UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:

INGENIERÍA DE SISTEMAS

Trabajo de titulación previo a la obtención del título de:

INGENIERA E INGENIERO DE SISTEMAS

TEMA:

ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LAS NORMAS ISO 27001 Y 27002 PARA LA SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO.

AUTORES:

FABIOLA LORENA LANDETA GUACHAMIN

DANIEL FERNANDO QUILLE SIMBAÑA

TUTOR:

FRANKLIN EDMUNDO HURTADO LARREA

Quito, septiembre de 2016

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Fabiola Lorena Landeta Guachamin, con documento de identificación N° 171799855-1 y Daniel Fernando Quille Simbaña, con documento de identificación N° 171935547-9 respectivamente, manifestamos nuestra voluntad y cedo a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de grado intitulado: ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LAS NORMAS ISO 27001 Y 27002 PARA LA SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO, mismo que ha sido desarrollado para optar por el título de: INGENIERA E INGENIERO DE SISTEMAS, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en mi condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la Biblioteca de la Universidad Politécnica Salesiana.

FABIOLA LORENA
LANDETA GUACHAMIN
CI. 171799855-1

DANIEL FERNANDO
QUILLE SIMBAÑA
CI. 171935547-9

Fecha: septiembre de 2016

DECLARATORIA DE COAUTORIA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el trabajo de titulación, ANÁLISIS Y DISEÑO DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN BASE A LAS NORMAS ISO 27001 Y 27002 PARA LA SUPERINTENDENCIA DE CONTROL DEL PODER DE MERCADO realizado por Fabiola Lorena Landeta Guachamin y Daniel Fernando Quille Simbaña, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana, para ser considerados como trabajo final de titulación.

Quito, septiembre del 2016

Franklin Hurtado Larrea

C.C. 1713382016

Dedicatoria

Dedico este proyecto especialmente a mi padre Fausto Landeta, mi madre Fabiola Guachamin a mis hermanos Marisol Landeta, Xavier Landeta, Cristina Landeta y Marcelo Landeta quienes fueron y han sido un pilar fundamental en mi vida profesional y personal, gracias a su esfuerzo y sacrificio me dieron la mejor herencia que es la educación. También dedico este esfuerzo a las personas que amo con mi vida: mi esposo Pablo Burgos que con su amor y apoyo me dio fuerzas para seguir adelante junto con nuestra hija, quien fue el motivo más importante para cumplir mis metas.

Fabiola Lorena Landeta Guachanín

Este proyecto de titulación es dedicado a mis padres y mi familia por haber confiado en mí y que me han apoyado durante mi vida para que pueda llegar a cumplir mis sueños y metas, una etapa de la vida termina, pero comienzan nuevos retos y con el mismo apoyo y confianza de todos espero cumplirlos y así enorgullecer a mis padres.

Daniel Fernando Quille Simbaña

Agradecimiento

Damos gracias a Dios por llenarnos de sabiduría y fortaleza para poder culminar esta etapa importante de nuestras vidas.

A nuestras familias que nos ayudaron a cumplir con nuestras metas, a nuestro tutor el Ing. Franklin Hurtado por su apoyo y conocimiento brindado en toda la realización de este proyecto de titulación.

A la vida por enseñarnos que debemos superarnos en este mundo profesional tan competitivo que existe en la actualidad.la

A todos nuestros maestros y a la Universidad Politécnica Salesiana que nos enseñaron a formarnos como personas y buenos profesionales.

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

Las entidades están amenazadas a diario por riesgos que atentan contra la integridad, confidencialidad, disponibilidad de la información, además de la tecnología que la soporta, lo que puede ocasionar la interrupción de las actividades de negocio.

El presente proyecto de titulación se enfoca en el análisis y diseño un Sistema de Gestión de Seguridad de la Información (SGSI) para la Superintendencia de Control del Poder de Mercado (SCPM), de acuerdo al estándar expuesto en la norma internacional ISO/IEC 27001:2005.

La norma ISO/IEC 27001:2005 se presenta como una guía para favorecer el desarrollo del SGSI, de esta manera se logra analizar, definir y se diseñar estándares que pueden ser aplicados posteriormente dentro de la entidad, otra de las ventajas es tener un avance significativo y cumplir con las recomendaciones que se definen en la norma regulatoria (Acuerdo 166) aplicando normas técnicas y controles de seguridad, esto permite recomendar las medidas apropiadas que deben adoptarse en la entidad, para tener un proceso adecuado en el manejo de posibles riesgos que atenten contra la seguridad de la información. Finalmente, como resultado se realiza la propuesta con lineamientos y buenas prácticas de seguridad de acuerdo a las necesidades de la entidad.

ABSTRACT

Entities are threatened daily by risks that endanger the integrity, confidentiality, availability of the information and technology that hold it up, this may affect the business continuity.

The current titling project is focused on the design of a Security Management System of the Information for the Superintendence of Market power´s control according to the stardard established by the international rule ISO/IEC 27001:2005.

The rule ISO/IEC 27001.2005 is used as a guide for the development of the SGSI to analize, define and design standars which can be applied within the entity so it can have an important progress and also the accomplishment of a regulatory rule (Deal 166) applying technical norms and effective safety practices, through this its allowed to recommend appropiate measures which can be applied within the entity for the management against potential risk that can affect the information´s safety. Finally as a result a propose is made with guidelines and good practices of security according to the entity's necesity.

INTRODUCCIÓN

El manejo de información actual en entidades públicas es de vital importancia para establecer un sistema de gestión de seguridad de la información. El sistema puede brindar soluciones y mejores prácticas para la transmisión de la información, detectando así sus limitaciones y oportunidades de mejora partiendo de análisis de resultados. La Superintendencia de Control del Poder de Mercado (SCPM) requiere establecer procesos que les ayuden a solventar o atacar a las amenazas y vulnerabilidades de seguridad, tomando en cuenta un control estricto de cumplimiento de las políticas y controles diseñados. La finalidad del proyecto es proponer un diseño de un sistema de gestión de seguridad de la información SGSI, basándose en la ISO/IEC 27001:2005 y ISO/IEC 27002:2005 y utilizando un modelo de cascada; cabe indicar que para la implementación de este SGSI se debe utilizar el método PDCA que es un plan de mejora continua.

CAPITULO 1

ESTADO DEL ARTE

1.1. Antecedentes

La Superintendencia de Control del Poder de Mercado (SCPM), debido a que una de sus tareas principales es el control del abuso de poder de mercado, se ve abocada a manejar información legal de procesos judiciales que no son de acceso público, en este contexto, el mayor riesgo que esta entidad puede sufrir, es el inadecuado manejo de la información, situación que puede acarrear efectos negativos que afectarían el correcto funcionamiento de la organización.

La información, en la era del conocimiento, es considerado un activo, y más aún para una organización que su función principal es el control; con lo anterior se pretende disponer de técnicas de seguridad, con la finalidad de reducir en mayor medida, las vulnerabilidades o atentados efectuadas en la seguridad.

Posterior a lo descrito se procederá a realizar el diseño del sistema de gestión de seguridad de la información (SGSI) para la SCPM, tomando como referencia el Acuerdo 166 que se encuentra vigente para las entidades públicas, y estándares establecidos en la norma ISO/IEC 27001:2005 y ISO/IEC 27002:2005.

1.2. Justificación

El siguiente proyecto describe el análisis y diseño de un sistema de gestión de seguridad de la información (SGSI) para la Superintendencia de Control del Poder de Mercado. El 5 de septiembre del 2013, la Secretaria nacional de la administración hace público el Acuerdo 166 donde se expone que las entidades que conforman la Administración Pública Central, Institucional y la Función Ejecutiva, deben usar las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 como referencia a la hora de establecer procesos de seguridad y de esta manera puedan construir en el tiempo un

sistema de gestión de seguridad de la información (SGSI) o Esquema Gubernamental de Seguridad de la Información (EGSI) dirigida a las entidades públihacer:cas. (Peñaherrera, 16)

En el caso de la entidad, con el análisis de la situación actual (figura20) y lo que recomienda el acuerdo 166 y la ISO/IEC 27002:2005, se obtiene los resultados de seguridad en la organización; para ello se diseña un sistema de gestión de seguridad de la información (SGSI), con la finalidad de minimizar riesgos y vulnerabilidades que puedan provocar la interrupción de las actividades del negocio.

1.3. Objetivo general

Diseñar un Sistema de Gestión de Seguridad de la Información para la Superintendencia de Control del Poder de Mercado basado en el estándar internacional ISO/IEC 27001:2005.

1.4. Objetivos específicos

Establecer un diagnóstico del manejo de la información en la Superintendencia de Control del Poder de Mercado comparando controles de seguridad actuales que lleva a cabo la empresa, con los requisitos que establece de la norma ISO 27001/ 27002:2005.

Plantear un análisis adecuado de controles y lineamientos indispensables para salvaguardar la información crítica y confidencial que es manejada dentro de la SCPM.

Diseñar un sistema de gestión de seguridad de la información (SGSI), estableciendo recomendaciones a ser ejecutadas en procedimientos para dominios específicos e indicadores de control, midiendo la efectividad y calidad de los procesos que garanticen el buen funcionamiento del negocio, esto permite que la Superintendencia de poder de control del mercado (SCPM) posteriormente implante controles de seguridad que permita minimizar el riesgo.

Proveer lineamientos que son parte de los indicadores para establecer buenas prácticas de seguridad y el buen manejo de la información.

1.6. Marco metodológico

ISO 27001 establece utilizar el modelo *Plan – Do – Check – Act* (PDCA) para estructurar los procesos del sistema de gestión de seguridad (SGSI), sin embargo, por el tipo de trabajo de titulación se ha intentado establecer una metodología que permita construir de forma coherente el modelo de gestión; para esto se ha priorizado la investigación y se han combinado varias técnicas o perspectivas. Por lo tanto, este proyecto de titulación empieza coordinando horarios para reuniones con los funcionarios de la Superintendencia de control de poder del mercado (SCPM), lugar de reuniones, instrumentos, técnicas, y formatos donde se reflejarán los resultados.

Para la construcción del sistema de gestión de seguridad de la información (SGSI), se ha optado por utilizar el modelo de fases tipo cascada, que tiene la finalidad de interactuar entre sí en forma secuencial hasta lograr el objetivo propuesto.

1.6.1 Modelo de cascada.

Este modelo será usado para exponer las fases que se emplearán durante la realización del proyecto:

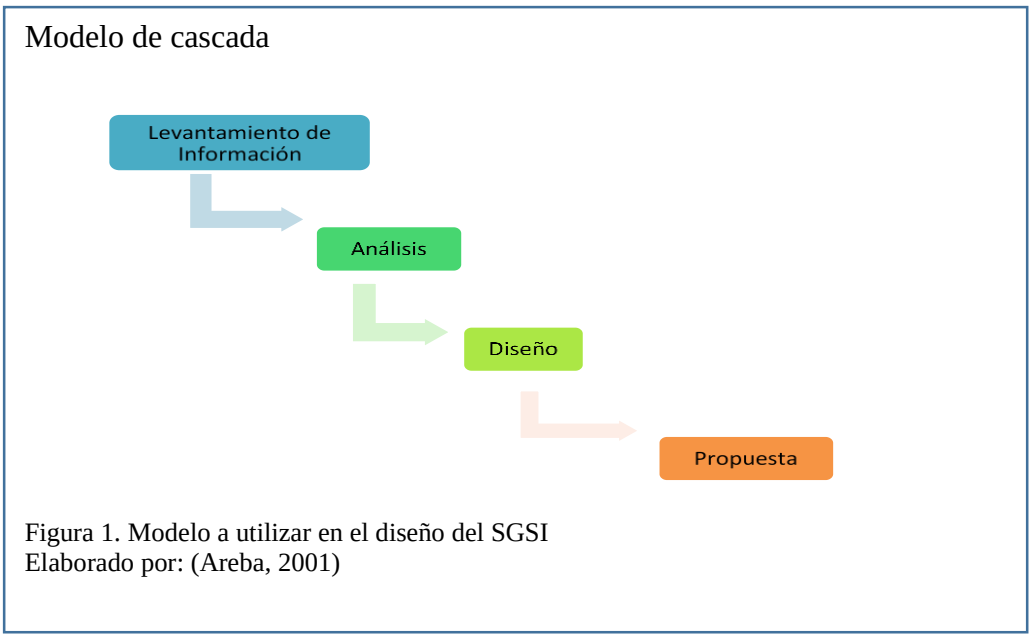

Figura 1. Modelo a utilizar en el diseño del SGSI
Elaborado por: (Areba, 2001)

1.6.1.1 Levantamiento de información.

Esta primera fase se inicia con la elaboración de instrumentos que han sido construidos de acuerdo a todos los requerimientos que establece la norma ISO 27002:2005 que se aportan para el levantamiento de la siguiente información y las entrevistas realizadas a varias áreas de la entidad utilizando las siguientes técnicas:

Entrevistas**:** La mayor cantidad de información será obtenida a través del uso de esta técnica, realizada a los directores departamentales, coordinadores de áreas y personal involucrado en los principales sistemas de la SCPM.

Encuestas**:** Esta técnica es establecida para la recopilación de información procedente del manejo de los sistemas tecnológicos y procedimientos internos de la SCPM, esto permite tener claridad sobre la situación actual de seguridad dentro de la entidad.

Esta fase se realiza con reuniones semanales y trabajo a jornada completa en la SCPM y de esta manera se establecen las siguientes fases para la realización del proyecto:

1.6.1.1.1 Desarrollo del análisis diferencial.

Para el análisis diferencial de la situación actual se construye un cuestionario en el que se exponen los objetivos de control que contiene cada dominio establecida por la norma ISO 27002:2005, este levantamiento ayuda a obtener estadísticas claras de la situación actual sobre el manejo de la seguridad en la información.

La elaboración de esta fase, depende de la participación de varias áreas/departamentos de la entidad, de esta manera con los resultados obtenidos, se verifica las brechas de seguridad entre la situación actual y la situación deseable. (Areba, 2001).

Para cada entrevista se utilizará los siguientes instrumentos:

- Cuestionario: instrumento utilizado en las reuniones previstas y/o planificadas.
- GAP: Formato utilizado para registrar la información adquirida en la entidad.

Los resultados son presentados en cuadros con las preguntas y respuestas, incluyendo un resumen con un gráfico tipo pastel, sobre el cumplimiento y no cumplimiento.

1..6.1.1.2 Identificación y clasificación de activos.

Para la identificación de activos se elabora una matriz de información, este levantamiento será orientado siguiendo las recomendaciones que establece el sistema de gestión de seguridad de la información (SGSI) para la identificación y clasificación de la información. Se emplea de igual manera el método de Magerit (p. 22), el cual se utiliza para realizar agrupaciones en dependencia de la utilidad que se le dé a los mismos. Toda la recopilación que se realizó fue en conjunto con los responsables de las diferentes áreas.

1.6.1.2 Análisis.

De acuerdo al levantamiento realizado, se obtiene el siguiente resultado:

1.6.1.2.1 Análisis de la situación actual.

Una vez finalizado el levantamiento de información, se obtienen los resultados de su situación actual, los mismos que son mostrados en la Tabla 17 y se elabora un gráfico tipo radar que refleje la situación actual, situación deseable y situación óptima de la seguridad.

1.6.1.2.2 Análisis de la valorización de activos.

Una vez identificados y clasificados los activos se procede a valorizar e identificar la criticidad de los mismos con las dimensiones referenciadas, Confidencialidad, Integridad y Disponibilidad como se especifican en las siguientes tablas:

Tabla 1.
Valoración de disponibilidad.

DISPONIBILIDAD	VALOR	PONDERACIÓN
Disponibilidad no es crítica y es suficiente para este activo el estar disponible dentro de 1 semana o más	Bajo	1
La no disponibilidad del activo al menos un día ocasionaría un impacto menor al negocio	Medio	2

La no disponibilidad del activo ocasionaría un impacto importante para el negocio y debe estar disponible todo el tiempo	Alto	3

Nota. Valor estipulado según la información levantada
Elaborado por: Landeta & Quille

Tabla 2.
Valoración de confiabilidad

CONFIDENCIALIDAD	VALOR	PONDERACIÓN
Es libremente accesible por cualquiera	Bajo	1
El activo puede ser accesible únicamente por cualquier miembro de la empresa sin ninguna restricción.	Medio	2
Este activo debería ser solamente accesible con una autorización explícita.	Alto	3

Nota. Valor estipulado según la información levantada
Elaborado por: Landeta & Quille

Tabla 3.
Valoración de integridad.

INTEGRIDAD	VALOR	PONDERACIÓN
La pérdida de integridad no tiene influencia, o influencia negativa en los negocios de la empresa	Bajo	1
La integridad es importante y debería ser mantenida, tiene una influencia menor en el negocio de la empresa	Medio	2
La pérdida de integridad tiene una importante influencia negativa en el negocio, y se debería evitar.	Alto	3

Nota. Valor estipulado según la información levantada
Elaborado por: Landeta & Quille

1.6.1.2.3 Análisis del riesgo de activos.

Para la realización del análisis del riesgo se toma como referencia el método de Magerit. Obteniendo resultados visibles de la situación real de la entidad, obligando a entregar soluciones para minimizar.

Las importancias de los activos se definen de acuerdo a los tres factores de la seguridad que son confidencialidad, disponibilidad e integridad que se establece en las Tablas 1, 2 y 3.

A continuación, en la siguiente tabla se refleja el nivel de importancia que tienen los activos en la entidad.

Tabla 4.
Nivel de importancia

Nivel	Impacto
1 – 9	Bajo
10 – 18	Medio
19 – 27	Alto

Nota. Valor estipulado según la información levantada
Elaborado por: Landeta & Quille

Para el análisis del nivel de riesgo de los activos, es importante conocer el impacto y la probabilidad aplicando la siguiente ecuación.

Tabla 5.
Nivel de Probabilidad

Nivel	Probabilidad	Detalle
Bajo	1	Riesgo cuya probabilidad de ocurrencia es muy baja de 1% al 30% de incidentes de seguridad
Medio	2	Riesgo cuya probabilidad ocurrencia es media es decir 30% al 80% de incidentes de seguridad
Alto	3	Riesgo cuya probabilidad es alta del 90% al 100% de incidentes de seguridad

Nota. Valor estipulado según la información levantada
Elaborado por: Landeta & Quille

$$\text{Nivel de Riesgo} = \text{Impacto} * \text{Probabilidad}$$

Tabla 6.
Nivel de riesgo

Probabilidad Impacto	Bajo	Medio	Alto
Bajo	1	2	3
Medio	2	4	6
Alto	3	6	9

Nota. Los resultados de la probabilidad del riesgo son en base al cálculo mostrado en la formula anterior.
Elaborado por: Landeta & Quille

Para la realización del análisis del impacto y probabilidad se toman en cuenta las entrevistas realizadas a los diferentes integrantes responsables de los activos.

