad	1/100
	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/100
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/10
	A9	Re-encaminamiento de mensajes	1/100
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/100
	A12	Análisis de tráfico	1/100
	A13	Repudio	1/100
	A14	Interceptación de información	1/100
	A15	Modificación deliberada de la información	1/100
	A19	Divulgación de información	1/100
	A23	Manipulación de los equipos	1/100

	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**Canal MPLS**	
Responsable		**Área de Sistemas**	
Tipo activo		**Servicios**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/100
	I4	Contaminación electromagnética	1/100
	I5	Avería de origen físico o lógico	1/100
	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/100
	I9	Interrupción de otros servicios	1/10
	I11	Emanaciones electromagnéticas	1/100
Er ro s	E1	Errores de los usuarios	1/100

	E2	Errores del administrador	1/100
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/100
	E9	Errores de re-encaminamiento	1/100
	E10	Errores de secuencia	1/100
	E15	Alteración accidental de la información	1/100
	E18	Destrucción de información	1/10
	E19	Fugas de información	1/100
	E23	Errores de mantenimiento/actualización (HW)	1/100
	E24	Caída del sistema por agotamiento de recursos	1/100
	E25	Perdida de equipos	1/100
Ataques intencionados	A3	Manipulación de los registros de actividad	1/100
	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/100
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/10
	A9	Re-encaminamiento de mensajes	1/100
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/100
	A12	Análisis de tráfico	1/100
	A13	Repudio	1/100
	A14	Interceptación de información	1/100
	A15	Modificación deliberada de la información	1/100
	A19	Divulgación de información	1/100
	A23	Manipulación de los equipos	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**Red de datos**	
Responsable		**Área de Sistemas**	
Tipo activo		**Servicios**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Desastres naturales	N1	Fuego	1/10
	N2	Daños por agua	1/10
	N*	Desastres naturales	1/10
De origen industrial	I1	Fuego	1/10
	I2	Daños por agua	1/10
	I*	Desastres industriales	1/10
	I3	Contaminación mecánica	1/100
	I4	Contaminación electromagnética	1/100
	I5	Avería de origen físico o lógico	1/100
	I6	Corte del suministro eléctrico	1/10
	I7	Condiciones inadecuadas de temperatura o humedad	1/10
	I8	Fallo de servicios de comunicaciones	1/100
	I9	Interrupción de otros servicios	1/10
	I11	Emanaciones electromagnéticas	1/100
Errores y/o fallos no intencionados	E1	Errores de los usuarios	1/100
	E2	Errores del administrador	1/100
	E3	Errores de monitorización	1/100
	E4	Errores de configuración	1/100
	E9	Errores de re-encaminamiento	1/100
	E10	Errores de secuencia	1/100

	E15	Alteración accidental de la información	1/100
	E18	Destrucción de información	1/10
	E19	Fugas de información	1/100
	E23	Errores de mantenimiento/actualización (HW)	1/100
	E24	Caída del sistema por agotamiento de recursos	1/100
	E25	Perdida de equipos	1/100
Ataques intencionados	A3	Manipulación de los registros de actividad	1/100
	A4	Manipulación de la configuración	1/10
	A5	Suplantación de la identidad del usuario	1/100
	A6	Abuso de privilegios de acceso	1/100
	A7	Uso no previsto	1/10
	A9	Re-encaminamiento de mensajes	1/100
	A10	Alteración de secuencia	1/100
	A11	Acceso no autorizado	1/100
	A12	Análisis de tráfico	1/100
	A13	Repudio	1/100
	A14	Interceptación de información	1/100
	A15	Modificación deliberada de la información	1/100
	A19	Divulgación de información	1/100
	A23	Manipulación de los equipos	1/100
	A24	Denegación de servicio	1/100
	A25	Robo	1/100
	A26	Ataque destructivo	1/100

Activo TI		**Jefe de sistemas**	
Responsable		**Área de Sistemas**	
Tipo activo		**Servicios**	
Tipo	**ID**	**Amenaza**	**Frecuencia**

Errores de los usuarios	E2	Errores del administrador	1/100
	E7	Deficiencias de la organización	1/10
	E19	Fugas de información	1/100
	E28	Indisponibilidad del personal	1/10
Ataques intencionados	A28	Indisponibilidad del personal	1/100
	A29	Extorsión	1/100
	A30	Ingeniería social	1/100

Activo TI		**Profesional Área de sistemas**	
Responsable		**Área de Sistemas**	
Tipo activo		**Servicios**	
Tipo	**ID**	**Amenaza**	**Frecuencia**
Errores de los usuarios	E2	Errores del administrador	1/100
	E7	Deficiencias de la organización	1/10
	E19	Fugas de información	1/100
	E28	Indisponibilidad del personal	1/10
Ataques intencionados	A28	Indisponibilidad del personal	1/100
	A29	Extorsión	1/100
	A30	Ingeniería social	1/100

10.3 ANÁLISIS ANEXO A DE LA NORMA EN LA INFORMACIÓN RECOLECTADA

10.3.1 Aplicabilidad en Dominios, Objetivos de control y Controles acorde a la norma ISO 27001:2013

Tabla 12. Controles identificados

DECLARACIÓN DE APLICABILIDAD

REF.	CONTROL			
A.5	**POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN**	**CUMPLIMIENTO**		**RECOMENDACIONES**
A.5.1	**Orientación de la dirección para la gestión de la seguridad de la información**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.5.1.1	Políticas para la seguridad de la información		X	Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.
A.5.1.2	Revisión de las políticas para la seguridad de la información		X	Las políticas se deben ser revisadas en intervalos planificados.
A.6	**ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN**			
A.6.1	**Organización interna**			
		Cumple	**No**	**Recomendaciones a**

			cumple	implementar
A.6.1.1	Roles y responsabilidades para la seguridad de la información		X	Se deben definir y asignar todas las responsabilidades de la seguridad de la información.
A.6.1.2	Separación de deberes		X	Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización.
A.6.1.3	Contacto con las autoridades		X	Se deben mantener contactos apropiados con las autoridades pertinentes.
A.6.1.4	Contacto con grupos de interés especial	X		
A.6.1.5	Seguridad de la información en la gestión de proyectos		X	La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.
A.6.2	**Dispositivos móviles y teletrabajo**			
A.6.2.1	Política para dispositivos móviles		X	Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.
A.6.2.2	Teletrabajo		X	Se deben mantener una política y unas medidas de seguridad de soporte, para proteger la información a la se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.
A.7	**SEGURIDAD DE LOS RECURSOS HUMANOS**			
A.7.1	**Antes de asumir el empleo**			

