DIÁGNÓSTICO DE CUMPLIMIENTO DEL MODELO GESTIONADO POR EL SISTEMA DE ADMINISTRACION DE LA SEGURIDAD DE LA INFORMACION DE GOBIERNO EN LINEA – SASIGEL ALINEADO CON LA NORMA 27000 PARA EL INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL DE LA GUAJIRA

Presentado Por:

ING. ANTONIO RAFAEL GALLO OÑATE

CODIGO. 7603023

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR, CESAR - COLOMBIA
2014

DIÁGNÓSTICO DE CUMPLIMIENTO DEL MODELO GESTIONADO POR EL SISTEMA DE ADMINISTRACION DE LA SEGURIDAD DE LA INFORMACION DE GOBIERNO EN LINEA – SASIGEL ALINEADO CON LA NORMA 27000 PARA EL INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL DE LA GUAJIRA

Presentado Por:

ING. ANTONIO RAFAEL GALLO OÑATE

CODIGO. 7603023

Monografía como Trabajo de Grado presentado ante la Escuela de Ciencias Básicas, Tecnología e ingeniería (ECBTI) como parte de los requisitos para optar al Título Académico de Especialista en Seguridad Informática.

Directora de Proyecto

MSC. LORENA SUAREZ SIERRA

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA (ECBTI)
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
VALLEDUPAR, CESAR - COLOMBIA
2014

Nota de Aceptación:

_____

Firma del Presidente Jurado

_____

Firma del Jurado

_____

Firma del Jurado

Valledupar, 06 de Octubre de 2014

Dedicatoria

Con todo mi cariño y amor a Dios por la fuerza que me brindo para sacar adelante este proyecto de vida, a mi padre que siempre lo recuerdo y llevo en mi corazón, mi madre, esposa e hijas que con su paciencia y apoyo lograron mantenerme motivado, lleno de ánimo y valor para que pudiera lograr este triunfo.

Ahora puedo decir que esta tesis lleva a cada uno de ustedes por estar incondicionalmente siempre a mi lado.

Agradecimientos

A mi directora de proyecto, MSC. Lorena Suarez Sierra, por su acompañamiento, experiencia y observaciones que fortalecieron mi proceso de aprendizaje.

A la Universidad Nacional Abierta y a Distancia UNAD, por brindarme la oportunidad de prepararme como Especialista en Seguridad informática.

Son muchas las personas que con sus consejos, apoyo, animo y compañía en los momentos difíciles mantuvieron siempre la comprensión y oraciones puestas en mí.

Para todos, Muchas gracias y que Dios los bendiga.

CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

RESUMEN

Dentro de la presente monografía se determina cual es el nivel de madurez del Sistema de Gestión de Seguridad de la Información del Instituto Nacional de Formación Técnica Profesional "INFOTEP" de La Guajira aplicando el Sistema de Administración de la Seguridad de la Información de Gobierno en Línea que toma como base metodológica el ciclo de Demming o ciclo de mejora PDCA.
Es importante reconocer

Inicialmente se contextualiza ampliamente sobre la de Seguridad de la Información, el Sistema Administrativo de Seguridad de la Información y algunos conceptos básicos de los estándares ISO/IEC 27000, posteriormente se relaciona como las organizaciones deben identificar los prerrequisitos, requisitos para poder lograr la Implementación del SGSI bajo el modelo SASIGEL para finalmente realizar la verificación sobre el nivel de madurez con que cuenta el INFOTEP.

ABSTRACT

In this paper determines what level of maturity of the Management System of Information Security, National Institute of Technical Vocational "INFOTEP" La Guajira using the System Management Information Security Government Online taking as a methodological basis Demming cycle or PDCA improvement cycle.

Initially it was widely contextualized on the Security of Information, the Administrative System Information Security and some basic concepts of ISO / IEC 27000 standards, then relates how organizations should identify prerequisites, requirements to achieve Implementation ISMS under SASIGEL model to finally perform verification on the level of maturity that has INFOTEP.

INTRODUCCIÓN

Es necesario reconocer la importancia que tiene la implementación del Sistema de Gestión de Seguridad de la Información **(SGSI)** dentro de las entidades, este proceso hace necesaria la identificación del recurso humano, financiero y tecnológico los cuales son el insumo clave para la preparación y puesta en marcha de dicho sistema.

SASIGEL es un modelo sostenible, surge por el interés del Gobierno Colombiano para tomar acciones estratégicas y definir los lineamientos que permitan la implementación, seguimiento y mantenimiento del Modelo de Seguridad de la Información los cuales son necesarios para fortalecer la adecuada gestión de la seguridad de la información dentro de las Organizaciones.

Lo que se pretende por medio del presente documento es identificar los parámetros que establece el Sistema de Administración de la Seguridad de la Información de Gobierno en Línea **(SASIGEL)** y abordar algunos aspectos que servirán como base para lograr la verificación sobre el Nivel de madurez del Instituto Nacional de Formación Técnica Profesional con respecto a la implementación del modelo SASIGEL

El SGSI incluye los sistemas de información los cuales se han convertido en un elemento esencial para la supervivencia de toda empresa, el éxito de dicha supervivencia depende directamente de las buenas prácticas y la evolución constante de los procesos, minimizando los posibles riesgos y aumentando la calidad y confianza de los sistemas de información por lo cual el SASIGEL se convierte en una buena elección para la implementación del SGSI, a través del conjunto de lineamientos, políticas, normas y procesos que lo componen.

La función o necesidad de aplicar el SASIGEL va enfocado a coordinar las actividades que se encuentran relacionadas con la ejecución, formulación, seguimiento y mantenimiento de las políticas y lineamientos del modelo los cuales son necesarios para fortalecer la adecuada gestión de seguridad de la información en las entidades públicas de Colombia o empresas privadas que desean adoptar este Modelo.

El desarrollo de la presente monografía comienza con la definición de Seguridad de la Información, el Sistema Administrativo de Seguridad de la Información y algunos conceptos básicos de los estándares ISO/IEC 27000, posteriormente se relaciona como las organizaciones deben identificar los prerrequisitos, requisitos para poder lograr la Implementación del SGSI bajo el modelo SASIGEL para finalmente realizar la verificación sobre el nivel de madurez con que cuenta el instituto nacional de Formación Técnica Profesional de La Guajira.

DEFINICION DEL PROBLEMA

La mayoría de las Organizaciones no cuentan con un Sistema de Gestión de Seguridad de la información establecido, se genera una gran necesidad en cuanto a su implementación que resulta ante la constante fuga de información y por el avance mismo de las nuevas tecnologías de la información y las comunicaciones. Por medio del modelo SASIGEL se pueden establecer parámetros y mecanismos para estructurar y garantizar que los riesgos de la seguridad de la información sean minimizados por nuestra empresa de manera oportuna.

Existen dos aspectos relevantes a tener en cuenta dentro del modelo SASIGEL, el primero que hace referencia a su conocimiento por parte de las entidades que resulta de la escasa divulgación. El segundo aspecto se refiere a su estructura, ya que se muestra de manera dispersa, por lo cual surge el interés de ampliar algunos conceptos que la componen y presentarla dentro del presente documento para su fácil adaptación dentro de las organizaciones.

El Gobierno Nacional a través de su leyes está obligando a las entidades a cumplir con estrategias como la de Gobierno en Línea (GEL) (Decreto 1151 de 14 de Abril de 2008), el cual dentro de manual de implementación en su versión actual (3.1), relaciona dentro de las herramientas para los lineamientos de la arquitectura, el modelo de Seguridad de la Información que tiene inmerso el Sistema de Administración de Seguridad de la Información de Gobierno en Línea (SASIGEL).

El Archivo General de la Nación quiere también hacer cumplir la ley 527 de 1999, es decir darle validez a los documentos electrónicos, pero esta validez esta soportada en unos controles de seguridad informática que permitan establecer quién es el iniciador de una transacción o quien participa en una comunicación que sea efectivamente quien dice ser, o no se niegue cuando reciba una notificación.

La complejidad de este panorama nos enfrenta a un momento en la gestión de la información en donde se hace necesario desarrollar un sistema de gestión de seguridad de la información, que cumpla con las normativas nacionales; sin olvidar que ya desde hace unos años se habla de protección datos (ley 1273 de 2009) y de las penas por los daños y uso no autorizado de la información.

Las entidades del estado Colombiano deben apuntar sus esfuerzos económicos y de personal en desarrollar una estrategia de seguridad basándose en las mejores prácticas de aseguramiento de la información expuesta en la norma internacional ISO/IEC 27001, la cual se sincroniza con el modelo SASIGEL el cual plantea el estado colombiano.

Considerando aquellas entidades que no cuentan con información clara sobre cómo crear una estrategia de seguridad, cómo definir sus políticas, cuáles son los recursos que se deben proteger, qué procedimientos se debe tener en la entidad para cumplir los objetivos de seguridad, qué personas están involucradas en el establecimiento de dichas políticas y quiénes deben velar por hacerlas cumplir; se hace importante la apropiación de conocimiento en el modelo SASIGEL que se presenta en esta monografía.

En base a este contexto, en el caso de la empresa que nos ocupa, que es, el Instituto Nacional de Formación Técnica Profesional se pretende determinar en qué nivel de madurez del Sistema de Gestión de Seguridad de la Información con respecto al modelo SASIGEL.

FORMULACIÓN DEL PROBLEMA

Por consiguiente, la pregunta a la cual se busca dar respuesta por medio del presente estudio es la siguiente:

¿La aplicación del modelo SASIGEL alineado con la norma ISO 27000 permitirá hacer el diagnóstico de cumplimiento y establecer el nivel de madurez en que se encuentra el Instituto Nacional de formación Técnica Profesional de la Guajira con respecto al Sistema de Gestión de seguridad de la Información SGSI?

JUSTIFICACIÓN

Es de gran importancia reconocer que la implementación del sistema de Gestión de Seguridad de la Información "SGSI" es de carácter obligatorio en las entidades públicas y el estado Colombiano por medio del programa de Gobierno en Línea creó este modelo sostenible que cubre acciones estratégicas para definir los lineamientos que permitan la implementación, seguimiento y mantenimiento del SGSI.

El SGSI empleando el modelo "SASIGEL" aporta un gran beneficio tanto en las entidades públicas como las privadas generando en estas últimas un valor agregado que es la aplicación de modelos establecidos por el estado Colombiano, además de esto, permiten una implementación sencilla ya que el modelo tiene establecido algunos formatos para su aplicación desde el proceso de recolección de información donde se establecen los prerrequisitos, hasta los niveles de seguridad de la entidad, implementación de controles, políticas y métricas entre otras.

La Constitución Nacional nos habla de la obligación de permitir el acceso a la información que es pública, pero también de proteger la información cuando tiene alguna reserva legal.

Para las empresas privadas existe la obligación de mantener el secreto industrial para todas las personas físicas o jurídicas, organismos o instituciones de cualquier naturaleza que intervengan en cualquiera de las fases del proceso de producción. Esto significa que igual para todas las empresas independientemente de si son de naturaleza pública o privada, en el desarrollo y funcionamiento de sus servicios, la información es un activo que tiene un alto valor.

La actividad institucional debe por tanto, salvaguardar también las previsiones del Habeas Data en cuanto afecta, también, a datos personales protegidos, así, el responsable del archivo y, en su caso, el encargado de su tratamiento deberán adoptar las medidas de índole técnica y organizativas necesarias para garantizar la seguridad de los datos de carácter personal y evitar su alteración, pérdida, tratamiento o acceso no autorizado.

Por tanto, ante este contexto legal que regula la actividad misional aparecen requisitos que obligan de alguna manera a velar por la seguridad de la información en todas las fases de su tratamiento. Ello consiste, básicamente, en garantizar la confidencialidad, integridad y

disponibilidad de la información que deben manejar las organizaciones, teniendo en cuenta para ello todos los aspectos lógicos, físicos, legales y organizativos implicados. Para poder satisfacer estos requisitos y dentro de los planes de las entidades que adopten el modelo en materia de seguridad de la información, la responsabilidad y el apoyo sostenido debe realizarlo la alta dirección de las entidades las cuales deben abordar el problema de la "gestión" de la seguridad de la información.

La seguridad no es un producto: es un proceso. Un proceso continuo que debe ser controlado, gestionado y monitorizado. Dicha gestión no sería posible sin una herramienta básica, el Sistema de Gestión de la Seguridad de la Información, que comprende todos los procesos, procedimientos y recursos necesarios para mantener la seguridad de la entidad en unos adecuados niveles de eficiencia.

Las entidades para lograr el cumplimiento de las obligaciones antes citadas, debe adoptar una estrategia basada en la prevención, detección y reacción ante cualquiera de las amenazas que afecten a los datos cuya custodia ostenta.

Es necesario establecer con la alta dirección el compromiso que se tiene con el cumplimiento y preparación de los prerrequisitos para iniciar la implementación del SGSI, establecer las directrices para la gestión de la seguridad y finalmente obtener el más alto nivel de garantía en el tratamiento y custodia de la información.

Para conseguir las metas, se deben identificar y evaluar permanentemente los riesgos que amenazan los sistemas de información, se debe planificar el control y la reducción de aquéllos cuando sea posible al igual que su seguimiento continuo en el resto de los casos.

Fundamentados en la necesidad de garantizar la integridad, coherencia, confiabilidad de la información y los servicios que se realicen a través de los medios electrónicos como se estipula en los elementos de Gobierno en Línea, es importante que las entidades implementen un sistema de gestión de seguridad que logre el aseguramiento de todas las tareas que se llevan a cabo dentro de las mismas, tomar todas las precauciones para lograr la reducción en cuanto a los incidentes. En relación a esta necesidad, se hace necesaria la adopción de un modelo alineado con esta estrategia como lo es SASIGEL, el cual se basa en procesos, orientado hacia todas las entidades

y recurso humano involucrado, convirtiéndose de esta manera en una pieza fundamental para la identificación de las amenazas y riesgos apoyándonos en procesos de presentación de informes, auditorías, investigaciones, acciones correctivas, preventivas y de mejora.

Es necesario reconocer que dentro de los elementos transversales del Manual actual de Gobierno en Línea 3.1 en su actividad 4, se encuentra la implementación del SGSI tanto en los procesos misionales como los de apoyo que permita manejar los riesgos de las entidades del Estado Colombiano y los privados que ejercen funciones públicas, por ende el gobierno propone el modelo SASIGEL que dentro de la presente monografía ampliamente se contextualiza.

Finalmente se realiza un diagnostico para establecer el nivel de madurez del Instituto Nacional de Formación Técnica Profesional (INFOTEP) con respecto al Sistema de Gestión de Seguridad de la Información - SGSI, empleando el Sistema de Administración de la Seguridad de la Información de Gobierno en Línea - SASIGEL lo cual permitirá que el INFOTEP conozca el estado de su Sistema de Seguridad actual y basado bajo este modelo propuesto por el estado colombiano.

1. OBJETIVOS

1.1. OBJETIVO GENERAL

Diagnosticar el nivel de madurez del Instituto Nacional de Formación Técnica Profesional (INFOTEP) con respecto al Sistema de Gestión de Seguridad de la Información - SGSI, aplicando el modelo Sistema de Administración de la Seguridad de la Información de Gobierno en Línea - SASIGEL.

1.2. OBJETIVOS ESPECIFICOS

- ✓ Revisar el estado del arte de la norma ISO 27001 y del modelo SASIGEL para determinar las variables y la escala de madurez que serán aplicadas para realizar el diagnóstico

- ✓ Establecer los parámetros y seleccionar los criterios a evaluar y diseñar las listas de chequeo para verificar el cumplimiento de cada uno de ellos.

- ✓ Aplicar las listas de chequeo para determinar el nivel de cumplimiento y medirlo en la escala de madurez del modelo SASIGEL

- ✓ Determinar el nivel de madurez en la escala de madurez de SASIGEL y del SGSI.

- ✓ Hacer el análisis y discusión de resultados obtenidos para establecer planes de mejora.

2. ANTECEDENTES

Se revisaron diversas fuentes referentes a la implementación del Sistema Administrativo de Seguridad de la Información para Gobierno en línea – SASIGEL y se encontró que no hay estudios ni investigaciones al respecto en lo nacional e internacional diferentes al propuesto por el ministerio de las tecnologías de la Información y las comunicaciones.

SASIGEL es un modelo para **Estrategia de Gobierno en línea** "GEL", hace parte de las cinco políticas que se deberá implementar como una herramienta dinamizadora en lo relacionado con el uso de los medios electrónicos y, en general, de tecnologías de información y comunicaciones, siguiendo los lineamientos definidos por el Ministerio de Tecnologías de Información y Comunicaciones[1].

Un Sistema de Gestión de Seguridad de la Información (**SGSI**) es un enfoque sistemático para la gestión de la información confidencial de la empresa para que siga siendo segura. Abarca personas. Procesos y sistemas de Tecnologías de la Información.

El trabajo de Heredero, López, Agius, Romo, Medina, Montero, Nájera (2006) acerca de la dirección y gestión de los sistemas de información en la empresa al igual que el trabajo de Merino y Cañizales (2011) sobre la Implantación de sistemas de gestión de seguridad de la información, permitieron establecer que el apoyo prestado por la dirección, el personal asignado, la formación y al igual que las herramientas disponibles dentro de la organización son aspectos muy relevantes y necesarios para la implementación del SGSI.

Dentro de las investigaciones realizadas en el año 2006 Carlos Manuel Fernández Sánchez diseña y desarrolla un modelo de gobierno y gestión de las normas ISO, racionalizando y simplificando el entramado normativo y su aplicación. Desde su creación, hasta el 2012, realizaron distintos pilotos de implantación y certificación en grandes corporaciones y pymes, tanto en España y Europa como en Latinoamérica, llegando a alcanzar casi un total de quinientas empresas y entidades certificadas en algún sistema del modelo, con el objetivo de alcanzar la

[1] Tomado del Metodología para la implementación del Modelo Integrado de Planeación y Gestión, elaborado en Diciembre de 2012.

calidad y seguridad de los servicios de tecnología de la información, y la madurez del ciclo de ingeniería del software.

En el 2012 como respuestas a las investigaciones de Fernández Sánchez resulto en conjunto con Mario Piattini un modelo para el gobierno de las TIC basado en las normas ISO. La obra ofrece una panorámica de la normalización que abordan el área del gobierno y la gestión de la Seguridad de la Información basados en experiencias.

En el año 2011 el Ministerio de Tecnologías de la Información y las Comunicaciones por medio de la Estrategia Gobierno en línea, promueven la construcción de un Estado más eficiente, transparente y participativo, y que a su vez, preste mejores servicios con la colaboración de toda la sociedad mediante el aprovechamiento de la tecnología. Lo anterior con el fin de impulsar la competitividad y el mejoramiento de la calidad de vida para la prosperidad de todos los colombianos[2].

En el año 2012 Luis Gómez Fernández y Ana Andrés Álvarez crean una guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes, cuyo objetivo es facilitar la comprensión de los diversos conceptos involucrados en un sistema de gestión normalizado y contemplar las recomendaciones generales para la implementación de un SGSI en una pequeña empresa, utilizando la Norma UNE-ISO/IEC 27001. También dentro de la misma ofrecen una visión general de cómo hacerlo en el caso de utilizar el modelo del Esquema Nacional de Seguridad que es de carácter obligatorio por ley en España, para la protección de los sistemas que soportan la administración electrónica.

Dentro de los lineamientos en la actualidad para la implementación de la Estrategia Gobierno en línea brindan como apoyo el Sistema de Administración de Seguridad de la Información de Gobierno en Línea (SASIGEL) el cual cubre desde la preparación de la entidad para comenzar la implementación del Modelo, la definición de las brechas, la alineación y la implementación del Sistema de Gestión de Seguridad de la Información.

[2] 2014 Que es Gobierno en Línea Recuperado de: http://vive.gobiernoenlinea.gov.co/

3. MARCO CONCEPTUAL

SASIGEL, es un modelo creado y promovido por el Gobierno Nacional para la alineación e implementación de un proyecto de Gestión de la Seguridad de la Información planteado bajo el modelo Demming o ciclo de mejora y el estándar ISO, que igualmente lo adopta en el estándar ISO 27001 para el SGSI y en la ISO 9001 para el Sistema de Gestión de Calidad, el cual también promovido en el gobierno para su implementación dentro de las Organizaciones pero dentro de la presente monografía no pretende ampliar sobre lo que propone el modelo ISO .

La razón más importante para realizar la implementación del sistema de gestión de seguridad de la Información **(SGSI),** es lograr el aseguramiento de todas las tares que se llevan a cabo dentro de las organizaciones, tomar todas las precauciones para lograr la reducción en cuanto a los incidentes. Reconocer que la implementación del Sistema de Gestión de Seguridad se convertirá en pieza fundamental para la identificación de las amenazas y riesgos entre otros basándonos o apoyándonos en procesos de presentación de informes, auditorías, investigaciones, acciones correctivas, preventivas y de mejora.

Para la identificación del nivel de madurez de las organizaciones SASIGEL se apoya en la **ISO 27001** ya que por medio de este estándar se puede determinar el progreso de la implementación de controles en términos de políticas y métricas. La ISO 27001, se ha convertido en la principal norma a nivel mundial motivo por el cual es utilizado por otros modelos como referencia.