1.6.1.3 Diseño.

Para el diseño de un sistema de gestión de seguridad de la información (SGSI) se empezó con el análisis de riesgo de los activos de información y validar cada objetivo de control para la declaración de aplicabilidad, donde se procedió a definir

lineamientos y el camino que se ha de llevar a cabo para establecer la propuesta de mejora en procesos y controles disponibles en la SCPM; tomando como referencia las buenas prácticas y controles que establece la norma ISO/IEC 27002:2005.

1.6.1.3.1 Declaración de aplicabilidad.

En el levantamiento de la declaración de aplicabilidad se construye un GAP (Guidelines for the Assessment Process), este documento permite definir qué controles de seguridad son necesarios y aplicables en la entidad.

1.6.1.4 Propuesta.

Una vez completadas las fases anteriores se realiza la propuesta enfocada a las necesidades de la entidad, donde se establecen lineamientos, controles e instrumentos necesarios que se adecuen a una efectiva implementación de procesos y buenas prácticas.

1.5. Marco institucional

La Superintendencia de Control del Poder de Mercado es un organismo técnico de investigación, control, prevención, regulación, sanción y resolución en materia de libre competencia. Inició su labor en septiembre del 2012 previa aprobación de la Ley Orgánica de Regulación y Control del Poder de Mercado un año antes. (Ley Orgánica de Regulación y Control del Poder de Mercado - Superintendencia de Control del Poder de Mercado, 2016).

La institución tiene como misión controlar el correcto funcionamiento de los mercados, previniendo de esta manera el abuso de poder de mercado de los operadores económicos nacionales e internacionales evitando todas aquellas prácticas contrarias a la competencia que vayan en perjuicio de los consumidores, a fin de construir con competitividad y eficiencia el bienestar general de la sociedad. La máxima autoridad es el Superintendente, designado por el Consejo de Participación Ciudadana y Control

Social. (Nosotros - Superintendencia de Control del Poder de Mercado - Superintendencia de Control del Poder de Mercado, 2016).

En cuanto a su estructura, la Superintendencia cuenta con la Coordinación General de Planificación y Relaciones Internacionales que dirige, coordina, asesora y realiza el seguimiento y evaluación de los procesos de la planificación institucional y relaciones internacionales mientras que la Coordinación General de Asesoría Jurídica es la encargada del asesoramiento legal y jurídico en las áreas de derecho público, constitucional, laboral, procesal y privado para las gestiones que se realicen por parte de las autoridades de la Superintendencia; así como la coordinación de las acciones de carácter administrativo y/o judicial que se generen en el desenvolvimiento de las actividades de la SCPM. (Coordinación General de Planificación y Relaciones Internacionales - Superintendencia de Control del Poder de Mercado, 2016).

La coordinación General Administrativa Financiera se dedica al diseño de proyectos de políticas, normas, procedimientos y la Coordinación General de Tecnología sistematiza el trabajo de los diferentes procesos de la Superintendencia mediante el uso y aplicación de técnicas, software y hardware que permitan proporcionar la información necesaria y oportuna para el desarrollo de sus operaciones. (Coordinación General Administrativa Financiera - Superintendencia de Control del Poder de Mercado, 2016).

Entre los servicios que implementa este organismo ecuatoriano están: la investigación de prácticas desleales, el control de concentraciones, la investigación de abuso del poder de mercado, acuerdos y prácticas restrictivas y consultas a la máxima autoridad. Además, la institución ha desempeñado su papel por medio de normas técnicas, resoluciones, recomendaciones y manuales de obligatorio cumplimiento para entidades e industrias. De igual manera ha encauzado indagaciones y solicitado

información a grandes entidades privadas por abusos del poder de mercado. (Ley Orgánica de Regulación y Control del Poder de Mercado - Superintendencia de Control del Poder de Mercado, 2016).

Para alcanzar sus objetivos, la SCPM considera de suma importancia difundir el contenido de la Ley Orgánica de Regulación de Control del Poder de Mercado (LORCPM) y su reglamento, por medios de varios canales de comunicación, entre ellos, las herramientas informáticas y los medios de comunicación digitales. (Ley Orgánica de Regulación y Control del Poder de Mercado - Superintendencia de Control del Poder de Mercado, 2016).

Estructura orgánica Planta Central.

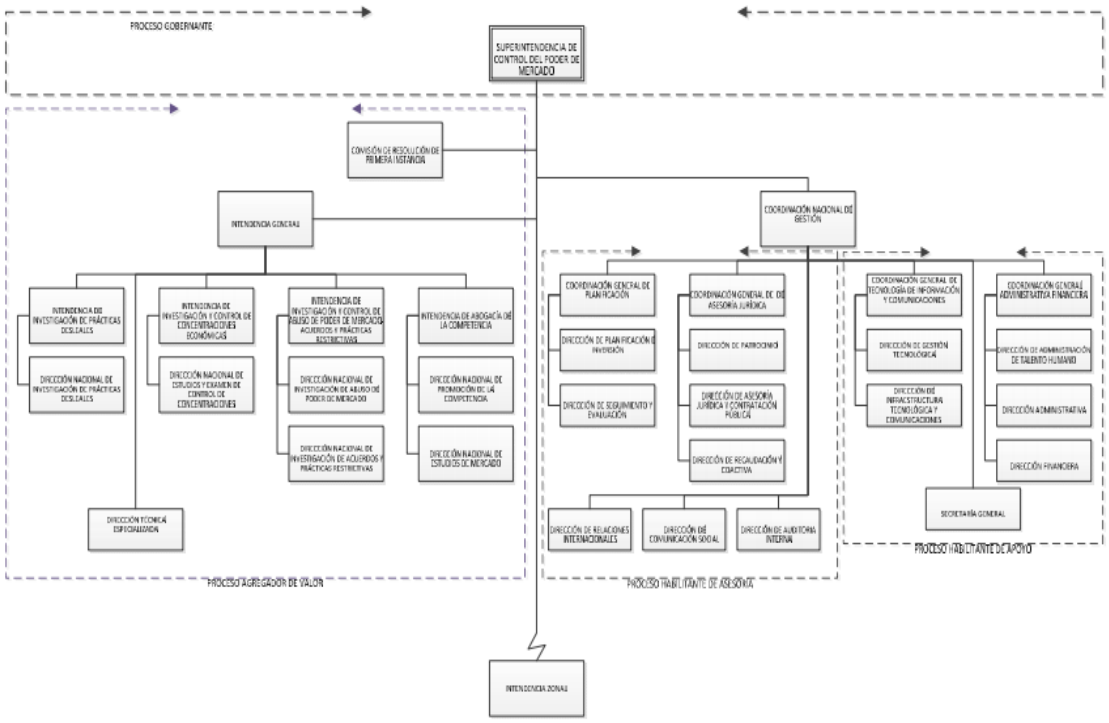

Figura 2. Diagrama organizacional de la SCPM
Elaborado por: Superintendencia de control del poder de mercado (SCPM)

1.7. Marco teórico

El Sistema de gestión de seguridad de la información abarca varios temas que se debe conocer para la investigación y estos son los siguientes:

- Organización Internacional de Normalización (ISO)
- Norma internacional ISO/IEC 27001
- Norma internacional ISO/IEC 27002
- Activos de Información
- Análisis de Brecha

1.7.1. Organización Internacional de Normalización (ISO).

La Organización Internacional de Normalización o ISO y la Comisión Electrotécnica Internacional (IEC) desarrollaron una serie de normas internacionales.

La ISO es una red de institutos de normas nacionales que conforman alrededor de 163 países, fue creada en 1947, desde su creación se han establecido más de 19000 normas internacionales que abarcan la tecnología y negocios. (The International Organization for Standardization, 1997).

Las ISO son para estandarizar normas sobre la gestión de calidad y seguridad que son parte y manejadas por varios países y organizaciones del mundo. Su misión promueve el desarrollo de la estandarización y actividades relacionadas, con el propósito de facilitar el intercambio internacional de bienes y servicios.

1.7.2. Serie de la ISO 27000.

- ISO/IEC 27000: En esta serie se define todo el vocabulario estándar que es empleado dentro de la familia 27000 donde se especifican términos, definiciones y conceptos.
- ISO/IEC 27001: Esta serie da a conocer cuáles deben ser los requisitos para implantar un sistema de gestión que puede ser certificable, de manera que sea

conforme a las normas que dicta el 27000, de igual manera ayuda a conocer de manera más precisa sobre en qué consiste el sistema de gestión de seguridad de la información (SGSI), de qué manera se gestiona y cuáles son las diferentes responsabilidades de los participantes en la misma. Sigue un modelo PDCA (Plan-Do-Check-Act) que consta de unos puntos clave: Gestión de riesgos + Mejora continua.

- ISO/IEC 27002: Consiste en la creación de un código de buenas prácticas para gestionar de manera más eficiente la seguridad, incluye además recomendaciones sobre las medidas más favorables para la seguridad en una organización. Esta norma describe objetivos de control de seguridad que son recomendables a implantar. Antes ISO 17799, basado en estándar BS 7799 (en España norma UNE-ISO 17799).
- ISO/IEC 27003: En esta norma se presenta como una guía para implementar el sistema de gestión de seguridad de la información (SGSI) y describe acerca del uso del modelo PDCA (Plan-Do-Check-Act) y los requerimientos que componen cada fase.
- ISO/IEC 27004: Esta serie da a conocer de una manera más específica el tipo de métricas y las diferentes técnicas de medida que se deberán aplicar para comprobar que tan eficaz es el SGSI y a su vez muestra los controles que se relacionan con la medición de los componentes de la fase conocida como “Do” especifica técnicas para determinar la capacidad de un SGSI y los controles relacionados con los componentes del ciclo PDCA correspondientes con la fase “Do” (Implementar y Utilizar).
- ISO/IEC 27005: Esta norma corresponde a la gestión de riesgo de la seguridad de la información.

- ISO/IEC 27006: En esta norma se exponen los requisitos que las entidades encargadas de la emisión de certificaciones ISO/IEC 27001 deben cumplir a la hora de acreditar las entidades de auditoría y certificación.
- ISO/IEC 27007: A la hora de realizar una auditoría se dispone de esta guía en la que se exponen las maneras de actuación que se deben realizar para auditar un sistema de gestión de seguridad de la información (SGSI) basándose en las normas con las que cuenta el 27000.
- ISO/IEC 27011: Esta serie corresponde como una guía de gestión de seguridad de una información específica elaborada de manera directa para las telecomunicaciones que han sido elaboradas en conjunto con la ITU (Unión Internacional de Telecomunicaciones).
- ISO/IEC 27031: En esta norma se conoce como una guía de continuidad de negocio con relación a las tecnologías de la información y comunicaciones.
- ISO/IEC 27032: Esta serie tiene relación con todo lo que corresponde a la ciberseguridad expuesta en la norma ISO/IEC 27033, la cual está dedicada específicamente a la seguridad en todo tipo de redes.
- ISO/IEC 27034: Detalla la guía de seguridad que deberá aplicarse en las aplicaciones dentro de una organización.
- ISO/IEC 27035: En esta serie se expone una guía de los diferentes patrones a seguir para realizar una efectiva gestión de las incidencias que puedan presentarse dentro de la seguridad de la información de la entidad.
- ISO/IEC 27036: -Esta norma consiste en una guía dividida en cuatro diferentes partes que conforman la seguridad en las relaciones comerciales con los proveedores.

1.7.3. Norma internacional ISO/IEC 27001.

La ISO 27001 es para la gestión de la seguridad de la información en las entidades, permite asegurar la confidencialidad, integridad y disponibilidad de los datos, información y de los activos tecnologicos que procesan. La norma puede ser implementada en cualquier entidad sea pública y privada, esto permite tener una diferenciación respecto al resto que mejora la competitividad y la imagen de una organización sea grande, mediana o pequeña (Gestión de Seguridad ISO 27001, 2016). En ella especifican los requisitos necesarios para analizar y establecer mejoraras en el sistema de gestión de seguridad de la información (SGSI), norma certificable por las entidades auditoras. En la versión 2005, se implementa su metodología a partir del ciclo PHVA (Planificar, Hacer, Verificar, Actuar). También se especifican lineamientos de seguridad de acuerdo a la necesidad del negocio que ayudan a identificar los riesgos en los activos de información más críticos. . (Gestión de Seguridad de la Información ISO/IEC 27001).

Metodología de la Norma ISO 27001:2005

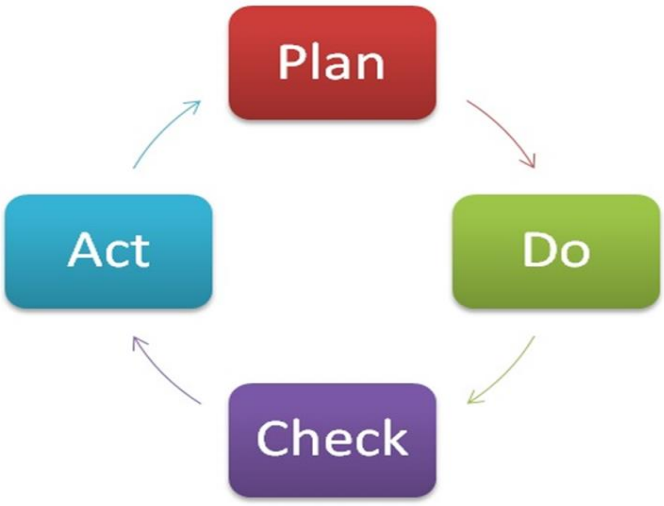

Figura 3. Metodología PDCA
Elaborado por: ISO 27001:2005

Planificar: Esta etapa es de planificación, en ella se construyen objetivos y se realiza el levantamiento de procesos indispensables para la organización, a su vez se determinan lineamientos que serán utilizados para controlar y establecer mejoras en los procesos.

Hacer: Es la implementación de cambios para mejorar procedimientos, con la finalidad de establecer mejoras durante el tiempo en caso de ocurrir errores al momento de la ejecución.

Verificar: Una vez se ha puesto en marcha el plan para mejoras, se crea una fase de prueba el mismo que permitirá analizar la efectividad de los cambios.

Actuar: Una vez realizados las estadísticas de los resultados se procede a realizar las correcciones y modificaciones necesarias para establecer una mejora continua.

La última versión de la ISO 27001 fue publicada en el 2013 y cuyo nombre completo es ISO/IEC 27001:2013, en esta norma no se establece un modelo como curso necesario de implementación; se da a las entidades la libertad de definir el patrón para la mejora continua que quieran utilizar para el SGSI. La norma pasó a tener de 114 objetivos de control como requisitos, la versión 2005 tenía 133.

1.7.3.1 Historia de la norma ISO 27001.

"ISO/IEC 27000 es un conjunto de estándares desarrollados, en fase de desarrollo por ISO (*International Organization for Standardization*) e IEC (*International Electrotechnical Commission*) que proporcionan un marco de gestión de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.*"* (Carmen de Pablos Heredero, 2011).

ISO 27000 se compone de distintas normas donde se establece un proceso para la implementación de un sistema de gestión de seguridad de la información (SGSI),

basado en ISO 27001 en conjunto con otras normas de la serie 27k pero también con otros sistemas de gestión.

Historia de la ISO 27001 e ISO 17799

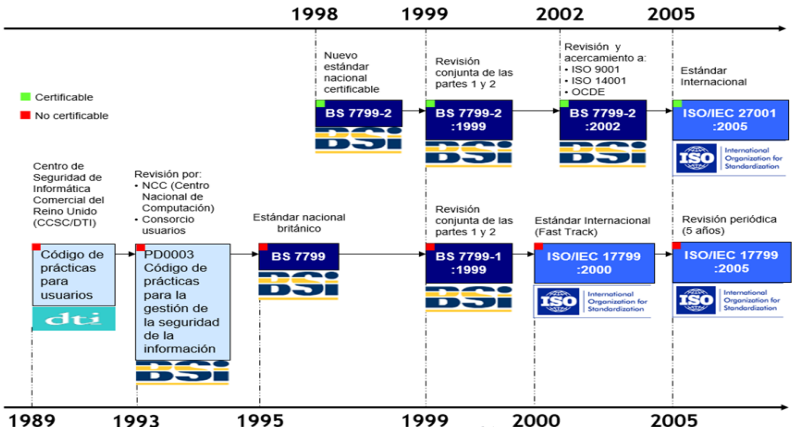

Figura 4. Todas las ISO existentes en los años correspondientes
Elaborado por: ISO27000

- BS 7799 fue creada en 1995 para establecer un conjunto de buenas prácticas útiles para la gestión de seguridad de la información.
- BS 7799-1 fue una guía de buenas prácticas, la cual no tenía establecido ningún proceso de certificación.
- BS 7799-2 fue establecida en 1998 y se basa en implantar un sistema de gestión de seguridad de la información (SGSI) que posteriormente es certificada por una organización independiente.
- La BS 7799-1 y BS 7799-2 que son parte de la norma BS 7799 se revisaron en el año 1999, mientras que la primera parte fue adoptada por la ISO, aquí no se realizaron cambios sustanciales, como ISO 17799 en el 2000.
- En el 2002, la BS 7799-2 se adecuo a la filosofía de normas ISO de sistemas de gestión

- En el 2005, con más de 1700 entidades certificadas en BS 7799-2. Esta norma se publicó con algunos cambios por ISO, como estándar ISO 27001. (ISO/IEC 27001:2005, 2016).
- Al tiempo se revisó y actualizó ISO 17799, este último estándar se renombró como ISO 27002: 2005 el 1 de julio de 2007.

La historia de la ISO 27000 dieron origen a las normas ISO-27000, ISO-27001 e ISO-27002.

Cronología mezclada

Figura 5. Diferentes años de publicación de ISO
Elaborado por: ISO 2700

Cronología de ISO-27002.

Figura 6. Diferentes años de publicación de ISO-27002
Elaborado por: ISO 2700

Cronología de ISO-27001.

Figura 7. Diferentes años de publicación de ISO-27001
Elaborado por: ISO 2700

1.7.3.2 Beneficios de la norma ISO/IEC 27001.

Los riesgos de seguridad representan una amenaza considerable para las entidades teniendo como consecuencia una lesión financiera y entre otros daños que pueden ocasionar la pérdida de confianza de los clientes. Las entidades se exponen a una

variedad de amenazas informáticas como la filtración de información mediante web; en la gestión del riesgo es importante la prevención del fraude.

1.7.4 Norma Internacional ISO/IEC 27002.

La ISO/IEC 27002 es un estándar de seguridad de la información que se publicó con el nombre de ISO/IEC 17799:2000 por la ISO e IEC en el 2000, tras ser revisada y actualizada fue publicada en el 2005 con el nombre de ISO/IEC 17799:2005.

La ISO/IEC 27002 ofrece recomendaciones a las entidades interesadas en implementar un sistema de gestión de seguridad de la información (SGSI), donde ofrece mejora de procesos en la gestión de seguridad. En la norma, la seguridad de la información se define como:

> La preservación de la confidencialidad (asegurando que sólo quienes estén autorizados pueden acceder a la información), integridad (asegurando que la información y sus métodos de proceso son exactos y completos) y disponibilidad (asegurando que los usuarios autorizados tienen acceso a la información y a sus activos que son asociados cuando lo requieran) (ISO/IEC 27002, 2016).