		Cumple	No cumple	Recomendaciones a implementar
A.7.1.1	Selección	X		
A.7.1.2	Términos y condiciones del empleo		X	Los acuerdos contractuales con empleados y contratistas deben establecer sus responsabilidades y las de la organización en cuanto a la seguridad de la información.
A.7.2	**Durante la ejecución del empleo**			
A.7.2.1	Responsabilidades de la dirección		X	La dirección debe exigir a todos los empleados y contratistas la aplicación de la seguridad de la información de acuerdo con las políticas y procedimientos establecidos por la organización.
A.7.2.2	Toma de conciencia, educación y formación en la seguridad de la información		X	Todos los empleados de la organización y en donde sea pertinente, los contratistas, deben recibir educación y concientización sobre las políticas y procedimientos de seguridad en la organización.
A.7.2.3	Proceso disciplinario		X	Se debe contar con un proceso formal, el cual debe ser comunicado, para emprender acciones contra empleados que hayan cometido una violación a la seguridad de la información.
A.7.3	**Terminación y cambio de empleo**			

A.7.3.1	Terminación o cambio de responsabilidades de empleo		X	Las responsabilidades y deberes de seguridad de la información que permanecen válidos después de la terminación o cambio de empleo se deben definir y cumplir.
A.8	**GESTIÓN DE ACTIVOS**			
A.8.1	**Responsabilidad por los activos**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.8.1.1	Inventario de activos	X		
A.8.1.2	Propiedad de los activos	X		
A.8.1.3	Uso aceptable de los activos		X	Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.
A.8.1.4	Devolución de activos	X		
A.8.2	**Clasificación de la información**			
A.8.2.1	Clasificación de la información		X	La información se debe clasificar en función de los requisitos legales, valor, criticidad y susceptibilidad a divulgación o a modificación no autorizada.

A.8.2.2	Etiquetado de la información		X	Se deben desarrollar e implementar un conjunto adecuado de procedimientos para el etiquetado de la información, de acuerdo con el esquema de clasificación de información adoptado.
A.8.2.3	Manejo de activos		X	Se deben implementar procedimientos para el manejo de activos, de acuerdo con el esquema de información adoptado.
A.8.3	**Manejo de medios**			
A.8.3.1	Gestión de medios removibles		X	Se deben implementar procedimientos para la gestión de medios removibles.
A.8.3.2	Disposición de los medios		X	Se debe disponer en forma segura de los medios cuando ya no se requieran, utilizando procedimientos formales.
A.8.3.3	Transferencia de medios físicos	X		
A.9	**CONTROL DE ACCESO**			
A.9.1	**Requisitos del negocio para control de acceso**			
A.9.1.1	Política de control de acceso		X	Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de SI.
A.9.1.2	Acceso a redes y a servicios en red	X		

A.9.2	**Gestión de acceso de usuarios**			
A.9.2.1	Registro y cancelación del registro de usuarios		X	Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.
A.9.2.2	Suministro de acceso de usuarios		X	Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.
A.9.2.3	Gestión de derechos de acceso privilegiado		X	Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado
A.9.2.4	Gestión de información de autenticación secreta de usuarios		X	La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.
A.9.2.5	Revisión de los derechos de acceso de usuarios		X	Los propietarios de los activos deben revisar los derechos de acceso de los usuarios.
A.9.2.6	Retiro o ajuste de los derechos de acceso	X		Se deben retirar todos los derechos de acceso a la información cuando los empleados o usuarios terminan su empleo.
A.9.3	**Responsabilidades de los usuarios**			
A.9.3.1	Uso de información de autenticación secreta		X	Se debe exigir a los usuarios que cumplan las prácticas de la organización para el uso de información de autenticación

				secreta.
A.9.4	**Control de acceso a sistemas y aplicaciones**			
A.9.4.1	Restricción de acceso a la información		X	El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.
A.9.4.2	Procedimiento de ingreso seguro	X		
A.9.4.3	Sistema de gestión de contraseñas	X		
A.9.4.4	Uso de programas utilitarios privilegiados	X		
A.9.4.5	Control de acceso a códigos fuente de programas		X	Se debe restringir el acceso a los códigos fuente de los programas.
A.10	**CRIPTOGRAFÍA**			
A.10.1	**Controles criptográficos**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.10.1.1	Política sobre el uso de controles criptográficos		X	Se debe implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.10.1.2	Gestión de llaves		X	Se debe implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas durante todo su ciclo de vida.
A.11	**SEGURIDAD FÍSICA Y DEL ENTORNO**			

A.11.1	Áreas seguras			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.11.1.1	Perímetro de seguridad física		X	Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o crítica, e instalaciones de manejo de información.
A.11.1.2	Controles de acceso físicos		X	Las áreas seguras se deben proteger mediante controles de acceso apropiados para asegurar que solo se permite el acceso a personal autorizado.
A.11.1.3	Seguridad de oficinas, recintos e instalaciones		X	Se debe diseñar y aplicar seguridad física a oficinas, recintos e instalaciones.
A.11.1.4	Protección contra amenazas externas y ambientales		X	Se debe diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.
A.11.1.5	Trabajo en áreas seguras		X	Se deben diseñar y aplicar procedimientos para trabajo en áreas seguras.
A.11.1.6	Áreas de despacho y carga		X	Se deben controlar áreas o puntos donde pueden entrar personas no autorizadas, y si es posible, aislarlos de las instalaciones de procesamiento de información para evitar el acceso no autorizado.
A.11.2	**Equipos**			