Posterior a la identificación o selección de controles mencionados anteriormente SASIGEL durante la segunda fase permite la implementación de controles apoyados en la **ISO 27002,** ya que este modelo ofrece las directrices al igual que los principios generales los cuales son necesarios para iniciar, implementar, mantener y mejorar la gestión de seguridad de la información como lo son; el apoyo y compromiso por parte de la alta dirección, formación, sensibilización y Revisión (Auditorias) del SGSI.

La identificación del nivel de madurez de las entidades es importante y necesario a la hora de implementar un **SGSI** aplicando el modelo **SASIGEL** ya que esto determinara en que etapa o nivel se encuentra la organización, de igual manera permite establecer las falencias o vacios actuales y poder de esta manera llevar a la entidad a un nivel de madurez de mejoramiento permanente en seguridad.

Para la implementación del SGSI por medio de SASIGEL se requiere inicialmente la preparación y el análisis de la situación actual y la definición de brechas ***"establecer el nivel de madurez"*** de la entidad y de esta manera iniciar el ciclo **PHVA** en donde ***Planear***; es establecer el SGSI, ***Hacer;*** es implementar y utilizar el SGSI, ***Verificar***; es monitorear y revisar el SGSI, ***Actuar;*** mantener y mejorar el SGSI.

Dicho nivel de madurez propuesto por **SASIGEL** se compone de cuatro niveles que se describen de la siguiente manera:

Nivel Inicial **-** Por medio del cual la entidad debe definir una política de seguridad que garantice la protección de la información, los datos personales y los activos de información con que cuenta.

Nivel básico **-** Con base en el análisis de procesos realizado en el nivel inicial y la política o plan de seguridad definido, la entidad inicia la ejecución de dicho plan de seguridad para implementar los controles que mitigarán los riesgos identificados, lo cual implica que la entidad presenta avances en la implementación de tales controles.

Nivel avanzado **-** La entidad documenta la totalidad de políticas y procedimientos de seguridad, ejecuta las actividades de capacitación en temas de seguridad, con todos los servidores públicos, define el plan de verificación periódica de los controles, procedimientos y políticas de seguridad y reporta los avances del cumplimiento del plan**.**

Mejoramiento permanente **-** La entidad refuerza la divulgación de las políticas de seguridad, ejecuta los procedimientos y políticas de seguridad, de manera repetitiva, realiza la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles para finalmente evaluar sus políticas de seguridad e implementa acciones para mejorarlas.

4. MARCO TEORICO

El marco teórico que fundamenta la presente monografía permitirá al lector una idea más clara acerca de los conceptos básicos, específicos y complementarios que comprenden Sistema de Administración de la Seguridad de la Información de Gobierno en Línea.

Las personas y entidades buscan implementar o mejorar sus sistemas de Gestión de seguridad de la información. El SASIGEL es un sistema que merece sea tomado en cuanta porque brinda los elementos necesarios para definir los lineamientos que permiten la implementación del SGSI, tomar acciones estratégicas al igual que el seguimiento y mantenimiento del mismo.

4.1 LA SEGURIDAD DE LA INFORMACIÓN

La información representa valor para las empresas; por lo tanto es un activo ya que es un conjunto de datos, es esencial para el negocio de una organización, y en consecuencia es necesario asegurar su protección.

La seguridad de la Información trata por tanto de proteger activos, tanto tangibles, como por ejemplo un disco duro o una base de datos con la información de clientes, como intangibles, como por ejemplo la reputación, la privacidad o el nombre de marca[3].

Como resultado del crecimiento tecnológico y la globalización, la información ahora está expuesta a un número cada vez mayor y una variedad más amplia de amenazas y vulnerabilidades. La información puede existir en muchas formas: puede estar impresa o escrita en un papel, almacenada en magnético, enviada por correo o utilizando medios electrónicos, videos o grabaciones de voz. Sin importar la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debe estar protegida.

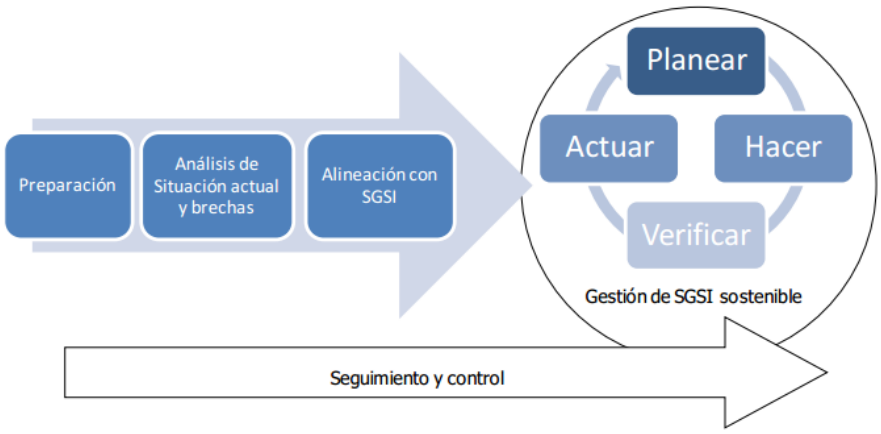
Tomando como base la información es fundamental definir las características de los tres pilares que la conforman de la siguiente manera:

[3] Álvarez Marañón, Gonzalo, Pérez García, Pedro Pablo. Seguridad informática para empresas y particulares. España: McGraw-Hill España, 2004.

- ✓ ***La integridad*** **-** Es la capacidad por medio de la cual la información y sus métodos de procesamiento tienden a permanecer constantemente exactos y completos.
- ✓ ***La confidencialidad*** **-** Por medio de esta propiedad, se permite que la información siempre sea accesible sólo a aquellas personas que se les autorice.
- ✓ ***La disponibilidad*** **-** Permite que la información y los servicios estén disponibles cuando se les requiera.

El estado Colombiano en su impulso por promover mejores prácticas en cuanto al SGSI, por medio de la estrategia de Gobierno en línea que es liderada por el ministerio de Tecnologías de la información y las comunicaciones (MINTIC), ha creado unos elementos normativos, técnicos y de política pública con la finalidad de prestar mejores servicios por medio del aprovechamiento de la tecnología. Uno de estos elementos es el manual GEL 3.1 que determina los lineamientos que deben seguir las entidades públicas y los particulares que desempeñan funciones administrativas por medio de la ejecución de cuatro etapas como se muestra en la figura. 1.

Figura 1. Plan de Implementación Modelo de Seguridad de información GEL



Fuente: Centro de Investigación de Telecomunicaciones. 2011. Modelo de seguridad de la información para la estrategia de Gobierno en Línea 2.0.

4.2. FAMILIA DE ESTÁNDARES DE SEGURIDAD DE LA INFORMACIÓN ISO 27000

La serie de normas ISO/IEC 27000 son estándares los cuales publico la International Organization for Standardization - ISO e International Electrotechnical Commission – IEC, donde se proporcionan los lineamientos para la gestión de la seguridad de la información en cualquier empresa; ISO ha reservado la serie de numeración 27000 para las normas relacionadas con sistemas de gestión de seguridad de la información. En el 2005 incluyó en ella la primera de la serie (ISO 27001), las demás son:

- ISO27000 (términos y definiciones),
- ISO27002 (objetivos de control y controles),
- ISO27003 (guía de implantación de un SGSI),
- ISO27004 (métricas y técnicas de medida de la efectividad de un SGSI),
- ISO27005 (guía para la gestión del riesgo de seguridad de la información) y
- ISO27006 (proceso de acreditación de entidades de certificación y el registro de SGSI).

Para efectos se definen a continuación tres normas que son esenciales dentro de todo SGSI, pero no son objeto de estudio de la presente monografía.

4.2.1. ISO 27001: Es la norma principal, la base de la serie la cual contiene los requisitos del SGSI por la cual las organizaciones se certifican por auditores externos de las mismas. Este es un estándar Internacional el cual específica los requerimientos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar continuamente un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Específica los requerimientos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella[4].

Esta norma es reconocida internacionalmente la cual permite a las organizaciones gestionar sus activos de información de una manera organizada y a su vez permite proteger los sistemas contra el fraude informático, ataque cibernético, sabotaje y los virus. Las infracciones en seguridad de la información permiten que la información de vital importancia sea susceptible al

[4] ISO 27001:2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos.

robo, daño o perdido y como esta resulta un interrogante… ¿Qué tan seguro está usted de que cuenta con los controles y procedimientos adecuados para evitar este tipo de incidentes?

La ISO 27001 (anteriormente conocida como BS 7799) se basa en el ciclo *"Plan - Hacer - Verificar - Actuar"*, por lo cual es un modelo en común con la ISO 9001 e ISO 14001, se utiliza para la identificación, análisis, evaluación y gestión de los riesgos en pro del aseguramiento de los pilares de la información; confidencialidad, integridad y disponibilidad.

Cada vez más, los clientes querrán saber qué tan seguros son los sistemas de tecnologías de la información y las comunicaciones con quienes tienen relaciones, por lo cual mas empresas ahora ven la certificación ISO 27001 como un requisito previo para hacer negocios. Convertirse en ISO 27001 asegurará a los interesados o clientes que la organización toma sus obligaciones en serio.

Lo que la norma pretende es que exista un sistema documentado (política, análisis de riesgos, procedimientos, etc.), donde la dirección colabore activamente y se implique en el desarrollo y gestión del sistema.

Se controlará el funcionamiento del sistema para que marche correctamente y la mejora sea continua, practicándose auditorías internas y revisiones del sistema para verificar que se están obteniendo los resultados esperados, igualmente se activarán acciones encaminadas a solucionar los problemas detectados en las actividades de comprobación (auditorías y revisiones), a prevenir problemas y a mejorar aquellos asuntos que sean susceptibles[5].
Puede consultar la historia de ISO27001 en el siguiente link: http://www.iso27000.es/download/HistoriaISO27001.pps

4.2.2. ISO 27002: Desde el 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Esta es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable. La norma ISO 27001 contiene un anexo que resume los controles de ISO 27002:2005 (Anexo 2). Esta norma es la mejor práctica que da a los responsables los

[5] Gómez Fernández, Luis, Andrés Álvarez, Ana. 2012. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España: ENOR - Asociación Española de Normalización y Certificación.

elementos necesarios para gestionar la seguridad de la información, las pautas para estructurar el plan y los objetivos de control, controles necesarios para implementar la seguridad y acciones fundamentales para minimizar los riesgos que la vulneren[6].

Dentro del contenido de la ISO 27002 se observa que las secciones de su contenido son:

- Estructura
- Política de Seguridad
- Organización de la Seguridad de la Información
- Recursos de la Seguridad Humana
- Gestión de activos
- Control de Acceso
- Criptografía
- Física y Seguridad Ambiental
- Operaciones de seguridad
- Seguridad en las Comunicaciones
- Sistemas de Información de Adquisición, desarrollo, mantenimiento
- Relaciones con los proveedores
- Gestión de la información a Incidentes de Seguridad
- Aspectos de Seguridad de Información de la Continuidad del Negocio
- Cumplimiento

Lo que esta ISO proporciona es un conjunto de prácticas la cual tiene como objetivo principal proveer una guía para la implementación de los controles del Sistema de Gestión de Seguridad de la Información que propone la ISO 27001.

4.2.3. ISO 27005: Fue publicada el 4 de Junio de 2008. Proporciona las directrices para la gestión del riesgo en la seguridad de la información. No es certificable[7]. Esta permite apoyar

[6] Toro, M. 2011. Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28.

[7] Escrivá Gascó, Gema, Romero Serrano, Rosa María, Ramada, David Jorge. Seguridad informática. España: Macmillan Iberia, S.A., 2013. ProQuest ebrary. P 210.

los conceptos generales especificados en la norma ISO/IEC 27001 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Esta norma apoya el desarrollo de uno de los requisitos base para la implementación de la ISO 27001:2005 y el cumplimiento de otros como es la "valoración de los riesgos" que incluye la identificación, análisis, evaluación y tratamiento de los riesgos en la seguridad de la información. Adicionalmente brinda soporte y conceptos generales que se especifican en la 27001, y está diseñada con el objetivo de facilitar la implementación de la seguridad de la información, con base en el enfoque de gestión de riesgo8.

La norma ISO 27005 tiene como ventaja principal su aplicabilidad dentro de cualquier tipo de entidad teniendo en cuenta ciertos factores como lo son el alcance real del Sistema de Gestión de Seguridad de la Información y el tipo de sector (comerciales - industriales) - (Publico - Privado).

Esta norma utiliza los conceptos comunes la ISO27001 e ISO27002. El uso de este estándar con los otros de la familia ISO / IEC 27000 proporciona un marco eficaz para la gestión de seguridad de la información.

4.3. CICLO PHVA

Llamado ciclo Demming o de mejora continua, el cual permite gestionar y establecer el SGSI y que en base al modelo SASIGEL encontramos las respectivas etapas de la siguiente manera:

- **Planear (Nivel inicial de madurez)**

  Obtener soporte de la dirección de la entidad, Identificar legislación y normatividad aplicable, Definir el alcance del SGSI, Definir la política de la seguridad de la información, Análisis del riesgo, Definir la aproximación para la gestión del riesgo, Identificación de activos, Identificar los riesgos, Analizar el riesgo, Enumerar las opciones para el tratamiento/reducción del riesgo, Plan de tratamiento del riesgo y Generar la declaración de aplicabilidad.

[8] Moreno, F. 2009. La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. ICONTEC. Cuarta edición. P 28 – 32.

- **Hacer (Nivel básico de madurez)**

  Implementar el plan de tratamiento del riesgo, Documentar los controles del SGSI, Implementar políticas y controles de seguridad de la fase de planeación, Implementar los planes de concientización y entrenamiento, Establecer y gestionar la operación del SGSI y sus recursos e Implementar la infraestructura de repuesta a incidentes.

- **Verificar (Nivel avanzado de madurez)**

  Revisiones regulares de eficacia, Revisar el nivel del riesgo residual, Realizar auditorías internas, Revisión de la dirección del SGSI y Registro del impacto en el SGSI.

- **Actuar (Nivel de madurez de mejora continua)**

  Implementar las mejoras identificadas y aprobadas al SGSI en un nuevo ciclo, Tomar medidas preventivas y correctivas, Aplicar las lecciones aprendidas, Comunicar los resultados, Realizar un proceso continuo y Gestión auto sostenible del modelo.

4.4. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN "SGSI"

El SGSI es un conjunto de elementos y controles que deben cumplir con un objetivo, dicho objetivo es, la seguridad de la información y la cual debe apuntar siempre a mantener el equilibrio de los tres pilares que son; la confiabilidad, Integridad y disponibilidad de la información, así como de los sistemas implicados en su tratamiento, dentro de una organización.

4.5. MODELO DE SEGURIDAD DE LA INFORMACION EN LAS ENTIDADES DEL ESTADO

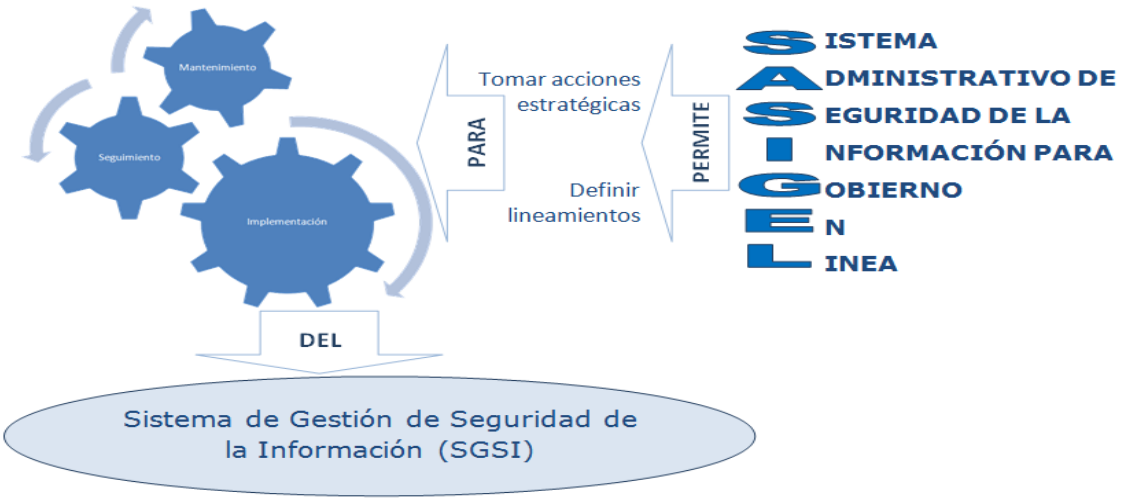
El Modelo de Seguridad de la Información para las entidades del Estado, se apoya en la creación del Sistema Administrativo de Seguridad de la Información para Gobierno en línea– SASIGEL y en la conformación de la Comisión de Seguridad de la Información para Gobierno en línea, para tomar acciones estratégicas y definir los lineamientos que permitan la implementación, seguimiento y mantenimiento del Modelo de Seguridad de la Información en

cada una de las entidades públicas de orden nacional y territorial y en las entidades privadas que sean proveedoras de los servicios de Gobierno en línea.

Gracias a mecanismos normativos que se están diseñando y parametrizando actualmente, se podrán sentar las herramientas para la creación del Sistema Administrativo de Seguridad de la Información para Gobierno en línea, lo cual constituye un paso muy importante hacia adelante para el cumplimiento de los principios definidos en la Ley 1341 de 2009 y en la Estrategia de Gobierno en línea, que corresponden a la protección de la información del individuo y la credibilidad y confianza en el Gobierno en línea.

En particular, para lograr el cumplimiento de estos principios, se requiere que tanto los servicios de Gobierno en línea como la Intranet Gubernamental y las entidades que participen en la cadena de prestación de los servicios de Gobierno en línea, cumplan con los tres elementos fundamentales o pilares de la seguridad de la información: disponibilidad de la información y los servicios, integridad de la información y los datos y confidencialidad de la información. Para la correcta administración de la seguridad de la información, se deben establecer y mantener programas y mecanismos que busquen cumplir con los tres requerimientos mencionados.

Figura 2. Integración de SASIGEL sobre el SGSI



Fuente: Autor.

Es así, como se confirma la sugerencia sobre la creación del Sistema Administrativo de Seguridad de la Información para Gobierno en línea (SASIGEL), cuyo eje central es la Comisión

de Seguridad de la Información para Gobierno en línea (CSIGEL). El SASIGEL surge, entonces, como el conjunto de todos los actores (públicos, privados y de la sociedad civil) que afectan la seguridad de la información nacional. Así mismo, incorpora el conjunto de las reglas de juego que rigen las interacciones entre todos estos actores. Dentro de la implementación del Modelo SASIGEL se deben tener en cuenta ciertas etapas las cuales son:

1.- Etapa de Preparación:

Es necesario Involucrar y sensibilizar a la alta dirección. Revisar con la alta dirección y acordar el compromiso con el cumplimiento y preparación de los prerrequisitos para iniciar la implementación del SGSI, y así mismo de los requisitos los cuales la entidad debe cumplir.

Identificación de los responsables - Es importante que las responsabilidades asignadas se encuentren plasmadas de manera organizada para garantizar la correcta implementación, seguimiento y mantenimiento del Sistema. Para llevar a cabalidad esta fase de la primera etapa se hace necesario apoyarnos en el Organigrama para el Modelo de seguridad de la información que propone el **SASIGEL**.

Figura 3. Organigrama para el Modelo de Seguridad de la Información

Fuente: Centro de Investigación de Telecomunicaciones. 2011. Anexo 1: Organigrama Modelo y SASIGEL - Modelo de seguridad de la información para la estrategia de Gobierno en Línea 2.0.

Estratificación de entidades - La estratificación de las entidades permite identificar de manera general, el nivel de complejidad que puede significar para estas, la implementación del SGSI con el cual será revisado y dentro del cual es importante tener en cuenta los parámetros establecidos por el Modelo de seguridad de la información para la Estrategia de Gobierno en línea, el cual corresponde a la Estratificación de las entidades como se muestra en la tabla 01.

La estratificación de la cual hace referencia el modelo SASIGEL se basa o clasifica de acuerdo al Presupuesto, numero de equipos de computo, Servidores, empleados de Sistemas "Tecnología", existencia y funciones del área de sistemas, existencia y objeto de la WAN, transaccionalidad Web, Desarrollo de Software los cuales se puntúan por medio de la siguiente tabla:

TABLA No. 1 PARAMETROS PARA LA ESTRATIFICACIÓN DEL SASIGEL

Presupuesto en Millones de Pesos	Existencia y función del Área de sistemas	No. PC's	No. Servidores	Existencia y Objeto de la WAN	Transaccionalidad en la WEB	Desarrollo de Software	No. Empleados de Sistemas	Puntos que otorga
0 – 2.999	No hay área de sistemas	0 - 99	0 - 3	Internet Solo correo (externo) y navegación	Solo consulta	No. Incluye hosting básico de WEB y correo	0 - 5	**1**
3.000 – 50.000	Soporte Básico día a día y de usuario final. Reactiva	100 - 500	4 - 20	Internet con servicios públicos ofrecidos	Transaccionalidad Local (solo datos propios)	Aplicativos Internos	6 - 50	**2**
>50.000	Área con funciones definidas, administración de presupuesto y desarrollo de proyectos a futuro. Proactiva	>500	>20	Todo lo anterior más WAN privada	Transaccionalidad e interoperabilidad (utiliza datos propios y provee o consulta datos de otras entidades o terceros)	Aplicativos externos (servicios a terceros). Puede o no incluir desarrollos internos	>50	**3**

Puntos	Clasificación (estrato)
Menor a 11	Bajo
Entre 11 y 22	Medio
Mayor a 22	Alto

Fuente: Centro de Investigación de Telecomunicaciones. 2011. Anexo 3: Estratificación de Entidades - Modelo de seguridad de la información para la estrategia de Gobierno en Línea 2.0.