1.7.4.1 Recomendaciones de la norma ISO/IEC 27002:2005.

Esta norma está compuesta por 11 Dominios, 39 Objetivos de control y 133 controles. (ISO/IEC 27002, 2016).

1. Política de Seguridad de la Información.
2. Organización de la Seguridad de la Información.
3. Gestión de Activos de Información.
4. Seguridad de los Recursos Humanos.
5. Seguridad Física y Ambiental.
6. Gestión de las Comunicaciones y Operaciones.
7. Control de Accesos.

8. Adquisición, Desarrollo y Mantenimiento de Sistemas de Información.
9. Gestión de Incidentes en la Seguridad de la Información.
10. Gestión de Continuidad del Negocio.
11. Cumplimiento.

1.7.5. Sistema de gestión de seguridad de la información (SGSI).

Un SGSI abarca las personas, procedimientos y activos tecnológicos de la información (TI) por lo que se pueden evitar las amenazas de terrorismo cibernético. El diseño y la implementación de un SGSI ofrece seguridad y credibilidad garantizando seguridad en la información manejando de manera responsable en las entidades, estando a la vanguardia en la aplicación de la técnica de procesos para estar atentos a las amenazas y los problemas de la seguridad que puede causar en la información. (Gestión de Seguridad ISO 27001, 2016).

Se denomina Sistema de Gestión de la Seguridad de la Información un conjunto de políticas, directrices, procedimientos, instrumentos y registros en varios niveles que permiten administrar y gestionar la información, minimizando el riesgo y permitiendo un mejor control.

Figura 8. Pilares fundamentales de la Seguridad de la Información
Elaborado por: Landeta & Quille,

1.7.5.1 Beneficios del sistema de gestión de seguridad de la información.

La implementación de un SGSI provee una serie de beneficios para las entidades, considerándose como buena alternativa para establecer una metodología y una serie de medidas que garantizan la seguridad de la información.

Las entidades se pueden beneficiar de:

- Mayor seguridad en:
    - ✓ La información.
    - ✓ Los sistemas que maneja de información.
    - ✓ Los sistemas tecnológicos y comunicaciones.
    - ✓ Las personas.
    - ✓ Las infraestructuras.
- Mejor gestión del presupuesto.
- Cumplimiento legal.
- Aumento de la eficiencia y productividad.
- Continuidad del negocio.
- Oportunidades de negocio.
- Confianza a terceros.
- Imagen de excelencia.

1.7.6. Seguridad de la información.

La seguridad de la información consiste en un conjunto de métodos preventivos y técnicas como para el manejo correcto de la seguridad, esto ayuda a proteger y resguardar los activos que tienen un alto valor en la entidad como la información. (ISO/IEC 27001:2005, 2016).

Dentro de la seguridad es importante identificar y clasificar los activos de información por lo que su objetivo es protegerlos, estableciendo medidas preventivas y correctivas ante las posibles amenazas.

Para preservar la seguridad primero se identifica el ciclo de vida de la información, garantizando los tres pilares importantes de la seguridad: su C-I-D (Confidencialidad, Integridad y Disponibilidad).

1.7.6.2. Pilares de la seguridad de la información.

En la seguridad, la protección de la información es importante conocer los tres pilares vitales y necesarios para alcanzar el objetivo del negocio, que son:

- Confidencialidad: A la información solo puede tener acceso un personal autorizado puesto que para su protección se cuenta con métodos de identificación y autenticación, como usuario y contraseña.
- Integridad: A la información se conserva su esencia cuando no es alterada por personal no autorizado.
- Disponibilidad: La información debe estar disponible cuando el personal autorizado lo necesite; para minimizar el riesgo de disponibilidad se debe disponer un plan de contingencia.

1.7.7. Activos de información.

Un activo de información se refiere a todo elemento humano, físico o electrónico que tiene valor muy importante y de alta criticidad para la entidad, que conoce, administra y/o procesa información que sustenta procesos de negocio y por lo tanto debe protegerse frente a riesgos y amenazas, por este motivo un activo de información es aquel elemento que contiene u opera información y su protección es el objetivo de todo SGSI. (Zabala, 2008).

1.7.7.1. Método de Magerit para clasificación de activos y análisis de riesgo.

Es una metodología que consiste en el análisis y la gestión de riesgos, basándose en analizar el impacto de la vulnerabilidad de los activos y las violaciones de seguridad que surgen por el uso de tecnologías de información. (Dirección General de Modernización Administrativa, Octubre 2012).

Para el levantamiento de activos de información es importante tener en cuenta los siguientes tipos para realizar una clasificación de los mismos:

Este método permite generalizar el uso de las tecnologías y saber el valor de la información, están distribuidos en 10 fases:

- Toma de datos y proceso de información
- Establecimiento de parámetros
- Análisis de activos
- Análisis de amenazas
- Establecimiento de vulnerabilidades
- Valoración de impactos
- Análisis de riesgos intrínseco
- Influencia de salvaguardas
- Análisis de riesgos efectivos
- Gestión de riesgos.

1.7.7.2. Tipos de activos.

Según la metodología de Magerit (Instituto Nacional de Cyberseguridad de España, 2016), los activos se agrupan de acuerdo a las funciones que desempeña en el tratamiento de la información, los activos se clasifican en los siguientes tipos:

- Servicios: son los procesos de negociación que realiza la organización con el exterior.

- Datos de Información: Todos aquellos datos (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen dentro de la organización.
- Software / Aplicación: Son sistemas tecnológicos donde se utiliza para la gestión de la información, además existen herramientas que son desarrollados, software, etc.
- Hardware: El hardware de una organización en aquel que agrupa los diferentes equipos de oficina utilizados para gestionar la información (PC, portátiles, servidores, dispositivos móviles, etc.)
- Personal: funcionarios contratados.
- Red: Son redes de comunicación para el transporte de información de un lugar a otro por medio de dispositivos de conectividad tales como router, switch, concentradores, etcétera.
- Equipamiento Auxiliar: son los equipos de destrucción de documentación o los equipos de climatización que son equipos de soporte de la información.
- Instalaciones: Cableado estructurado, instalaciones eléctricas.
- Servicios: Son servicios como la conexión a internet, correo electrónico, etc.

1.7.7.3. Valoración de activos.

Es el proceso para la determinación de activos de información y la determinación de las posibles amenazas que pueden surgir sobre los mismos para el cálculo de acuerdo a los niveles de escala que se presenta en la tabla de valorización.

Es necesario identificar el tipo de valorización que se le otorga a cada activo, la cual debe ser en función a la importancia que tenga en el negocio, para de esta manera valorar si pueden ser afectados por posibles incidencias.

Valorización cuantitativa: con esta valorización se asignan valores económicos al activo, considerando la importancia de cada uno para determinar la pérdida potencial de la amenaza.

Valorización cualitativa: Esta valorización está asignada mediante la calificación, cumpliendo con los tres pilares de seguridad conocidos para la seguridad como confidencialidad, integridad y disponibilidad de los activos de información y definiendo la valorización como alto, medio y bajo.

Es necesario identificar los tipos de amenazas presentes en la entidad, ya sean:

- Humanas
- Técnicas
- Naturales y ambientales

1.7.7.4. Análisis de riesgo.

Hoy en día, todas las entidades optan por automatizar todos los sistemas informativos e integración, por lo cual aumenta el riesgo de pérdida de esta información, por lo cual se debe tener en cuenta el valor de los activos existentes en la organización y el riguroso control de riesgo y amenazas. (AREITIO J, 2008).

Riesgo: Impacto * Probabilidad

Para el análisis de riesgo se debe tener conocimiento de los siguientes conceptos:

- Importancia: En la actualidad debido al crecimiento constante del negocio, la información es considerada como el valor más importante, esta misma puede ser vulnerable ante robos o pérdidas afectando la competitividad y continuidad de la entidad. (Espinoza, 2016).

I = Confidencialidad * Integridad * Disponibilidad

- Vulnerabilidad: es la posibilidad de aumentar el riesgo de que se plasme una amenaza en un activo. Forma parte del estado de seguridad del activo; también se puede establecer que una vulnerabilidad es la falla que puede ser aprovechada por una amenaza.
- Amenaza: Las amenazas se consideran lógicas y físicas en todo evento que puede desencadenar un incidente en la organización, produciendo daños materiales e inmateriales en la misma. Los activos están sujetos a varias amenazas que puede causar pérdidas de información, accesos no deseados, fallo en equipos tecnológicos, daño en la confidencialidad, integridad y disponibilidad de la información. (AREITIO J, 2008).
- Impacto: El impacto se calcula en base al máximo valor de degradación que la amenaza produce sobre un activo, y la criticidad del activo definida en los pasos anteriores, por ejemplo, mediante la multiplicación de tales valores.
- Probabilidad: Es la posibilidad o estimación de que se presente una situación o evento específico sobre un activo.

1.7.8. Análisis de brecha

El análisis de brecha permite conocer las debilidades de la entidad, para este análisis se debe identificar los procesos existentes y deseables, aquellos que deben ser mejorados y los que deben ser introducidos dentro de la entidad.

“Las brechas se definen como las diferencias que ocurre entre los productos presentes y deseados, entre los insumos existentes los necesarios, y entre los procesos que necesitan ser mejorados y los procesos que deben ser introducidos.” (Alfaro, enero 1997).

1.7.9. Declaración de aplicabilidad

En la ISO 27001 establece que las organizaciones deben tener un documento en el que se refleje la declaración de aplicabilidad, mediante este documento facilita a conocer los controles más adecuados para implementar dentro de una organización, así como los objetivos de los mismos y también la manera en las que estos se van a implementar. (Albacete, 2014).

En el documento se deben considerar los siguientes puntos:

- Controles donde se debe identificar seleccionados, implementados y excluidos.
- Procesos identificados que deben ser mejorados, implementados y excluidos.

1.7.10. Aplicación de modelo de cascada en proyectos

Este modelo es conocido como el ciclo convencional o línea secuencial, la elaboración de etapas permite tener un orden de construcción de un proyecto, cada una de ellas se inicia cuando haya finalizado la etapa anterior. (Toni Granollers i Saltiveri, Octubre 20005).

Las principales etapas de este modelo son:

- Análisis y definición de los requerimientos.
- Diseño.
- Implementación.
- Integración.
- Funcionamiento y mantenimiento.

1.7.11. Definiciones

- Entrevistas: Son técnicas que permiten obtener información en relación a un tema específico, estas pueden ser usadas bajo las necesidades del entrevistador.
- Encuestas: Es una técnica de captación de información, utilizando cuestionarios relacionado al objetivo del encuestador.

- Funcionario: Persona que presta sus servicios laborales para una entidad pública.
- Entidad: Grupo/asociación de personas que realizan una actividad laboral sea pública o privada.

CAPITULO 2

Situación actual de la gestión de la seguridad de la información en La Superintendencia de control de poder y mercado

2.1. Análisis diferencial

El análisis diferencial tiene como finalidad la evaluación del estado actual de la Superintendencia de Control de Poder y Mercado en seguridad de la información. Este estudio está basado en la norma ISO/IEC 27002:2005, esto permite encontrar brechas existentes entre lo ideal de la norma y lo que dispone la entidad en la actualidad.

Para la elaboración de este análisis, fue necesario realizar entrevistas en varios departamentos de la entidad que arrojaron los siguientes resultados:

- Política de seguridad

Este documento conforma un conjunto de reglas, normas y procedimientos que compromete a la entidad que esta disponga de buenas prácticas de seguridad.

Tabla 7.
Resultados de las entrevistas sobre política de seguridad.

POLÍTICA DE SEGURIDAD	Cumple	No Cumple
¿Existe un departamento o área de Seguridad de la Información?		x
¿Existe una política de Seguridad de la Información en la SCPM?	x	
¿Existe un responsable de las políticas, normas y procedimientos en la SCPM de SDI?	x	
¿La Política de Seguridad es conocida por los funcionarios de la SCPM?		x
¿Existe mecanismos de Información de las normas que existe en la SCPM?		x
¿Existe periodos de revisión o cambio significativos en la Política de Seguridad?	x	

Elaborado por: Landeta & Quille

Análisis de las entrevistas sobre política de seguridad

Figura 9. Porcentaje de cumplimiento y no cumplimiento en la política de seguridad.
Elaborado por: Landeta & Quille

Conclusión: En este dominio se logra identificar que en la entidad tienen construida una política de seguridad, pero no se encuentra aprobada por la alta dirección, por lo tanto, es importante que la política luego de la aprobación sea difundida a todos los funcionarios de la entidad para su conocimiento.

- Aspectos organizativos de la seguridad de la información:

En este dominio, la entidad a nivel interno debe conformar una estructura organizativa gerencial para el comité de seguridad, algunas de las funciones que deben llevar a cabo son: la validación y aprobación de la política, apoyo para la implementación y definir funciones y responsabilidades de la seguridad.

Tabla 8.
Resultados de las entrevistas sobre aspectos organizativos de la seguridad de la información.

ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	Cumple	No Cumple
¿Existe definidas las responsabilidades para el Oficial de seguridad?		x
¿Existe comité de Seguridad?		x
¿La dirección y las áreas de la SCPM participan en temas de seguridad?		x
¿Cuándo ingresa de nuevos funcionarios firman un Acuerdo de Responsabilidad?	x	
¿Existe ayuda de terceros en temas de Seguridad para la SCPM?		x

¿Existe programas para la formación de seguridad a empleados, clientes y terceros de Seguridad?		x
¿Existen procedimientos y controles de seguridad para la evaluación, selección y adquisición de hardware?	x	
¿Existe algún procedimiento para el contrato de proveedores externos?	x	

Elaborado por: Landeta & Quille

Análisis de los aspectos organizativos de la seguridad de la información.

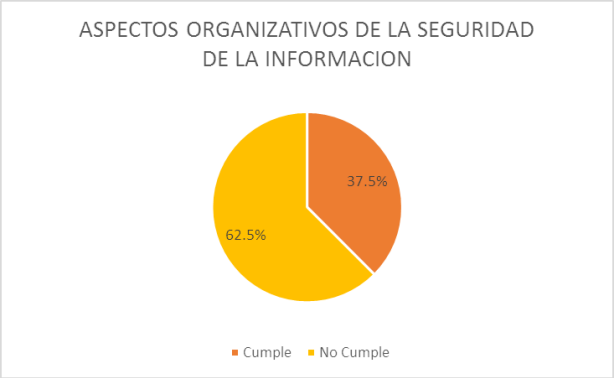

Figura 10. Porcentaje de cumplimiento y no cumplimiento en los aspectos organizativos de la seguridad de la información.
Elaborado por: Landeta & Quille

Conclusión: La entidad a pesar de no tener un oficial de seguridad y un comité de seguridad, dispone de controles de seguridad implementados que se cumplen dentro de la Superintendencia.

- Gestión de activos

Este dominio consiste en identificar la responsabilidad y clasificación de activos, esto permite tener un control de protección en los activos para lograr que el negocio sea confiable.

Tabla 9.
Resultados de las entrevistas sobre gestión de activos.

GESTIÓN DE ACTIVOS.	Cumple	No Cumple
¿Existe algún detalle del inventario de activos identificados en la SCPM?	X	
¿El inventario de los activos de información tecnológicos?	X	
¿El inventario de los activos posee responsable de cada uno?	X	
¿Existen valor de clasificación de activos de información según la criticidad?		x

¿Existe procedimientos para la identificación y clasificación de los activos de información?		x
¿Existe una política para el uso adecuado de los activos de información en la SCPM?	X	
¿Existen procedimientos para etiquetar los activos de información?		x
¿Existe alguna directriz para la clasificación de la información basado Sensibilidad y criticidad para la Organización?		x

Elaborado por: Landeta & Quille

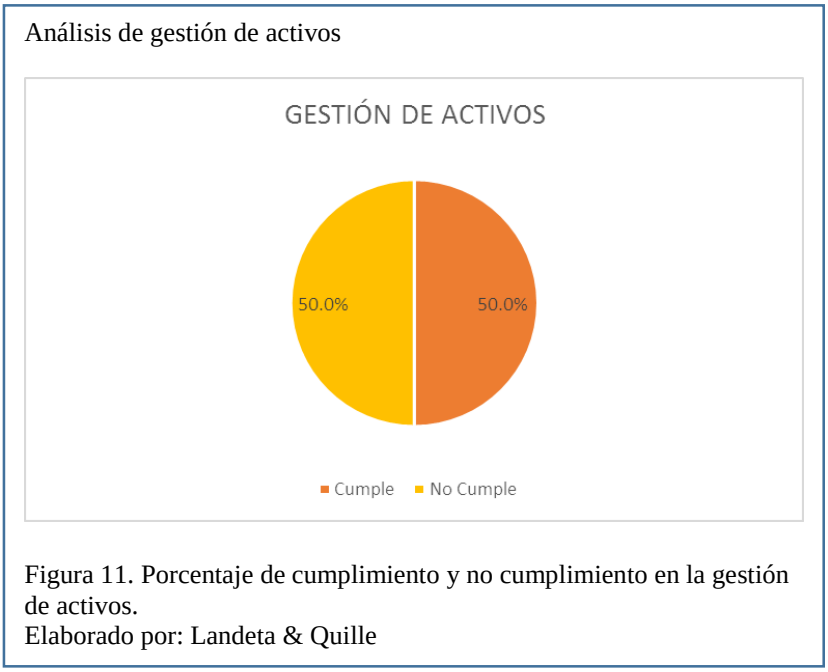

Figura 11. Porcentaje de cumplimiento y no cumplimiento en la gestión de activos.
Elaborado por: Landeta & Quille

Conclusión: Mediante la gestión de activos se logró identificar un 50% de cumplimiento de controles establecidos en la ISO 27002. Pero es menester poseer un análisis más completo de los activos que posee la entidad, analizar el riesgo de los activos de información y garantizar que se otorgue un apropiado nivel de protección.

- Seguridad ligada a los Recursos Humanos

La seguridad ligada a los Recursos Humanos es muy importante, pues corresponde al ciclo de trabajo de una persona donde se debe conocer el antes, durante y la culminación del empleo.

Todo personal contratado debe trabajar con ética y responsabilidad, esto permite que los funcionarios estén comprometidos con el manejo correcto de los activos y el cumplimiento de las políticas establecidas en la entidad.

Tabla 10.
Resultados de las entrevistas sobre seguridad ligada a los recursos humanos.

SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	Cumple	No Cumple
¿Se tienen definidos las descripciones de funciones y responsabilidades de la seguridad con la política de seguridad de la información de la SCPM?	x	
¿Se llevan a cabo la validación de datos y antecedentes penales antes de una contratación?	x	
¿Se maneja un acuerdo de confidencialidad en la SCPM ?	x	
¿Hacen firmar un acuerdo y responsabilidad del buen manejo de la información posterior al otorgamiento de accesos cuando necesiten tener acceso a la información?	x	
¿Existe proceso para la entrega de vienes cuando finalizan su contrato?	x	
¿Realizan proceso de backup de toda la información que tiene los empleado, contratista o usuario de terceras partes dentro de la institución?	x	
¿Existe procedimiento los ingresos y desvinculaciones de contratos dentro de la SCPM?	x	
¿Validan el cumplimiento de las responsabilidades respecto a la seguridad de la información?		x
¿Los funcionarios nuevos al ingresar a la SCPM reciben una capacitación de Seguridad y tratamiento de activos?		x
¿Existe un proceso reglamentario para los funcionarios cuando hayan incumplido la política de seguridad?	x	
¿Existe documento formalizado para procedimiento del alta y baja de contratos en la SCPM para el retiro de los accesos?		x

Elaborado por: Landeta & Quille

Análisis de la seguridad ligada a los recursos humanos

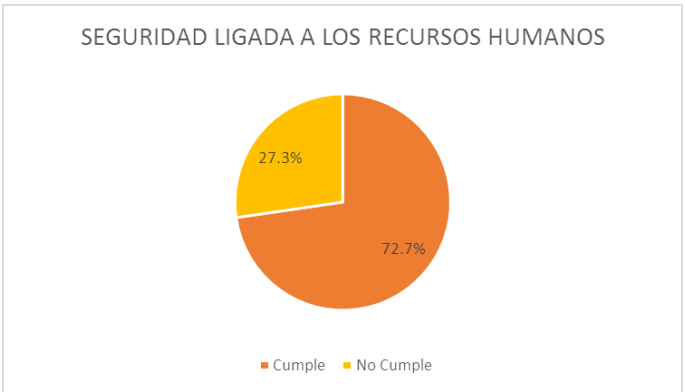

Figura 12. Porcentaje de cumplimiento y no cumplimiento en los Recursos Humanos
Elaborado por: Landeta & Quille

Conclusión: Se identificó que el área de Recursos Humanos tiene procesos correctos implementados para la contratación del personal. En este dominio es importante contratar un oficial de seguridad que será responsable de trabajar con Recursos

Humanos para que los funcionarios nuevos y antiguos reciban una capacitación de Seguridad y el buen manejo de activos.

- Seguridad física y del entorno:

La seguridad física y ambiental es la preparación de áreas seguras y protección de equipos, esto permite minimizar los riesgos que son producidos por daños en la información y las operaciones de la entidad.

Tabla 11.
Resultados de las entrevistas sobre la seguridad física y del entorno.

SEGURIDAD FÍSICA Y DEL ENTORNO.	Cumple	No Cumple
¿Existe control de ingreso en la SCPM para personal no autorizado?	x	
¿Existe seguridad para el acceso de las instalaciones del SCPM?		x
¿Existe seguridad física para oficinas, salas e instalaciones?		x
¿Se encuentran aislados los medios de procesamiento con control de acceso no autorizado?	x	
¿Existen protecciones frente a fallos en la alimentación eléctrica?		x
¿Existe seguridad en el cableado general del DataCenter, frente a daños e intercepciones?	x	
¿Existe mecanismo de seguridad física en la sala de servidores?	x	
¿Existe un plan de mantenimiento de los equipos para permitir su continua disponibilidad e Integridad?	x	
¿Existe procedimientos para el control de seguridad de equipos que encuentran fuera de la entidad?		x
¿E n la reutilización de un equipo se aseguran de que todo se encuentre removido como la información, software?	x	
¿Existe una política de reemplazo de equipos en la empresa, donde se contemple la autorización y justificación del reemplazo, impacto de la implantación a nivel de aplicaciones y costos?		x
¿Existen procedimientos poder trasladar un equipo o medio de almacenamiento a otro lugar con autorizaciones fuera de la organización?		x

Elaborado por: Landeta & Quille

Análisis de la seguridad física y del entorno

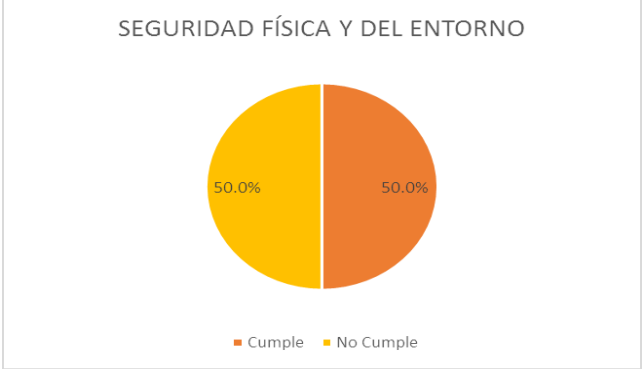

Figura 13. Porcentaje de cumplimiento y no cumplimiento en la seguridad física y del entorno
Elaborado por: Landeta & Quille

Conclusión: En la Superintendencia se maneja información confidencial almacenada físicamente, por lo que es importante establecer pautas de seguridad que ayude en la conservación de la documentación.

- Gestión de comunicaciones y operaciones:

Uno de los objetivos de este dominio, es tener un control que asegure la comunicación de los sistemas de información debido a los peligros existentes como software maligno, virus, etc., es importante que se establezca controles de seguridad para prevenir cualquier tipo de amenaza informática en cualquier sistema.

Tabla12
Resultados de las entrevistas sobre gestión de comunicaciones y operaciones.

GESTIÓN DE COMUNICACIONES Y OPERACIONES	Cumple	No Cumple
¿Los procedimientos de operación están documentados y disponibles para los usuarios que los requieran?		x
¿Existe procedimiento de Control de Cambios (versiones) en los sistemas de procesamiento de información?		x
¿Están documentando en el proceso los responsables que asegure una respuesta efectiva frente a incidentes de seguridad?		x
¿Se encuentran separados los entornos de desarrollo, contingencia y producción?	x	
¿Existe una persona responsable del paso del sistema de desarrollo a producción?	x	
¿Se realizan informes de la capacidad de uso de los recursos del sistema?		x
¿Existen definiciones de aceptación para los sistemas tecnológicos nuevos, actualizaciones o versiones nuevas?	x	
¿Se llevan a cabo las pruebas durante su desarrollo y antes de la subida a producción?	x	
¿Existe un registro de aceptación de los cambios realizados por parte de los usuarios?	x	
¿Existen controles de detección, prevención para el código malicioso (antivirus)?	x	
¿Existe logs de auditoría para el monitoreo de los servicios a terceros?	x	
¿Existe un procedimiento para la gestión de cambios de los servicios que se tiene en la organización por parte de terceros?		x
¿Existe un control para detección, prevención y recuperación para software malicioso (antivirus) en la organización?	x	
¿Existen políticas de actualización de antivirus, activación periódica en las versiones instaladas en los computadores de los usuarios?	x	
¿Se realiza cursos de concienciación al personal por el uso de los equipos y sobre software malicioso?	x	
¿Se realizan copias de backup de los sistemas que maneja información confidencial?	x	
¿Existen logs (registro de actividad de un sistema) para las actividades realizadas por los operadores y administradores?	x	
¿Existen logs de los fallos detectados en los sistemas?	x	

¿Existen procedimientos formales de verificación física de los respaldos?		x
¿Existe una política para la recuperación del sistema?		x
¿Se administra adecuadamente la red para protegerla de amenazas y mantener la seguridad de los sistemas de información?	x	
¿Se tiene implementado controles de seguridad para proteger la confidencialidad e integridad de información publicada?		x
¿Existen procedimientos para la protección de almacenaje de la información evitar un mal uso?	x	
¿Existe un adecuado manejo de la seguridad para mensajería electrónica?	x	
¿Se administra el comercio electrónico de la empresa acorde a los requisitos legales?		x
¿Se tiene un manejo de las herramientas adecuado para el comercio electrónico acorde a los contratos con terceros?		x
¿Se tiene una política para el manejo de las transacciones en línea para prevenir el enrutamiento, alteración o divulgación no autorizada del mensaje?		x
¿Existen pistas de auditoría y se mantienen por un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso?	x	
¿Se tiene una bitácora de actividades realizada por los operadores del sistema y administradores?	x	
¿Se tiene un registro de fallos y se toman las acciones apropiadas?	x	
¿Los relojes de los sistemas de procesamiento de información relevantes de la organización están sincronizados con una fuente de tiempo exacta acordada?		x

Elaborado por: Landeta & Quille

Análisis de la gestión de comunicaciones y operaciones

Figura 14. Porcentaje de cumplimiento y no cumplimiento en la gestión de comunicaciones y operaciones.
Elaborado por: Landeta & Quille

Conclusión: Es muy importante establecer procedimientos que garanticen la calidad y eficiencia de los procesos operativos que permite evitar incidentes que se produce por

el mal manejo de la información en cualquier ambiente, además los ambientes deben separar de pruebas, desarrollo y producción.

- Control de accesos

Para la seguridad en este dominio se deben establecer procesos y controles que limiten a los usuarios el acceso a la información crítica de la organización, control de usuarios personales, usuarios genéricos, usuarios de servicios y lineamiento de seguridad que debe tener cada sistema.

Tabla 13.
Resultados de las entrevistas sobre control de accesos**.**

CONTROL DE ACCESOS	Cumple	No Cumple
¿Existe una política o directriz de control de accesos?	x	
¿Tienen proceso de alta y bajas de accesos?	x	
¿Existe un administrador que controle a los usuarios y gestione los perfiles?	x	
¿Existe un procedimiento para la otorgación de claves?	x	
¿La gerencia revisa periódicamente los accesos otorgados a los usuarios utilizando un proceso formal?	x	
¿Tienen establecida una directriz de identificación y autenticación en los sistemas informáticos?	x	
¿Se aplica una política de encriptación de claves?		x
¿Se tienen deshabilitados los usuarios genéricos en las aplicaciones o repositorio? ¿Si se encuentran habilitadas estas son reseteadas de sus contraseñas genéricas?		x
¿Se obliga cada cierto tiempo a cambiar la contraseña automáticamente?	x	
¿Se tienen políticas o directrices de uso de contraseñas?	x	
¿Existen listados de intentos de accesos no satisfactorios o denegados al repositorio o Aplicaciones?	x	
¿Se les solicita a los usuarios que tenga medidas de protección apropiada al equipo desatendido?	x	
¿Dentro de la política de seguridad se tiene definido el mantener el escritorio limpio para los documentos y medios de almacenamiento removibles?	x	
¿Existe una directriz donde se establezca una técnica de autenticación para todos los usuarios?	x	
¿Existen pistas de auditorías habilitadas para el monitoreo de los súper usuarios?	x	
¿Se tiene métodos de autenticación adecuados para los accesos remotos del personal de la organización?	x	
¿Tienen definido mecanismos de control en los usuarios, para lectura, escritura, eliminación y ejecución de información?	x	
¿Tienen una política de inactividad para el bloqueo de la sesión luego de un período de inactividad definido?	x	
¿Las aplicaciones de alto riesgo tiene algún control de conexión?		x
¿Los sistemas sensibles se encuentran en un ambiente de cómputo dedicado?		x

¿Existe una política formal de las medidas de seguridad para los recursos móviles y telecomunicaciones?		x
¿Existen procedimientos para actividades de conexión fuera de trabajo como una VPN?		x

Elaborado por: Landeta & Quille

Análisis de control de accesos

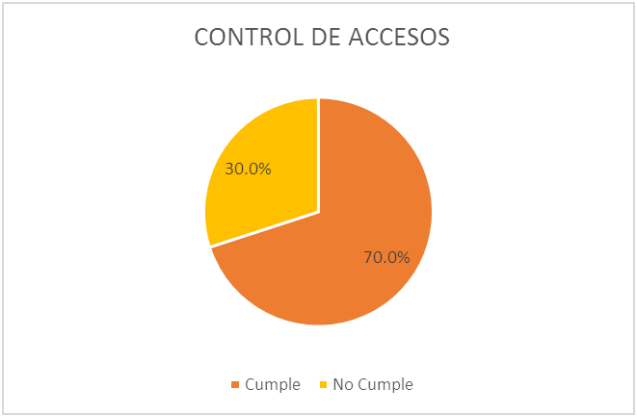

Figura 15. Porcentaje de cumplimiento y no cumplimiento en el control de accesos.
Elaborado por: Landeta & Quille

Conclusión: El control de acceso en la SCPM, tiene más de un 50% implementado, pero es necesario establecer directrices, procesos, manuales de usuarios que deben estar formalmente aprobados, esto ayuda en la implementación de lineamiento de control para la asignación de los privilegios de acceso a los sistemas y servicios.

- Adquisición, desarrollo y mantenimiento de sistemas de trabajo

En este dominio se debe establecer requerimientos y controles de prueba y soporte siempre que vaya a ejecutarse un desarrollo o se realicen cambios en cualquier sistema, pues esto permite evitar vulnerabilidades y establecer un tratamiento de los sistemas informáticos.

Tabla 14.
Resultados de las entrevistas sobre adquisición, desarrollo y mantenimiento de sistemas de trabajo.

ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE TRABAJO.	Cumple	No Cumple
¿Está implantada seguridad en los Sistemas de Información propios de la entidad?	X	
¿Existe requerimientos de seguridad dentro de las aplicaciones?	X	
¿Existe política de controles criptográficos?		x
¿Existe alguna protección de las claves criptográficas?		x
¿Existe seguridad en los ficheros de los sistemas?		x

¿Existe algún procedimiento en los desarrollos, testing y soporte?	X	
¿Tienen política o directriz para el uso de dispositivos para la salida de información?		x
¿Existe control de cambios en los Sistemas Operativos?	X	
¿Existe algún control para las vulnerabilidades de los equipos?	X	

Elaborado por: Landeta & Quille

Análisis de adquisición, desarrollo y mantenimiento de sistemas de trabajo.

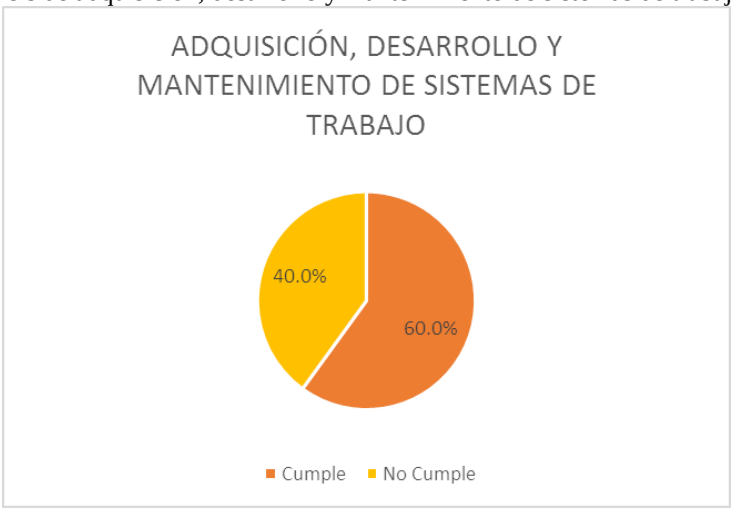

Figura 16. Porcentaje de cumplimiento y no cumplimiento en el control de adquisición, desarrollo y mantenimiento de sistemas de trabajo.
Elaborado por: Landeta & Quille

Conclusión: Se puede indicar que se dispone de controles de seguridad dentro de los sistemas de producción y desarrollo, pero es necesario definir y documentar normas, procedimientos e instrumentos con métodos de control para proteger la información que puede ser crítica o sensible.

- Gestión de incidentes en la seguridad de la información:

Es substancial que luego de un incidente se siga un procedimiento y métodos necesarios que permita analizar, reforzar y mejorar la seguridad.

Todo incidente compromete un fallo en un sistema y es importante identificar vulnerabilidades en un SGSI e implementar mejoras.

Tabla 15.
Resultados de las entrevistas sobre la gestión de incidentes en la seguridad de la información.

GESTIÓN DE INCIDENTES EN LA SEG. DE LA INFORMACIÓN	Cumple	No Cumple
¿Se tiene un procedimiento documentado para la gestión de incidentes y se toman las acciones apropiadas?		x

¿El personal informa si ha observado alguna debilidad o sospecha de debilidad o violación de las seguridades de los sistemas?	x	
¿Existe un encargado de los procedimientos de gestión para el control de manera rápida y efectiva de los incidentes reportados?		x
¿Existe un mecanismo para monitorear y cuantificar los incidentes reportados?		x
¿Se tiene un procedimiento para el manejo de las evidencias obtenidas del incidente reportado?		x
¿Tiene un procedimiento para realizar acciones correctivas hacia una incidencia?		x
¿El Oficial de Seguridad de la Información, emite algún informe a las áreas afectadas por los incidentes?		x

Elaborado por: Landeta & Quille

Análisis de la gestión de incidentes en la seguridad de la información

Figura 17. Porcentaje de cumplimiento y no cumplimiento en la gestión de incidentes en la seguridad de la información.
Elaborado por: Landeta & Quille

Conclusión: Se evidenció que el manejo de incidentes no tiene procedimiento ni responsable para la solución y el tratamiento por esta razón es importante establecer un método a seguir cuando se produzca un incidente de seguridad, esto permite aprender de los errores y lograr evitar que un ataque de seguridad ocurra nuevamente e interrumpa la operatividad de la entidad.

- Gestión de la continuidad del negocio

Es importante establecer un plan de continuidad en el que se implementen controles para minimizar el impacto que pueda ocasionar un incidente y que implique la interrupción de la operatividad del negocio, garantizando así la continuidad y disponibilidad de los sistemas de información.

Tabla 16.
Resultados de las entrevistas sobre la gestión de la continuidad del negocio.

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	Cumple	No Cumple
¿Se tiene un plan de continuidad del negocio o contingencia acorde a los objetivos de la organización?		x
¿El plan de continuidad de negocio es revisado periódicamente por la alta gerencia?		x
¿El plan se encuentra difundido formalmente en la organización?		x
¿Existe un responsable de la seguridad en caso de contingencia?		x
¿En el plan se identifican todos los riesgos, probabilidad de ocurrencia de impacto y sus posibles alternativas de solución?		x
¿Están definidos formalmente los procedimientos manuales de los procesos claves que se pondrían en ejecución en caso de una contingencia?		x
¿Se han realizado pruebas de eficacia al plan de continuidad de negocio?		x
¿Existe un procedimiento que garantice la continuidad y disponibilidad del equipo de cómputo en caso de desastre o contingencia?		x

Elaborado por: Landeta & Quille

Análisis sobre la gestión de la continuidad del negocio.

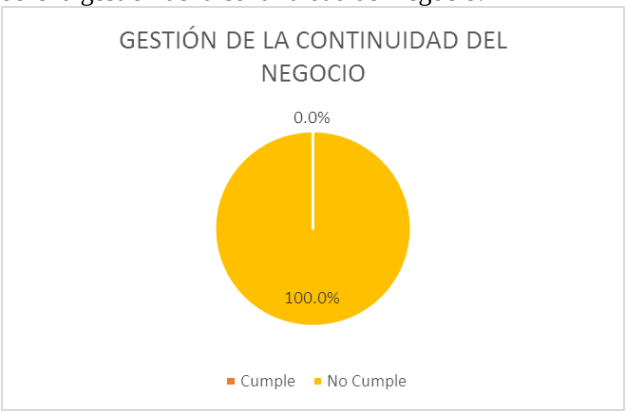

Figura 18. Porcentaje de cumplimiento y no cumplimiento en la gestión de continuidad del negocio
Elaborado por: Landeta & Quille

Conclusión: La entidad tiene 100% de no cumplimiento de los objetivos de control que establece el dominio continuidad de negocio, por lo tanto, se deberán incluir planes de control para la identificación y tratamiento de riesgos, donde permita analizar y asegurar la reanudación de los sistemas evitando interrupción causada por desastres o fallas, como por ejemplo un BCP (Business Bontinuity Plan).