A.11.2.1	Ubicación y protección de los equipos		X	Los equipos deben estar ubicados y protegidos para reducir los riesgos de amenazas y peligros del entorno y las posibilidades de acceso no autorizado.
A.11.2.2	Servicios de suministro	X		
A.11.2.3	Seguridad del cableado		X	El cableado de energía eléctrica y de telecomunicaciones que porta datos o brinda soporte a los servicios de información se debe proteger contra interceptación, interferencia o daño.
A.11.2.4	Mantenimiento de equipos	X		
A.11.2.5	Retiro de activos		X	Los equipos, información o software no se deben retirar de su sitio sin autorización previa.
A.11.2.6	Seguridad de equipos y activos fuera de las instalaciones		X	Se deben aplicar medidas de seguridad a los activos que se encuentran fuera de las instalaciones de la organización, teniendo en cuenta diferentes riesgos de trabajar fuera de las oficinas.
A.11.2.7	Disposición segura o reutilización de equipos	X		
A.11.2.8	Equipos de usuario desatendido	X		
A.11.2.9	Política de escritorio limpio y pantalla limpia		X	Se debe adoptar una política de escritorio limpio para los papeles y medios de almacenamiento removibles, y una política de pantalla limpia en las instalaciones de procesamiento de información.

A.12	**SEGURIDAD DE LAS OPERACIONES**			
A.12.1	**Procedimientos operacionales y responsabilidades**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.12.1.1	Procedimientos de operación documentados		X	Los procedimientos de operación se deben documentar y poner a disposición de todos los usuarios que los necesitan.
A.12.1.2	Gestión de cambios		X	Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afecten la SI.
A.12.1.3	Gestión de capacidad		X	Se debe hacer seguimiento al uso de recursos, hacer los ajustes y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.
A.12.1.4	Separación de los ambientes de desarrollo, pruebas y operación		X	Se deben separar los ambientes de desarrollo, prueba y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.
A.12.2	**Protección contra códigos maliciosos**			
A.12.2.1	Controles contra códigos maliciosos		X	Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios.

A.12.3	**Copias de respaldo**			
A.12.3.1	Respaldo de la información		X	Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.
A.12.4	**Registro y seguimiento**			
A.12.4.1	Registro de eventos		X	Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de SI.
A.12.4.2	Protección de la información de registro		X	Las instalaciones y la información de registro se deben proteger contra la alteración y acceso no autorizado.
A.12.4.3	Registros del administrador y del operador		X	Las actividades del administrador y del operador del sistema se deben registrar, y los registros se deben proteger y revisar con regularidad.
A.12.4.4	Sincronización de relojes	X		
A.12.5	**Control de software operacional**			
A.12.5.1	Instalación de software en sistemas operativos		X	Se deben implementar procedimientos para la instalación de software en los sistemas operativos.
A.12.6	**Gestión de la vulnerabilidad técnica**			

A.12.6.1	Gestión de las vulnerabilidades técnicas		X	Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización y tomar las medidas para tratar el riesgo.
A.12.6.2	Restricciones sobre la instalación de software	X		
A.12.7	**Consideraciones sobre auditorías de sistemas de información**			
A.12.7.1	Controles de auditorías de sistemas de información	X		
A.13	**SEGURIDAD DE LAS COMUNICACIONES**			
A.13.1	**Gestión de la seguridad de las redes**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.13.1.1	Controles de redes	X		
A.13.1.2	Seguridad de los servicios de red	X		
A.13.1.3	Separación en las redes		X	Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.
A.13.2	**Transferencia de información**			
A.13.2.1	Políticas y procedimientos de transferencia de información		X	Se deben contar con políticas, procedimientos y controles de transferencia formales para proteger la transferencia de información mediante el uso de todo tipo de instalaciones de comunicaciones.
A.13.2.2	Acuerdos sobre transferencia de información	X		

A.13.2.3	Mensajería electrónica		X	Se debe proteger adecuadamente la información incluida en la mensajería electrónica.
A.13.2.4	Acuerdos de confidencialidad o de no divulgación		X	Se deben identificar, revisar regularmente y documentar los requisitos para los acuerdos de confidencialidad para la protección de la información.
A.14	**ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS**			
A.14.1	**Requisitos de seguridad de los sistemas de información**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información		X	Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras en los existentes.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas		X	La información involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales, divulgación y modificación no autorizadas.

A.14.1.3	Protección de transacciones de los servicios de las aplicaciones		X	La información involucrada en las transacciones de los servicios de las aplicaciones se debe proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada y la duplicación o reproducción de mensajes no autorizada.
A.14.2	**Seguridad en los procesos de desarrollo y de soporte**			
A.14.2.1	Política de desarrollo seguro		X	Se deben establecer y aplicar reglas para el desarrollo de software y de sistemas, a los desarrollos dentro de la organización.
A.14.2.2	Procedimientos de control de cambios en sistema		X	Los cambios a los sistemas dentro del ciclo de vida de desarrollo se deben controlar mediante el uso de procedimientos formarles de control de cambios.
A.14.2.3	Revisión técnica de las aplicaciones después de cambios en la plataforma de operación		X	Cuando se cambian las plataformas de operación, se deben revisar las aplicaciones críticas del negocio, y someter a prueba para asegurar que no haya impacto adverso en las operaciones o seguridad de la organización.