2.- Etapa de Análisis de la situación actual y definición de brechas:

La aplicación de encuestas - La encuesta se plantea para realizar el diagnóstico actual de la entidad dentro de la cual como lo fija el SASIGEL, busca brindarle a las entidades un conjunto de preguntas que les ayuden al levantamiento de la información[9]. En dicha encuesta se verifica la situación actual y la definición de brechas de la siguiente manera:

"Infraestructura física, acceso y medio ambiente"

a) Centro de Datos. Definir qué es un centro de datos y averiguar si en la entidad existen o no.
b) Control de Acceso. Definir control de acceso y averiguar si en la entidad se utilizan.
c) Barreras. Existen barreras físicas que aíslen las áreas coyunturales de la entidad.
d) CCTV. ¿Se utilizan circuito cerrado de televisión?
e) Cableado y Canaletas
f) Datos. Existencia y estado del cableado eléctrico (fotos).
g) Eléctrico. Existencia y estado del cableado de datos (fotos).
h) Seguridad Perimetral. ¿Existe un Firewall en la entidad y se entiende para qué debe existir?
i) Switches y Hubs. Averiguar cómo está construida la red de área local en cuanto a equipos activos.
j) Equipos en el Piso (fotos). ¿En la entidad hay equipos en el piso?
k) Aire Acondicionado. ¿Necesitan y utilizan aire acondicionado?
l) Reguladores y UPS. ¿Hay reguladores y UPS?
m) Planta de Emergencia. ¿Hay planta de generación de emergencia?

"Lógico"

a) Actualización de Servidores. ¿Se actualizan y parchan con regularidad los servidores? ¿Cuál de los métodos siguientes utilizan?

- YUM

[9] Tomado del proyecto Modelo de Seguridad Informática para la Estrategia de Gobierno En Línea Programa Agenda de Conectividad Ministerio de Comunicaciones, elaborado en Octubre de 2008.

- WSUS
- Manual

b) Pruebas de Intrusión. Definir qué son prueba s de intrusión y averiguar si se han hecho o se hacen con regularidad.

- Hacking Ético
- Ingeniería Social

"Metodológico".

Averiguar cuáles de los siguientes puntos metodológicos existe y se utilizan en la entidad.

a) Políticas. ¿Hay un manual como tal?
b) Procedimientos. ¿Para qué labores?
c) Normas. ¿Cuáles?
d) Estándares. ¿Aplicados a qué?
e) Concientización. ¿Hacen regularmente procesos de concienciación en lo referente a seguridad de la información? ¿Se hace inducción a los empleados nuevos?
f) Acuerdos de Confidencialidad. ¿Los hay como tal o están embebidos en el contrato laboral?
g) Renuncia de Propiedad de Información. ¿Se ha firmado aparte o existe dentro del contrato laboral?
h) Código de Buena Conducta. ¿Existe?

Definir el nivel de madurez – Autoevaluación; Utilizando el resultado de la encuesta, junto con el resultado de la determinación de la posición actual de madurez, se procede a definir el estado de seguridad de la información de la entidad, al comparar punto a punto, con lo mínimo esperado para el nivel actual de la entidad definido en el Manual de Gobierno en línea 3.1.

La entidad debe evidenciar el análisis donde se registre el cumplimiento o ausencia de cada elemento analizado, se debe definir y acordar con el líder del proceso de SGSI que se debe designar dentro de la Entidad, el plan o cronograma para disminuir la brecha y alinearse con el nivel de madurez más adecuado. Posteriormente comunicarlo al el líder de nivel central.

El SASIGEL brinda un conjunto de herramientas que permiten medir de manera objetiva el nivel de implementación actual en cuanto a seguridad de la información dentro de la cual se encuentran tres tipos de autoevaluaciones descritos dentro de la siguiente manera:

- ✓ **Auto evaluación del Estructura organizacional.** Para determinar el nivel de integración, relevancia y apoyo transversal y vertical de la entidad a la iniciativa de seguridad de la información.
- ✓ **Auto evaluación del nivel de gestión de seguridad de la información.** Con el cual se determina el nivel de madurez aproximado en el cuál se encuentra la entidad.
- ✓ **Auto evaluación de políticas, controles, métricas.** Por medio de la cual se determina el progreso en la implementación de controles en términos de políticas, y métricas con las cuales cuenta la entidad.

3.- Etapa de alineación con el SGSI.

En esta sección se debe establecer una estrategia dependiendo del nivel de madurez con que cuenta la organización, que identificado estarán cubiertos, serán validados y homologados, o deberán ser trabajados para cubrir la brecha y alinearse con el Modelo SASIGEL.

Se debe contar con el **compromiso por parte de directores** y alta gerencia de la empresa para promover y soportar la implementación, la operación y los recursos del SGSI. (La motivación, energía, apoyo y liderazgo debe partir de la dirección y luego extenderse hacia toda la entidad a todos sus niveles hasta convertirse en operaciones)

Políticas de seguridad alineadas con la misión y objetivos de la entidad, que se ajusten a la cultura corporativa, y donde se articulen todas las áreas de las entidades para concertar sobre la definición del alcance, la creación y aplicación de políticas, procedimientos y aseguramiento de los procesos y servicios ofrecidos.

4.6. ESTRATEGIA DE GOBIERNO EN LÍNEA

La Estrategia Gobierno en línea, liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones, es el conjunto de instrumentos técnicos, normativos y de política pública

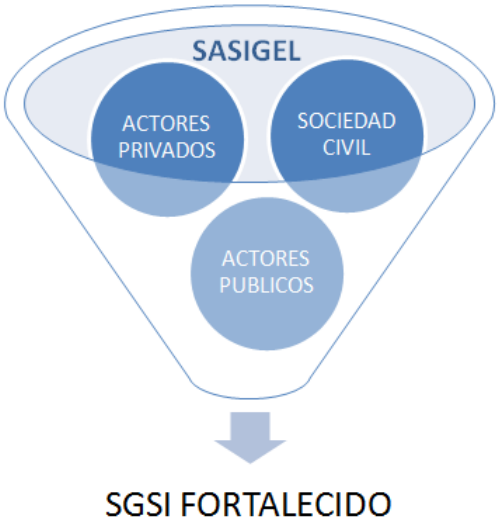
que promueven la construcción de un Estado más eficiente, transparente y participativo, y que a su vez, preste mejores servicios con la colaboración de toda la sociedad mediante el aprovechamiento de la tecnología. Lo anterior con el fin de impulsar la competitividad y el mejoramiento de la calidad de vida para la prosperidad de todos los colombianos.

Mediante el decreto 1151 del 2008 estableció los lineamientos generales que la Administración pública debe adelantar en la implementación de la Estrategia de Gobierno en línea.

5. ALINEACIÓN DEL SASIGEL CON EL SGSI

El sistema de Sistema de Administración de Seguridad de la Información de Gobierno en Línea debe estar alineado e integrado con el Sistema de Gestión de seguridad de la información, lo que en este sentido pretende SASIGEL es enfocar la estrategia hacia los objetivos del SGSI, coordinar todas aquellas actividades como lo es, la formulación, ejecución, seguimiento y mantenimiento de las políticas y lineamientos, los cuales son necesarios para fortalecer la adecuada gestión de la seguridad de la información de las empresas. En la figura 4 se puede observar que se muestra SASIGEL como un sistema que permite el fortalecimiento del SGSI por medio de la regulación en cuanto a las interacciones de los actores que intervienen dentro del Sistema. Es de saber que los requerimientos a ser evaluados en un sistema de gestión de seguridad de la información se encuentran definidos en el estándar NTC: ISO/IEC 27001:2005. En caso de que la entidad requiera demostrar cumplimiento y eventualmente decida certificarse bajo esta normativa de seguridad ISO de manera internacional, la entidad debe cumplir con los requisitos allí definidos[10].

Figura 4. Articulación SASIGEL - SGSI



Fuente: Autor

[10] Modelo de seguridad de la Información Para la estrategia de GEL, Centro de Investigación de Telecomunicaciones - CINTEL, Bogotá, D.C., Diciembre de 2011.

6. METODOLOGIA PARA LA IMPLEMENTACION DEL MODELO SASIGEL

Es de saber que actualmente las organizaciones cuentan con estructuras diferenciadas por su tamaño, criticidad de la información y modelo de operación entre otras y estas por lo tanto requieren un diferente tratamiento. En este sentido, lo que se debe realizar es detallar los requerimientos basados en el nivel de madurez de la organización, establecer los roles necesarios, así como las etapas fundamentales para la implementación del SGSI

Para la definición de los procesos relacionados con el SGSI apoyados en SASIGEL, se pretende establecer una metodología para las organizaciones la cual permita definir y constituir un enfoque basado en procesos, es de saber que la presente monografía no pretende ampliar sobre lo que propone el modelo ISO en relación a lo que plantea el modelo SASIGEL, sino describir cada uno de los procedimientos que el modelo SASIGEL presenta y los cuales son descritos a continuación:

6.1. DISEÑO METODOLÓGICO DE SASIGEL

Las actividades requeridas para la implantación del sistema de gestión de seguridad de la Información que se realizan según el ciclo de Demming o ciclo de mejora PDCA de SASIGEL, dentro de las salidas de cada etapa se convierten en entradas de la siguiente lo cual se convierte en un modelo auto-sostenible, que funciona de manera eficaz y se presenta mediante las siguientes fases:

6.1.1. PLAN – Planificación y diseño del SGSI

Es la fase inicial de diseño y en su ejecución se realizan las siguientes actividades:

- **Definir el alcance del SGSI:** en función de características del negocio o actividad, organización, localización, activos y tecnología, definir el alcance y los límites del SGSI.

- **Definir la política de seguridad:** que incluya el marco general y los objetivos de seguridad de la información de la organización, teniendo en cuenta los requisitos de negocio, legales y contractuales que afecten a la seguridad, esté alineada con la gestión de

riesgo general, establezca criterios de evaluación de riesgo y sea aprobada por la Dirección. La política de seguridad es un documento muy general, una especie de "declaración de intenciones" de la Dirección.

- **Definir el enfoque para evaluar los riesgos**: Establecer una metodología de evaluación de riesgos apropiada para el SGSI y las necesidades de la organización, desarrollar criterios de aceptación de riesgos y determinar el nivel de riesgo aceptable. Existen muchas metodologías de evaluación de riesgos aceptadas internacionalmente; la organización puede optar por una de ellas, hacer una combinación de varias o crear la suya propia. ISO/IEC 27001:2005. no impone ninguna ni da indicaciones adicionales sobre cómo definirla (en el futuro, ISO 27005 proporcionará ayuda en este sentido). El riesgo nunca es totalmente eliminable -ni sería rentable hacerlo-, por lo que es necesario definir una estrategia de aceptación de riesgo.

- **Realizar el inventario de activos**: Identificar todos aquellos activos de información que tienen algún valor para la organización y que quedan dentro del alcance del SGSI.

- **Identificar amenazas y vulnerabilidades:** Establecer los diferentes tipos de eventos que pudieran dañar a los activos del inventario en cualquiera de sus propiedades de seguridad: disponibilidad, integridad y confidencialidad atendiendo a la naturaleza del activo, el funcionamiento dentro de la Organización y como de posible es que dicha amenaza acabe finalmente afectando al elemento.

- **Identificar los impactos:** Estimar qué daños podría suponer una pérdida de confidencialidad, integridad o disponibilidad en cada uno de los activos. Se trata de valorar que pasaría si una hipotética amenaza llegara a materializarse sobre el activo en cuestión. Para ello, se utilizan diferentes criterios de valoración según la Organización desee considerar aspectos económicos, jurídicos, de imagen corporativa, etc.

- **Analizar y evaluar de los riesgos.** El daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad y se materialice en un impacto) y la posibilidad de ocurrencia del fallo dan como resultado el nivel de riesgo resultante que

determina si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

Identificar y evaluar opciones para el tratamiento del riesgo: Frente al riesgo solo hay cuatro opciones de gestión posibles:

a. Aceptar el riesgo

b. Reducir o mitigar mediante controles a las amenazas

c. Transferirlo a un tercero

d. Minimizar el impacto y la probabilidad de ocurrencia del riesgo.

Seleccionar controles de seguridad: Identificar diferentes tipos de soluciones y salvaguardas para el tratamiento del riesgo en función de las decisiones de gestión del riesgo adoptadas por la organización sobre cada par activo-amenaza. Para ello, se pueden utilizar el catálogo de controles del Anexo A de la norma ISO/IEC 27001:2005. y otros adicionales que se pudieran considerar necesarios.

Aprobar el riesgo residual y autorizar la implementación por parte de la Dirección del SGSI: hay que recordar que los riesgos de seguridad de la información son riesgos de negocio y sólo la Dirección puede tomar decisiones sobre su aceptación o tratamiento. El riesgo residual es el resultante aún después de haber aplicado controles (el "riesgo cero" no existe prácticamente en ningún caso).

Confeccionar una Declaración de Aplicabilidad: El documento llamado SOA (Statement of Applicability) es una lista de todos los controles seleccionados del anexo A de la norma ISO/IEC 27001:2005 y la razón de su selección así como la justificación de cualquier control del Anexo A excluido. Es, en definitiva, un resumen de las decisiones tomadas en cuanto al tratamiento del riesgo.

6.1.2. DO - Implementación del SGSI bajo el modelo SASIGEL

Es la fase de construcción de las medidas identificadas como necesarias en base al criterio de gestión del riesgo establecido. El SASIGEL presenta para mayor aplicación un documento que es la tabla de contenido para que las entidades sepan cómo estructurar el desarrollo de la fase "Hacer" del ciclo PHVA planteado en el Modelo de Seguridad de la Información, la cual supone el desarrollo de las siguientes actividades[11]:

1.- Definir plan de tratamiento de riesgos: Se deben identificar las acciones y tareas a realizar para implantar los controles que se hayan seleccionado en la Declaración de aplicabilidad, los recursos necesarios, los responsables de la ejecución de dichas tareas así como los plazos y prioridades en la gestión de los riesgos de seguridad de la información que se van a abordar. Normalmente fruto del plan surgen una serie de proyectos destinados a construir e implantar los controles seleccionados.

2.- Implantar el plan de tratamiento de riesgos: con la meta de alcanzar los objetivos de control identificados.

3.- Implementar los controles: todos los que se seleccionaron en la fase anterior.

4.- Formación y concienciación: de todo el personal en lo relativo a la seguridad de la información.

5.- Desarrollo del marco normativo necesario: normas, manuales, procedimientos e instrucciones.

6.- Definir los procesos de gestión del propio SGSI. La mayoría de los sistemas de información no son intrínsecamente seguros y las soluciones técnicas son sólo una parte de un enfoque holístico de la seguridad de la información por lo cual el establecimiento o definición de los procesos son pieza fundamental para una buena implementación.

[11] Tomado del Anexo 14: Tabla de contenido – Fase hacer, Modelo de Seguridad Informática para la Estrategia de Gobierno En Línea Programa Agenda de Conectividad Ministerio de Comunicaciones, elaborado en Diciembre de 2011.

7.- Implantar procedimientos y controles de detección y respuesta a incidentes de seguridad.

6.1.3. CHECK - Monitoreo y supervisión del SGSI

Es la fase de vigilancia del funcionamiento de las medidas y de identificación de ajustes. Durante su ejecución se realizan las siguientes actividades:

1.- Ejecutar procedimientos y controles de monitorización y revisión: para detectar errores en resultados de procesamiento, identificar brechas e incidentes de seguridad, determinar si las actividades de seguridad de la información están desarrollándose como estaba planificado, detectar y prevenir incidentes de seguridad mediante el uso de indicadores y comprobar si las acciones tomadas para resolver incidentes de seguridad han sido eficaces.

2.- Revisar regularmente la eficacia del SGSI: en función de los resultados de auditorías de seguridad, incidentes, mediciones de eficacia, sugerencias y feedback de todos los interesados.

Se debe debe crear una revisión independiente de la Seguridad de la Información, programar e incluir:

- ✓ La evaluación de la eficacia de las operaciones del Programa de Seguridad de la Información;
- ✓ Realizar la documentación de los resultados y,
- ✓ Elaborar informes sobre los resultados de la revisión a la alta dirección.

Esta revisión debe ser realizada por una tercera parte “de manera independiente”.

3.- Medir la eficacia de los controles: para verificar que se cumple con los requisitos de seguridad. Una forma de hacerlo es realizar un proceso de análisis de riesgos para determinar los controles que deban aplicarse. El proceso de análisis de riesgos se definen las variables críticas como; que, cuando se controla, nos muestra el nivel de exposición al riesgo y luego determinar los indicadores que permitan medir la eficacia de los controles.

4.- Revisar regularmente la evaluación de riesgos: los cambios en la organización, tecnología, procesos y objetivos de negocio, amenazas, eficacia de los controles o el entorno tienen una influencia sobre los riesgos evaluados, el riesgo residual y el nivel de riesgo aceptado.

5.- Realizar regularmente auditorías internas: para determinar si los controles, procesos y procedimientos del SGSI mantienen la conformidad con:

a. Los requisitos de la norma ISO/IEC 27001:2005.

b. El marco legal de aplicación a la Organización

c. Los requisitos y objetivos de seguridad que la organización se haya planteado

6.- Revisar regularmente el SGSI por parte de la Dirección: Es necesario mantener y adaptar el SGSI a los cambios tanto del entorno como de objetivos que se vayan produciendo. Para ello, con cierta periodicidad debe evaluarse si el alcance definido sigue siendo adecuado, se tienen que identificar mejoras al SGSI, a la política de seguridad o a los objetivos de seguridad de la información.

7.- Actualizar planes de seguridad: teniendo en cuenta los resultados de la monitorización, el registro de incidentes y los informes que las diferentes revisiones y auditorías produzcan, se deben ir ajustando los planes de seguridad para incorporar las mejoras o correcciones que se estimen pertinentes.

8.- Registrar acciones y eventos que puedan tener impacto en la eficacia o el rendimiento del SGSI: sirven como evidencia documental de conformidad con los requisitos y uso eficaz del SGSI.

6.1.4. ACT – Proceso de mejora continua

Es la fase donde se realizan los ajustes y cambios necesarios para lograr los objetivos planteados en base a la información que se obtiene de la revisión del funcionamiento de las medidas de seguridad. Durante su ejecución se realizan las siguientes actividades:

1. **Implantar mejoras:** poner en marcha todas las mejoras que se hayan propuesto en la fase anterior.

2. **Acciones correctivas:** para solucionar no conformidades detectadas.

3. **Acciones preventivas:** para prevenir potenciales no conformidades.

4. **Comunicar las acciones y mejoras:** a todos los interesados y con el nivel adecuado de detalle.

5. **Asegurar que las mejoras alcanzan los objetivos pretendidos:** la eficacia de cualquier acción, medida o cambio debe comprobarse siempre.

El mejoramiento es un proceso que tiene como propósito asegurar la eficiencia y efectividad de las empresas; puede ser gradual o radical. El mejoramiento gradual se enfoca en la gerencia de la calidad total. El mejoramiento radical se apoya en la reingeniería de proceso, cuyo enfoque es reinventar los procesos a partir de cero[12].

6.2. SOBRE EL LEVANTAMIENTO DE PRERREQUISITOS DEL MODELO SASIGEL

Es necesario reconocer el estado en que se encuentra la entidad para poder dar inicio a la implementación del SGSI Aplicando el Sistema administrativo de la Seguridad de Gobierno en Línea para lo cual se deben tener en cuenta ciertas necesidades:

- La entidad debe contar con un líder de Gobierno en línea (líder GEL)
- La entidad debe contar con el comité de segundad de Gobierno en línea.
- La entidad debe contar con el oficial de seguridad.
- La entidad debe contar con personal técnico para realizar las tareas de la seguridad de la información.
- La entidad debe contar con una integración con los demás sistemas de gestión.
- La entidad debe contar con el apoyo y participación de planeación.
- La entidad debe contar con el apoyo y participación de control interno.

[12] Aldana de Vega, Luz Ángela, Álvarez Builes, María Patricia, Bernal Torres, César Augusto. Administración por calidad. México: Alfaomega Grupo Editor, 2011.

- Los funcionarios deben conocer sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad
- Los proveedores deben conocer sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad.
- Los ciudadanos deben conocer sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad

6.3. SOBRE LOS REQUISITOS DEL SGSI PARA IMPLEMENTACIÓN DEL MODELO SASIGEL

La organización o entidad debe como primera medida definir una política de seguridad por medio de la cual se garantice la protección de los activos en general. Dentro de la aplicación de dicho documento se debe hacer referencia a los ocho dominios o políticas los cuales se dividen en:

- Políticas de control de acceso
- Políticas de no repudio
- Políticas de privacidad y confidencialidad
- Políticas de integridad
- Políticas de disponibilidad del servicio
- Políticas de disponibilidad de la información
- Políticas de protección del servicio
- Políticas de registro y auditoría

El SASIGEL cuenta con la guía para la implementación de las políticas de de seguridad de la información para las entidades que proveen servicios para la Estrategia de Gobierno en Línea y que busquen alinearse con el Modelo de Seguridad de la Información, dichas políticas se relacionan en el apartado 4.6 del presente documento "Implementación de las Políticas de SGSI".