- Cumplimiento:

En este dominio se plantea una evaluación en diferentes factores tales como requisitos legales, normas de seguridad, cumplimiento de seguridad y revisión de procesos donde debe involucrarse auditorías internas y externas.

Tabla 17.
Resultados de las entrevistas sobre el cumplimiento de las legislaciones vigentes.

CUMPLIMIENTO	Cumple	No Cumple
¿Existe algún procedimiento cumplimiento con la legislación por parte de los sistemas?		x
¿Existe el resguardo de la propiedad intelectual?		x
¿Existe el resguardo de los registros de la organización?		x
¿Existe la prevención del uso indebido de recursos de tratamiento de la información?	X	
¿Salvaguarda los servicios de procesamiento de información y las herramientas de auditoría durante las auditorías de los sistemas de información?		x
¿Existen consideraciones sobre las auditorías de los sistemas?		x

Elaborado por: Landeta & Quille

Análisis sobre el cumplimiento de las legislaciones vigentes.

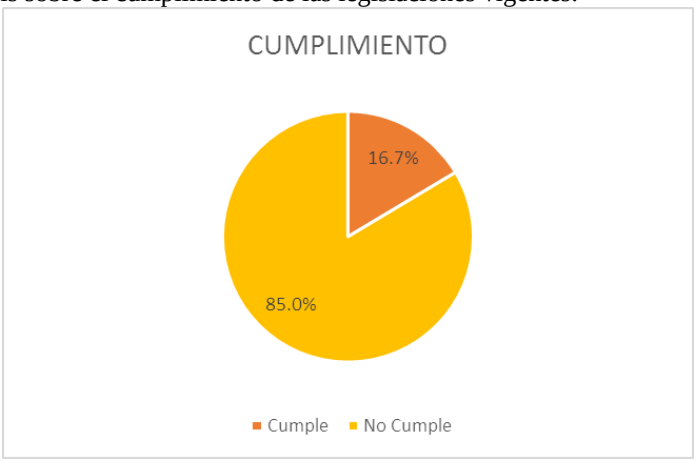

Figura 19. Porcentaje de cumplimiento y no cumplimiento de las legislaciones vigentes.
Elaborado por: Landeta & Quille

Conclusión: La entidad actualmente se encuentra en un proceso de la revisión y validación de la implementación de políticas y procesos, pero es muy importante revisar los procesos de seguridad con una auditoría externa cada cierto tiempo.

2.2. Estado actual de la superintendencia de control del poder de mercado

Llegando a este punto se realizó un levantamiento de controles de seguridad manejadas por la organización sobre la base de los controles establecidos en la norma ISO/IEC

27002:2005 y se generó como resultado, el estado actual del cumplimiento del estándar y un análisis de la Guía para el Proceso de Evaluación (GAP).

Tabla 18.
Estado actual del cumplimiento del estándar la norma ISO/IEC 27002:2005.

DOMINIOS	Cumple	No Cumple
POLÍTICA DE SEGURIDAD	50,0%	50,0%
ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	37,5%	62,5%
GESTIÓN DE ACTIVOS	40,0%	60,0%
SEGURIDAD LIGADA A LOS RECURSOS HUMANOS	72,0%	28,0%
SEGURIDAD FÍSICA Y DEL ENTORNO	50,0%	50,0%
GESTIÓN DE COMUNICACIONES Y OPERACIONES	61,3%	38,7%
CONTROL DE ACCESOS	70,0%	30,0%
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE TRABAJO	60,0%	40,0%
GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN	10,0%	90,0%
GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0,0%	100,0%
CUMPLIMIENTO	15,0%	85,0%

Nota. Estadística general de todos los dominios
Elaborado por: Landeta & Quille

Leyenda: Se establece un análisis referencial donde se identifica la situación actual de la entidad en base a la seguridad, por lo tanto, es importante tener planes de acción para seguir construyendo un SGSI e implementar controles de seguridad para llegar al estado deseable.

Estado Óptimo

Estado Deseable

Estado Actual

Radar resumen del análisis diferencial.

Figura 20. Diseño de radar elaborado con la información levantada para el análisis diferencial.
Elaborado por: Landeta & Quille

Con respecto a las normas de referencia la superintendencia no tiene los suficientes conocimientos sobre su funcionamiento (ISO 27001 e ISO 27002), conocen sobre el tema, pero no se han implementado en ella políticas, controles y otros elementos que le permita estar más protegida en temas de seguridad de la información por esta razón no posee un área específica encargada para ese fin.

La figura 20 presenta los resultados poco alentadores que motivan a la organización a tomar la decisión de brindar más apoyo; en los resultados se refleja que la entidad no cumple con más del 50% de los controles. Lo importante para la entidad es llegar a obtener un estado deseable dentro de cada dominio.

2.3. Determinación de activos

Activo de información: Este grupo dispondrá de la información de documentación, manuales de usuarios, normativas, contratos, etc., que son usados en la SCPM para la gestión del negocio.

Tabla 19.
Distribución de activos de información.

GRUPO	TIPO	NOMBRE DE ACTIVO	FORMATOS	DESCRIPCIÓN
Activo de Información	Documentación	Resolución	1	Formato de resolución
		Recomendaciones	1	Formato de recomendaciones generales
		Oficio	1	Formato de oficio con firmas de responsables
		Oficio Circular	1	Formato de oficio circular con firmas de responsables en grupo o varias o personas
		Memorando	1	Formato de Intercambio de Información entre departamentos de la SCPM
		Memorando Circular	1	Formato de intercambio de Información entre departamentos de la SCPM con fin Informativo
		Informe	1	Formato para información de lo realizado
		Providencia	1	Formato para prevenir cualquier daño o peligro
		Notificación	1	Formato de notificación de algún problema generado en la SCPM

		Norma Técnica	1	Formato establecido por consenso y aprobado por autoridades de la SCPM
		CONTRATO CODIGO DE TRABAJO	1	Documento necesario para ser parte de la SCPM
		CONTRATOS OCASIONALES	1	Documento que estipula la permanencia temporal de un empleado en la SCPM
		NOMBRAMIENTO LIBRE REMOCIÓN	1	Documento que garantiza al empleado de la SCPM permanencia indefinida en la entidad
		NOMBRAMIENTO PROVISIONAL	1	Documento que indica al empleado de la SCPM permanencia en la entidad por 2 años con opción a renovación
		ACUERDOS DE RESPONSABILIDAD	1	Documento que estipula las responsabilidades en la SCPM
		IMAGEN INSTITUCIONAL	1	La imagen es utilizada en la entidad tanto en documentos institucionales como logotipos web o de rotulación

Nota. Distribución de documentación
Elaborado por: Landeta & Quille

Software o Aplicación: Este grupo determinarán los activos de aplicativos desarrollados, sistemas de información, sistemas desarrollos, sistemas operativos, licencias, etc.

Tabla 20.
Distribución de software o aplicación.

GRUPO	TIPO	NOMBRE DE ACTIVO	CANTIDAD	DESCRIPCIÓN
Software / Aplicación	Aplicativos Desarrollados	ANKU	1	Control de tiempos y acciones procesales
				Dos meses de desarrollo
		KUMIR	1	Desarrollo dos semanas
				Gestión de roles de pago e inventarios de cada funcionario (Bienes)
		MEGA	1	Formulario de registro de operadores económicos
		AYLLU	1	Registro de comités de usuarios y el seguimiento
		MAKANA	1	Disposiciones de despacho
		ÑAKA	1	Gestión de garantías
		RIMACHI	1	Control interno según reglamento de la contraloría general del estado
		WAQAY	1	Denuncias externas

		ÑAWI	1	Registra y administra eventos y convenios
		RUNA	1	Gestión de talento humano
				Se une con el AD
				interactúa con los otros sistemas para los accesos
		Intranet	1	Joomla, php y MYSQL
		Página Web	1	Wordpress, en un hosting, es informativo e interactiva
				enlaces a los aplicativos públicos
	Licencias	IMPRESIÓN	1	Licencia de impresión denominadas Pccounter
		WINDOWS 7	240	Licencias de Sistema Operativo Microsoft Windows 7 de los computadores de los usuarios de la entidad
		TELEFONÍA	300	Licencias de comunicación de Telefonía Avaia para los usuarios de la entidad
		POLYCOM	100	Licencias de Video Conferencia
		OFFICE	240	Licencias Office
		VISIO	3	Licencia Office Visio
		PROJECT	3	Licencias de Administración de proyectos
		STATAN	5	Licencias de Software estadístico
		SPSS	10	Licencias de Software estadístico
		WINDOWS 2012	3	Licencias Sistema Operativo
		KASPERSKY	250	Licencias de Antivirus
		CORREO ELECTRÓNICO	300	Licencias de Correo Electrónico ZIMBRA

Nota. Distribución de software y aplicación
Elaborado por: Landeta & Quille

Hardware: se refiere a los activos tangibles disponibles de la entidad tales como equipos de oficina que se subcategorizan en PC, portátiles, servidores, dispositivos móviles, etc.

Tabla 21.
Distribución de hardware.

GRUPO	TIPO	NOMBRE DE ACTIVO	UNIDADES	DESCRIPCIÓN
Hardware	Equipos de Oficina	Portátiles - EliteBook 8470p	135	Equipos Portátiles de los usuarios de la SCPM
		PC - Compaq Pro 6300 MT	35	Equipos Pc de escritorio de los usuarios de la SCPM
		PC - Probook 640 G1	70	Equipos Portátiles de los usuarios de la SCPM
		Portátiles - Compaq Elite 8300	20	Equipos Pc de escritorio de los usuarios de la SCPM

		Proyectores	9	Equipos de oficina para las presentaciones de los usuarios
		Impresora LaserJet 600 B/N	16	Equipos de impresión para documentos de la SCPM
		Impresora LaserJet 551 Color	9	Equipos de impresión para documentos de la SCPM
		Impresora LaserJet 575 Multifunción	19	Equipos de impresión para documentos de la SCPM
		HP SCANNER 7500	9	Equipo de impresión digital para la SCPM
		Scanfront 300	2	Equipo de impresión digital para la SCPM
		Docking	50	Equipo de ventilación para equipos portátiles
		Telefonía IP	220	Equipos de comunicación telefónica marca AVAYA
		Servidor SRKAL BDD	1	Base de resoluciones de competencia a nivel de mercado se sincroniza con servidores de México de otra organización
		Servidor WEB	1	Alojado un sitio web de mercado
		Servidor NUUO	1	Servidor de video vigilancia de seguridad para la SCPM
		Servidor de Video conferencia	2	Servidor de comunicación para los empleados de la SCPM
		Servidor vmware	1	Servidor de virtualización de Sistemas Operativos
		Servidor Pc-sistel	1	Software tarifado de telefonía para las comunicaciones, software marca AVAYA
		UTM – FIREWALL	1	Gestionado de control de tráfico entrante y saliente de la red de la SCPM
		UTM - RELAY DE CORREO	1	Servidor de Gestión de Correo para la SCPM
		ACK	1	Sistema de Monitoreo del centro de datos temperatura
		LECTOR BIOMÉTRICO	10	Equipo de control de ingreso y salida del personal de la SCPM

Nota. Categorización por hardware
Elaborado por: Landeta & Quille

Red: en este punto se agrupan de los activos que ayudan a la entidad a estar comunicada tecnológicamente mediante dispositivos de conectividad de redes como router, swicth, concentradores, etc.

Tabla22.
Distribución de red.

GRUPO	TIPO	NOMBRE DE ACTIVO	UNIDADES	DESCRIPCIÓN
Red	Dispositivos de Conectividad de Redes	SWITCH CORE	9	Equipo centralizador de tráfico de red
		SWITCH ACCESO QUITO	8	Equipo de control de tráfico y comunicación con otros equipos de la red
		SWITCH HOME ZONALES	10	Equipo de comunicación entre zonas de la SCPM
		ROUTERS	2	Equipo de interconexión y control de tráfico de red entre sucursales de la SCPM
		Troncal sip de 10 canales	1	Equipo de comunicación de telefonía

Nota. Categorización por distribución de red
Elaborado por: Landeta & Quille

Equipamiento Auxiliar: Este grupo hace referencia a activos adicionales que complementan a los activos ya mencionados en las diferentes categorías expuestas anteriormente, estos pueden ser UPS, infraestructura, seguridad, etc.

Tabla 23.
Distribución de equipamiento auxiliar.

GRUPO	TIPO	NOMBRE DE ACTIVO	UNIDADES	DESCRIPCIÓN
Equipamiento Auxiliar	UPS	UPS (Uninterrumptible Power System,)	1	Equipo de respaldo de energía de 30 kva
		UPS (Uninterrumptible Power System,)	5	Equipo de respaldo de energía de 5 kva
		UPS (Uninterrumptible Power System,)	1	Equipo de respaldo de energía de 20 kva
	Infraestructura	RACK DE PISO	7	Equipo que contiene hardware de comunicación informática
		RACK DE PARED	2	Equipo que contiene hardware de comunicación informática

	Seguridad	CÁMARA DE VIGILANCIA	47	Equipos de seguridad colocados en sitios específicos de la entidad
		SENSORES AMBIENTALES	4	Equipos ubicados en toda el área de la entidad en caso de incendios

Nota. Categorización por equipamiento auxiliar
Elaborado por: Landeta & Quille

Instalación: en esta categoría se agrupan todo lo que tiene relación con el cableado, estructurado y las instalaciones eléctricas.

Tabla 24.
Distribución de instalación.

GRUPO	TIPO	NOMBRE DE ACTIVO	DESCRIPCIÓN
Instalación	Cableado Estructurado	Cableado	Cableado Estructurado LAN categoría 6
		Cableado entre bloques	Cableado estructurado de fibra óptica

Elaborado por: Landeta & Quille

Personal: La información detallada en esta categoría es aquella que hace referencia a todos los funcionarios que laboran en la SCPM.

Tabla 25.
Distribución de personal.

GRUPO	TIPO	NOMBRE DE ACTIVO	CANTIDAD	DESCRIPCIÓN
Personal	Empleados	Analistas	63	Cantidad de Funcionarios de la organización con el cargo de Analistas
		Asesor	22	Cantidad de Funcionarios de la organización con el cargo de Asesores
		Asistentes	22	Cantidad de Funcionarios de la organización con el cargo de Asistentes
		Auxiliar	10	Cantidad de Funcionarios de la organización con el cargo de Auxiliares

		Comisionado	2	Cantidad de Funcionarios de la organización con el cargo de Comisionados
		Conductor	16	Cantidad de Funcionarios de la organización con el cargo de Conductores
		Conserje	2	Cantidad de Funcionarios de la organización con el cargo de Conserjes
		Contador	1	Cantidad de Funcionarios de la organización con el cargo de Contadores
		Coordinador	4	Cantidad de Funcionarios de la organización con el cargo de Coordinadores
		Director	18	Cantidad de Funcionarios de la organización con el cargo de Directores
		Especialistas	2	Cantidad de Funcionarios de la organización con el cargo de Especialistas
		Experto	24	Cantidad de Funcionarios de la organización con el cargo de Expertos
		Intendente	11	Cantidad de Funcionarios de la organización con el cargo de Intendentes
		Médico General	1	Cantidad de Funcionarios de la organización con el cargo de Médico General
		Presidente	1	Cantidad de Funcionarios de la organización con el cargo de Presidente
		Secretaria	5	Cantidad de Funcionarios de la organización con el cargo de Secretarias
		Servidor Público	1	Cantidad de Funcionarios de la organización con el cargo de Servidor Público
		Superintendente	1	Cantidad de Funcionarios de la organización con el cargo de Súper Intendente
		Técnico	1	Cantidad de Funcionarios de la organización con el cargo de Técnicos
		Tesorero	1	Cantidad de Funcionarios de la organización con el cargo de Tesoreros

Nota. Categorización por personal
Elaborado por: Landeta & Quille

2.4. Valorización de activos

Activos de información.

Tabla 26.
Descripción de activos de información.

Documentación física / Digital		VALORIZACIÓN DE ACTIVOS			
TIPO	NOMBRE DE ACTIVO	D	C	I	VALOR
Información	Anexo 1 Resolución	2	1	3	Medio
	Anexo 3 Recomendaciones	2	1	3	Medio
	Anexo 4 Oficio	2	1	3	Medio
	Anexo 5 Oficio Circular	2	1	3	Medio
	Anexo 6 Memorando	2	1	3	Medio
	Anexo 7 Memorando Circular	2	1	3	Medio
	Anexo 8 Informe	2	1	3	Medio
	Anexo 9 Providencia	2	1	3	Medio
	Anexo 10 Notificación	2	1	3	Medio
	Anexo 11 Norma Técnica	2	1	3	Medio
	CONTRATO CODIGO DE TRABAJO	3	3	3	Alto
	CONTRATOS OCASIONALES	3	3	3	Alto
	NOMBRAMIENTO LIBRE REMOCIÓN	3	3	3	Alto
	NOMBRAMIENTO PROVISIONAL	3	3	3	Alto
	ACUERDOS DE RESPONSABILIDAD	3	3	3	Alto
	IMAGEN INSTITUCIONAL	3	3	3	Alto

Nota. Valorización de activos según el dominio
Elaborado por: Landeta & Quille

Software / Aplicación.

Tabla 27.
Descripción de software / aplicación.

Software / Aplicación		VALORIZACIÓN DE ACTIVOS			
TIPO	NOMBRE DE ACTIVO	D	C	I	VALOR
Aplicativos Desarrollados	ANKU	3	3	3	Alto
	KUMIR	2	2	2	Medio
	MEGA	3	3	3	Alto
	AYLLU	3	3	3	Alto
	MAKANA	3	3	3	Alto
	ÑAKA	2	2	2	Medio
	RIMACHI	2	2	2	Medio
	WAQAY	3	3	3	Alto
	ÑAWI	2	2	3	Medio
	RUNA	3	3	3	Alto
	Intranet	1	1	1	Bajo
	Página Web	3	3	2	Alto
Licencias	IMPRESIÓN	3	3	3	Alto
	WINDOWS 7	3	3	3	Alto
	TELEFONÍA	3	3	3	Alto

	POLYCOM	3	3	3	Alto
	OFFICE	3	3	3	Alto
	VISIO	3	3	3	Alto
	PROJECT	3	3	3	Alto
	STATAN	3	3	3	Alto
	SPSS	3	3	3	Alto
	WINDOWS 2012	3	3	3	Alto
	KASPERSKY	3	3	3	Alto
	CORREO ELECTRÓNICO	3	3	3	Alto

Nota. Valorización de activos según el dominio
Elaborado por: Landeta & Quille

Hardware.

Tabla 28.
Descripción de hardware.