A.14.2.4	Restricciones en los cambios a los paquetes de software		X	Se deben desalentar las modificaciones a los paquetes de software, los cuales se deben limitar a los cambios necesarios, y todos los cambios se deben controlar estrictamente.
A.14.2.5	Principios de construcción de los sistemas seguros		X	Se deben establecer, documentar y mantener principios para la construcción de sistemas seguros, y aplicarlos a cualquier actividad de implementación de sistemas de información.
A.14.2.6	Ambiente de desarrollo seguro		X	Las organizaciones deben establecer y proteger adecuadamente los ambientes de desarrollo seguros para las actividades de desarrollo e integración de sistemas que comprendan todo el ciclo de vida de desarrollo de sistemas.
A.14.2.7	Desarrollo contratado externamente	X		
A.14.2.8	Pruebas de seguridad de sistemas		X	Durante el desarrollo se deben llevar a cabo pruebas de funcionalidad de la seguridad.
A.14.2.9	Prueba de aceptación de sistemas		X	
A.14.3	**Datos de prueba**			
A.14.3.1	Protección de datos de prueba		X	Los datos de prueba se deben seleccionar, proteger y controlar cuidadosamente.
A.15	**RELACIONES CON LOS PROVEEDORES**			

A.15.1	**Seguridad de la información en las relaciones con los proveedores**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.15.1.1	Política de seguridad de la información para las relaciones con proveedores		X	Los requisitos de seguridad de la información para mitigar los riesgos asociados con el acceso de proveedores a los activos de la organización se deben acordar con estos y se deben documentar.
A.15.1.2	Tratamiento de la seguridad dentro de los acuerdos con proveedores		X	Se deben establecer y acordar todos los requisitos de seguridad de la información pertinentes con cada proveedor que pueda tener acceso, procesar, almacenar, comunicar o suministrar componentes de infraestructura de TI para la información.
A.15.1.3	Cadena de suministro de tecnología de información y comunicación		X	Los acuerdos con proveedores deben incluir requisitos para tratar los riesgos de seguridad de la información asociados con la cadena de suministro de productos y servicios de tecnología.
A.15.2	**Gestión de la prestación de servicios de proveedores**			
A.15.2.1	Seguimiento y revisión de los servicios de los proveedores		X	La organización debe hacer seguimiento, revisar y auditar con regularidad la prestación de servicios de los proveedores.

A.15.2.2	Gestión de cambios en los servicios de los proveedores		X	Se deben gestionar los cambios en el suministro de servicios por parte de los proveedores, incluido el mantenimiento y la mejora de las políticas, procedimientos y controles de seguridad de la información existentes, teniendo en cuenta la criticidad de la información, sistemas y procesos del negocio involucrados.
A.16	**GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN**			
A.16.1	**Gestión de incidentes y mejoras en la seguridad de la información**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.16.1.1	Responsabilidades y procedimientos		X	Se deben establecer las responsabilidades y procedimientos de gestión para asegurar una respuesta rápida, eficaz y ordenada a los incidentes de seguridad de la información.
A.16.1.2	Reporte de eventos de seguridad de la información	X		
A.16.1.3	Reporte de debilidades de seguridad de la información		X	Se debe exigir a todos los empleados y contratistas que usan los servicios y sistemas de información de la organización, que observen y reporten cualquier debilidad de seguridad de la información observada o sospechada en los sistemas.

A.16.1.4	Evaluación de eventos de seguridad de la información y decisiones sobre ellos.		X	Los eventos de seguridad de la información se deben evaluar y se debe decidir si se van a clasificar como incidentes de seguridad de la información.
A.16.1.5	Respuesta a incidentes de seguridad de la información		X	Se debe dar respuesta a los incidentes de seguridad de la información de acuerdo con procedimientos documentados.
A.16.1.6	Aprendizaje obtenido de los incidentes de seguridad de la información	X		
A.16.1.7	Recolección de evidencia		X	La organización debe definir y aplicar procedimientos para la identificación, recolección, adquisición y preservación de información que pueda servir como evidencia.
A.17	**ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE CONTINUIDAD DE NEGOCIO**			
A.17.1	**Continuidad de seguridad de la información**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.17.1.1	Planificación de la continuidad de la seguridad de la información		X	La organización debe determinar sus requisitos para la 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		X	La organización debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido 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		X	La organización debe verificar a intervalos regulares los controles de continuidad de la seguridad de la información establecidos e implementados, con el fin de asegurar que con válidos y eficaces durante situaciones adversas.
A.17.2	**Redundancias**			
A.17.2.1	Disponibilidad de instalaciones de procesamiento de información		X	Las instalaciones de procesamiento de la información se deben implementar con redundancia suficiente para cumplir los requisitos de disponibilidad.
A.18	**CUMPLIMIENTO**			
A.18.1	**Cumplimiento de requisitos legales y contractuales**			
		Cumple	**No cumple**	**Recomendaciones a implementar**
A.18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	X		

A.18.1.2	Derechos de propiedad intelectual		X	Se deben implementar procedimientos apropiados para asegurar el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software patentados.
A.18.1.3	Protección de registros		X	Los registros se deben proteger contra pérdida, destrucción, falsificación, acceso no autorizado y liberación no autorizada, de acuerdo con los requisitos legislativos, de reglamentación pertinentes, cuando sea aplicable.
A.18.1.4	Privacidad y protección de información de datos personales	X		
A.18.1.5	Reglamentación de controles criptográficos		X	Se deben usar controles criptográficos, en cumplimiento de todos los acuerdos, legislación y reglamentación pertinentes.
A.18.2	**Revisiones de seguridad de la información**			
A.18.2.1	Revisión independiente de la seguridad de la información		X	El enfoque de la organización para la gestión de la seguridad de la información y su implementación.

A.18.2.2	Cumplimiento con las políticas y normas de seguridad		X	La dirección debe revisar con regularidad el cumplimiento del procesamiento y procedimientos de información dentro de su área de responsabilidad, con las políticas y normas de seguridad apropiadas, y cualquier otro requisito de seguridad.
A.18.2.3	Revisión del cumplimiento técnico		X	Los sistemas de información se deben revisar periódicamente para determinar el cumplimiento con las políticas y normas de seguridad de la información.