La entidad debe tener clasificado los activos de información ya que es una pieza fundamental a la hora de administrar los riesgos y es necesario para establecer como las personas deben proteger dichos activos de los accesos no autorizados o impropios. El modelo SASIGEL dentro de los anexos propone la siguiente tabla de clasificación de los activos de información.

TABLA No. 2 CLASIFICACIÓN DE LOS ACTIVOS DE INFORMACIÓN

Inventário de Activos										
Nombre del Área:										
Gerencia:										
Tipo de Activo	**Nombre**	**Proceso**	**Proprietário del activo**	**Sistema de información Relacionado**	**Clasificación de la información**	**Áreas Asociadas**	**Criticidad**			
							Conf	**Integ**	**Disp**	**Total**
Activos de la información										0
										0
Activos de software										0
										0
Activos físicos										0
										0
Servicios										0
										0
Personas										0
										0
Imagen Reputación										0
										0

Fuente: Centro de Investigación de Telecomunicaciones. 2011. Anexo 7: Metodología de clasificación de los Activos - Modelo de seguridad de la información para la estrategia de Gobierno en Línea 2.0.

Posteriormente se debe realizar un levantamiento de los riesgos y su evaluación en cada uno de los procesos y así mismo definir el plan de acción con los controles y políticas que se implementarán para mitigar los riesgos identificados. Es necesaria la divulgación permanente de las políticas de Seguridad, así como la revisión periódica de los riesgos que han resultado de las evaluaciones realizadas.

6.4. ORGANIZACION DE LA RESPONSABILIDAD DE LA INFORMACION

6.4.1. La Dirección

La Dirección tiene varias de las responsabilidades clave en la puesta en marcha y funcionamiento del SGSI. Es la Dirección la que debe:

- Aprobar la Política y los objetivos de seguridad.
- Aprobar los riesgos residuales, aquellos que quedan tras la aplicación de controles de seguridad y que en ese momento no se pueden reducir más, por lo que la Entidad debe asumirlos.
- Aprobar los planes de formación y auditorías.
- Realizar la revisión del SGSI.
- Demostrar su compromiso con la seguridad de la información para promover una cultura efectiva dentro de la Entidad.

6.4.2. El Comité de Seguridad de la Información

Dentro del ejercicio del SGCI el comité de seguridad de la información debe:

- Revisar y proponer al director para su aprobación la Política de Seguridad de la Información y las funciones generales en materia de seguridad de la información;
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes;
- Tomar conocimiento y supervisar la investigación y monitoreo de los incidentes relativos a la seguridad;
- Aprobar las principales iniciativas para incrementar la seguridad de la información, de acuerdo a las competencias y responsabilidades asignadas a cada área, así como acordar y aprobar metodologías y procesos específicos relativos a seguridad de la información;
- Garantizar que la seguridad sea parte del proceso de planificación de la información;

- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas o servicios;

- Promover la difusión y apoyo a la seguridad de la información dentro de la Entidad al igual que coordinar el proceso de administración de la continuidad de las actividades institucionales.

6.4.3. El Responsable de Seguridad de la Información

Tendrá a su cargo, entre otros:

- Llevar a cabo las actividades de gestión del SGSI.

- Administrar y gestionar las cuentas de los usuarios y los privilegios de acceso de cada uno de ellos.

- Asegurarse de que sólo las personas autorizadas van a tener acceso a la información y los sistemas cuentan con él.

- Asegurarse de que los sistemas tienen los niveles de disponibilidad requeridos por la Entidad.

- Incluir en los requisitos para nuevos desarrollos los aspectos de seguridad que apliquen.

- Dirigir las investigaciones sobre incidentes y problemas relacionados con la seguridad, así como recomendar las medidas pertinentes.

- Definir procedimientos para el control de cambios a los procesos operativos documentados.

- Definir y documentar una norma clara con respecto al uso del correo electrónico (políticas del correo electrónico).

- Definir y documentar controles para la detección y prevención del acceso no autorizado, la protección contra software malicioso y para garantizar la seguridad de los datos y los servicios conectados en las redes de la Entidad.

- Desarrollar procedimientos adecuados de concientización de usuarios en materia de seguridad.

- Verificar el cumplimiento de las normas, procedimientos y controles establecidos.

- Monitorear las necesidades de capacidad de los sistemas en operación y proyectar las futuras demandas de capacidad, a fin de evitar potenciales amenazas a la seguridad del sistema o a los servicios del usuario.

- Implementar los controles de seguridad definidos.

- Definir e implementar procedimientos para la administración de medios informáticos de almacenamiento, como USB, discos, e informes impresos y para la eliminación segura de los mismos.

6.4.4. EL área de sistemas es responsable de:

- Implantar y velar por el cumplimento de las políticas, normas, pautas, y procedimientos de seguridad en la Entidad, todo esto en coordinación con el responsable de seguridad, con el jefe de oficina de planeación y con el área de Control Interno.

- Evaluar, e implantar productos de seguridad informática, y realizar las demás actividades necesarias para garantizar un ambiente informático seguro. Además debe ocuparse de proporcionar apoyo técnico y administrativo en todos los asuntos relacionados con la seguridad, y en particular en los casos de infección de virus, penetración de hackers, y otras situaciones.

- Un representante del área participará notificando a los clientes, proveedores sobre las modificaciones que se efectúen a la Política de Seguridad, además de participar en la definición del Compromiso de Confidencialidad a firmar por los empleados y terceros que desarrollen funciones en la entidad, en el asesoramiento sobre las sanciones a ser aplicadas por incumplimiento y en el tratamiento de incidentes de seguridad que requieran de su intervención.

6.4.5. Propietario de activos.

El propietario de un activo, entendiendo por tal al responsable de dicho activo, tendrá las siguientes responsabilidades:

- Definir si el activo está afectado por la Ley de Protección de Datos y aplicarle en su caso, los procedimientos correspondientes.
- Definir quienes pueden tener acceso a la información, cómo y cuándo, de acuerdo con la clasificación de la información y la función a desempeñar.
- Informar al Responsable de Seguridad de la Información cuando detecte cualquier incidencia para tratarla y corregirla.
- Implementar las medidas de seguridad necesarias en su área para evitar fraudes, robos o
- interrupción en los servicios.
- En los casos que aplique, asegurarse de que el personal y los contratistas tienen cláusulas de confidencialidad en sus contratos y son conscientes de sus responsabilidades.

6.4.6. Sobre los Usuarios

Son responsables de cumplir con todas las políticas de la Entidad relativas a la seguridad de la información y en particular:

- Conocer y aplicar las políticas y procedimientos apropiados en relación al manejo de la información y de los sistemas informáticos.
- No divulgar información confidencial de la Entidad a personas no autorizadas.
- No permitir y no facilitar el uso de los sistemas informáticos de la Entidad a personas no autorizadas.
- No utilizar los recursos informáticos (hardware, software o datos) y de telecomunicaciones (teléfono, fax) para otras actividades que no estén directamente
- relacionadas con el trabajo en la Entidad.

- Proteger meticulosamente su contraseña y evitar que sea vista por otros en forma inadvertida.

- Reportar inmediatamente a su jefe inmediato y al responsable de la Seguridad de información cualquier evento que pueda comprometer la seguridad de la Entidad y sus recursos informáticos, como por ejemplo contagio de virus, intrusos, modificación o pérdida de datos y otras actividades poco usuales.

6.4.7. Personal en general

Deberá:

•Conocer y comprender la Política de Seguridad y los procedimientos que apliquen a su trabajo.

•Llevar a cabo su trabajo, asegurándose de que sus acciones no producen ninguna infracción de seguridad.

•Comunicar los incidentes de seguridad que detecte mediante el canal establecido para ello.

6.4.8. Terceras partes

Cualquier entidad externa a la Entidad que de alguna manera tenga acceso a los activos de información de la misma (clientes, usuarios, contratistas, etc.) debería:

- Conocer la Política de Seguridad y entender su impacto en las relaciones con la Entidad.

- Cumplir lo estipulado en los contratos respecto a la seguridad de la información de los activos con los que trabajan.

- Comunicar las incidencias de seguridad que detecten.

6.4.9. Proveedores de Sistemas Informáticos

Son responsables de:

- Establecer los controles de acceso apropiados para cada usuario de Base de Datos, revisar las bitácoras de acceso y de llevar a cabo las tareas de seguridad relativas a los sistemas que administra,
- Informar al Encargado de Sistemas sobre toda actividad sospechosa o evento insólito.

6.5. ESTABLECER LA DECLARACIÓN DE APLICABILIDAD DDA

La declaración de aplicabilidad es un aspecto muy importante, ya que por medio de esta la entidad se orientara a dar cumplimiento a la norma ISO 27001 y de esta manera poder posteriormente optar en un futuro por la certificación. Lo que pretende esta declaración es convenir un compromiso por la dirección en relación con los controles que serán aplicados en la entidad, para su establecimiento se debe realizar una breve descripción de como se aplica, como se van a implementar los controles escogidos junto con las razones del porque se seleccionan dichos controles y en caso de no implantar describir los motivos de esta decisión lo cual debe ser justificado adecuadamente.

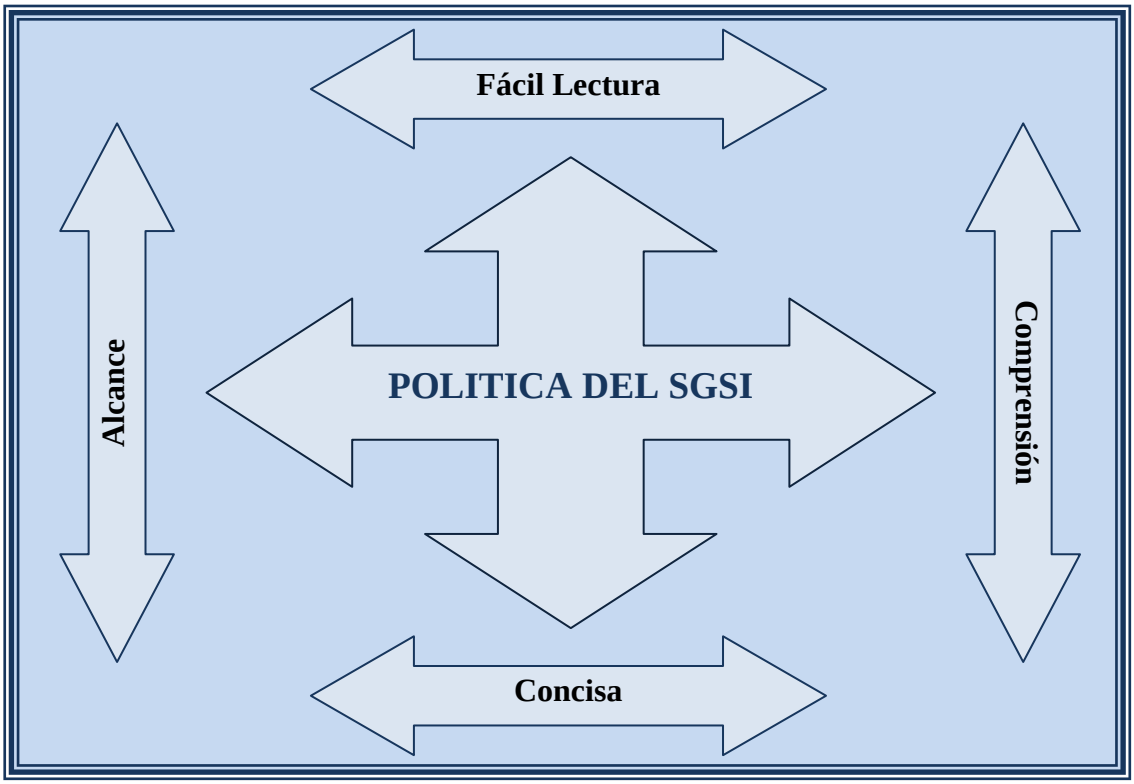
Deben de establecerse unos objetivos y controles apropiados, aquellos que se consideran que cubren los requisitos en cuanto a la seguridad de la entidad y que son visibles. Una vez que este esto claro debe prepararse un plan para la realización de todo lo trazado dentro de la estrategia el cual dentro de la norma se denomina plan de tratamiento de Riesgos que debe contar con los recursos humanos, técnicos y económicos para lograr el objetivo para finalmente medir la eficacia de los controles y establecer mecanismos de recogida y análisis.

6.6. IMPLEMENTACIÓN DE POLITICAS DEL SGSI

La Política es un documento por medio del cual se describe la necesidad sobre la implementación del Sistema de gestión de seguridad de la información. El documento debe enmarcar los principios que guían las actividades dentro de la entidad y debe contener ciertas

características que permitan su fácil lectura, comprensión, conciso y tener un alcance que se pueda cumplir.

Figura 5. Características de la Política del SGSI



Fuente: Autor

La política viene como una plantilla definida desde SASIGEL y será adaptada a las condiciones específicas y particulares de cada entidad, según corresponda, para que sean aprobadas por la entidad al igual que los siguientes aspectos para su elaboración:

- Se debe establecer un reglamento de prácticas favorables para la gestión de la seguridad.
- Establecer las especificaciones para la adopción de un Sistema de Gestión de la Seguridad de la Información.
- Establecer un conjunto de normas que se apliquen en nuestro entorno y sector, y que utilicen tecnologías de la información para lograr los objetivos propuestos.
- Mejorar los niveles de competitividad, optimizando la seguridad y el funcionamiento de la entidad.

- Promover servicios para que la entidad se incorpore más fácil y eficientemente a la sociedad de la información.
- Establecer el Estándar ISO-IEC 27001, código aceptado internacionalmente, en nuestra práctica de la seguridad de la información.

Para implementar una solución de Sistemas de Gestión de Seguridad de la Información es propicio aplicar un método compuesto de cuatro fases:

- **Fase 1: Establecimiento**. Determinar la situación de la seguridad actual y definir los requisitos para la seguridad de la información basada en un riesgo de negocio aceptable (deseada).

  Desarrollar un diseño de solución de sistemas de administración de seguridad de la información con recomendaciones específicas y un plan detallado para implementarla.

- **Fase 2: implementación**. Probar el diseño y desarrollar una configuración de producción estándar. Definir y documentar las directrices, estándares y procedimientos necesarios para implementar y administrar la solución de una manera efectiva.

- **Fase 3: Monitoreo.** Establecer una arquitectura básica que sea posible de ampliar para proporcionar una plataforma de administración con todas las características.

- **Fase 4: mantenimiento.** Tener en cuenta los parámetros que establece el estándar para desarrollar una directiva de seguridad y garantizar que la seguridad se implementa y mantiene en toda la organización; para esto se deben incluir los objetivos de seguridad globales, un esquema del nivel global de la seguridad requerida, los estándares de seguridad, incluidas las estrategias de auditoría y supervisión, y las definiciones de formación y procesos para mantener la seguridad.

El modelo SASIGEL dentro del formato de política de SGSI, propone una plantilla la cual se puede adaptar a las condiciones específicas y particulares de cada entidad según corresponda para que sean aprobadas por la entidad la cual se detalla de la siguiente manera[13]:

[13] Tomado del Anexo 5: Formato Política SGSI, Modelo de Seguridad Informática para la Estrategia de Gobierno En Línea Programa Agenda de Conectividad Ministerio de Comunicaciones, elaborado en Diciembre de 2011.

La Política de Seguridad de la Información es la declaración general que representa la posición de la administración de *NOMBRE DE LA ENTIDAD* con respecto a la protección de los activos de información (los funcionarios, la información, los procesos, las tecnologías de información incluido el hardware y el software), a la implementación del Sistema de Gestión de Seguridad de la Información y al apoyo, generación y publicación de sus políticas, procedimientos e instructivos.

NOMBRE DE LA ENTIDAD, para el cumplimiento de su misión, visión, objetivo estratégico y apegado a sus valores corporativos, establece la función de Seguridad de la Información en la Entidad, con el objetivo de:

- Minimizar el riesgo en las funciones más importantes de la entidad.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de sus clientes, socios y empleados.
- Apoyar la innovación tecnológica.
- Implementar el sistema de gestión de seguridad de la información.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, aprendices, practicantes y clientes del *NOMBRE DE LA ENTIDAD*
- Garantizar la continuidad del negocio frente a incidentes.

Alcance/Aplicabilidad

- Esta política aplica a toda la entidad, sus funcionarios, terceros, aprendices, practicantes, proveedores del *NOMBRE DE LA ENTIDAD* y la ciudadanía en general.

Nivel de cumplimiento

- Todas las personas cubiertas por el alcance y aplicabilidad se espera que se adhieran en un 100% de la política

De igual manera adentro del documento se establecen las 12 políticas de seguridad que soportan el SGSI de *NOMBRE DE LA ENTIDAD:*

- *NOMBRE DE LA ENTIDAD* ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del negocio, y a los requerimientos regulatorios.
- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los empleados, proveedores, socios de negocio o terceros.
- *NOMBRE DE LA ENTIDAD* protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores o clientes), o como resultado de un servicio interno en outsourcing.
- *NOMBRE DE LA ENTIDAD* protegerá la información creada, procesada, transmitida o resguardada por sus procesos de negocio, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.
- *NOMBRE DE LA ENTIDAD* protegerá su información de las amenazas originadas por parte del personal.
- *NOMBRE DE LA ENTIDAD* protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.
- *NOMBRE DE LA ENTIDAD* controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.
- *NOMBRE DE LA ENTIDAD* implementará control de acceso a la información, sistemas y recursos de red.
- *NOMBRE DE LA ENTIDAD* garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.
- *NOMBRE DE LA ENTIDAD* garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- *NOMBRE DE LA ENTIDAD* garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.
- *NOMBRE DE LA ENTIDAD* garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

6.7. APLICACIÓN DE CONTROLES

Es necesario e importante definir claramente los controles, estos son necesarios, se debe plantear toda la normativa que debe seguir el personal de la empresa. Por medio de políticas se deben considerar aspectos generales y específicos sobre acceso a la información, responsabilidad y manejo de activos de información, procedimientos a seguir cuando se presente un incidente de seguridad.

La información es un recurso que, como el resto de los activos, tiene valor para el organismo y por consiguiente debe ser debidamente protegida. Las políticas de seguridad de la información protegen a la misma de una amplia gama de amenazas, a fin de garantizar la continuidad de los sistemas de información, minimizar los riesgos de daño y asegurar el eficiente cumplimiento de los objetivos de las entidades del Estado (Centro de investigación de las Telecomunicaciones - CINTEL, Controles y lineamientos de seguridad, 2011, p. 8).

El factor terminante para la implantación de un SGSI es el apoyo de la dirección, puesto que esta es la que aprueba las acciones a tomar y facilita los recursos necesarios para llevarlas a cabo. El principal impedimento a la hora de implantar un sistema de gestión en una empresa es la resistencia al cambio por parte del personal. Para vencerla, es fundamental una labor de sensibilización y concienciación a través de la formación. El objetivo es que todos los miembros de la entidad sepan cuáles son sus responsabilidades y su papel dentro del sistema. Esta formación debe ser de manera presencial: podría ser apoyados en una presentación o un pequeño manual colgado en un la web. La realización de este tipo de acciones a la hora de la implantación facilita su desarrollo, contribuyendo a que todo el personal involucrado tome parte de una forma positiva. Igualmente, una vez finalizada dicha implantación es conveniente volver a realizar una breve presentación para fijar conceptos e incidir en las responsabilidades de cada integrante del

sistema. Asimismo, la repetición periódica de este tipo de acciones contribuye al buen funcionamiento y mantenimiento del sistema.

La mejor forma de abordar una implantación es cumplir con los requisitos de la norma, planteándose objetivos realistas y fáciles de causar. Con ello se consiguen resultados positivos inmediatos que animan a los implicados a continuar y favorecer la buena disposición al cambio, minimizando el tiempo y el esfuerzo de la implantación. Asimismo, se facilita la integración gradual de la empresa en el ciclo de mejora continua. Todas aquellas acciones que se planteen deben estar alineadas con el negocio y la realidad de la empresa.

Cuanto más sencillo sea el sistema, más probabilidades de éxito tendrá. La complejidad lleva a la sobrecarga de trabajo y a dificultar la realización de tareas. La implementación de un sistema simple facilita su comprensión; por lo tanto, seria notable su aceptación y seguimiento.

La metodología de análisis de riesgos que se utilice debe ser fácilmente reproducible y comparable, consiguiendo una selección de controles realmente ajustada a los requisitos. No es recomendable tratar todos los riesgos a la vez. La dirección decide sobre cuáles va actuar por su importancia para la entidad y aplicará controles para ellos. Muchos de estos controles ayudan a rebajar el nivel de riesgo en otros activos., si no en todos. La elaboración y ejecución del plan de riesgos anual contribuirá a mejorar el nivel de riesgo asistido.