Hardware		VALORIZACIÓN DE ACTIVOS			
TIPO	NOMBRE DE ACTIVO	D	C	I	VALOR
Equipos de Oficina	EliteBook 8470p	3	2	3	Alto
	Compaq Pro 6300 MT	3	2	3	Alto
	Probook 640 G1	3	2	3	Alto
	Compaq Elite 8300	3	2	3	Alto
	Proyectores	3	1	1	Medio
	Impresora LaserJet 600 B/N	3	1	1	Medio
	Impresora LaserJet 551 Color	3	1	1	Medio
	Impresora LaserJet 575 Multifunción	3	1	1	Medio
	HP SCANNER 7500	3	3	3	Alto
	Scanfront 300	3	3	3	Alto
	Docking	2	1	1	Bajo
	Telefonía IP	3	3	1	Medio
	Servidor SRKAL BDD	2	3	3	Alto
	Servidor WEB	2	3	3	Alto
	Servidor NUUO	3	3	3	Alto
	Servidor de Video conferencia	3	3	3	Alto
	Servidor vmware	3	3	3	Alto
	Servidor Pc-sistel	3	3	3	Alto
	FIREWALL	3	3	3	Alto
	RELAY DE CORREO	3	3	3	Alto
	ACK	3	3	3	Alto
	LECTOR BIOMÉTRICO	3	3	3	Alto

Nota. Valorización de activos según el dominio
Elaborado por: Landeta & Quille

Equipamiento Auxiliar.

Tabla 29.
Descripción de equipamiento auxiliar.

Equipamiento Auxiliar		VALORIZACIÓN DE ACTIVOS			
TIPO	NOMBRE DE ACTIVO	D	C	I	VALOR
UPS	UPS (Uninterrumptible Power System,)	3	3	3	Alto
	UPS (Uninterrumptible Power System,)	3	3	3	Alto
	UPS (Uninterrumptible Power System,)	3	3	3	Alto
INFRAESTRUCTURA	RACK DE PISO	1	1	1	Bajo
	RACK DE PARED	1	1	1	Bajo
SEGURIDAD	CÁMARA DE VIGILANCIA	3	3	3	Alto
	SENSORES AMBIENTALES	3	3	3	Alto

Nota. Valorización de activos según el dominio
Elaborado por: Landeta & Quille

Instalación.

Tabla 30.
Descripción de instalación.

Instalación		VALORIZACIÓN DE ACTIVOS			
TIPO	NOMBRE DE ACTIVO	D	C	I	VALOR
Cableado Estructurado	Cableado	3	3	3	Alto
	Cableado entre bloques	3	3	3	Alto

Nota. Valorización de activos según el dominio
Elaborado por: Landeta & Quille

Personal.

Tabla 31.
Descripción de personal.

Personas		VALORIZACIÓN DE ACTIVOS			
TIPO	NOMBRE DE ACTIVO	D	C	I	VALOR
Empleados	Analistas	3	3	3	Alto
	Asesor	3	3	3	Alto
	Asistentes	3	3	3	Alto
	Auxiliar	3	3	3	Alto
	Comisionado	3	3	3	Alto
	Conductor	3	3	3	Alto
	Conserje	3	3	3	Alto
	Contador	3	3	3	Alto
	Coordinador	3	3	3	Alto
	Director	3	3	3	Alto
	Especialistas	3	3	3	Alto
	Experto	3	3	3	Alto
	Intendente	3	3	3	Alto
	Médico General	3	3	3	Alto
	Presidente	3	3	3	Alto
	Secretaria	3	3	3	Alto
	Servidor Publico	3	3	3	Alto

	Superintendente	3	3	3	Alto
	Técnico	3	3	3	Alto
	Tesorero	3	3	3	Alto

Nota. Valorización de activos según el dominio
Elaborado por: Landeta & Quille

2.5. Análisis de riesgo

El análisis de riesgos proporciona importantes puntos en los que se enfoca para realizar la propuesta del Sistema de Gestión de Seguridad de la Información, en este proceso se analiza la criticidad valorizando al activo de manera cuantitativa (ISO/IEC 27001:2005, 2016)

Recursos Humanos

Tabla 32.
Análisis de recursos humanos.

GRUPO	DESCRIPCIÓN	CANT.	VALOR $	CRITICIDAD
EMPLEADOS	JEFES	15	69123	ALTO
	ESPECIALISTAS	46	130614	ALTO
	OPERARIOS	136	148952	ALTO
	ADMINISTRACIÓN	11	10427	ALTO

Nota. Criticidad de activos según el dominio
Elaborado por: Landeta & Quille

Hardware

Tabla 33.
Análisis de hardware.

GRUPO	DESCRIPCIÓN	CANT.	VALOR $	CRITICIDAD
EQUIPOS DE OFICINA	PORTÁTILES	260	273980	ALTO
	PROYECTORES	9	5400	BAJO
	IMPRESORAS	44	21631	MEDIO
	SCANNER	11	6550	BAJO
	DOCKING	50	5500	BAJO
COMUNICACIÓN	TELÉFONOS IP	220	50600	MEDIO
	TRONCAL SIP	1	2000	MEDIO
	SERVIDORES	7	147000	ALTO
	DISPOSITIVOS DE RED	35	79500	ALTO
INFRAESTRUCTURA	BIOMÉTRICOS	10	2000	BAJO
	UPS	7	5400	BAJO
	CÁMARAS	47	13160	BAJO
	SENSORES	4	128	BAJO
	RACKS	9	2500	BAJO

Nota. Criticidad de activos según el dominio
Elaborado por: Landeta & Quille

Licencias.

Tabla 34.
Análisis de licencias.

GRUPO	DESCRIPCIÓN	CANT.	VALOR $	CRITICIDAD
SERVIDORES	SISTEMAS OPERATIVOS Y APLICACIONES	259	63700	MEDIO
ESTACIONES DE TRABAJO	OFIMÁTICA	246	15300	BAJO
	ANTIVIRUS	250	12500	BAJO
	CORREO ELECTRÓNICO	300	6000	BAJO
	COMUNICACIÓN	400	27500	BAJO

Nota. Criticidad de activos según el dominio
Elaborado por: Landeta & Quille

Software.

Tabla 35.
Análisis de software.

GRUPO	DESCRIPCIÓN	CANT.	VALOR $	CRITICIDAD
DESARROLLO	APLICATIVOS DESARROLLADOS	92	105000	ALTO

Nota. Criticidad de activos según el dominio
Elaborado por: Landeta & Quille

Otros.

Tabla 36.
Análisis de otros activos.

GRUPO	DESCRIPCIÓN	CANT.	VALOR $	CRITICIDAD
INFORMATIVOS	DOCUMENTOS SCPM	218	0	0
MERCADO	IMAGEN INSTITUCIONAL	1	15000	MEDIO

Nota. Criticidad de activos según el dominio
Elaborado por: Landeta & Quille

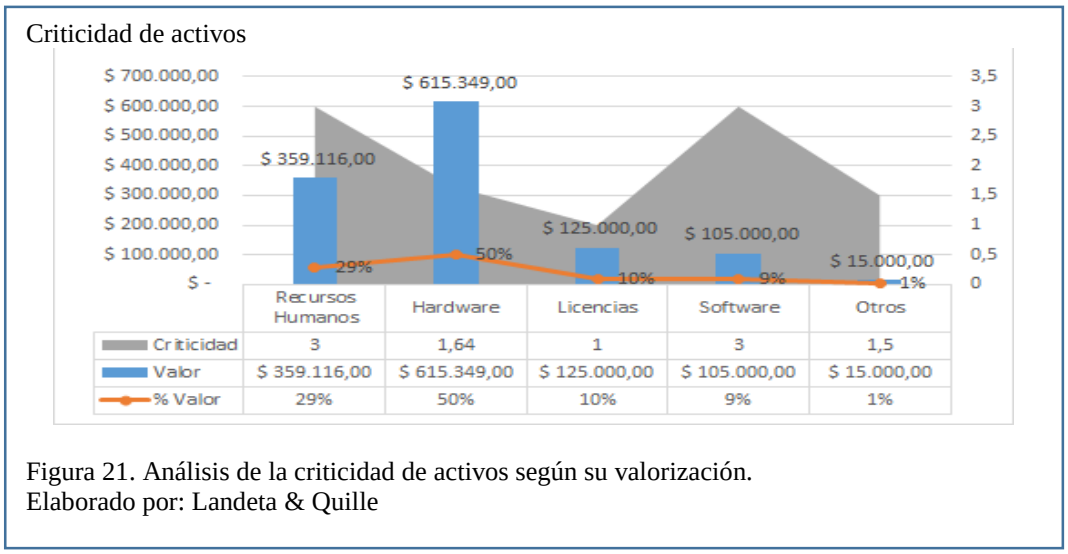

Figura 21. Análisis de la criticidad de activos según su valorización.
Elaborado por: Landeta & Quille

Determinación de amenazas por activo.

Natural: desastres naturales

Humana: falla propia del operador

Entorno: fallos que no se pueden identificar a primera instancia

Tabla 37.
Muestra de análisis de Determinación de amenazas por activo.

N	AMENAZA	ORIGINADA			ORIGEN	MOTIVACIÓN
		NATURAL	HUMANA	ENTORNO		
1	Fallo de Hardware			X	Indeterminado	Indeterminado
2	Virus / Malware		X		Dispositivos externos o archivos desconocidos	Daño de equipos, información. Beneficio económico
3	Acceso no autorizado		X		Robots / Usuarios	Obtención de información
4	Robo de información confidencial		X		Funcionarios descontentos o desleales	Obtención de beneficio económico.
5	Fallo eléctrico	X			Indeterminado	Indeterminado
6	Robo de equipos		X		Funcionarios descontentos o desleales	Obtención de beneficio económico
7	Daños provocados al Hardware		X		Funcionarios descontentos o desleales	Ocasionar daños a la entidad o funcionarios
8	Fallo lógico de aplicativos o software			X	Indeterminado	Indeterminado
9	Incendio	X			Indeterminado	Indeterminado
10	Propagación código malicioso		X		Funcionarios descontentos o desleales. Entidades competidoras	Obtención de beneficio económico o daño a sistemas de la entidad

Nota. Amenazas detectadas en la entidad en base a entrevistas
Elaborado por: Landeta & Quille

Análisis de las diferentes amenazas

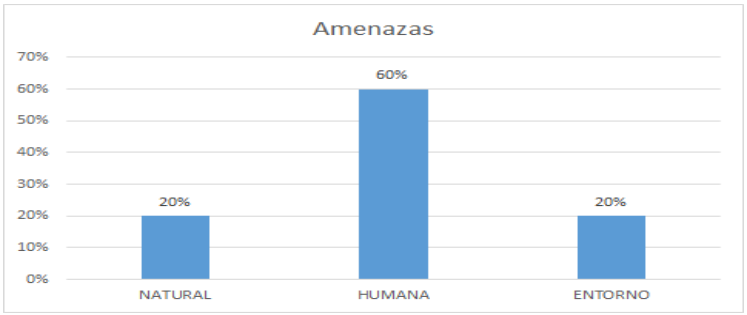

Figura 22. Análisis de las amenazas identificadas en la entidad.
Elaborado por: Landeta & Quille

Se logró identificar que el mayor porcentaje de riesgo es en el Hardware; la entidad tiene una gran inversión realizada en tecnología, este hecho implica asumir buenas prácticas en el uso de los equipos y desarrollar planes de contingencia óptimos en caso de algún daño que pueda afectar el equipamiento

De igual manera se constató que el mayor porcentaje de amenazas puede ser originado por el humano (60%), por lo cual se deben tener planes de mejora que involucren las gestiones que relacionen a las personas. La propuesta que se deberá elaborar para reducir el riesgo de seguridad y las amenazas debe estar enfocada en fortalecer las aplicaciones de la entidad, así como en su infraestructura que ayuda a los funcionarios a minimizar problemas o errores por falla humana.

2.6. Declaración de aplicación

A continuación, se detallará la Declaración de Aplicación (SOA) para determinar los controles que se debe realizar por medio del SGSI.

Tabla 38.
Leyenda.

CDI	Controles documentados e implementados
CIND	Controles implementados que deben ser documentados
CDNI	Controles documentados, pero no implementados
CNA	Controles que no se encuentra aplicados

Nota. Siglas a considerar en la declaración de aplicación
Elaborado por: Landeta & Quille

Es importante mencionar que los dominios y controles indicados en la siguiente tabla se escriben tal cual como los menciona la norma debido que se los requiere usarlos exactamente como fueron propuestos; sin embargo, en las columnas adicionales se coloca contenido relativo al análisis.

Tabla 39.
Especificación la declaración de aplicación.

CONTROL	APLICA	ESTADO DE CONTROL
5.1 Política de seguridad de la información.		
5.1.1 Documento de política de seguridad de la información.	SI	CDNI
5.1.2 Revisión de la política de seguridad de la información.	SI	CNA
6.1 Organización interna.		
6.1.1 Compromiso de la Dirección con la seguridad de la información.	SI	CNA
6.1.2 Coordinación de la seguridad de la información.	SI	CNA
6.1.3 Asignación de responsabilidades relativas a la seguridad de la información	SI	CNA
6.1.4 Proceso de autorización de recursos para el tratamiento de la información.	SI	CNA
6.1.5 Acuerdos de confidencialidad.	SI	CDI
6.1.6 Contacto con las autoridades.	SI	CIND
6.1.7 Contacto con grupos de especial interés.	SI	CNA
6.1.8 Revisión independiente de la seguridad de la información.	SI	CNA
6.2 Terceros.		
6.2.1 Identificación de los riesgos derivados del acceso de terceros.	SI	CIND
6.2.2 Tratamiento de la seguridad en la relación con los clientes.	SI	CIND
6.2.3 Tratamiento de la seguridad en contratos con terceros.	SI	CDI
7.1 Responsabilidad sobre los activos.		
7.1.1 Inventario de activos.	SI	CIND
7.1.2 Propiedad de los activos.	SI	CIND
7.1.3 Uso aceptable de los activos.	SI	CDI
7.2 Clasificación de la información.		
7.2.1 Directrices de clasificación.	SI	CNA
7.2.2 Etiquetado y manipulado de la información.	SI	CIND
8.1 Antes del empleo.		
8.1.1 Funciones y responsabilidades.	SI	CIND
8.1.2 Investigación de antecedentes.	SI	CDI
8.1.3 Términos y condiciones de contratación.	SI	CDI
8.2 Durante el empleo.		
8.2.1 Responsabilidades de la Dirección.	SI	CDI
8.2.2 Concienciación, formación y capacitación en seguridad de la información	SI	CDI
8.2.3 Proceso disciplinario.	SI	CDI
8.3 Cese del empleo o cambio de puesto de trabajo.		

8.3.1 Responsabilidad del cese o cambio.	SI	CIND
8.3.2 Devolución de activos.	SI	CIND
8.3.3 Retirada de los derechos de acceso.	SI	CIND
9.1 Áreas seguras.		
9.1.1 Perímetro de seguridad física.	SI	CIND
9.1.2 Controles físicos de entrada.	SI	CNA
9.1.3 Seguridad de oficinas, despachos e instalaciones.	SI	CIND
9.1.4 Protección contra las amenazas externas y de origen ambiental.	SI	CDI
9.1.5 Trabajo en áreas seguras.	SI	CDI
9.1.6. Áreas aisladas de carga y descarga	SI	CDI
9.2 Seguridad de los equipos.		
9.2.1 Emplazamiento y protección de equipos.	SI	CDI
9.2.2 Instalaciones de suministro.	SI	CDI
9.2.3 Seguridad del cableado.	SI	CDI
9.2.4 Mantenimiento de los equipos.	SI	CDI
9.2.5 Seguridad de los equipos fuera de las instalaciones.	SI	CIND
9.2.6 Reutilización o retirada segura de equipos.	SI	CIND
9.2.7 Retirada de materiales propiedad de la empresa.	SI	CIND
10.1 Responsabilidades y procedimientos de operación.		
10.1.1 Documentación de los procedimientos de operación.	SI	CIND
10.1.2 Gestión de cambios.	SI	CIND
10.1.3 Segregación de tareas.	SI	CIND
10.1.4 Separación de los recursos de desarrollo, prueba y operación.	SI	CDNI
10.2 Gestión de la provisión de servicios por terceros.		
10.2.1 Provisión de servicios.	SI	CDI
10.2.2 Supervisión y revisión de los servicios prestados por terceros.	SI	CDI
10.2.3 Gestión del cambio en los servicios prestados por terceros.	SI	CNA
10.3 Planificación y aceptación del sistema.		
10.3.1 Gestión de capacidades.	SI	CIND
10.3.2 Aceptación del sistema.	SI	CNA
10.4 Protección contra el código malicioso y descargable.		
10.4.1 Controles contra el código malicioso.	SI	CDI
10.4.2 Controles contra el código descargado en el cliente.	SI	CDI
10.5 Copias de seguridad.		
10.5.1 Copias de seguridad de la información.	SI	CIND
10.6 Gestión de la seguridad de las redes.		
10.6.1 Controles de red.	SI	CDI
10.6.2 Seguridad de los servicios de red.	SI	CDI
10.7 Manipulación de los soportes.		
10.7.1 Gestión de soportes extraíbles.	SI	CIND
10.7.2 Retirada de soportes.	SI	CIND
10.7.3 Procedimientos de manipulación de la información.	SI	CIND
10.7.4 Seguridad de la documentación del sistema.	SI	CIND

10.8 Intercambio de información.		
10.8.1 Políticas y procedimientos de intercambio de información.	SI	CDNI
10.8.2 Acuerdos de intercambio.	SI	CDNI
10.8.3 Soportes físicos en tránsito.	SI	CDNI
10.8.4 Mensajería electrónica.	SI	CDNI
10.8.5 Sistemas de información empresariales.	SI	CDNI
10.9 Servicios de comercio electrónico.		
10.9.1 Comercio electrónico.	SI	CDNI
10.9.2 Transacciones en línea.	SI	CDNI
10.9.3 Información públicamente disponible.	SI	CDNI
10.10 Supervisión.		
10.10.1 Registros de auditoría.	SI	CIND
10.10.2 Supervisión del uso del sistema.	SI	CIND
10.10.3 Protección de la información de los registros.	SI	CIND
10.10.4 Registros de administración y operación.	SI	CNA
10.10.5 Registro de fallos.	SI	CIND
10.10.6 Sincronización del reloj	SI	CNA
11.1 Requisitos de negocio para el control de acceso.		
11.1.1 Política de control de acceso.	SI	CDNI
11.2 Gestión de acceso de usuario.		
11.2.1 Registro de usuario.	SI	CIND
11.2.2 Gestión de privilegios.	SI	CIND
11.2.3 Gestión de contraseñas de usuario.	SI	CDI
11.2.4 Revisión de los derechos de acceso de usuario.	SI	CIND
11.3 Responsabilidades de usuario.		
11.3.1 Uso de contraseñas.	SI	CDI
11.3.2 Equipo de usuario desatendido.	SI	CDI
11.3.3 Política de puesto de trabajo despejado y pantalla limpia.	SI	CDNI
11.4 Control de acceso a la red.		
11.4.1 Política de uso de los servicios en red.	SI	CIND
11.4.2 Autenticación de usuario para conexiones externas.	SI	CIND
11.4.3 Identificación de los equipos en las redes.	SI	CIND
11.4.4 Protección de los puertos de diagnóstico y configuración remotos.	SI	CIND
11.4.5 Segregación de las redes.	SI	CIND
11.4.6 Control de la conexión a la red.	SI	CIND
11.4.7 Control de encaminamiento (routing) de red.	SI	CIND
11.5 Control de acceso al sistema operativo.		
11.5.1 Procedimientos seguros de inicio de sesión.	SI	CIND
11.5.2 Identificación y autenticación de usuario.	SI	CIND
11.5.3 Sistema de gestión de contraseñas.	SI	CIND
11.5.4 Uso de los recursos del sistema.	SI	CIND
11.5.5 Desconexión automática de sesión.	SI	CDI
11.5.6 Limitación del tiempo de conexión.	SI	CIND
11.6 Control de acceso a las aplicaciones y a la información.		