10.4 PLAN DE IMPLEMENTACIÓN DEL SISTEMA DE SEGURIDAD DE LA INFORMACIÓN PARA EL ÁREA DE INFORMATICA.

10.4.1 Liderazgo y compromiso

Es de gran importancia que las directivas (Gerencia y Consejo de Administración) de la Cooperativa del Magisterio de Túquerres sean conscientes de la importancia de implementar un sistema de gestión de la seguridad de la información (SGSI) no solo en el área informática sino en toda la organización. Por lo tanto es necesario comprometerse con lo siguiente:

a) Asegurar que se establezca la política y los objetivos de la seguridad de la información y que estos sean viables con la dirección estratégica de la organización.

b) Asegurar la integración de los requisitos del sistema de gestión de la seguridad de la información en los procesos de la organización.

c) Asegurar que los recursos necesarios para el sistema de gestión de la seguridad de la información estén disponibles.

d) Comunicar la importancia de una gestión de la seguridad de la información eficiente y de conformidad con los requisitos del SGSI.

e) Asegurar y supervisar que el SGSI logre los resultados previstos.

f) Promover la mejora continua del SGSI y apoyar otros roles pertinentes de la dirección, para demostrar su liderazgo aplicado a las áreas de responsabilidad.

10.4.2 Política

La información es un activo que tiene valor para la cooperativa y por consiguiente debe ser protegida y resguardada adecuadamente, garantizando la continuidad de los sistemas de información, minimizando los riesgos de daño y contribuyendo así, a una mejor gestión del área de informática.

Para la Cooperativa del Magisterio de Túquerres es evidente la necesidad de implementar políticas adecuadas al propósito de la organización para la seguridad de la información, las cuales deben ser analizadas y aprobadas por la alta dirección, además de ser difundidas, comunicadas y cumplidas por todo el personal externo e interno de la empresa.

A continuación se proponen que la Cooperativa debe desarrollar e implementar las siguientes políticas:

Tabla 13. Políticas propuestas

POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
El área de sistemas debe crear y aprobar un documento de política de seguridad de la información y lo debe publicar y comunicar a todos los empleados y partes externas pertinentes.
PARTES EXTERNAS
El área de sistemas debe identificar los riesgos de la información y los servicios de procesamiento así como los procesos que involucran partes externas e implementar los controles apropiados antes de autorizar el acceso.
RESPONSABILIDAD POR LOS ACTIVOS
Todos los activos del área de sistemas deben estar claramente identificados y se debe elaborar y mantener un inventario de todos los activos importantes.
POLÍTICA DE SEGURIDAD EN DISPOSITIVOS MOVILES
Se deben asignar privilegios con la mayor seguridad que permitan acceder solo a los usuarios autorizados, con la integridad y confidencialidad que requiere el proceso, además se debe dejar registro de todos los accesos.
POLÍTICA PARA LA CONTRATACIÓN DE PERSONAL
Tanto al momento de realizar la contratación como el tiempo que dure el empleo, se debe divulgar, aceptar y cumplir las políticas de seguridad de la información que se hayan establecido

en el área de informática de la cooperativa.
SEGURIDAD FÍSICA Y DEL ENTORNO
El área de sistemas debe utilizar perímetros de seguridad (barreras tales como paredes, puertas de acceso controladas con tarjeta o mostradores de recepción atendidos) para proteger las áreas que contienen información y servicios de procesamiento de información, esto con el fin de controlar de restringir el acceso solo al personal autorizado.
SEGURIDAD DE LOS EQUIPOS
Los equipos deben estar ubicados o protegidos para reducir el riesgo debido a amenazas o peligros del entorno (pérdida, robo, ausencia de energía), y las oportunidades de acceso no autorizado.
GESTIÓN DE COMUNICACIONES Y OPERACIONES
Los procedimientos de operación se deben documentar, mantener y estar disponible para todos los usuarios autorizados que los requieran, manteniendo registros del uso y cambio en la configuración de los servicios de procesamiento y transmisión de información.
PROTECCIÓN CONTRA CÓDIGOS MALICIOSOS
Se deben implementar controles de detección, prevención y recuperación para proteger la información contra códigos maliciosos, así como procedimientos apropiados de concientización a los usuarios.
POLÍTICA DE RESPALDO
Se deben hacer copias de respaldo de la información y del software y poner a prueba cada cierto tiempo para comprobar el restablecimiento adecuado de los datos.
GESTIÓN DE LA SEGURIDAD EN REDES
Las redes de datos se deben mantener y controlar adecuadamente para protegerlas de las amenazas y mantener la seguridad de los sistemas y aplicaciones que usan la red incluyendo la información en tránsito.
POLÍTICA DE CONTROL DE ACCESO
En el área de sistemas debe existir un procedimiento formal para el registro y cancelación de usuarios con el fin de conceder y revocar el acceso a todos los sistemas y servicios de información, además de restringir y controlar la asignación y uso de privilegios y contraseñas.
RESPONSABILIDADES DE LOS USUARIOS
El área de sistemas debe exigir a los usuarios el cumplimiento de buenas prácticas de seguridad en la selección y el uso de las contraseñas, además de concientizarlos sobre el uso adecuado de los equipos y programas que se tienen a su disposición.
CONTROL DE ACCESO A LAS APLICACIONES Y A LA INFORMACIÓN
El área de sistemas debe restringir el acceso a la información y a las funciones del sistema de aplicación por parte de los usuarios y del personal de soporte, de acuerdo con la política definida de control de acceso.