6.8. PROCESO PARA LA IDENTIFICACIÓN Y ADMINISTRACIÓN DE RIESGOS BAJO EL MODELO SASIGEL

Esta etapa se basa en la evaluación de riesgos, dentro del modelo SASIGEL se ofrece una Guía para la gestión de riesgos teniendo en cuenta que el proceso de gestión del riesgo no debiera ser tratado como una función únicamente técnica llevada a cabo por los expertos de TI, este proceso debe ser implementado desde las áreas de negocio a nivel funcional y estratégico, hasta las áreas operativas y de infraestructura IT ya que es una función esencial de cada entidad[14].

[14] Tomado del Anexo 6: Metodología de gestión de Riesgo - Modelo de seguridad de la Información Para la estrategia de GEL, Centro de Investigación de Telecomunicaciones - CINTEL, Bogotá, D.C., Diciembre de 2011.

Es esencial para asegurar que los controles son plenamente acordes con los riesgos a los que está expuesta la organización. Sin embargo, existen algunos métodos convencionales para la realización de dicho análisis de riesgos de seguridad que son cada vez más insostenible en términos de facilidad de uso y flexibilidad entre otras.

La comprensión de los riesgos y la aplicación de la metodología de administración de riesgos es necesaria, con la finalidad de crear de manera eficiente y eficaz un entorno informático seguro. Por infortunio, esto sigue siendo un área difícil para los profesionales de la información, debido las nuevas tecnologías y el crecimiento impresionante del Internet, y quizás la prevalencia de la actitud de que la evaluación del riesgo y la identificación de retorno de la inversión es simplemente demasiado difícil de hacer.

El precepto fundamental de la seguridad de la información es para apoyar la misión de las entidades, estas se encuentran expuestas a incertidumbres, algunos de los cuales afectan a dichas entidades de una manera negativa. Con el fin de apoyar a la organización, a los profesionales de seguridad se debe ser capaz de contar con una buena gestión, a entender y manejar estas fluctuaciones.

Los sistemas de gestión de seguridad de la información (SGSI) se inician con los procesos de análisis, valoración y mitigación de riesgos, pues las medidas de seguridad deben apuntar hacia los riesgos más importantes para el negocio. La norma ISO 27000, exige de las organizaciones a nivel general:

- La comprensión de los requerimientos de seguridad de la información (integridad, disponibilidad y confidencialidad).
- La implementación y operación de controles para administrar los riesgos de la información del negocio.
- El monitoreo del desempeño efectivo del sistema de seguridad (SGSI)
- El mejoramiento continuo basado en la medición de objetivos. (Centro de investigación de las Telecomunicaciones - CINTEL, Metodología de gestión del riesgo, 2011, p. 50).

El riesgo con respecto a los sistemas de información, es el daño potencial que puede surgir de un proceso en curso o en algún acontecimiento futuro, este se encuentra presente en cada aspecto de nuestras vidas y muchas áreas o disciplinas. Desde la perspectiva de la seguridad de Tecnologías de la Información, la gestión del riesgo es el proceso de comprender y responder a los factores que pueden conducir a un fracaso en la confidencialidad, integridad o disponibilidad del activo más valioso de la entidad que es la información.

6.8.1. Identificación de Amenazas

Se puede afirmar que el activo más importante para cualquier tipo de organización o empresa, es la información, pero dicho activo se enfrenta constantemente a diferentes tipos de amenazas, que pueden llevar a la pérdida total o parcial de este activo; por lo anterior se hace necesario analizar minuciosamente las vulnerabilidad con las que cuentan la entidad o empresa, además de identificar las amenazas que se presentan, para analizar el nivel de riesgo y desarrollar mecanismos o controles que permitan minimizar o anular estas falencias, tomando como base las entradas que dentro de ellas se pueden encontrar, el historial de ataques al Sistema o datos estadísticos de organismos de inteligencia, para proceder a proteger a cada una de dichas amenazas y vulnerabilidades las cuales pueden ocasionar una baja de recursos. Dentro de la tabla No. 3 Se observan algunos tipos de amenaza y sus orígenes.

TABLA No. 3 AMENAZAS Y ORIGEN

		ORIGEN		
TIPO	**AMENAZA**	**A**	**D**	**E**
Daño físico	Fuego	X	X	X
	Daños por agua	X	X	X
	Destrucción del equipo o los medios	X	X	X
	Polvo, Corrosión	X	X	X
Eventos naturales	Fenómenos climáticos			X
	Fenómenos meteorológicos			X
	Inundación			X
perdida de servicios esenciales	Corte de suministro eléctrico o Falla en el aire acondicionado	X	X	
	Perdida de suministro de energía	X	X	X
	Falla en el equipo de telecomunicaciones	X	X	

Compromiso de la información	Espionaje remoto		X	
	Hurto de medios o documentos		X	
	Hurto de equipos		X	
	Recuperación de medios reciclados		X	
	Divulgación	X	X	
	Datos provenientes de fuentes no confiables	X	X	
	Manipulación con hardware		X	
	Manipulación con software	X	X	
Fallas técnicas	Falla del equipo	X		
	Mal funcionamiento del equipo	X		
	Saturación del sistema de información	X	X	
	Mal funcionamiento del software	X		
	Incumplimiento en el mantenimiento del sistema de información	X	X	
Acciones no autorizadas	Uso no autorizado del equipo		X	
	Copia fraudulenta del software		X	
	Uso de software falso o copiado	X	X	
	Corrupción de los datos		X	
	Procesamiento ilegal de los datos		X	
Compromiso de las funciones	Error en el uso	X		
	Abuso de derechos	X	X	
	Falsificación de derechos		X	
	Negación de acciones		X	
	Incumplimiento en la disponibilidad del personal	X	X	X

A ACCIDENTALES
D DELIBERADOS
E AMBIENTALES

Establecer los diferentes tipos de eventos que pudieran dañar a los activos del inventario en cualquiera de sus propiedades de seguridad: disponibilidad, integridad y confidencialidad atendiendo a la naturaleza del activo, el funcionamiento dentro de la Organización y como de posible es que dicha amenaza acabe finalmente afectando al elemento.

Según el ámbito de la acción esta amenaza se divide y la describimos de la siguiente manera:

6.8.1.1. Desastre del entorno (seguridad física)

Seguridad Física - Se debe establecer una clasificación de las áreas en cuanto a la confidencialidad de la información o criterio, evitar en lo máximo el acceso no autorizado, la clasificación a la se realiza referencia es a la clasificación de las zonas según el nivel de seguridad.

Es uno de los aspectos más olvidado al diseñar un sistema de información. La seguridad física consiste en la aplicación de la barrera física y procedimiento de control, como medidas de prevención y contra medidas de amenazas a los recursos e información confidencial. Nos referimos a los controles y mecanismo de seguridad, dentro y alrededor de los computo, así como los medios de acceso remoto al y desde el mismo, implementados para proteger el hardware y los medios de almacenamiento de datos.

Este tipo de amenazas son ocasionadas tanto como por el hombre, como por la naturaleza del medio físico en que se encuentra ubicada la empresa.

Debe existir un órgano de control para la protección de la información clasificada, etiquetada según su nivel, estar adecuadamente almacenados, protegidos e identificados

Incendio **--** Los incendios son caudados por el uso inadecuado de combustible, fallas de instalaciones eléctricas defectuosas, y el inadecuado almacenamiento y tratado de sustancia peligrosa.

Los diversos factores a contemplar, para reducir el riesgo de incendios son:

- ✓ El área en que se encuentran las computadoras deben estar en un local que no sea combustible e inflamable.
- ✓ El lugar no debe situarse, encima, debajo o adyacente o eras donde se procesan o fabriquen, o almacenen material inflamable, explosivos, gases tóxicos o sustancias radioactivas.
- ✓ Las paredes deben hacerse en material incombustibles y extenderse desde suelo al techo.
- ✓ Debe construirse un" falso piso" instalado sobre el piso real, con material incombustible y resistente al fuego.
- ✓ No debe estar permitido fumar en el área de proceso.
- ✓ Debe emplearse muebles incombustible, y cesto metálicos para papeles, se deben evitar los materiales plásticos e inflamables,

- ✓ El piso y el techo en el recinto de cómputo y de almacenamiento de los medios magnéticos deben ser impermeable.

Inundación **-** Para prevenir se pueden tomar las siguientes medidas: construir un techo impermeable para evitar el paso del agua desde un nivel superior, y acondicionar las puertas para contener el agua que bajarse por las escaleras.

Sabotaje **-** El peligro más temido en los centros de procesamiento de datos, es el sabotaje, siendo uno de los más duros retos. Este puede ser un empleado o un sujeto ajeno a la empresa. Para la empresa sugerimos los siguientes:

- ✓ Circuito cerrado de televisión.
- ✓ Edificios inteligentes para ir a la vanguardia con la tecnología.
- ✓ Detención electrónica (sensores).
- ✓ Detectores de metales en las entradas.

6.8.1.2. Amenaza del sistema (seguridad lógica)

La seguridad lógica consiste en la aplicación de barreras y procedimientos que resguarden el acceso a los datos, y solo se permita acceder a ellos a la persona autorizada para hacerlo.

Dentro de sus objetivos se encuentran los siguientes:

- ✓ Restringir el acceso a los programas de archivos.
- ✓ Asegurar que los trabajadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- ✓ Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- ✓ Que la información transmitida sea recibida por el destinatario al cual ha sido enviada y no a otro.
- ✓ Que la información recibida sea la misma que ha sido trasmitida.
- ✓ Que existan sistemas alternativos secundarios de transmisión entre los diferentes puntos.

- ✓ Que se disponga de pasos alternativos de emergencia para la trasmisión de información

Implementación de Controles de acceso **-** Estos controles se implementaran en el Sistema Operativo sobre los sistemas de aplicación, en base de datos, en un paquete específico de seguridad o en cualquier orto utilitario.

- ✓ Identificación y autentificación.(PASSWORD)
- ✓ Roles como: programador, líder del proyecto, gerente de una área usuaria, administrador del sistema, etc.
- ✓ Limitación de las transacciones.
- ✓ Modalidad del acceso: si es de lectura, escritura, ejecución, y borrado.
- ✓ Controles de acceso interno: el password, protección mediante la encriptación.
- ✓ Controles de acceso externo: como los dispositivos de control de puertos del firewalls.
- ✓ Control de acceso al público.

6.8.1.3. Amenaza de la red (comunicaciones)

El acceso externo al sistema de información debe estar limitado, asegurado dicho acceso solamente al personal autorizado. Una medida que ayudara a garantizar este acceso es exigir la identificación automática del equipo que accede, evitando así la conexión desde equipo no seguro, o equipo no autorizado.

Para asegurar un nivel de seguridad legalmente establecido y dado que la confiabilidad de los datos así lo requiere, dentro de las medidas de seguridad de información, es importante la utilización de sistemas y técnicas criptográficas, por lo cual sería un valor agregado el establecimiento de un procedimiento y mecanismo que contemplen los casos en el que la información debe cifrarse.

El control de acceso para validar que los usuarios que acceden a los recursos estén autorizados es necesario al igual que el almacenamiento de evidencia de cualquier intento de acceso no

autorizado. Estos registros de acceso deberían estar protegidos ante cualquier manipulación o alteración.

6.8.1.4. Amenaza de persona (Insiders-Outsiders)

Dentro de las amenazas Insiders, se encuentra generalmente en las entidades, que el personal que trabaja con el administrador, el programador, conoce perfectamente el sistema, sus puntos fuertes y débiles, de manera que un ataque por parte de esta persona podría ser directo y difícil de detectar y mucho más efectivo que el atacante externo.

Todo el personal que tiene acceso a los sistemas que manejan información de tipo clasificada debe encontrarse autorizadas y capacitadas en el manejo de la misma evitando en parte el mal uso de los recursos, robos y fraudes entre otros.

Es de saber que con esto no se está exento de dichos riesgos, es necesaria la planificación de auditorías para realizar el seguimiento y cumplimiento.

6.8.2. Identificación de Vulnerabilidades

Hoy en día, se habla mucho sobre intentar penetrar las capas de seguridad de un sistema con el fin de demostrar que el riesgo de seguridad existe. Aunque este tipo de análisis son útiles y eficaces, tienden a requerir habilidades específicas, capacitación y experiencia en áreas que profesionales de la red por lo general no están expuestos. Por ende es muy importante tener en cuenta los reportes de análisis de riesgos anteriores, los resultados de los procesos de auditoría, los requerimientos de seguridad y los Pen-Testing o resultados de las pruebas de seguridad realizadas.

La identificación de vulnerabilidades es lo más básico que se debe tener y es preciso notar que la mayoría de personas desconocen o no les da la importancia. Este proceso debe ser cíclico y debe ser revisado con regularidad y en el cual se deben tener un derrotero o listado de potenciales vulnerabilidades como se muestra en la Tabla No. 4.

TABLA No. 4 TIPOS DE AMENAZAS - POSIBLES VULNERABILIDADES

Tipo	Amenazas	Vulnerabilidades
Hardware	Incumplimiento en el mantenimiento del sistema de información	Mantenimiento insuficiente / instalación fallida de los medios de almacenamiento
	Destrucción de equipos o medios	Ausencia de esquema de reemplazo periódico
	Polvo, corrosión, congelamiento	Susceptibilidad a la humedad, el polvo y la suciedad
	Error en el uso	Ausencia de un eficiente control de cambios en la configuración
	Perdida de suministro de energía	Susceptibilidad a las variaciones de voltaje
	Fenómenos meteorológicos	Susceptibilidad a las variaciones de temperatura
	Hurto de medios o documentos	Almacenamiento sin protección
	Hurto de medios o documentos	Falta de cuidado en la disposición final
	Hurto de medios o documentos	Copia no controlada
Software	Abuso de derechos	Ausencia de insuficiencia de pruebas de software
	Abuso de derechos	Defectos bien conocidos en el software
	Abuso de derechos	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo
	Abuso de derechos	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado
	Abuso de derechos	Ausencia de pistas de auditoria
	Abuso de derechos	Asignación errada de los derechos de acceso
	Corrupción de datos	Software ampliamente distribuido
	Corrupción de datos	En termino de tiempo utilización de datos errados en los programas de aplicación
	Error en el uso	Interfaz de usuario compleja
	Error en el uso	Ausencia de documentación
	Error en el uso	Configuración incorrecta de parámetros
	Error en el uso	Fechas incorrectas
	Falsificación de derechos	Ausencia de mecanismos de identificación y autenticación, como la autenticación de usuario
	Falsificación de derechos	Tablas de contraseñas sin protección
	Falsificación de derechos	Gestión deficiente de las contraseñas
	Procesamiento ilegal de datos	Habilitación de servicios innecesarios
	Mal funcionamiento del software	Especificaciones incompletas o no claras para los desarrolladores
	Mal funcionamiento del software	ausencia de control de cambios eficaz
	Manipulación con software	Descarga y uso no controlados de software
	Manipulación con software	Ausencia de copias de respaldo
	Hurto de medios o documentos	Ausencia de protección física de la edificación, puertas y ventanas
	Uso no autorizado del equipo	Fallas en la producción de informes de gestión
Red	Negación de acciones	Ausencia de pruebas de envió o recepción de mensajes
	Escucha encubierta	Líneas de comunicación sin protección
	Escucha encubierta	Trafico sensible sin protección

	Falla del equipo de telecomunicaciones	conexión deficiente de los cables
	Falla del equipo de telecomunicaciones	Punto único de falla
	Falsificación de derechos	Ausencia de identificación y autentificación de emisor y receptor
	Espionaje remoto	Arquitectura insegura de la red
	Espionaje remoto	Transferencia de contraseñas en claro
	Saturación del sistema de información	Gestión inadecuada de la red (tolerancia a fallas en el enrutamiento)
	Uso no autorizado del equipo	Conexiones de red pública sin protección
Personal	Incumplimiento en la disponibilidad del personal	Ausencia del personal
	Destrucción de equipos o medios	Procedimientos inadecuados de contratación
	Error en el uso	Entrenamiento insuficiente en seguridad
	Error en el uso	Uso incorrecto de software y hardware
	Error en el uso	Falta de conciencia acerca de la seguridad
	Procesamiento ilegal de datos	Ausencia de mecanismos de monitoreo
	Hurto de medios o documentos	Trabajo no supervisado del personal externo o de limpieza
	Uso no autorizado del equipo	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería
Lugar	Destrucción de equipos o medios	Uso inadecuado o descuido del control de acceso físico a las edificaciones y los recintos
	Inundación	Ubicación en un área susceptible de inundación
	Perdida de suministro de energía	Red energética inestable
	Hurto de equipo	Ausencia de protección física de la edificación, puertas y ventanas
organización	Abuso de derechos	Ausencia de procedimiento formal para el registro y retiro de usuarios
	Abuso de derechos	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso
	Abuso de derechos	Ausencia o insuficiencia de las disposiciones (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes
	Abuso de derechos	Ausencia de procedimiento de monitoreo de los recursos de procesamiento de información
	Abuso de derechos	Ausencia de auditorías (supervisiones)
	Abuso de derechos	Ausencia de procedimientos de identificación y valoración de riesgos
	Abuso de derechos	Ausencia de reportes de fallas de los registros de administradores y operadores
	Incumplimiento en el mantenimiento del sistema de información	Respuesta inadecuada de mantenimiento del servicio
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos
	Incumplimiento en el mantenimiento del sistema de información	Ausencia de procedimiento de control de cambios
	Corrupción de datos	Ausencia de procedimiento formal para el control de la documentación del SGSI
	Corrupción de datos	Ausencia de procedimiento formal para la

		supervisión del registro del SGSI
	Datos provenientes de fuentes no confiables	Ausencia de procedimiento formal para la autorización de la información disponible al publico
	Negación de acciones	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información
	Falla del equipo	Ausencia de planes de continuidad
	Error en el uso	Ausencia de políticas sobre el uso del correo electrónico
	Error en el uso	Ausencia de procedimientos para la introducción de software en los sistemas operativos
	Error en el uso	Ausencia de registros en las bitácoras (logs) del administrador y operario
	Error en el uso	Ausencia de procedimientos para el manejo de la información clasificada
	Error en el uso	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos
	Procesamiento ilegal de datos	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados
	Hurto de equipo	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información
	Hurto de equipo	Ausencia de política formal sobre la utilización de computadores portátiles
	Hurto de equipo	Ausencia de control de los activos que se encuentran fuera de las instalaciones
	Hurto de medios o documentos	Ausencia o insuficiencia de política sobre limpieza de escritorio y de pantalla
	Hurto de medios o documentos	Ausencia de autorización de los recursos de procesamiento de la información
	Hurto de medios o documentos	Ausencia de mecanismos de monitoreo establecidos para las brechas en la seguridad
	Uso no autorizado del equipo	Ausencia de revisiones regulares por parte de la gerencia
	Uso no autorizado del equipo	Ausencia de procedimientos para la presentación de informes sobre las debilidades en la seguridad
	Uso del software falso o copiado	Ausencia de procedimientos del cumplimiento de las disposiciones con los derechos intelectuales

6.8.3. Proceso de Evaluación de riesgos.

El daño resultante de un fallo de seguridad (es decir, que una amenaza explote una vulnerabilidad y se materialice en un impacto) y la posibilidad de ocurrencia del fallo dan como resultado el nivel de riesgo resultante que determina si el riesgo es aceptable (en función de los niveles definidos previamente) o requiere tratamiento.

Dentro del análisis de riesgo siempre se debe suponer que pueden ocurrir cosas negativas.

- Evaluación del impacto económico de un suceso.
- Determinación de un plan de acción para el caso de un suceso.
- Determinación de lo que se quiere proteger, donde y como, asegurando que los costos en los que se incurran se obtengan beneficios efectivos. Identificación de los recursos: (hardware, software, información, personal, accesorios etc.) con que se cuentan y a las amenazas que se están expuestos.
  En la evaluación de riesgos se debe someter a consideración, un conjunto de preguntas que nos ayudan en la identificación como son:

  1. ¿Cuál es el costo de una hora sin procesar, un día, una semana?
  2. ¿Cuánto tiempo se puede estar off-line sin que los clientes se vayan a la competencia?
  3. ¿Se tiene la forma de detectar un empleado deshonesto en el sistema?
  4. ¿Se tiene el control de las operaciones de los distintos sistemas?
  5. ¿Cuántas personas dentro de la empresa (sin considerar su honestidad), están en condiciones de inhibir el procesamiento de datos?
  6. ¿A que se llama información confidencial y/o sensitiva?
  7. ¿la información confidencial y sensitiva permanece en los sistemas?
  8. ¿la seguridad actual cubre los tipos ataques existentes y está preparada para adecuarse a los avances tecnológicos esperados?
  9. ¿A quién se le permite utilizar los recursos?
  10. ¿Quién es el propietario de los recursos? Y a ¿Quién es el usuario con mayor privilegio sobre los recursos?
  11. ¿Cuál serán los privilegios y responsabilidades del administrador vs la del usuario?
  12. ¿Cómo se actúa en la seguridad si violada?

Terminada la lista, se puede realizar el procedimiento de diagnostico mediante la siguiente tabla:

TABLA No. 5 DIAGNOSTICO DEL RIESGO

Tipos de riesgos	Factor
Robo de hardware	Alto
Robo de información	Alto
Vandalismo	Medio
Fallas en los equipos	Medio
Virus informáticos.	Medio
Equivocaciones	Medio
Acceso no autorizados	Medio
Fraudes	Bajo
Fuego	Muy bajo
Terremotos	Muy bajo

6.8.4. Análisis de Controles

La entidad debe establecer mecanismos y definir los procedimientos necesarios para realizar el monitoreo que como del control dentro del cual se encuentran como elementos de entrada los controles existentes y los planeados.