11.6.1 Restricción del acceso a la información.	SI	CIND
11.6.2 Aislamiento de sistemas sensibles.	SI	CIND
11.7 Ordenadores portátiles y teletrabajo.		
11.7.1 Ordenadores portátiles y comunicaciones móviles.	SI	CNA
11.7.2 Teletrabajo.	SI	CNA
12.1 Requisitos de seguridad de los sistemas de información.		
12.1.1 Análisis y especificación de los requisitos de seguridad.	SI	CIND
12.2 Tratamiento correcto de las aplicaciones.		
12.2.1 Validación de los datos de entrada.	SI	CIND
12.2.2 Control del procesamiento interno.	SI	CIND
12.2.3 Integridad de los mensajes.	SI	CIND
12.2.4 Validación de los datos de salida.	SI	CIND
12.3 Controles criptográficos.		
12.3.1 Política de uso de los controles criptográficos.	SI	CNA
12.3.2 Gestión de claves.	SI	CNA
12.4 Seguridad de los archivos de sistema.		
12.4.1 Control del software en explotación.	SI	CDI
12.4.2 Protección de los datos de prueba del sistema.	SI	CDNI
12.4.3 Control de acceso al código fuente de los programas.	SI	CDI
12.5 Seguridad en los procesos de desarrollo y soporte.		
12.5.1 Procedimientos de control de cambios.	SI	CIND
12.5.2 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.	SI	CIND
12.5.3 Restricciones a los cambios en los paquetes de software.	SI	CIND
12.5.4 Fugas de información.	SI	CIND
12.5.5 Externalización del desarrollo de software.	SI	CIND
12.6 Gestión de la vulnerabilidad técnica.		
12.6.1 Control de las vulnerabilidades técnicas.	SI	CIND
13.1 Notificación de eventos y puntos débiles de seguridad de la información.		
13.1.1 Notificación de los eventos de seguridad de la información.	SI	CNA
13.1.2 Notificación de puntos débiles de seguridad.	SI	CIND
13.2 Gestión de incidentes y mejoras de seguridad de la información.		
13.2.1 Responsabilidades y procedimientos.	SI	CIND
13.2.2 Aprendizaje de los incidentes de seguridad de la información.	SI	CIND
13.2.3 Recopilación de evidencias.	SI	CIND
14.1 Aspectos de seguridad de la información en la gestión de la continuidad del negocio.		
14.1.1 Inclusión de la seguridad de la información en el proceso de gestión de la continuidad del negocio.	SI	CNA
14.1.2 Continuidad del negocio y evaluación de riesgos.	SI	CNA
14.1.3 Desarrollo e implantación de planes de continuidad que incluyan la seguridad de la información.	SI	CNA
14.1.4 Marco de referencia para la planificación de la continuidad del negocio.	SI	CNA
14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad.	SI	CNA

15.1 Cumplimiento de los requisitos legales.		
15.1.1 Identificación de la legislación aplicable.	SI	CIND
15.1.2 Derechos de propiedad intelectual (DPI).	SI	CNA
15.1.3 Protección de los documentos de la organización.	SI	CDI
15.1.4 Protección de datos y privacidad de la información de carácter personal.	SI	CDI
15.1.5 Prevención del uso indebido de recursos de tratamiento de la información.	SI	CDI
15.1.6 Regulación de los controles criptográficos.	SI	CNA
15.2 Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico.		
15.2.1 Cumplimiento de las políticas y normas de seguridad.	SI	CNA
15.2.2 Comprobación del cumplimiento técnico.	SI	CNA
15.3 Consideraciones sobre las auditorías de los sistemas de información.		
15.3.1 Controles de auditoría de los sistemas de información.	SI	CNA
15.3.2 Protección de las herramientas de auditoría de los sistemas de información.	SI	CNA

Nota. Aplicabilidad de los controles en la entidad
Elaborado por: Landeta & Quille

CAPITULO 3

Desarrollo de la propuesta para la implementación del sistema de gestión de seguridad de la información

3.1. Gestión de indicadores

En la propuesta final se procede a definir indicadores que permita medir la eficiencia en la implementación de los controles de seguridad que establece ISO/IEC 27002:2005, en la implementación de un SGSI uno de los indicadores es la documentación dentro de cada dominio que son políticas/directrices, procedimientos e instrumentos.

3.2. Alcance y límites de la gestión de seguridad

Para dar una definición del alcance en el SGSI, se deben identificar los procesos principales en la institución, validar los responsables e identificar qué activos de información se involucran en estos procesos y para determinar cuáles son los controles o recursos indispensables que la institución debe emplear para cumplir con sus objetivos de negocio.

La presente propuesta tiene como finalidad entregar posibles soluciones planteadas para la implementación de controles de seguridad que ayuden a construir un SGSI en la SCPM, tomando en cuenta todas las falencias resultantes de la comparación con lo que se indica en la ISO/IEC 27001:2005 y 27002.

3.3. Organización de seguridad

La norma está organizada en 11 dominios, los cuales contiene un total de 133 controles que abarcan desde los aspectos estratégicos de un SGSI hasta los más operativos. (UNIT, s.f.)

3.3.1. Política de seguridad de la información.

La Política de Seguridad, tiene como finalidad ser una guía de apoyo para resguardar la información y protegerla en relación con los objetivos que establezca la entidad para su desarrollo.

El conjunto de políticas, procedimientos, directrices e instrumentos que se vayan a implementar, deben tener un sustento de las máximas autoridades para su aprobación y ejecución. La dirección responsable debe constar evidencias de su compromiso con la entidad, para la implementación, revisión, mantenimiento y cumplimiento de los documentos establecidos en la Política de Seguridad.

Políticas/Directrices

La SCPM tiene elaborada una política de seguridad, pero no posee la aprobación de una máxima autoridad, por lo que no es posible su difusión ni su aplicación por parte de la dirección responsable, esta misma dirección es la encargada de solicitar la revisión y aprobación de la política de seguridad para empezar con la difusión y mantenimiento en cada artículo establecido en la Política de Seguridad.

La dirección encargada debe difundir la política de seguridad a todos los funcionarios y áreas relevantes.

La política debe ser revisada en tiempos planificados y en caso de que se produzcan algún cambio significativo, garantizando a la entidad el cumplimiento con eficacia de las buenas prácticas establecidas por los estándares que establece la ISO 27002:2005.

Instrumentos:

- Documento Físico/Digital de la Política de Seguridad de la SCPM.

Prioridad de Ejecución:

- Inmediata.

Responsables: Comité de Seguridad.

3.3.2. Aspectos organizativos para la seguridad.

Es indispensable que participe un representante de cada área para cubrir todas las necesidades de la SCPM.

Procedimientos:

La Superintendencia debe crear una estructura para el Comité de Seguridad de la Información con el objetivo de controlar e implementar la seguridad teniendo en cuenta los siguientes requisitos que se deben incorporar dentro de la política de seguridad:

Procedimiento para definir responsabilidades de seguridad.

1. Definir un área responsable de la seguridad en la organización, que debe estar conformado principalmente por un oficial de seguridad de la información.
2. Identificar responsabilidades de la seguridad donde se debe detallar las funciones del equipo.

Procedimiento para la revisión de la política de seguridad.

- Establecer tiempos para revisar, validar y aprobar la política de seguridad.
- Validar que la política de seguridad dentro de la organización se implemente.
- La entidad debe implementar medios de comunicación para dar a conocer la política de seguridad a todos los funcionarios que conforma la organización, ya sean carteleras o un medio tecnológico como un e-learning.
- Definir procedimiento para el control del cumplimiento de la política.

Instrumentos:

- Acuerdo de confidencialidad para terceros.
- Formulario para gestión de accesos para terceros.

3.3.3. Gestión de activos.

Los activos de toda organización deben tener una protección adecuada respetando la base que indica la ISO 27002, los mismos deben ser justificados y asignados a un propietario o usuario. El usuario tiene que hacerse responsable del buen manejo y protección del activo para su óptimo funcionamiento, esto permite que las organizaciones tengan claro la vida útil y el cumplimiento de su misión, esa es la manera que recomienda la ISO 9001 (Norma International ISO 9001:2008).

Políticas/Directrices:

- Generar una matriz de identificación de activos de información con cada dueño del proceso crítico.
- El control y mantenimiento de los activos se debe llevar a cabo con un riguroso seguimiento tanto de los usuarios como de los responsables de los activos.
- Todos los activos deben estar claramente identificados, clasificados e identificados, para el etiquetado se recomienda el uso de códigos de barra para facilitar de esta forma la tarea de inventario, así como la entrada y salida de equipos de las instalaciones con los funcionarios.

Procedimientos:

Procedimiento de clasificación y autenticación de activos.

- El oficial de seguridad junto con los dueños de la información es responsable de educar a los usuarios que poseen los activos para el uso adecuado de los mismos, de esta manera se garantiza la vida útil del activo.

- El oficial de seguridad junto con los dueños de la información es responsables de registrar todos los activos de la entidad que contengan la información más importante para de esta manera asignar un responsable por cada uno.
- El oficial de seguridad es responsable de programar el mantenimiento preventivo de todos los activos registrados en sus formatos o sistemas autorizados.

Procedimiento de registro de ingreso y salida de equipos.

- El departamento de bienes en conjunto con el de tecnología son quienes tienen la responsabilidad de aprobar el ingreso y salida de los activos de la entidad que deben ser registrados y actualizados para poder tomar acciones en caso de pérdida de uno de ellos.

Procedimiento para dar de baja los equipos tecnológicos.

- Cuando un activo se determine totalmente inservible, el personal de TI es responsable de notificar al departamento de bienes mediante un informe el estado del activo para que el área tome acciones correspondientes, para este fin se debe disponer de un formato específico que deberá ser registrado posteriormente en la matriz de activos de tipo hardware.
- El personal de TI es responsable de tener un respaldo de los activos que se les entrega a los usuarios. Se puede usar un acta de entrega de activos, firmado por el usuario que recibe y el que entrega.

Instrumentos:

- Formato de inventario de equipos.
- Formato control de entrada y salida de equipo.
- Formato equipos dados de baja.
- Formato acta entrega de activos.

3.3.4. Seguridad en los recursos humanos.

Recursos Humanos debe asegurar que cada persona tiene claro sus responsabilidades, lo que constituye un factor muy importante para el cumplimiento de sus actividades.

Políticas/Directrices:

La SCPM tiene elaborada la política y se encuentra en proceso de aprobación por la máxima autoridad. La dirección responsable debe realizar una revisión cada cierto tiempo determinado.

Procedimientos:

1. Procedimiento de reclutamiento e incorporación de personal.
    - Definir responsabilidades de los funcionarios de la organización y entregar formalmente a los mismos.
    - El proceso de inclusión y exclusión de funcionarios se debe documentar y formalizar junto con el comité de seguridad para la entrega de bienes y eliminación de accesos.
2. Procedimiento disciplinario.
    - Implementar procesos disciplinarios de seguridad y actividades para que los funcionarios nuevos tengan conocimiento de la seguridad y se comprometan garantizar el manejo correcto de los activos dentro de la organización.
    - Se recomienda para la protección los activos de información de carácter confidencial los funcionarios deben tener pleno conocimiento de las responsabilidades que adquieren al ingresar a la organización mediante el acuerdo de responsabilidad para el buen uso de los activos de información.

Instrumentos:

- Acuerdo de confidencialidad para terceros.
- Descripción del cargo
- Formulario para la calificación de gestión de desempeño.

3.3.5. Gestión de incidentes.

Este control debe ser revisado y se revalidará en función de los incidentes reportados y remediados por el Área de Seguridad de la Información. En caso de existir modificaciones, éstas deben someterse a una validación previa por parte del Comité de Seguridad de la Información. Posteriormente, dichos cambios se comunican y difunden a los involucrados.

Políticas/Directrices:

- Las vulnerabilidades de seguridad en activos informáticos de la SCPM deben ser revisadas constantemente para asegurar un tratamiento efectivo del riesgo asociado.
- La revisión de vulnerabilidades se efectuará individualmente por activo o grupos de activos informáticos específicos, de acuerdo al criterio de nivel de riesgo.
- Se establecerán y llevarán a cabo planes de tratamiento de las vulnerabilidades identificadas. Las áreas de Infraestructura y Desarrollo serán las encargadas de ejecutar los planes.
- Se establecerán pruebas de vulnerabilidades que ayudarán a establecer un plan de mejora y solución.
- Los criterios, resultados y planes de tratamiento de vulnerabilidades serán informados y reportados a las áreas pertinentes garantizando un adecuado criterio de confidencialidad.

- Toda implementación de actualizaciones debe ser efectuada mediante el uso de herramientas automáticas, en el caso de ser posible deberá realizarse de manera controlada.

Procedimientos:

1. Identificación de debilidades en la seguridad.

Debe existir procedimientos y/o mecanismos formales para la identificación de las debilidades, los cuales se aplicarán con enfoque preventivo y detectivo / correctivo, serían los siguientes:

- Los criterios para pruebas de penetración serán definidos por el área de Seguridad de la Información en contacto directo con tecnología.
- Las pruebas se aplicarán sobre la base de criterios claramente establecidos por los riesgos de los activos evaluados.
- Se efectuarán pruebas de penetración sobre los activos informáticos, a fin de conocer su estado de seguridad.

2. Solución a debilidades de seguridad.

- Los resultados de las pruebas de penetración serán analizados a fin de establecer planes y programas de solución de las vulnerabilidades que se identifiquen.
- Previo a la instalación de las actualizaciones, el administrador del activo es el que deberá aprobar este proceso en un ambiente estable de prueba o en un conjunto representativo de sistemas o equipos, con el fin de garantizar la compatibilidad y reducir riesgos de afectación de sistemas o servicios.

3.3.6. Gestión de continuidad de negocios.

La finalidad de este control es exigir a las entidades un plan de recuperación de desastres que de alguna manera afecten la operación tecnológica y detenga súbitamente el flujo del negocio.

Políticas/Directrices:

- La continuidad del negocio debe velar por la seguridad que aplica al personal de la organización que es parte de contingencia.
- La dirección de la SCPM se responsabilizará de la gestión de los riesgos que supone la clave para la continuidad operativa de los procesos considerados críticos en la organización.
- Se garantizará que los procesos críticos sean recuperados dentro de los márgenes de tiempo requeridos en los Planes de Continuidad de Negocio.
- Se establece planificación de comunicación al personal interno y externo los mismos que serán auditados en tiempos determinados.
- La activación del Plan de Continuidad debe producirse sólo en situaciones de emergencia o cuando las seguridades hayan fallado.

Procedimientos:

Prevención para la continuidad del negocio.

La prevención a fallos es lo primordial en las entidades, permitiendo así la continuidad de la operación sin afectar el giro del negocio, los procedimientos a seguir son:

1. Seguridad y controles ambientales permitiendo reducir las amenazas internas/externas.
2. Identificar amenazas físicas internas/externas y debilidades existentes en los controles

3. Procedimiento de respuesta de incidentes, donde se especifique las acciones a tomar y tiempos de solución antes estos inconvenientes.
4. Procedimientos de respaldos bien almacenados y en lugares seguros, recomendable tener respaldos: diarios, semanales, mensuales y anuales.

Ejecución para la continuidad de negocio.

1. Verificación de los estados físicos en los equipos, así como también en su software, en caso de requerir cualquier cambio, se lo debe realizar inmediatamente.
2. Se establecerá una fase de recuperación, donde se seleccionarán los métodos operativos alternativos que se van a utilizar en el caso de que ocurra un incidente de seguridad que provoque una interrupción en la organización.
3. Plan de contingencia, debe ser puesto en práctica por lo menos una vez al año. Al realizarse esta actividad se debe desarrollar sugerencias y recomendaciones para reducir la probabilidad de ocurrencia de las amenazas, incluyendo acciones de prevención y corrección.

3.3.7. Control de accesos.

En este dominio consiste en el control de los accesos y activos de información que tiene la SCPM donde se debe tener en cuenta directrices, procedimientos, autorizaciones e instrumentos

Políticas/Directrices:

La directriz de control de accesos deberá tener definido y documentado los requisitos del negocio para el control de accesos, precisando reglas que se debe establecer para los usuarios. Deberá contemplar:

1. Definición de accesos.

2. Requisitos de la implementación de requerimientos de seguridad.
3. Segregación de roles en el control de acceso.
4. Procedimiento de control y la gestión de accesos.
5. Administración de accesos privilegiados de control y/o administración.
6. Periodos de revisión de accesos otorgados a los usuarios normales y terceros.
7. Política para el bloqueo de las máquinas por inactividad.
8. Administración de contraseñas de usuarios
9. Registros de logs de auditoría por aplicación.

Procedimientos:

Se debe definir procedimientos para el derecho de accesos a los activos, los cuales incluirán como mínimo lo siguiente:

1. Procedimiento de identificación y autenticación en sistemas informáticos.

- Establecer lineamientos para la autenticación segura en sistemas informáticos a través de métodos de autenticación fuertes, así también la protección de la confidencialidad.
- Definiciones sobre las cuentas de usuario donde se debe especificar accesos y privilegios para usuarios internos y externos.
- Definición de las contraseñas en los sistemas informáticos donde configuraran los lineamientos de seguridad, de tal forma que las contraseñas mantengan características que las protejan de ser obtenidas, descifradas, deducidas y/o descubiertas por personal ajeno al responsable.

2. Procedimiento de certificación de cuentas de usuario y perfiles.

- Confirmación de que se ha obtenido la autorización de la Gerencia apropiada antes de otorgar el acceso a la información de SCPM.

- Establecer una matriz formal de todos los usuarios a las que se les asigna acceso a los distintos activos de información validando con nómina de la SCPM y validar que no exista usuarios egresados que se encuentren activos o usuarios con privilegios que no están autorizados.

3. Procedimientos de creación y modificación de cuentas de usuarios.

- Registro del otorgamiento de derechos de acceso privilegiados y las acciones que realicen los usuarios con dichos derechos.
- En caso de cambio en el estado laboral de un usuario (por ejemplo, cambio de puesto) se deben revisar y actualizar los privilegios de acceso de dicho usuario.