ADQUISICIÓN DE DESARROLLO Y MANTENIMIENTO A SISTEMAS DE INFORMACIÓN
Las declaraciones sobre los requisitos del negocio para nuevos sistemas de información o mejoras de los sistemas existentes deben especificar los requisitos para los controles de seguridad establecidos por la cooperativa. En este caso es importante incorporar verificaciones de validación en las aplicaciones para detectar cualquier corrupción de la información por errores de procesamiento o actos deliberados.
CONTROLES CRIPTOGRÁFICOS
El área de sistemas debe implementar un sistema de gestión de llaves para apoyar el uso de las técnicas criptográficas, las cuales se deben desarrollar e implementar en una política sobre el uso de los controles criptográficos para la protección de la información.
GESTIÓN DE LA VULNERABILIDAD TÉCNICA
El área de sistemas debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información que están en uso, evaluar la exposición a dichas vulnerabilidades y tomar las acciones apropiadas para tratar los riesgos asociados.
GESTIÓN DE LOS INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN
Los eventos de la seguridad de la información se deben informar a través de los canales de gestión apropiados tan pronto como sea posible.
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO
El área de informática debe desarrollar y mantener un proceso de gestión para la continuidad del negocio en toda la organización el cual trate los requisitos de seguridad de la información necesarios para su continuidad.
CUMPLIMIENTO DE LOS REQUISITOS LEGALES
Todos los requisitos estatutarios, reglamentarios y contractuales pertinentes, así como el enfoque de la organización para cumplir estos requisitos se deben definir explícitamente, documentar y mantener actualizados para cada sistema de información y para el área de informática.
POLÍTICA DE CONFORMACIÓN Y SUPERVISIÓN DEL COMITÉ DE SEGURIDAD
Se debe definir un comité de seguridad de la información, el cual validara, monitoreara y actualizara el sistema de seguridad de la información.

10.4.3 Procedimientos de seguridad

Teniendo en cuenta las políticas de seguridad de la información documentadas anteriormente, es necesario establecer procedimientos de seguridad que faciliten el cumplimiento de las mismas en el área de sistemas de la Cooperativa del Magisterio de Túquerres, por lo tanto se proponen las siguientes:

Tabla 14. Procedimientos de seguridad

PROCEDIMIENTO DE BACKUP DE SERVIDORES
Objetivo: Garantizar copias de respaldo de los datos y archivos de configuración de los diferentes servidores tanto operativos como de aplicaciones del área de sistemas.
Alcance: Aplicara a los servidores; proxy, aplicaciones y base de datos.
PROCEDIMIENTO DE DADO DE BAJA Y/O RECICLADO DE EQUIPOS
Objetivo: Establecer un procedimiento que garantice que al dar de baja y/o reciclar equipos de cómputo, la información contenida en dichos elementos sea efectivamente destruida.
Alcance: Aplicara a todos los equipos que constituyan la infraestructura informática de la entidad.
PROCEDIMIENTO DE GESTIÓN DE VULNERABILIDADES Y ASEGURAMIENTO DE PLATAFORMA
Objetivo: Identificar vulnerabilidades en los activos de información de la entidad y reducir su exposición a ataques internos y/o externos.
Alcance: Este procedimiento aplica a todo el sistema de información de la entidad.
MONITOREO DE CONTROLES
Objetivo: Establecer las actividades que permitan realizar el monitoreo de los controles especificados en las políticas de seguridad de la información.
Alcance: Este procedimiento debe aplicar a todos los controles especificados.
PROCEDIMIENTO PARA LA GESTIÓN DE MEDIOS REMOVIBLES
Objetivo: Definir los lineamientos que deben tenerse en cuenta para habilitar los puertos USB en cualquier equipo de la entidad, con el propósito de preservar los principios de seguridad (integridad, confidencialidad y disponibilidad) de la información.
Alcance: Este procedimiento está definido para llevar a cabo la activación de puertos USB en los equipos, desde su requerimiento hasta su habilitación total.
PROCEDIMIENTO PARA LA ELIMINACIÓN SEGURA DE INFORMACIÓN DE MEDIOS DE ALMACENAMIENTO
Objetivo: Definir el mecanismo apropiado para la eliminación segura de información de dispositivos de almacenamiento electrónico.
Alcance: Este procedimiento está definido para llevar a cabo la eliminación segura de información de equipos o elementos electrónicos.
PROCEDIMIENTO PARA LA ACTUALIZACIÓN DE LA POLÍTICA DE SEGURIDAD DE LA INFORMACIÓN
Objetivo: Revisar y mantener actualizadas las políticas de seguridad de la información de la entidad.
Alcance: Políticas de seguridad.

10.4.4 Roles y responsabilidades

La alta dirección debe asegurarse de que las responsabilidades y autoridades para los roles pertinentes a la seguridad de la información se asignen y comuniquen, para esto se debe asignar la responsabilidad y autoridad para:

a) Asegurarse de que el SGSI sea conforme con los requisitos de la norma ISO 27001:2013.

b) Informar oportunamente el desempeño del SGSI.

10.4.5 Planificación

10.4.5.1 Valoración de riesgos de la seguridad de la información

El área de informática debe definir y aplicar un proceso de valoración de riesgos de la seguridad de la información que permita:

a) Establecer y mantener los criterios de riesgos y de aceptación de la misma.

b) Asegurar que las valoraciones repetidas de riesgos de la seguridad de la información produzcan resultados consistentes, válidos y comparables.

c) Aplicar el proceso de valoración de riesgos de la seguridad de la información para Identificar riesgos asociados a la perdida de la confidencialidad, integridad y disponibilidad, al igual que a los dueños de los mismos.
d) Analizar y evaluar los riesgos para priorizar los que mayor impacto puedan ocasionar para el área de informática de la Cooperativa.

10.4.5.2 Plan de tratamiento de riesgos

Para cada uno de los riesgos identificados después de la evaluación de riesgos es necesario dar un tratamiento. Las opciones posibles para el tratamiento del riesgo deberían incluir:

Aplicación de los controles apropiados para reducir el riesgo.

Aceptación objetiva y con conocimiento de los riesgos, siempre y cuando ellos satisfagan la política respectiva para la seguridad de la información.

Evitación de los riesgos al no permitir acciones que pudieran hacer que estos se presentaran.

Transferencia de riesgos asociados a otras partes.

Para aquellos riesgos en donde la decisión de tratamiento del riesgo ha sido la aplicación de controles apropiados, dichos controles se encuentran descritos anteriormente y se deben implementar adecuadamente.

10.4.6 Objetivos de seguridad de la información

Es importante que la organización establezca los objetivos de seguridad de la información en las funciones y niveles pertinentes, los cuales deben:

a) Ser coherentes con la política de seguridad de la información y medibles dentro de las posibilidades.

b) Tener en cuenta los requisitos de la seguridad de la información, los resultados de la valoración y del tratamiento de riesgos.

c) Ser comunicados y actualizados cuando sea pertinente.