TABLA No. 6 ESTRUCTURA PARA LA DOCUMENTACIÓN DE CONTROLES APLICADA AL NUMERAL 6.1 DE LA ISO 27000:2005

Núm.	Núm.	Nombre	Justificación	Protección del servicio	Registro y auditoría	No repudiación	Control de acceso	Disponibilidad de la información	Disponibilidad del servicio	Integridad	Privacidad y confiabilidad	Políticas generales
	6.	ORGANIZACIÓN SEGURIDAD										
	6.1.	ORGANIZACIÓN INTERNA										
1	6.1.1.	Compromiso de la Dirección con la seguridad de la información.										X
2	6.1.2.	Coordinación de la seguridad.										X
3	6.1.3.	Asignación de responsabilidades.										X

4	6.1.4.	Proceso de autorización a áreas de procesamiento de información.										X
5	6.1.5.	Se realizan acuerdos de confidencialidad.										X
6	6.1.6.	Contacto con las autoridades.										X
7	6.1.7.	Contacto con grupos de interés.										X
8	6.1.8.	Se realiza auditoría interna.			x							

6.8.5. Determinación del Riesgo

Es necesario contar con el conocimiento de la entidad con respecto a la probabilidad de explotación de amenazas, la magnitud del impacto, la validez de los controles actuales y planeados y de este análisis crear una lista de vulnerabilidades potenciales para ser evaluadas. Dentro de dicha determinación del riesgo se expresan unas funciones de:

- Probabilidad de que una amenaza intente explotar una vulnerabilidad
- magnitud del impacto de la explotación resulte exitosa de la vulnerabilidad
- que los controles existentes o planeados para mitigar o reducir los riesgos sean lo suficientemente efectivos.

6.8.6. Recomendaciones de Control

La necesidad existe ya que es importante lograr el aseguramiento de nuestra entidad y el Sistema en general dentro del cual se abarcaran ciertos puntos como lo son la Administración de las comunicaciones y operaciones, los Control de accesos, la adquisición de sistemas de información, desarrollo y mantenimiento, la administración de los incidentes de seguridad, la administración de la continuidad de la entidad y entre otros el marco legal y buenas prácticas.

Los controles pueden variar dependiendo el tipo de la actividad, lo que si es necesario en toda organización es proteger el pilar más grande con que estas cuentan, el cual es la valiosa información. Dentro de la Tabla No. 7 Se pueden encaminar las acciones sobre el manejo de los activos.

TABLA No. 7 CONTROLES Y ACCIONES SOBRE EL MANEJO DE ACTIVOS

OBJETIVOS DEL CONTROL	CONTROLES	ACCIÓNES
Gestionar la seguridad de la información dentro de la organización	Compromiso por parte de la dirección	Firmar compromiso
	Proceso de Coordinación	Se debe crear y consolidar un grupo para dicha coordinación
	Asignación de responsable	Crear acto administrativo
	Autorización de recursos	Se debe asignar disponibilidad presupuestal
	Acuerdos de confidencialidad	Socialización y compromiso frente a las clausulas de confidencialidad
	Sistemas de comunicación con las autoridades y/o grupo de interés	Contactar en caso de emergencia a las autoridades competentes y contar con el apoyo y mejora y buenas prácticas de seguridad
	Análisis y revisión de la Seguridad de la Información	Realización de las auditoria internas del SGSI
Conservar y mantener la seguridad en cuanto al tratamiento de los activos e información en general.	Identificación de los riesgos en relación con terceros	Realizar el análisis de riesgos
	Tratamiento de la seguridad en relación con clientes	Realizar el debido tratamiento de riesgos
	Tratamiento de la seguridad en relación con contratos	
Alcanzar y mantener una protección adecuada de los activos de la entidad	Realización de inventario	Realizar la clasificación de los activos
	Responsables y propiedad de los activos	
	Acuerdo sobre el uso adecuado de los activos	Diseñar las clausulas para la clasificación de la información.
Alcanzar y mantener una protección adecuada de la información de la entidad	Contar con las directrices	Diseñar las guías para el inventario y clasificación de la información.
	Manipulado y etiquetado de la información	Diseñar mecanismo para el etiquetado y manipulación de la información

Sensibilizar las responsabilidades y funciones con la finalidad de reducir el riesgo de robo, fraude y mal uso de las instalaciones y medios.	Inclusión del Sistema de seguridad de la información dentro de las responsabilidades.	Además de incluir dentro del contrato una clausula se aplica en la Inducción y re-inducción la clausula de responsabilidades
	Aplicación de la política de personal y selección.	Definir bien los procedimientos para la contratación
Asegurar las responsabilidades y obligaciones para cumplir con la política de seguridad, para reducir el riesgo asociado a los errores humanos.	Responsabilidad y supervisión por la dirección.	Se debe contar con la supervisión relacionada con la contratación.
	Sensibilización y formación en el área de Seguridad de la información.	Implementar estrategia para la sensibilización y divulgación.
	Con respecto al proceso disciplinario	Contar con los procesos disciplinarios bien definidos
Garantizar a las personas que abandonan la institución o cambian de empleo de manera organizada.	Responsabilidad de cese al cambio	Contar con los procesos bien definidos cuando se presenten transadlos.
	Devolución de Activos	Contar con actividades que reflejen que se debe hacer para la devolución de Activos.

6.8.7. Documentación de Resultados

Este punto es muy importante ya que por medio de dicha documentación proporcionara la base o apoyo en la elaboración del reporte de valoración del riesgo. Dentro de esta documentación se debe registrar el porcentaje de riesgos identificados evaluados como su tipo de importancia ya sea; alta, media o baja, más los no evaluados.

6.9. DOCUMENTACIÓN REQUERIDA PARA LA IMPLEMENTACIÓN DEL SGSI

Es importante tener bien claro cuál es la documentación necesaria para la implementación de un Sistema de Gestión de Seguridad de la Información, se requiere un respaldo documentado donde se deben incluir los Manuales de Seguridad, procedimientos, formatos y los registros que contribuyen a la provisión de servicios confiables a partir de unos procesos con los que se pueda crear, distribuir y manipular información electrónica masiva, protegiendo de esta manera la información del cliente y a su vez permita a la organización servir de apoyo en la toma de decisiones de una manera más asertiva.

La estructura de la Documentación **-** Debe ser clara, precisa, entendible y acorde con su alcance y política del Sistema de Gestión de Seguridad de la Información de la empresa.

6.9.1. Documentos de nivel 1 (Manual de Seguridad)

Este es el documento que inspira y enmarca el sistema, expone y especifica las intenciones, alcance, objetivos, responsabilidades, políticas y directrices principales. Se podría decir que es un análogo al manual de calidad.

6.9.2. Documentos de nivel 2 (Procedimientos)

Son la estandarización de los procesos operativos que aseguran el cumplimiento de la planificación, operación y control de los procesos de seguridad de la información de una forma eficaz.

6.9.3. Documentos de nivel 3 (Formularios)

También conocidos como checklist o instrucciones los cuales describen las tareas y actividades específicas relacionadas con la seguridad de la información.

6.9.4. Documentos de nivel 4 (Registros)

Documentos que proporcionan evidencia del cumplimiento de los requisitos, están asociados a documentos de los otros niveles como elemento de salida que demuestra el cumplimiento de lo que se estipula en los mismos.

6.9.5. Control de documentos

Para todos los documentos que se generen en el SGSI se debe establecer, documentar, implementar y mantener un procedimiento que defina cuales es la gestión para: aprobar

documentos, revisar y actualiza documentos, garantizar la identificación de los cambios y el estado actual de revisión de los documentos, la vigencia de los documentos y la disponibilidad para el lugar donde se utiliza, garantizar que los documentos se mantengan legibles y fácilmente identificables, el control de la distribución de los documentos, prevenir el uso de los documentos obsoletos e identificar los documentos que son retenidos. Se deben establecer y mantener registros para brindar evidencia de la conformidad con los requisitos y la operación eficaz del SGSI.

7. ANÁLISIS DE LA SITUACIÓN ACTUAL DEL INSTITUTO NACIONAL DE FORMACIÓN TÉCNICA PROFESIONAL DE LA GUAJIRA

7.1. Reseña Institucional[15]

La INSTITUCIÓN EDUCATIVA, fue Creada por el Gobierno Nacional mediante decreto Nº 1098 del día 17 de marzo de 1979, con el nombre de Instituto de Carreras Intermedias Profesionales INCIP de San Juan del Cesar, La Guajira facultado para abrir tres programas académicos: administración de la producción agrícola, administración de la producción pecuaria y minería.

El 21 de julio de 1980 comienza la vida académica de los dos primeros programas con 19 estudiantes en administración de producción agrícola y 23 en el de producción pecuaria, la docencia estuvo a cargo por 10 catedráticos para los dos programas; el objetivo fundamental era formar técnicos en estas actividades en el sur del departamento de La Guajira, para lo cual se recibió el apoyo del ICFES, entidad que le concedió licencia de funcionamiento mediante acuerdo Nº 090 del 14 de abril de 1981 y secuencialmente aprobado por las resoluciones Nos.1992 del 1 de diciembre de 1982, 1235 del 4 de julio de 1983, 00972 del 13 de junio de 1987 y 001301 de julio de 1987.

El 21 de agosto de 1984 el Ministerio De Educación Nacional mediante el decreto 2011 eleva al instituto a la categoría de unidad docente, la ley 25 de 1987 reforma al decreto 80 de 1980 y cambia la modalidad de formación intermedia profesional por educación técnica profesional, quedando el nombre de Instituto Nacional De Educación Técnica Profesional INETEP.

El Gobierno Nacional en desarrollo de las facultades extraordinarias concedidas por la ley 24 de 1988, expide el decreto 758 del 26 de abril de 1988, a través del cual se denomina a este establecimiento Instituto Nacional de Formación Técnica Profesional de San Juan Del Cesar, Guajira, INFOTEP, organizándolo como establecimiento público de carácter académico, con autonomía administrativa y patrimonio independiente, adscrito al Ministerio de Educación Nacional.

[15] INFOTEP. (2014) Reseña histórica. Recuperado de: http://infotep.edu.co/images/pdf/resena_historica_infotep.pdf

En la actualidad el Instituto Nacional de Formación Técnica Profesional de San Juan del Cesar, La Guajira, INFOTEP se encuentra certificado bajo la ISO 9001 y NTCGP1000 con miras en el mantenimiento y la mejora continua del Sistema aportando un servicio de calidad el cual responde a las necesidades de la comunidad.

7.2. Determinación de la Estratificación de la entidad

Es necesario definir una estratificación, para identificar el nivel de responsabilidad de la institución en cuanto a la seguridad de la información.

Presupuesto, la institución pertenece al rango 2 ya que se encuentra dentro de los 3.000 millones y 50.000 millones de pesos establecidos, el cual para la vigencia del año 2014 es de la suma de $5.238.049.243=

Número total de Computadores, la institución pertenece al rango 2 ya que se encuentra dentro de los 100 y 500 computadores, con un total de 280.

Número de Servidores, la institución pertenece al rango 1 ya que se clasifica en este cuando son menos de cuatro Servidores y en la entidad cuentan con 3 Servidores
Vale la pena reconocer que dichos servidores pueden estar en hosting externo o en las instalaciones en la entidad.

Número de Empleados de Sistemas (tecnología), La institución pertenece al rango 1 ya que se clasifica en este cuando son menos de 6 empleados

Existencia y función del área de sistemas (tecnología), La institución pertenece al rango 1 ya que existe un área de sistemas o tecnología, enfocada en la operación del día a día, que cumple labores en su mayoría REACTIVAS

Existencia y objeto de la WAN, La institución pertenece al rango 1 ya que solo es utilizada para acceder a los correos y navegar.

Transaccionalidad en la WEB, La institución pertenece al rango 3 ya que se utilizada para ofrecer servicios de consulta, Transaccionalidad local. Generación de servicios y seguimiento de trámites, con base en datos, aplicativos propios y servicios de otras entidades y/o terceros.

Desarrollo de Software, La institución pertenece al rango 1 porque no desarrolla software. Incluye aquellas entidades que tienen en hosting una página WEB básica e informativa y un servidor de correo

TABLA No. 8 NIVEL DE ESTRATIFICACIÓN DEL INFOTEP

Presupuesto en Millones de Pesos	Existencia y función del Área de sistemas	No. PC's	No. Servidores	Existencia y Objeto de la WAN	Transaccionalidad en la WEB	Desarrollo de Software	No. Empleados de Sistemas
5.238.049.243	Reactivas	280	3	Wan Publica	Transaccionalidad e interoperabilidad	No. Incluye hosting básico de WEB y correo	1
2	**1**	**2**	**1**	**1**	**3**	**1**	**1**

TOTAL Puntos: 12

Estrato asignado: MEDIO

Esta clasificación que se ve reflejada en le tabla No 8, representa el nivel Medio que está íntimamente ligado a las responsabilidades y requerimientos tecnológicos que deberá cumplir la entidad en cuanto a seguridad de la información.

7.3. Autoevaluación sobre la estructura organizacional del INFOTEP

Inicialmente se realiza el proceso de autoevaluación el cual permitirá determinar el nivel de integración y relevancia a la seguridad de la información institucional, este proceso de autoevaluación se aplica por medio de encuesta que refleja sus resultados en la tabla No 9.

TABLA No. 9 ENCUESTA DE PRE REQUISITOS APLICADOS EN EL INFOTEP

Requisito	CUMPLE	
	SI	NO
La entidad cuenta con un líder de Gobierno en línea (líder GEL)	X	
La entidad cuenta con el comité de seguridad de Gobierno en línea.	X	
La entidad cuenta con el oficial de seguridad.	X	
La entidad cuenta con personal técnico para realizar las tareas de la seguridad de la información.		X
La entidad cuenta con una integración con otros sistemas de gestión.	X	
La entidad cuenta con apoyo y participación de planeación.	X	
La entidad cuenta con apoyo y participación de control interno.	X	
Los funcionarios conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad	X	
Los proveedores conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad		X
Los ciudadanos conocen sus responsabilidades con respecto a la iniciativa de seguridad de la información de la entidad		X

Se refleja la falta de recurso humano para las labores de seguridad de la información "SI", al igual que socializar a algunos grupos de interés como proveedores y ciudadanos sobre las responsabilidades que tienen con respecto a la iniciativa de SI.

7.4. Autoevaluación del nivel de gestión de seguridad de la información del INFOTEP.

Es necesario realizar un análisis para determinar el estado en que se encuentra la entidad e identificar las brechas o vacios que están presentes dentro de la organización para lo cual se aplica la encuesta que se refleja dentro de la tabla No 10.

TABLA No. 10 ENCUESTA PARA LA EVALUACIÓN DEL NIVEL DE SEGURIDAD DEL INFOTEP

NIVEL	REQUISITO	CUMPLE	
		SI	NO
Plan de Seguridad Nivel Inicial	La entidad debe definir una política de seguridad que garantice la protección de la información, los datos personales y los activos de información con que cuenta. Para ello, deberá implementar las siguientes acciones:		
	Definir la política de seguridad a ser implementada	**X**	
	Divulgar la política de seguridad al interior de la misma	**X**	
	Conformar un comité de seguridad o asignar las funciones de seguridad al comité GEL		**X**
	Identificar los activos de información en los procesos, incluyendo los activos documentales (records), de acuerdo con el análisis de procesos realizado		**X**
	Identificar los riesgos y su evaluación, en dichos procesos		**X**
	Definir el plan de acción con los controles y políticas que se implementarán para mitigar los riesgos identificados		**X**
Plan de Seguridad Nivel básico	Con base en el análisis de procesos realizado en el nivel inicial y la política o plan de seguridad definido, la entidad inicia la ejecución de dicho plan de seguridad para implementar los controles que mitigarán los riesgos identificados, lo cual implica que la entidad presenta avances en la implementación de tales controles.		**X**
	De acuerdo con el plan de capacitación definido por la entidad en el nivel inicial, esta ejecuta las acciones de capacitación en seguridad, con los responsables de los controles y procesos con los cuales se inicia la ejecución del plan.		**X**
	La entidad inicia la documentación de políticas y procedimientos de seguridad, de acuerdo con el plan definido.		**X**
Plan de Seguridad Nivel avanzado	La entidad culmina la implementación de controles definidos en el nivel inicial		**X**
	La entidad documenta la totalidad de políticas y procedimientos de seguridad		**X**
	La entidad ejecuta las actividades de capacitación en temas de seguridad, con todos los servidores públicos		**X**

	La entidad define el plan de verificación periódica de los controles, procedimientos y políticas de seguridad		**X**
	La entidad reporta los avances del cumplimiento del plan		**X**
Plan de Seguridad Nivel de mejoramiento permanente	La entidad refuerza la divulgación de las políticas de seguridad		**X**
	La entidad ejecuta los procedimientos y políticas de seguridad, de manera repetitiva		**X**
	La entidad realiza la revisión periódica interna de los riesgos inicialmente detectados, políticas, procedimientos y controles		**X**
	La entidad evalúa sus políticas de seguridad e implementa acciones para mejorarlas		**X**

Como resultado de la encuesta se puede observar que la institución se encuentra aplicando un 33% sobre el nivel inicial de la Seguridad de la Información.

7.5. Autoevaluación de Políticas y Controles del INFOTEP.

Para la determinación sobre el nivel del proceso de implementación de controles en términos de políticas, y métricas con las cuales cuenta la entidad se aplico el Anexo A del estándar ISO 27001 y el cual se representa en la tabla No 11.

TABLA No. 11 EVALUACIÓN DE CONTROLES DEL INFOTEP

Aplicación : **A=** aplicado	**P =** por aplicar	
Razones de selección :	**RL=** Requisitos legales	**OC=** Obligaciones contractuales
	RN/MP= requisitos del negocio, adoptado de mejores practicas	**RAR=** Resultado de análisis de riesgos

CONTROLES	APLICACIÓN	JUSTIFICACIÓN PARA EXCLUSIÓN	Controles Seleccionados y Razones de su selección	OBSERVACIONES DE LA IMPLEMENTACIÓN

					RL	OC	RN/MP	RAR	
Clausula	**Numeral**	**Objetivos de Control /Controles**							
POLÍTICA DE SEGURIDAD	5,1	Política de seguridad de la información.							
	5.1.1	Documento de la política de seguridad de la información	A				N	N	Documento de política
	5.1.2	Revisión de la política de seguridad de la información	P				N	N	Plan de revisión
ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	6,1	Organización interna							
	6.1.1	Compromiso de la dirección con la seguridad de la información	P				N	N	No existe un plan de proyecto
	6.1.2	Coordinación de la seguridad de la información	P				N	N	No existe el Comité
	6.1.3	Asignación de responsabilidades para la seguridad de la información	A				N	N	Los responsables de procesos y activos pero no está documentado
	6.1.4	Proceso de autorización para los servicios de procesamiento de información	P					N	No está creado el procedimiento
	6.1.5	Acuerdos sobre confidencialidad	P		N			N	No existe la política y acuerdos confidencialidad
	6.1.6	Contacto con las autoridades	P		N		N		No existe procedimiento para el reporte de incidentes
	6.1.7	Contacto con grupos de interés especiales	A				N	N	Foros – grupos
	6.1.8	Revisión independiente de la seguridad de la información	P				N	N	No existe un programa de auditoria
	6,2	Partes Externas							

	6.2.1	Identificación de los riesgos relacionados con las partes externas	P		N	N		N	No existe una lista de contratistas – servicios y tipos de acceso
	6.2.2	Abordaje de la seguridad cuando se trata con los clientes	P		N	N		N	No está establecida una política y acuerdos - Derechos de Propiedad intelectual (DPI)
	6.2.3	Abordaje de la seguridad en los acuerdos con terceras partes	P		N	N		N	No se encuentra establecida la política y acuerdos DPI, confidencialidad
GESTIÓN DE ACTIVOS	7,1	Responsabilidad por los activos							
	7.1.1	Inventario de activos	P				N	N	No se encuentra documentado
	7.1.2	Propietario de los activos	P				N	N	No se encuentra documentado
	7.1.3	Uso aceptable de los activos	A				N	N	Se encuentra establecido dentro de la política de Sistemas & Comunicación.
	7,2	Clasificación de la información							
	7.2.1	Directrices de Clasificación	P				N	N	No existe la Política o document

									o
	7.2.2	Etiquetado y manejo de la información	P				N	N	No se ha creado el procedimiento
SEGURIDAD LIGADA A LOS RR.HH	8,1	Antes de la contratación laboral							
	8.1.1	Roles y responsabilidades	P			N		N	No está establecido un documento
	8.1.2	Selección	A		N	N		N	Esta soportado en el manual de Procedimiento
	8.1.3	Términos y condiciones laborales	A		N	N		N	Establecido dentro del Manual de funciones
	8,2	Durante la vigencia del contrato laboral							
	8.2.1	Responsabilidades de la dirección	A		N			N	Se encuentra establecido
	8.2.2	Educación, formación y concientización sobre la seguridad de la información	A				N	N	Esta soportado en el manual de Procedimiento
	8.2.3	Proceso disciplinario	A		N	N		N	Esta soportado en el manual de Procedimiento
	8,3	Terminación o cambio de la contratación laboral							
	8.3.1	Responsabilidades en la terminación	A		N	N			Esta soportado en el manual de Procedimiento