4. Procedimiento para eliminar y bloquear cuentas de usuarios.

- En caso de desvinculación voluntaria o involuntaria de un usuario, se revocará con anterioridad a la desvinculación efectiva todos los accesos a información y activos de información que el usuario tuviera.
- En caso de reposos o vacaciones se debe establecer lineamientos de bloqueos para que no se compartan las contraseñas

3.3.8. Gestión de comunicaciones y operaciones.

La entidad debe disponer procesos operacionales en los que se pueda definir responsables que controlen cambios y cumplimiento en los procedimientos, contratos a terceros, protección de software, monitoreo, etc. Este control ayudará a las entidades a mantener un buen tratamiento de la información.

Políticas/Directrices:

La directriz de control de cambios debe tener bien definido los siguientes puntos:

- Solicitudes de cambio: Todas las solicitudes de cambio, así como la aprobación y los resultados de las mismas deben encontrarse formalmente documentadas,

además de contener la totalidad de la información solicitada en el proceso de gestión de cambios y entender la necesidad previa a una evaluación de cambios.

- Evaluación del cambio: Para los cambios propuestos, el Comité de Control de Cambios debe efectuar una evaluación de riesgos asociados y acorde a la necesidad identificar el impacto que podría producir el cambio.
- Control de calidad (QA): Los cambios deberán ser probados en un entorno aislado y controlado, antes de la puesta en producción para minimizar el efecto sobre el proceso de negocio relevante.
- Vuelta atrás (Rollback): Para todas las solicitudes de cambio, debe encontrarse definido un procedimiento de vuelta atrás, el cual deberá ser ejecutado en caso que se encuentren errores durante la implementación.
- Implementación: La implementación de los cambios en producción debe ser llevada a cabo sólo en caso de que las pruebas sean exitosas y se cuenten con la aprobación adecuada de las partes interesadas.
- Comunicación de los cambios: Todos los usuarios que puedan ser afectados significativamente por el cambio serán notificados cuando el mismo se encuentre implementado en el entorno productivo.
- Documentación: Debe archivarse la documentación resultante del proceso de gestión de cambios, la cual se encuentra compuesta por lo siguiente:
    - ✓ Solicitud del cambio.
    - ✓ Resultados de la evaluación del cambio.
    - ✓ Documentación de la implementación.

Procedimientos:

Se deberán documentar los procedimientos y hacerlos disponible para todos los usuarios que conforman el área de tecnología. Los procedimientos deberán especificar las instrucciones para la ejecución de las tareas, incluyendo:

1. Procedimiento para la gestión de cambios

- Las solicitudes de un desarrollo de nuevos sistemas informáticos o cambios de alto impacto en los sistemas existentes, deberían ser evaluadas, aprobadas y registrados en la matriz de control de cambios.
- Los procedimientos de recuperación del sistema se deben utilizar en caso de algún fallo del sistema.

2. Procedimiento de respaldos

- Se debe realizar un procedimiento de Backup con las instrucciones necesarias para manejar errores durante alguna ejecución de cambios.

3. Procedimiento para revisión de log

- La administración de auditoría e información de registro del sistema debe estar guardada en un log de auditoria para dar seguimiento cualquier cambio realizado sin autorizado y afecte los sistemas informáticos.

Instrumentos:

- Solicitud de Cambio
- Matriz de control de cambios

3.3.9. Desarrollo y mantenimiento de sistema.

Tiene como finalidad garantizar que la seguridad sea parte integral de los sistemas de información protegiendo la confidencialidad, integridad y disponibilidad de la información, evitando de esta manera la mala manipulación de los sistemas y disminuyendo la posibilidad de errores, pérdidas o modificaciones no autorizadas.

Políticas/Directrices:

- El diseño e implementación deben seguir este procedimiento: Planificación - Declaración de Requisitos - Acuerdo de Desarrollo - Desarrollo - Pruebas - Implementación – Documentación.
- Cada aplicación desarrollada e implementada debe contener sus propios controles, de esta manera se asegura el procesamiento correcto de la información.
- Los sistemas informáticos se deben controlar de la siguiente manera: Datos de entrada - Procesamiento de Datos Internamente- Datos de salida.
- Se debe disponer de controles criptográficos para la transmisión de información entre sistemas o/y terminales

Procedimientos:

1. **Requerimientos o cambios de desarrollo**

Todos los requerimientos de diseño deben ser parte integral de los sistemas de información y tener un orden para la implementación:

- Se deben identificar los requerimientos de desarrollo.
- Entregar al área de desarrollo los requerimientos en el formato propuesto, donde se debe registrar un acuerdo entre las partes solicitantes y desarrolladoras que servirá para la entrega o implementación del sistema.

2. **Implementación de requerimiento de desarrollo**

- Se debe establecer una fase de pruebas para que la parte solicitante valide lo requerido, una vez aprobado se lanza a producción.
- Solo el área de desarrollo dispondrá del control de accesos a los sistemas de ficheros y códigos fuente de los sistemas.

3. **Seguridad de la implementación y medidas de prevención.**

- Los encargados del desarrollo de los aplicativos deben responsabilizarse de la seguridad del proyecto y planes de mejora.
- Se deben identificar las vulnerabilidades que vayan surgiendo con el uso del sistema desarrollado, realizar mejoras y cierres de vulnerabilidades
- El monitoreo y buen funcionamiento del sistema desarrollado está a cargo del área de desarrollo.

Instrumentos:

- Formato Requerimiento funcional – Desarrollo.
- Formato Solicitud de cambios – Desarrollo.

3.3.10. Seguridad física y entorno.

Las áreas físicas de la entidad deben tener una infraestructura acorde a las necesidades de la misma para la protección del procesamiento de la información y teniendo como base los riesgos identificados. La información sensible debe ubicarse en un área protegida por controles de accesos y resguardada de daños e interferencias.

El objetivo principal es no permitir el acceso que no haya sido autorizado previamente a las instalaciones de la organización.

Políticas/Directrices:

- Las áreas accesibles deben estar claramente identificadas para todos los funcionarios de la entidad y personas externas que ingresen a la misma.
- Todos los funcionarios deben disponer de un medio de acceso a las diferentes áreas según sus funciones o responsabilidades, garantizando la seguridad de la información de los departamentos.
- Las áreas deben disponer de un detector de humos y alarmas en caso de intrusos.

Procesos/Procedimientos:

1. **Seguridad del visitante**

- La seguridad física de la entidad debe indicar a los visitantes el área hasta dónde podrán avanzar según la gestión que vayan a realizar, así como también se harán referencia por la buena señalización que debe disponer la entidad en todas sus áreas.
- La seguridad física de la entidad deberá registrar los equipos tecnológicos que ingresen y salgan de la entidad. En caso de que un usuario reporte que va a sacar un equipo, deberá presentar una autorización previa para poder retirar los equipos.
- Debe existir inspecciones periódicas de las instalaciones de la entidad, garantizando la seguridad del visitante.

2. **Seguridad del funcionario**

- El área de Administración encargada de la seguridad y salud ocupacional deberá garantizar el buen entorno para todos los funcionarios para velar por un buen desempeño y la salud de los mismos.

3. **Seguridad tecnológica**

- El personal de TI junto con el departamento de bienes se encargará de recomendar el área adecuada para la ubicación del equipamiento tecnológico, protegiéndolo así de amenazas físicas y ambientales, además de colocar equipos de apoyo para el suministro de energía eléctrica.

Instrumentos:

- Circuito cerrado de video vigilancia que es administrado por Talento Humano y Bienes.
- Control de accesos (Huellas - Tarjetas magnéticas) que es administrado por Talento Humano y Bienes.
- Registro para usuarios visitantes debe hacerlo el área de seguridad física.

- Sistemas de alertas.

3.3.11 Conformidad.

Este control tiene como objetivo garantizar que la entidad no sufra ningún inconveniente legal que pueda afectar su operación a causa de algún tipo de regulación u obligación contractual.

Políticas/Directrices:

- Los requisitos legales de los que debe disponer la entidad deben ser indicados por un departamento legal, propio o externo.
- La imagen de la organización usada en los sistemas de información tiene que estar regularizada por el Instituto Ecuatoriano de la Propiedad Intelectual.
- Las plataformas y sistemas de información deben ser auditadas según las políticas de seguridad elaboradas, controlando que se cumplan con los estándares y controles establecidos. En caso de disponer servicios tercerizados estos deben cumplir con los acuerdos establecidos entre ambas partes.
- Se deben implementar auditorías internas hasta tener controlados los procesos y la seguridad de los sistemas de información, de esta manera la organización estará mejor preparada ante cualquier auditoría externa.

Procedimientos:

1. **Procedimiento de cumplimiento legal**

- Todas las regulaciones y/u obligaciones relevantes y legales deben ser estrictamente definidas, documentadas y actualizadas para cada sistema de información.
- Para el uso de imagen con derechos de propiedad intelectual, se deben establecer los procedimientos adecuados y evitar posibles sanciones legales.

- Otro de los procesos fundamentales es establecer un procedimiento en el cual se garantice el buen manejo y custodia de los documentos legales del negocio.
- Se debe evitar que usuarios no permitidos realicen o utilicen recursos de tratamiento de información para propósitos no autorizados.
- Los directores de cada área o propietarios de la información son responsables de que los procedimientos de seguridad sean cumplidos con los estándares y políticas establecidas, estos mismos deben ser comprobados regularmente por las auditorías internas.
- Las auditorías deben ser planificadas y acordadas con el objetivo de minimizar el riesgo de interrupción del flujo del negocio.
- Las herramientas o materiales que se utilicen para las auditorías deben ser manipulados únicamente por sus responsables y se deberá evitar el acceso o manipulación de otro tipo de usuarios que no dispongan de autorización para manejarlos.

CONCLUSIONES

- Al inicio del proyecto, en el levantamiento de información, se identificó una debilidad muy importante que constaba de no tener formalmente documentados los procedimientos de gestión de seguridad, por lo que no había la certeza de que un control de seguridad se encuentre cien por ciento implementado con los estándares establecidos en la ISO/IEC 27001.
- Durante todo el proceso del levantamiento de información pudo comprobarse que la entidad si tenía una política de seguridad, pero este documento no contaba con una aprobación previa, por lo tanto, la SCPM se vuelve vulnerable por lo que puede haber filtraciones no autorizadas de información de cualquier sistema informático.
- La implementación de un sistema de gestión es muy importante para la SCPM, por lo que toda entidad pública debe cumplir con el acuerdo ministerial 166 donde establece que es importante aportar políticas, procesos y procedimientos que mantenga la seguridad dentro de la entidad.
- A partir de la información levantada, se puede concluir que la SCPM presenta problemas en cuanto a la protección de información en sus departamentos, incumpliendo de esta manera con lo que establece la ISO/IEC 27001:2005.
- El control de seguridad dentro del área tecnológica cumple con los requisitos según las buenas prácticas de seguridad indicadas en la norma, aun así, esto solo se presenta en la práctica porque estas actividades no son controladas ni mucho menos documentados, siendo así una debilidad de seguridad.
- Otros de los resultados posteriores al levantamiento de información es la poca documentación en el desarrollo de software, esto traería consecuencias graves

que podrían llevar a alcanzar un punto crítico que podría desembocar en la paralización de la operación general de la entidad.

- Al realizar el levantamiento de información se observó que las solicitudes de cambios en los sistemas de la entidad no tienen ningún formato o un proceso para realizarlo, ya sea de poca o gran magnitud lo que se va a modificar, siendo una debilidad en la continuidad del negocio.
- El resultado final dispone de una propuesta de mejora de los controles-dominios que se evidenciaron con incumplimientos según lo estipulado en la ISO/IEC 27001:2005, los mismos que pueden ser utilizados para la implementación del sistema de gestión de seguridad de la información (SGSI) si así lo requiere la entidad.
- Para el mejor control de incidentes, se ha entregado a la entidad un formato de indicadores, este formato ofrecerá la posibilidad de disponer de estadísticas mensuales de casos abiertos, tiempo que tardan en ser atendidos, casos terminados y promedio de tiempo de solución; de esta manera podrán establecer acciones en caso de no cumplir con la meta y tolerancia establecida, llamada también “Calidad de los procesos”.
- Para salvaguardar la información es importante que el área de tecnología junto con el oficial de seguridad sea responsable del cumplimiento de la política de seguridad, por lo que es parte de la gestión y la definición de procedimientos, estándares y controles de seguridad.

RECOMENDACIONES

- Para la implementación se recomienda tomar como referencia la ISO/IEC 27003, este estándar es una guía para la implementación de un sistema de gestión de seguridad de la información (SGSI) enfocado en el modelo PDCA plan-do-check-act, y cumplir con un proceso de establecimiento, monitoreo, revisión, mantenimiento y mejorar el sistema; definiendo el alcance y los límites que corresponderá a esta implementación con una debida documentación.
- Se propone a la Superintendencia de Poder de Control de Mercado cumplir con los controles de la ISO 27001:2005 con vistas a cumplir con el acuerdo 166 establecido para las entidades públicas.
- Para el adecuado manejo de la documentación empleada para el desarrollo de software, se deberían establecer los requerimientos en los formatos establecidos en la propuesta (Ver Anexos), para que de esta manera se pueda realizar un mejor seguimiento y entrega de lo solicitado a los usuarios. De igual manera debe documentarse todo lo relacionado al tema.
- Se sugiere controlar el ingreso y salida de equipos tecnológicos por seguridad de la información, así como el uso de dispositivos externos para extraer información confidencial como Pen Drive, Discos Externos, CD, etc.
- Se sugiere a la entidad, crear o establecer protocolos/normas de tratamiento de la información, categorizando por su importancia y criticidad en el giro del negocio. Se hace referencia a la norma DIN 66399, la misma que establece procesos de destrucción de la información certificada.
- Cuando se desee poner en marcha el sistema de gestión de seguridad de la información (SGSI), se deberá cumplir con un proceso de: establecimiento,

monitoreo, revisión, mantenimiento y mejorar el sistema; definiendo el alcance y los límites que corresponderá a esta implementación y con una debida documentación.

- Es importante comprometer a la máxima autoridad y a los miembros que conformen el comité de seguridad para dar seguimiento de la puesta en marcha de la implementación de los controles y procedimientos que tendrán cambios significativos dentro de la organización en la gestión de seguridad.
- Se recomienda establecer auditorías internas cada un periodo de tiempo determinado en la implementación de procesos, procedimientos e instrumentos que ayuden a establecer controles de seguridad en la entidad y que cumplan con la política interna. Una vez controlado internamente se recomienda contratar auditores externos que certifiquen la revisión interna.
- Se sugiere que luego de la implementación del SGSI se disponga un plan de mejora del mismo, sofisticando sus procesos y la estructura en el modo de operación de la entidad.
- Se recomienda que para proteger los activos de información de carácter confidencial los funcionarios deben tener pleno conocimiento de las responsabilidades que adquieren al ingresar a la organización mediante el acuerdo de responsabilidad para el buen uso de los activos de información.

REFERENCIAS

Albacete, J. F. (2014). Gestión de Sistemas Informaticos. En J. F. Albacete, *Gestión de Sistemas Informaticos.* ANTEQUERA, Malaga: Ic Editorial.

Alfaro, J. R. (enero 1997). Elementos metodológicos para planificación estrategica en programas de Educación superiror. En J. R. Anfaro, *Elementos metodológicos para planificación estrategica en programas de Educación superiror.* San Jose, Costa Rica: Serie Publicaciones Micelaneas.

AREITIO J, J. A. (2008). Seguridad de la información. Redes, informática y sistemas de información. En J. A. AREITIO J, *Seguridad de la información. Redes, informática y sistemas de información.* Madrid: Parainfor.

Cañizares, C. M. (s.f.). *Auditoria de Sistemas de Gestión de Seguridad de la información.* Madrid - España: Fundación Confemental.

Carmen de Pablos Heredero, J. J. (2011). *Organización y transformación de los sistemas de información en la empresa.* Madrid, España: ESIC EDITORIAL.

Dirección General de Modernización Administrativa, P. e. (Octubre 2012). Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. En P. e. Dirección General de Modernización Administrativa. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Espinoza, M. B. (02 de 2016). DISEÑO DE UN SGSI BASADO DE LA NORMA ISO27001:2013 PARA LA EMPRESA ECUATRONIX. Quito, Pichincha, Ecuador.

Gestión de Seguridad de la Información ISO/IEC 27001. (s.f.). Recuperado el 2016, de http://www.bsigroup.com/es-MX/seguridad-dela-informacion-ISOIEC-27001/

Gestión de Seguridad ISO 27001. (20 de enero de 2016). Obtenido de cidi.com.ar: http://www.cidi.com.ar/soluciones/iso-27001

Gómez Fernández, L. A. (January 2012). Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. En L. Gómez Fernández. AENOR - Asociación Española de Normalización y Certificación.

Instituto Nacional de Cyberseguridad de España. (2016). *Los Activos de Seguridad de la Información.* https://www.incibe.es/extfrontinteco/img/File/intecocert/sgsi/swf/video_07.swf.

ISO - International Organization for Standardization. (2016). Obtenido de http://www.iso.org/iso/home.html

ISO 27000. (2005). Obtenido de http://www.iso27000.es/iso27000.html

ISO/IEC 27001:2005. (2016). Obtenido de https://mmujica.files.wordpress.com/2007/07/iso-27001-2005-espanol.pdf

ISO/IEC 27002. (2016). Obtenido de http://www.iso27002.es/

Ley Orgánica de Regulación y Control del Poder de Mercado. (2016 de enero de 2016). Obtenido de http://www.scpm.gob.ec/wp-content/uploads/2014/03/LEY-y-RLORCPM-A4.pdf

Norma International ISO 9001:2008. (s.f.). Obtenido de https://www.mct.es/sites/default/files/archivos/ISO-9001.pdf

Norma ISO/IEC 27001:2013. (2016). Obtenido de http://www.pmg-ssi.com/2015/10/claves-norma-iso-27001/

seguridadinformaticaufps.wikispaces.com. (2016). Obtenido de https://seguridadinformaticaufps.wikispaces.com/MAGERIT

Superintendencia de Control del Poder de Mercado. (20 de enero de 2016). Obtenido de http://www.scpm.gob.ec/scpm-espaniol/

The International Organization for Standardization. (s.f.). Obtenido de The International Organization for Standardization: http://www.iso.org/

The International Organization for Standardization. (20 de Febrero de 1997). Obtenido de The International Organization for Standardization: http://www.sis.pitt.edu/mbsclass/standards/martincic/isohistr.html

Toni Granollers i Saltiveri, J. L. (Octubre 20005). Diseño de sistemas interactivos centrados en el usuario. En J. L. Toni Granollers i Saltiveri, *Diseño de sistemas interactivos centrados en el usuario.* Barcelona: U O C.

UNIT. (s.f.). *UNIT-ISO/IEC 27000 Gestión de la Seguridad de la Información*. Obtenido de UNIT-ISO/IEC 27000 Gestión de la Seguridad de la Información: http://www.unit.org.uy/normalizacion/sistema/27000/