Cuando se hace la planificación para lograr los objetivos de la seguridad de la información, es importante que la organización o en este caso el área de informática, determine lo que se va a hacer, los recursos que se requieren, quien será el responsable, cuando se finalizara y como se evaluarán los resultados.

10.4.7 Soporte

10.4.7.1 Recursos

La organización debe determinar y proporcionar los recursos necesarios para el establecimiento, implementación, mantenimiento y mejora continua del SGSI.

10.4.7.2 Competencia

La organización debe determinar la competencia necesaria de las personas que realizan, bajo su control, un trabajo que afecta su desempeño de la seguridad de la información, y de asegurarse que estas personas sean competentes, basándose en la educación, formación y experiencia adecuadas.

Cuando sea necesario se deben tomar las acciones para adquirir competencia necesaria para evaluar la eficacia de las acciones tomadas y así conservar la información documentada apropiada, como evidencia de la competencia.

10.4.8 Toma de conciencia

Las personas que realizan el trabajo bajo el control de la organización deben tomar conciencia de la política de la seguridad de la información, su contribución a la eficacia del SGSI, incluyendo los beneficios de una mejora del desempeño de la seguridad de la información.

Es importante realizar campañas de concientización y sensibilización a todo el personal involucrado en los procesos que afecten la confidencialidad, disponibilidad e integridad de la información.

10.4.9 Comunicación

El área de informática debe determinar la necesidad de comunicaciones internas y externas pertinentes al SGSI, las cuales deben incluir el contenido de la comunicación, cuando, quien y a quien comunicar, además de los procesos para llevar a cabo la comunicación.

10.4.10 Evaluación del desempeño

10.4.10.1 Seguimiento, medición, análisis y evaluación

El área de informática debe evaluar el desempeño de la seguridad de la información y la eficacia del SGSI.

La organización debe determinar:

a) A que es necesario hacer seguimiento y que es necesario medir, incluidos los procesos y controles de la seguridad de la información.

b) Los métodos de seguimiento, medición, análisis y evaluación, según sea aplicable, para asegurar resultados válidos.

c) Cuando se deben llevar a cabo el seguimiento y la medición.

d) Quien debe llevar a cabo el seguimiento y la medición.

e) Cuando se deben analizar y evaluar los resultados del seguimiento, la medición y quien debe analizar y evaluar los resultados.

La organización debe conservar la información documentada apropiada como evidencia de los resultados del monitoreo y de la medición.

10.4.10.2 Auditoria interna

La organización debe llevar a cabo auditorías internas de manera periódica y a intervalos planificados, para proporcionar información acerca de si el sistema de gestión de la seguridad de la información está conforme con los requisitos de la organización y de la norma ISO 27001:2013, además si esta implementado y mantenido eficazmente.

Por todo lo anterior la organización debe:

a) Planificar, establecer, implementar y mantener uno o varios programas de auditoria que incluyan la frecuencia, los métodos, las responsabilidades, los requisitos de planificación, y la elaboración de informes. Los programas de auditoria deben tener en cuenta la importancia de los procesos involucrados y las auditorias previas.

b) Para cada auditoria se debe definir los criterios y el alcance de esta, al igual que seleccionar los auditores y llevar a cabo auditorias para asegurarse la objetividad e imparcialidad del proceso.

c) Los resultados de las auditorias deben ser informados a la dirección pertinente y se debe conservar la información documentada como evidencia de la implementación del programa de auditoria y los resultados de esta.

10.4.10.3 Revisión por la dirección

La alta dirección debe revisar constantemente el sistema de gestión de la seguridad de la información del área de informática, para asegurarse de su conveniencia, adecuación y eficacia continuas.

La revisión efectuada por la dirección debe incluir las siguientes consideraciones:

a) El estado de las acciones con relación a las revisiones previas por la dirección.

b) Los cambios en las cuestiones externas e internas que sean pertinentes al sistema de gestión de la seguridad de la información.

c) La retroalimentación sobre el desempeño de la seguridad de la información, incluidas las tendencias relativas a; no conformidades y acciones correctivas, seguimiento y resultados de las mediciones, resultados de la auditoría y cumplimiento de los objetivos de la seguridad de la información.

d) Retroalimentación de las partes interesadas, resultados de la valoración de riesgos y estado del plan de tratamiento de riesgos y las oportunidades de mejora continúa

Los resultados de la revisión por la dirección deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el sistema de la gestión de la seguridad de la información.

La organización debe conservar información documentada como evidencia de los resultados de las revisiones efectuadas por la dirección.

10.4.11 Mejora

10.4.11.1 No conformidades y acciones correctivas

Cuando ocurra una no conformidad, la organización debe:

a) Reaccionar ante la no conformidad, y según sea aplicable; tomar las acciones para controlarla, corregirla y hacer frente a las consecuencias.

b) Evaluar la necesidad de acciones para eliminar las causas de la no conformidad, con el fin de que no vuelva a ocurrir ni ocurra en otra parte, mediante; la revisión de la no conformidad, la determinación de las causas y si existen no conformidades similares, o que potencialmente podrían ocurrir.

c) Implementar cualquier acción necesaria.

d) Revisar la eficacia de las acciones correctivas tomadas y hacer cambios al SGSI, si es necesario.

Las acciones correctivas deben ser apropiadas a los efectos de las no conformidades encontradas.
La organización debe conservar la información documentada adecuada, como evidencia de; la naturaleza de las no conformidades y cualquier acción posterior tomada y los resultados de cualquier acción correctiva.

10.4.11.2 Mejora continúa

El área de informática debe mejorar continuamente la conveniencia, adecuación y eficacia del sistema de gestión de la seguridad de la información.

11. CONCLUSIONES

- ✓ El levantamiento de los activos de información en el área de informática permitió reconocer algunas debilidades que requieren ser controladas para prevenir una posible pérdida o robo de información.