	8.3.2	Devolución de activos	A			N			No está documentado el procedimiento
	8.3.3	Retiro de los derechos de acceso	P			N			No está documentado el procedimiento
SEGURIDAD FÍSICA Y DEL ENTORNO	9,1	Áreas seguras							
	9.1.1	Perímetro de Seguridad física	P	existen controles		N		N	No se encuentra documentado
	9.1.2	Controles de acceso **físico**	P	existen controles		N	N	N	No se encuentra documentado
	9.1.3	Seguridad de oficinas, recintos e instalaciones	P	existen controles	N	N		N	No se encuentra documentado
	9.1.4	Protección contra amenazas externas y ambientales	P	existen controles				N	No se encuentra documentado
	9.1.5	Trabajo en áreas seguras	P	existen controles	N		N	N	No se encuentra documentado
	9.1.6	Áreas de carga, despacho y acceso publico	P	existen controles			N	N	No se encuentra documentado
	9,2	Seguridad de los equipos							
	9.2.1	Ubicación y protección de los equipos	P	existen controles				N	Política / normas
	9.2.2	Servicios de suministro	P	existen controles				N	Registro – servicios
	9.2.3	Seguridad del **cableado**	A			N		N	Soportando en la política de Sistemas
	9.2.4	Mantenimiento de los equipos	A	existen contro		N	N	N	Soportado en el plan de

				les					mantenimiento y registros
	9.2.5	Seguridad de los equipos fuera de las instalaciones	P					N	No existe un procedimiento definido
	9.2.6	Seguridad en la reutilización o **eliminación** de los equipos	P		N		N	N	No existe un procedimiento definido
	9.2.7	Retiro de activos	A	existen controles			N	N	Esta soportado en el manual de Procedimiento y registros
GESTIÓN DE COMUNICACIONES Y OPERACIONES	10,1	Procedimientos operacionales y Responsabilidades							
	10.1.1	Documentación de los procedimientos de operación	A					N	Soportan en procedimientos y registros
	10.1.2	Gestión del cambio	P				N	N	No está documentado dentro del procedimiento
	10.1.3	Distribución (segregación) de funciones	A				N		Se encuentra establecido procedimiento
	10.1.4	Separación de las instalaciones de desarrollo, ensayo y operación	P				N	N	No existe norma ni procedimiento
	10,2	Gestión de la prestación de servicios por terceras partes							
	10.2.1	Prestación del servicio	P				N	N	No hay nada documentado
	10.2.2	Monitoreo y revisión de los servicios por terceros	P				N	N	No existe un

									procedimiento para las interventorias y supervisiones
	10.2.3	Gestión de los cambios en los servicios por terceras partes	P				N	N	No existe un procedimiento
	10,3	A.10.3. Planificación y aceptación del sistema							
	10.3.1	Gestión de la capacidad	P				N	N	No hay Planificación – mejoras – proyección
	10.3.2	Aceptación del sistema	P				N	N	Criterios calidad – normas
	10,4	Protección contra código malicioso y descargable							
	10.4.1	Controles contra códigos maliciosos	P				N	N	Falta de procedimiento
	10.4.2	Controles contra códigos móviles	P				N	N	Carencia de Política / normas
	10,5	Respaldo							
	10.5.1	Respaldo de la información	A	existen controles			N	N	Existe un procedimiento y política
	10,6	Gestión de la seguridad de las redes							
	10.6.1	Controles de las redes	P				N	N	Falta de procedimiento y política
	10.6.2	Seguridad de los servicios de la red	P				N	N	Falta de procedimiento y política
	10,7	Manejo de los medios							
	10.7.1	Gestión de los medios removibles	P				N	N	Falta de procedimiento
	10.7.2	Eliminación de los medios – destrucción, disposición de equipos	P		N		N	N	Falta de procedimiento
	10.7.3	Procedimientos para el manejo de la información	A	existen contro	N		N	N	Existe un procedimiento y

			les					políticas
10.7.4	Seguridad de la documentación del sistema	P				N	N	Falta de Política o Norma
10,8	Intercambio de información							
10.8.1	Políticas y **procedimientos** para el Intercambio de información	P		N	N	N		No está establecido un Procedimiento y política
10.8.2	Acuerdos para el Intercambio	A	existen controles	N		N		Existen acuerdos
10.8.3	Medios físicos en transito	P				N		No existen Normas
10.8.4	Mensajería electrónica	P		N		N		No existen Normas
10.8.5	Sistemas de información de negocio	P				N		Falta de Procedimiento y política
10,9	Servicios de comercio electrónico							
10.9.1	Comercio electrónico	P						Normas – registros
10.9.2	Transacciones en línea	P						Normas – registros
10.9.3	Información disponible al publico	P		N		N		Procedimiento y política
10,10	Monitoreo							
10.10.1	Registro de auditorias	P		N		N		Falta de aplicación de Normas – registros
10.10.2	Monitoreo del uso del sistema	P				N	N	Falta de procedimiento
10.10.3	Protección de la información del registro	P				N		Falta de registro
10.10.4	Registros del administrador y del operador	P				N	N	Falta de registro
10.10.5	Registro de fallas	P				N	N	Falta de registro
10.10.6	Sincronización de relojes	P				N		Establecimiento de Procedimiento y política

CONTROL DE ACCESO	11,1	Requisitos de negocio para el control de acceso							
	11.1.1	Políticas de control de acceso	P		N		N	N	No está documentada la Política
	11,2	Gestión de acceso de usuario							
	11.2.1	Registro de usuarios	P				N	N	No existe un Procedimiento – política
	11.2.2	Gestión de privilegios	P				N	N	No existe un Procedimiento – política
	11.2.3	Gestión de contraseñas para usuarios	P				N	N	No existe un Procedimiento – política
	11.2.4	Revisión de los derechos de acceso de los usuarios	P				N	N	No existe un Procedimiento – política
	11,3	Responsabilidades de los usuarios							
	11.3.1	Uso de contraseñas	P				N	N	No existe un Procedimiento – política
	11.3.2	Equipo de usuario desatendido	P				N	N	No existe un Procedimiento – política
	11.3.3	Política de escritorio despejado y de pantalla despejada	A				N	N	Está documentado en la política de Sistemas
	11,4	Control de acceso a las **redes**							
	11.4.1	Política de uso de los servicios en red	A				N	N	Se evidencia en las políticas de sistemas
	11.4.2	autenticación de usuarios para conexiones externas	P				N	N	No están document

									ado
	11.4.3	Identificación de los equipos en las redes	A	existen controles			N	N	Registro – pruebas
	11.4.4	Protección de los puertos de configuración y diagnostico remoto	P				N	N	No existe un procedimiento, Registro o pruebas
	11.4.5	Separación en las redes	A	existen controles			N	N	Por medio de Servidor
	11.4.6	Control de conexión a las redes	A	existen controles			N	N	Por medio de Servidor
	11.4.7	Control de enrutamiento en la red	P	existen controles			N	N	Por medio de Servidor
	11,5	Control de acceso al sistema operativo							
	11.5.1	Procedimientos de registro de inicio seguro	A	existen controles			N	N	No está documentado
	11.5.2	Identificación y autenticación de usuarios	A	existen controles			N	N	No están documentadas las normas
	11.5.3	Sistema de gestión de contraseñas	A	existen controles			N	N	Registro – pruebas
	11.5.4	Uso de las utilidades del sistema	A	existen controles			N	N	Registro – pruebas
	11.5.5	Tiempo de inactividad de la sesión	A	existen controles			N	N	monitoreo
	11.5.6	Limitación del tiempo de conexión	A	existen controles			N	N	control
	11,6	Control de acceso a las aplicaciones y a la información							
	11.6.1	Restricción del acceso a la información	P	existen controles			N	N	No existe un Procedimiento –

									política
	11.6.2	Aislamiento de sistemas sensibles	P	existen controles			N	N	No existe un Procedimiento – política
	11,7	Computación móvil y trabajo remoto							
	11.7.1	Computación y comunicaciones móviles	P	existen controles			N	N	No existe una Política
	11.7.2	Trabajo remoto	P				N	N	No existe un Procedimiento – política
ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN	12,1	Requisitos de seguridad de los sistemas de información							
	12.1.1	Análisis y especificaciones de los Requisitos de seguridad	P				N	N	No existe procedimiento
	12,2	Procesamiento correcto en las aplicaciones							
	12.2.1	Validación de los datos de entrada	P				N	N	No existe procedimiento
	12.2.2	Control de procesamiento interno	P				N		No existe procedimiento
	12.2.3	Integridad del mensaje	P				N		No existe documento - registro
	12.2.4	Validación de los datos de salida	P				N		No existe procedimiento
	12,3	Controles criptográficos							
	12.3.1	Política sobre el uso de controles criptográficos	P				N	N	No cuenta con esta Política
	12.3.2	Gestión de claves	P				N	N	No hay Registro – auditoria
	12,4	Seguridad de los archivos del sistema							
	12.4.1	Control del software operativo	P				N	N	Procedimiento y política
	12.4.2	Protección de los datos de prueba del sistema	P				N	N	Procedimiento
	12.4.3	Control de acceso al código fuente de los programas	P				N	N	Procedimiento

	12,5	Seguridad en los procesos de desarrollo y soporte							
	12.5.1	Procedimientos de control de cambios	P				N	N	No existe un Procedimiento
	12.5.2	Revisión técnica de las aplicaciones después de los cambios en el sistema operativo	P				N	N	No existe un Procedimiento
	12.5.3	Restricciones en los cambios a los paquetes de software	P				N	N	No existe un Procedimiento y/o registro
	12.5.4	Fuga de información	P				N	N	Hace falta Monitoreo
	12.5.5	Desarrollo de software contratado externamente	P				N	N	No hay acuerdos, convenios, DPI
	12,6	Gestión de la vulnerabilidad técnica							
	12.6.1	Control de las vulnerabilidades técnicas	P				N	N	No existe un Procedimiento
GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	13,1	Notificación de eventos y debilidades de la Seguridad de la Información							
	13.1.1	Reportes sobre los eventos de seguridad de la información	P	existen controles			N		No existe un Procedimiento - política
	13.1.2	Reportes sobre las debilidades en la seguridad, Establecimiento	P	existen controles			N		No existe un Procedimiento - política
	13,2	Gestión de incidentes de seguridad de la información y mejoras							
	13.2.1	Responsabilidades y procedimientos	P				N		No existe un Procedimiento
	13.2.2	Aprendizaje debido a los incidentes de seguridad de la información	P				N		No se hace monitoreo
	13.2.3	Recolección de evidencias	P				N		No hay Registro – auditoria

GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO – GCN	14,1	Aspectos de la seguridad de la información en la GCN							
	14.1.1	Inclusión de la seguridad de la información en el proceso de GCN	P				N		No se encuentra documentado
	14.1.2	Continuidad del negocio y evaluación de riesgos	P				N		No se encuentra documentado
	14.1.3	Desarrollo e implementación de planes de continuidad que incluyan la seguridad de la información.	P				N		No se encuentra documentado
	14.1.4	Estructura para la planificación de la continuidad del negocio	P				N		No se encuentra documentado
	14.1.5	Pruebas, mantenimiento y reevaluación de los planes de continuidad del negocio	P				N		No existen registros
CUMPLIMIENTO	15,1	Cumplimiento de los requisitos **legales**							
	15.1.1	Identificación de la legislación aplicable	P		N		N		No está actualizado el normograma
	15.1.2	Derechos de propiedad intelectual (DPI)	P		N			N	No existe la Política – procedimiento
	15.1.3	Protección de los registros de la organización	P		N			N	No hay controles
	15.1.4	Protección de los datos y privacidad de la información personal	P		N			N	No existe la Política
	15.1.5	Prevención del uso inadecuado de los servicios de procesamiento de información	P		N				No existe la Política – procedimiento
	15.1.6	Reglamentación de los controles criptográficos	P		N				No se encuentra documentado ni hay controles
	15,2	Cumplimiento de las políticas y normas de seguridad y cumplimiento técnico							
	15.2.1	Cumplimiento con las políticas y las normas de seguridad	P				N	N	No existe Procedimi

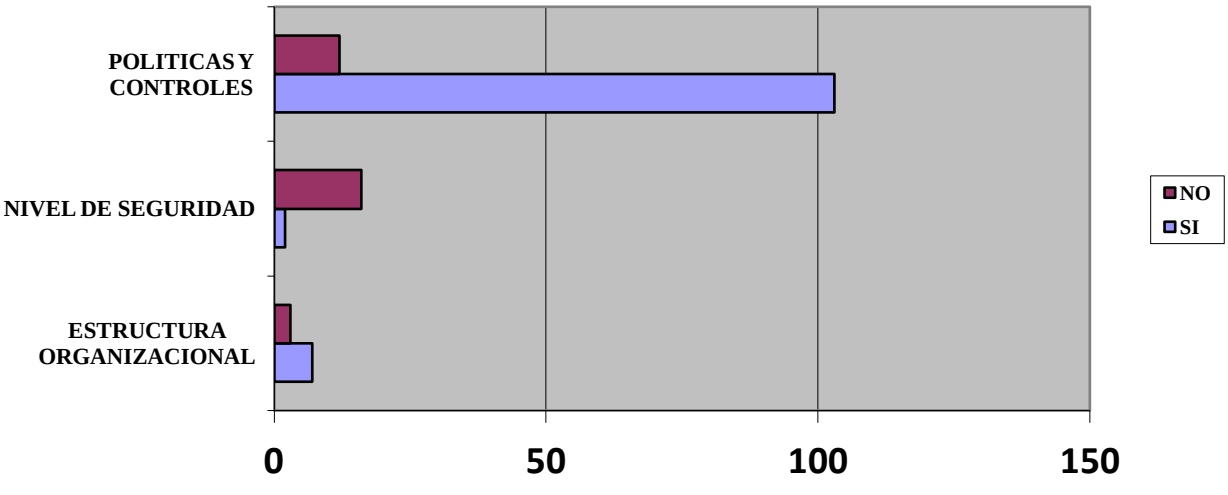
									ento y monitoreo
	15.2.2	verificación del cumplimiento técnico	P				N		No hay registro y monitoreo
	15,3	Consideraciones de la auditoría de los sistemas de información							
	15.3.1	Controles de auditoría de los sistemas de Información	P				N		No se cuenta con el Procedimiento
	15.3.2	Protección de las herramientas de auditoría de los sistemas de información	P		N		N		No existe control

8. ANÁLISIS Y DISCUSIÓN DE RESULTADOS

8.1. Resultados de la investigación

Como se puede observar dentro de la Autoevaluación, Encuesta y Evaluación aplicadas, el Instituto Nacional de Formación Técnica Profesional de la Guajira, muestra una ausencia parcial dentro de la estructura Organizacional pero es muy prominente la falta de requisitos dentro del nivel de seguridad, políticas y controles tal como se puede observar dentro de la figura 6.

Figura 6. Definición de brecha



	ESTRUCTURA ORGANIZACIONAL	NIVEL DE SEGURIDAD	POLITICAS Y CONTROLES
NO	3	16	12
SI	7	2	103

Como resultado de lo anterior basados en el modelo SASIGEL, se determina que el ***nivel de madurez es inicial***, por lo cual la entidad debe enfocar sus esfuerzos asía la fase planear de dicho modelo en caso de que desee realizar la Implementación del Sistema de Gestión de Seguridad de la Información.

El INFOTEP cuenta con las políticas sobre la seguridad de la información pero no es integral ay que debe incluir por lo menos; su definición, objetivos generales, alcance, Importancia, declaración de intención, referencias a documentos de soporte, responsabilidades, explicación sobre las normas y leyes: requisitos legales-contractuales, formación, Gestión de Continuidad de Negocio y las consecuencias de violación entre otras.

La institución carece del Plan para la revisión periódica de las políticas, Plan de capacitación, tendencias amenazas, incidentes, al igual que la relevante necesidad de creación del comité coordinador de seguridad.

.

8.2. Análisis Sobre los Resultados

8.2.1. Análisis General

Partiendo de los resultados obtenidos dentro de la investigación en cuanto a los prerrequisitos es fundamental que la institución cuente con el talento humano necesario para apoyar las labores de Seguridad, por otra parte en fundamental divulgar que existe una responsabilidad de todos los grupos de interés con respecto a la iniciativa de seguridad de la información.

Centrándonos ahora en los resultados obtenidos para contar con el nivel básico de Seguridad de la Información según lo contempla el SASIGEL la institución debe crear el Comité de Seguridad y a su vez asignar las debidas funciones, realizar el levantamiento de los activos de información por procesos, incluir los activos documentales e identificar los riesgos con su respectiva evaluación.

Es necesario que se defina un plan de acción con los controles y políticas para minimizar los riesgos identificados, con base en el análisis de procesos realizado en el nivel inicial y la política o plan de seguridad definido, la entidad inicia la ejecución de dicho plan de seguridad para implementar los controles que mitigarán los riesgos identificados, lo cual implica que la entidad presente avances en la implementación de tales controles.

Se debe establecer un plan de capacitación en el nivel inicial, por medio del cual se deben ejecutar las acciones de capacitación en seguridad, con los responsables de los controles y procesos con los cuales se inicia la ejecución del plan para final mente iniciar la documentación de políticas y procedimientos de seguridad, de acuerdo con el plan definido.

A pesar de que existe la política de seguridad de la información la cual es llamada dentro de la institución como "Política de Sistemas y Comunicación" es necesario que sea integral que reúna las características de concisa, fácil lectura, comprensión, flexible y fácil de hacer cumplir para todos aquellos dentro del alcance sin excepción.

8.2.2. Análisis de Seguridad según los dominio de la Norma ISO/ IEC 27002:2005

Para proporcionar una visión de situación actual de la seguridad en el INFOTEP, se realiza un análisis que mostró el nivel de seguridad y cómo la entidad ha venido salvaguardando sus activos de información.

Como resultado de la evaluación de los controles, se evidenció la necesidad de mantener la confidencialidad, integridad y disponibilidad de la información corporativa especialmente la clasificada como crítica y la información personal e implementar políticas para que los funcionarios actúen de acuerdo a las normas establecidas y aceptadas por todos.

A continuación se detallan los 11 Dominios, 39 objetivos de control y la evaluación en cada caso.

Dominio -5: POLITICA DE SEGURIDAD.

Objetivo 5.1. Política de seguridad de la información.

Se debe definir una Política de Seguridad, que se debe revisar y completar por parte del comité de seguridad y aprobar por parte de la Dirección.

Dominio -6: ORGANIZACION DE LA SEGURIDAD DE LA INFORMACION

Objetivo 6.1. Organización interna.

Los directivos tienen plena conciencia de la importancia de la seguridad en la entidad, pero no conocen los requisitos de un Sistema de Gestión de la Seguridad de la Información. Se deben programar otras capacitaciones sobre conceptos de seguridad desde el punto de vista legal, de las amenazas y organizacional.

Designar un Responsable de la seguridad de la información por medio de resolución y en el cargo de Oficial de Seguridad y esto con el fin de dar inicio a la fase de establecimiento del SGSI.

Elaborar el proceso de autorización de recursos y servicios para tratamiento de la información, el cual puede ser realizado complementando la Solicitud de Bienes y Servicios pero cuando sea para recursos tecnológicos debe llevar uso y propósito de los recursos, un campo

checklist que indique que el hardware y el software son compatibles con los demás componentes del sistema y finalmente la aprobación del Jefe de Seguridad de la Información.

Asignar a un responsable para cualquier nuevo servicio a implementar, además incluir la definición de las características de la información, tales como clasificación y definición de los diferentes niveles de acceso por usuario.

Hay algunos contratistas que usan sus equipos propios, es decir portátiles para uso corporativo por lo que re requiere implementar controles de esta información o firmar acuerdos sobre su manejo y entrega a la entidad al finalizar contrato.

Ni los funcionarios ni los contratistas han firmado acuerdos de confidencialidad: Todos los empleados del INFOTEP, contratistas, proveedores y terceros, que deban realizar labores dentro de INFOTEP, ya sea por medios lógicos o físicos que involucren el manejo de información, deben conocer, entender, firmar y aceptar el correspondiente acuerdo de confidencialidad de la información, para empleados y terceros.

Las políticas de seguridad de la información, normas, controles, estándares, formatos y procedimientos, deben ser revisados periódica y planificadamente, por un área independiente de sistemas dentro de INFOTEP o por un organismo consultor externo.

Este periodo debe ser de al menos una vez al año o cada vez que ocurra un cambio sustancial en la legislación colombiana, infraestructura o activos de información de la Institución.

Objetivo 6.2. Partes externas

Los acuerdos con terceros no están establecidos aunque existen desarrollos de aplicaciones, servicio de mantenimiento y otros servicios con empresas y personas naturales.

No se reportan los incidentes de seguridad y no existe procedimiento para contactar con las autoridades.

Dominio -7: GESTION DE ACTIVOS

Objetivo 7.1. Responsabilidad por los activos.

Durante el 2014 se mantuvo en la oficina de compras y mantenimiento el inventario de equipos pero hay carencia de inventario de software instalado, mapa de la red organizada por grupo con direcciones IP, Mac y grupos de trabajo, No se cuenta con un plano o topología de red para la ubicación física de equipos y red. También hay desorganización de información de

funcionarios responsables de los equipos. Durante el 2014 la gestión de los servicios de mantenimiento, actualización de la información de Hardware y software de los equipos quedo en la dependencia de compras y mantenimiento.