- ✓ Con el análisis de riesgos realizado se determinó la frecuencia, ocurrencia e impacto de los eventos negativos que pueden atentar contra la seguridad de la información, lo cual permite proporcionar controles para prepararse o prevenir dichos eventos.

- ✓ Los riesgos encontrados son importantes para establecer las medidas y mecanismos que permitan aumentar los niveles de confidencialidad, integridad y disponibilidad de la información.

- ✓ Las políticas de seguridad planteadas en este documento, permitirán mejorar los controles existentes para proteger y mantener la seguridad de la información que actualmente se maneja en el área de sistemas.

- ✓ Un riesgo informático es todo factor que pueda generar una disminución en la confidencialidad, integridad y disponibilidad de la información, es por esto que el área de sistemas debe propender por implementar y mantener actualizado el SGSI.

- ✓ Después de haber realizado el diseño del SGSI, es importante contar con el apoyo de la alta dirección y del personal de apoyo, para que se conforme un equipo y de esta manera se pueda implementar a futuro el sistema de gestión de seguridad de la información en el área de informática de la Cooperativa del Magisterio de Túquerres.

12. RECOMENDACIONES

- ✓ Deben tomarse las medidas e implementar los controles correspondientes para mantener la seguridad de la información en el área de informática, ya que es el activo más importante que tiene la organización.

- ✓ Se debe promover la implementación del sistema de gestión de la seguridad de la información, con el fin de mejorar los procesos que se llevan actualmente en el área de informática, de igual manera se deben fomentar las buenas prácticas para proteger los activos de información.

- ✓ Los servidores y la información contenida en los mismos, son los principales y más importantes activos de información que posee el área de informática, es por esto que se deben crear y mantener planes de contingencia en caso de un evento que atente contra la seguridad.

- ✓ Todas las políticas definidas en este documento y las que se adicionen cuando se implemente el SGSI, deben ser acatadas por todo el talento humano del área de informática, en caso contrario se deben penalizar las faltas de acuerdo al impacto causado sobre los activos de información.

- ✓ Se debe controlar el acceso a la sala de servidores utilizando dispositivos de seguridad electrónica con técnicas de autenticación biométrica, esto con el fin de evitar el acceso a personal no autorizado. De igual manera es importante realizar la reestructuración interna de dicha sala.

- ✓ Se deben realizar evaluaciones periódicas a las políticas de seguridad de la información y al sistema en general, esto con el fin de mantenerlas actualizadas y ajustadas a las necesidades del área de sistemas y la cooperativa.

- ✓ Es necesario identificar las vulnerabilidades que pueden existir en los servidores y dispositivos de red de la cooperativa, ya que un posible atacante puede aprovechar esta situación para violar la confidencialidad, integridad y disponibilidad de la información.

- ✓ El activo más importante para el área de informática de la Cooperativa del Magisterio de Túquerres es la información, por tanto debe almacenarse y protegerse con mecanismos altamente seguros que permitan mantener su integridad y confidencialidad.

BIBLIOGRAFÍA

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Ley 1273 de 2009 delitos informáticos”. {En linea}. {10 de Abril del 2015} disponible en: (http://www.mintic.gov.co/portal/604/w3-article-3705.html).

MINISTERIO DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. “Políticas gobierno de Colombia en SGSI para entidades públicas”. {En linea}. {25 de Marzo de 2015} disponible en: (http://www.mintic.gov.co/gestionti/615/w3-channel.html).

Coté, S. P. (2011). Ethical Hacking and Countermeasures Version 7.0. Taiwan: EC-COUNCIL, 2009, 352 p.

MAÑAS, José “Lección 11: Analisis y gestión de riesgos”. {En linea}. {1 de Marzo de 2015} disponible en: (http://www.criptored.upm.es/intypedia/docs/es/video11/GuionIntypedia011.pdf).

Herramientas. (s.f.). Recuperado el 21 de 04 de 2014, de Herramientas disponible en: http://www.iso27000.es/herramientas.html

IPUJAN, Jose Alexander. Auditoría de Sistemas Aplicada al Sistema de Información de la Cooperativa del Magisterio de Túquerres. San Juan de Pasto, 2013, 157p. Tesis de grado (Ingenieria de sistemas). Universidad de Nariño. Facultad de ingenieria.

CANO MARTINEZ, Jeimy. “Políticas de Seguridad Informática”. {En linea}. {10 de Mayo de 2015} disponible en: http://www.criptored.upm.es/guiateoria/gt_m142a.htm

QUIJANO VODNIZA, José. Mecanismos e instrumentos para la planificación, seguimiento y evaluación de los proyectos de investigación. San Juan de Pasto: Impresores Johndan, 2002. 129p.

CANOSA Maximiliano. “La importancia de los procesos de seguridad de la información”. {En línea}. {21 de Julio de 2015} disponible en: (http://www.slideshare.net/foroglobalcrossing/la-importancia-de-los-procesos-de-seguridad-de-la-informacin-ventajas-y-eficiencia-de-aprovechar-la-experiencia-global)

CRUZ, Rodríguez, E. D. (2010). “Modelo de seguridad para la medición de vulnerabilidades y reducción de riesgos en redes de datos”. {En línea}. {2 de Marzo del 2015} disponible en: (http://itzamna.bnct.ipn.mx/dspace/bitstream/123456789/8428/1/IF2.52.pdf)

Implementación SIG. “El ciclo de Deming”. {En línea}. {16 de Mayo de 2015} disponible en: (http://www.implementacionsig.com/index.php/generalidades-sig/55-ciclo-de-)

INTECO. (s.f.). “Implantación de un SGSI en la empresa”. {En línea}. {7 de Diciembre del 2014} disponible en: (http://cert.inteco.es/extfrontinteco/img/File/intecocert/sgsi/img/Guia_apoyo_SGSI.pdf)

PALLAS, Gustavo. “Metodología de implementación de un SGSI en un grupo empresarial jerárquico”. {En línea}. {31 de Marzo de 2015}. Disponible en: (http://www.fing.edu.uy/inco/pedeciba/bibliote/cpap/tesis-pallas.pdf)