Vale la pera resaltar que en este momento se está realizando la tarea de clasificación de la información, los instaladores de las aplicaciones utilizadas en la empresa se encuentran en sus CD´s originales en la dependencia de compras y mantenimiento.

Los funcionarios tienen asignadas responsabilidad sobre los activos que tienen a su cargo pero no se lleva un proceso formal de autorización para el procesamiento de la información, ni se tienen identificados los usos adecuados de los activos.

Con esta política se definirán las reglas para uso de internet, e-mail y dispositivos móviles.

El software financiero es el SIIF que cumple la Misión de permitir la gestión estandarizada de los recursos financieros, proporcionando información confiable al Estado Colombiano para la toma de decisiones[16], La base de datos de esta aplicativo reposa en los servidores del Ministerio de Hacienda.

Objetivo 7.2. Clasificación de la información.

La clasificación de la información no se ha realizado y todos los activos deberán ser revisados por los responsables de su seguridad y los responsables de los procesos. Tampoco se ha etiquetado la información crítica o sensible.

Dominio -8: SEGURIDAD DE LOS RECURSOS HUMANOS

Objetivo 8.1. Antes de la contratación laboral.

Existe un manual de funciones de la planta de personal de la Institución, pero no las funciones y responsabilidades de seguridad. Para cada funcionario se debe describir sus funciones y responsabilidades como actuar de acuerdo a la política, proteger activos, ejecutar funciones de seguridad, informar de eventos o incidentes de seguridad e incluirlos en la evaluación de desempeño.

Los cargos y funciones de seguridad y responsabilidades (funcionarios, contratistas y terceros) están definidos y documentados en el Manual General de funciones de la Institución. Éstas no

[16] SIIF (2014) Misión. Recuperado de: http://www.minhacienda.gov.co/HomeMinhacienda/siif

incluyen responsabilidades generales relacionadas con la implementación y el mantenimiento de la Política de Seguridad, y las responsabilidades específicas vinculadas a la protección de cada uno de los activos, o la ejecución de procesos o actividades de seguridad determinadas.

No hay roles establecidos y documentados para funcionarios y contratistas. También se surte un proceso de selección y se revisan los antecedentes de candidatos pero no se firman acuerdos con relación a la seguridad de la información

No se implementa ningún régimen de separación de tareas, para evitar que un solo empleado realice la totalidad de una operación.

Objetivo 8.2. Durante la vigencia del contrato laboral.

Cuando un funcionario ingresa a la entidad, el Jefe de talento humano algunas veces informa al líder de Sistemas y Comunicación, para que se de alta en los sistemas existentes y se cree el correo, sin embargo, existe un procedimiento formal a seguir para realizar estas tareas.

Se lleva a cabo periódicamente revisión y control sobre el buen funcionamiento de las cuentas de los usuarios y sobre los permisos que tienen asignados para el servidor, aplicaciones o en e-mail institucional.

No se ha formalizado el proceso disciplinario cuando se presente situaciones de violación de seguridad de la información.

Objetivo 8.3. Terminación o cambio de la contratación laboral.

No hay ningún procedimiento formal para dar de baja un usuario del sistema. Se hace devolución de activos cuando los funcionarios y contratistas terminan sus contratos sin embargo debe incluirse la información como un activo.

Dominio -9: SEGURIDAD FISICA Y DEL ENTORNO

Objetivo 9.1. Áreas seguras.

La edificación tiene paredes de altura completa, aunque las cerraduras de puertas de centros de cableado, áreas de servidores son del manejo de contratistas.

La entidad no dispone de un sistema de detección ni de extinción de incendios como son los extintores. No se protege del agua, ni hay un manejo adecuado de acceso físico.

La entidad cuenta con vigilancia interna " empleados de planta" pero no hay un sistema de monitoreo como apoyo.

Durante todas las horas de oficina no hay control de entrada ni revisión de pertenecías como bolsos, maletines, equipos y no existe registro de entradas y salidas en un libro.

Los funcionarios deben permanecer durante el horario laboral en sus oficinas a la cual acceden a través de sus propias llaves, si desean ingresar después del horario laboral lo pueden realizar sin autorización de la vicerrectoria administrativa y financiera.

Las áreas correspondientes a Dirección, Almacén y Tesorería no manejan un sistema de alarma. No hay tarjetas magnéticas o de llaves cifradas. La oficina de tesorería tiene una Caja de seguridad pero no existe un cambio de clave con cierta periodicidad aunque no se maneja efectivo.

Se han realizado visitas y diagnosticas de seguridad y salud ocupacional por parte del comité de COPASO y de las ARP pero no se han tomado las medidas pertinentes.

Objetivo 9.2. Seguridad de los equipos.

Dispositivos como lectoras de CD y unidades de USB están habilitadas y no hay ningún control sobre ellos, no se hacen controles automáticos de virus ni se prohíbe el booteo desde estos dispositivos. Sin embargo Nunca se ha reportado robo de información usando medios externos.

No se realizan controles periódicos sobre los dispositivos de hardware instalados en los PC´s, de manera que alguien podría instalar o sustraer alguno.

Una vez que se ha completado la instalación de algún equipo, no se realiza chequeos rutinarios o periódicos, solo se revisa los equipos ante fallas en los mismos, o por un problema reportado por el usuario.

No se realizan mediciones de temperatura y humedad desde el año 2014.

Los servidores no se apagan en horarios no laborales, debido a que se debe acceder a ellos a cualquier hora, normalmente permanecen prendidos las 24 horas del día.

Los gabinetes donde se ubican los switches, no están cerrados con llave, posibilitando que cualquier persona desconecte las entradas, y como medida de precaución, debido a que hay puntos libres en estos dispositivos.

Cableado

La instalación del cableado fue tercerizada, y se realizó un tendido con cable certificado, en el switch administrativo hay una salida dedicada para cada PC, y salidas libres para posible ampliación de la red.

Todos los equipos están protegidos con respecto a las posibles fallas en el suministro de energía u otras anomalías eléctricas. El suministro de energía está de acuerdo con las especificaciones del fabricante o proveedor de cada equipo. Para asegurar la continuidad del suministro de energía, cada PC está conectada a una UPS para asegurar el apagado regulado y sistemático o la ejecución continua de equipos que soportan las operaciones críticas de la Institución.

Recursos compartidos: El entorno de red de cada uno de los usuarios está configurado para que el usuario vea toda la red, no el grupo o parte de la misma. No hay ninguna medida tomada para que un usuario no comparta sus datos con otro usuario.

Internet: Existe un firewall, servidor de internet que evita que los usuarios usen software de mensajería instantánea, descarguen archivos, practiquen la piratería y entren a cualquier página sin ningún control ni protección.

Hosting: El servidor de hosting se eligió según el precio y los servicios ofrecidos. Estos ofrecen medidas de seguridad y política de respaldo en caso de problemas, y hasta el momento no se han registrado problemas.

Correo Electrónico: La Institución cuenta con un sistema de correo tanto para mail interno como externo, este se encuentra alojado en bajo la plataforma de google

La Institución tiene adquirido un dominio (infotep.edu.co), el mismo que es el dominio de todas las cuentas de correo que se crean.

Si un funcionario necesita una dirección de mail, porque su puesto de trabajo lo amerita, el jefe de talento humano debe reportar por e-mail al jefe de sistemas quien crea la cuenta de correo respectiva.

Los funcionarios usan el mail para funciones laborales, pero actualmente no se realizan controles, de manera que podrían usarlo también para fines personales.

No existe un software cliente definido por el INFOTEP para el manejo de los correos, Los correos pueden ser descargados a los equipos pero no existe una buena gestión de copia y seguridad de estos.

No existe política para recepción, envió de e-mail y uso eficiente del mismo. También desconocen el espacio asignado a cada usuario y forma de asignación de estos espacios.

Mantenimiento

Servicio de mantenimiento: cada vez que los usuarios necesitan asesoría o servicios se comunican al área de compras y mantenimiento quien es el que da solución por medio de contratación externa, se requiere un mayor control de este servicio como el cumplimiento con el procedimiento, uso de formatos y seguimiento a los incidentes. También se debe firmar el acuerdo de confidencialidad y buen uso de equipos.

Protección fuera de las instalaciones.

El único control que existe es el seguro que se adquirió con LA PREVISORA para amparar (en un 90%) los equipos de escritorio y portátiles contra amenazas naturales, destrucción y robo.

Reutilización o eliminación de equipos

El área de compras y mantenimiento emite el concepto acerca de si se debe dar de baja un equipo y generalmente este equipo es entregado a colegios. Cuando las partes de un equipo se pueden reutilizar la persona de almacén suministra el elemento para ser instalado en un equipo en uso. No se tiene el control de hacer un borrado seguro de la información en estos discos o equipos que son de reúsos.

Dominio -10: GESTION DE COMUNICACIONES Y OPERACIONES

Objetivo 10.1. Procedimientos operacionales y Responsabilidades.

Debido a la falta de personal no se hace una buena separación de funciones.

Como se encuentra implementado el SGC los procedimientos se encuentran documentados. En cada sistema los usuarios reconocen a quien deben contactar. Para el SGS hay que definir los procedimientos de seguridad necesarios para cumplir con cada uno de los dominios de la 27002.

Gestión de cambios.

No se lleva registro de los cambios solicitados por los usuarios.

El S.O. Hace actualizaciones automáticas. No se documenta los cambios de equipos en sus hojas de vida

A.10.2. Gestión de la provisión de servicios por terceras partes.

Se debe elaborar términos de referencia que incluya disponibilidad, seguridad, gestión y definición.

A.10.3. Planificación y aceptación del sistema.

Los equipos de cómputo y comunicación son totalmente nuevos, y están acordes con las tendencias de tecnologías y nuevas aplicaciones o por directiva gubernamental como VITAL y estrategia de Gobierno en línea.

A.10.4. Protección contra códigos maliciosos y móviles.

La Institución adquirió a inicios del 2013, 230 licencias corporativas del Kaspersky, las cuales tienen una vigencia de un año pero en la actualidad se encuentran desprotegidos.

Existen incidentes producidos por virus, y específicamente con los dispositivos extraíbles. Se ha reportado perdida de información en algunos equipos a los que se les ha tenido que formatear el disco.

Los escaneos periódicos buscando virus en los servidores y en los PC´s lo hace el contratista de mantenimiento dentro de su labor de Mantenimiento Preventivo. Está prohibido el uso de software pirata, descargar software de internet pero no se controla su cumplimiento.

A.10.5. Respaldo.

De datos en los servidores: Existe la programación dentro de los cinco primeros días de cada mes y cuando se hace un cambio en la configuración del servidor, se guardan copias de las configuraciones anterior y posterior al cambio y existe un procedimiento formal para la realización de la recuperación de los backups. Además se realizan chequeos para comprobar que el funcionamiento sea el correcto.

De datos en los PC's: Los usuarios deben realizar sus propios backups de los datos almacenados en sus PC's, ya que estos datos son responsabilidad de los funcionarios según la política de Sistemas y Comunicación. Si hacen un backup pueden hacerlo en sus propias máquinas, en CD´s y en dispositivos de almacenamiento externo.

Protección de los Backups: Los archivos de backups no están protegidos con ningún control de acceso ni encriptación. Esta situación puede resultar peligrosa ya que estos archivos contienen las bases de datos de la empresa y, ante cualquier incidente o extravío de los mismos, es fácil recuperar los datos en su formato original.

A.10.6. Gestión de la seguridad de las redes.

En la empresa no disponen de herramientas destinadas exclusivamente para prevenir los ataques de red, en principio debido a que no se han presentado, hasta el momento, problemas en este sentido. Nunca se han realizado escaneos, ni intentos de intrusión o de escucha. Tampoco se

hace pruebas periódicas (test) de puertos o de los servicios que están habilitados. Solo se revisan las instalaciones cuando hay quejas de los usuarios.

No hay controles con respecto a la ocurrencia de Denial of Service (denegación de servicio). No existen herramientas que lo detecten, ni hay líneas de base con datos sobre la actividad normal del sistema para así poder generar avisos y limitar el tráfico de red de acuerdo a los valores medidos.

No existe control por firewall, deshabilitar servicios de equipos lo que significa que se pueden acceder a los equipos de manera remota, todos los puertos de los PC's se encuentran habilitados permanentemente y algunos servicios requieren ser deshabilitados.

La red no se encuentra segmentada a través de switches, que efectivamente presenta la posibilidad de sniffing, ya que no direccionan los paquetes de red de acuerdo al destino que tienen (sector de la empresa al que están dirigidos).

No se tiene control de la configuración y la administración de la red inalámbrica. No se tienen las claves para la administración de los switches.

A.10.7. Manejo de los medios.

No existen procedimientos para la gestión de los medios informáticos removibles como cintas, discos o resultados impresos.

A.10.8. Intercambio de información.

No existen Políticas internas que regulen el intercambio de información.

A.10.9. Servicios de comercio electrónico.

Para la estrategia de gobierno en línea se debe tener implementado los pagos en línea y el código de barras, el convenio con Banco Agrario ya fue firmado por el director desde Junio de 2014.

A.10.10. Monitoreo

No se lleva registros de auditoría y uso de los sistemas.

Dominio -11: CONTROL DE ACCESOS

A.11.1. Requisitos de negocio para el control de acceso.

No se encuentra documentada una política para el control de acceso.

A.11.2. Gestión de acceso de usuario.

Para la aplicaciones desarrolladas para la Correspondencia se tienen identificados los usuarios que corresponden a cada una pero no se tiene documentado ni se monitorea su uso.

No existe en el sistema una lista de control de acceso que se utilice para identificar los tipos de permiso que tiene cada usuario con respecto a los datos.

No se tiene en cuenta ninguna restricción horaria para el uso de los recursos. Tampoco se considera una restricción física sobre la máquina desde donde se logea cada usuario.

Si el usuario permanece un período de tiempo logeado sin actividad, el sistema no ejecuta ninguna acción; se les ha advertido a los funcionarios sobre la necesidad de no dejar las máquinas logeadas e inactivas.

Si las cuentas de usuarios permanecen varios días sin actividad, por licencias o por vacaciones no pasan a un estado de suspensión.

El usuario administrador (root) se logea en los servidores durante las 24 horas del día, debido a que éstos equipos no se apagan en ningún momento.

A.11.3. Responsabilidades de los usuarios.

Los usuarios no cumplen ninguna práctica de seguridad de contraseñas.

No se eliminan los usuarios que vienen por default en el sistema operativo, como son las cuentas "Invitado", estas cuentas permanecen activas en el sistema sin que ningún usuario las utilice.

Existe, además, un servicio de mantenimiento que utiliza la misma cuenta del administrador para hacer modificaciones en los sistemas operativos de los PC's y servidores.

En cuanto a la configuración de los PC's de funcionarios, no hay ningún control de acceso a sus sistemas BIOS, de manera que al momento del encendido de la máquina cualquier persona podría modificar sus opciones de configuración.

Existe dentro de la política de Sistemas y Comunicación el control de escritorio despejado y de pantalla despejada pero no se hace control de la misma.

A.11.4. Control de acceso a las redes.

Los funcionarios utilizan todos los servicios de red y dentro de la política de Sistemas y Comunicación se encuentra documentado.

A.11.5. Control de acceso al sistema operativo.

No existe un sistema de gestión de contraseñas.

A.11.6 Control de acceso a las aplicaciones y a la información.

No existe tal control de acceso.

A.11.7 Computación móvil y trabajo remoto

Aunque muchos usuarios que poseen portátiles, celulares corporativos, no existen políticas de control y son retirados sin que se registre su salida. En la actualidad no existe acceso remoto.

Dominio -12: ADQUISICION, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACION

A.12.1. Requisitos de seguridad de los sistemas de información.

Cuando se han hecho desarrollos no se han incluido requisitos de seguridad ni se han exigido al proveedor de software.

A.12.2. Procesamiento correcto en las aplicaciones.

Control de Aplicaciones en PC's: Actualmente ningún usuario puede instalar aplicaciones en sus equipos, en caso de querer instalar una nueva aplicación se debe dar a conocer la necesidad de la misma a su jefe inmediato y solicitar al jefe de oficina de compras y mantenimiento la instalación respectiva.

No hay estándares definidos, no hay procedimientos a seguir ni tampoco documentación respecto a la instalación y actualización de la configuración de los PC's. Solo hay una instalación básica de alguna versión del Windows, Internet Explorer y Antivirus.

En el caso de que un equipo presente errores en su configuración, no se utilizan herramientas de reparación de errores, como el Norton Disk Doctor, con el fin de evitar la reinstalación total del sistema y así causar una pérdida innecesaria de tiempo y de información como correos, configuración de escritorios y algunas veces archivos, solo se restaura la ultima copia de seguridad después de formatear el disco duro.

Tampoco se realizan actualizaciones de los programas instalados, como el Internet Explorer y el Microsoft Office. No se buscan Service Packs ni nuevas versiones. No se tiene políticas de actualización de programas.

Solamente personal de mantenimiento debe instalar software en los PC's, para los usuarios existen restricciones con respecto a la instalación de programas. Pero realmente pueden bajar de la web cualquier aplicación e instalarla en su PC sin ningún control sobre las licencias ni autorización previa. Esto se debe a que el usuario utilizado posee este privilegio. Si se habilita solo el usuario adecuado se podrá controlar problemas de licencias, virus o programas no permitidos.

La página web fue diseñada para que todo el mantenimiento pueda desarrollarse desde el interior de la empresa, a excepción de las modificaciones que se llevan a cabo en la estructura de la página. Es una página dinámica en algunos temas sobre todo en los exigidos por GEL. Como información de la entidad y el avance de sus planes de gestión. La página se modifica desde el servidor de Internet, con un administrador desarrollado en CMS para este fin. El proveedor responde por la integridad de los datos.

A.12.3. Controles criptográficos.

Privacidad – Firma digital – Encriptación de mails: No se utilizan firmas digitales ni encriptación en el correo electrónico. Dentro de la entidad no se usa firma digital para servicio de trámites, ni para mensajes internos ni para los externos ya que los mensajes de importancia generalmente son enviadas vía mail.

Solo se utiliza firma digital para el envió de información al sistema SIIF Nación.

A.12.4. Seguridad de los archivos del sistema.

No existe control de versiones del S.O. Ni de actualizaciones, ni de accesos a esta información.

Los datos de prueba se eliminan pero no queda registro de esta operación. Los códigos fuente son solo manipulados por los desarrolladores pero no se gestionan los cambios.

A.12.5. Seguridad en los procesos de desarrollo y soporte.

No existe procedimiento de control de cambio de software o de página web.

Dominio -13: GESTION DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACION

A.13.1. Notificación de eventos y puntos débiles de la seguridad de la información.

Se notifican solo eventos de daños en PC y periféricos al igual que en daños de software de usuarios.

A.13.2. Gestión de incidentes de seguridad de la información y mejoras.

En la entidad no hay planes formales para la administración de incidentes, solo para servicio técnico en general.

Dominio -14: GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

No se ha documentado ni se han realizado acciones al respecto.

Dominio -15: CUMPLIMIENTO

A.15.1. Cumplimiento de los requisitos legales

La INSTITUCIÓN no ha identificado ni documentado los requisitos legales de protección de la privacidad, derechos de autor, licenciamiento de software, se está trabajando con el Normograma establecido en el SGC y se están incluyendo algunos requisitos *estatutarios, reglamentarios y contractuales.*

8. CONCLUSIONES

La implementación del Sistema de Gestión de Seguridad de la información cada día se convierte en un aspecto muy importante dentro de las organizaciones y por medio del SASIGEL le permitirá a dichas organizaciones adoptar un modelo Gubernamental que se adapta tanto para las entidades públicas como las privadas que lo deseen acoger.

Es importante reconocer que todas las organizaciones deben tomar las medidas de protección necesarias teniendo en cuenta que la información siempre está expuesta a innumerables amenazas y cada una de ellas con diferentes probabilidades de ocurrencia.

Es necesario tener en cuenta que el nivel de madurez de una entidad con respecto al SGSI, no se basa en la cantidad de computadores, puntos de red, servicios en línea "online" o las diversas plataformas tecnológicas que manejan, puesto a que las necesidades de seguridad se basan más que todo en el tipo de información utilizada..

Se piensa en un futuro cercano, todas las entidades deben tener implantadas buenas prácticas y sistemas que contribuyan a la mejora continúa de los procesos y se refleje como un síntoma de la madurez en las organizaciones.

La carencia de políticas y controles orientados a la seguridad conlleva a consecuencias que pueden afectar al cumplimiento de los objetivos de la entidad.

Debe existir un interés grande con respecto a la seguridad de la información, partiendo desde la alta dirección y que involucre a todos los líderes de proceso, este interés que se refleje claramente en las políticas, normas y controles de la entidad

El Sistema de Gestión de Seguridad de Información (SGSI) debe verse como la solución para el flujo de toda la información institucional que se emplean en todos los procesos, que dichos procesos, alcancen el nivel de seguridad adecuado y permitan garantizar el cumplimiento de los objetivos tanto del SGSI como los de la Institución.

El factor decisivo y fundamental en la implantación de todo Sistema de Gestión de Seguridad de la Información está en el apoyo de la dirección, puesto que esta es la que aprueba las acciones a tomar y facilita los recursos necesarios para llevarlas a cabo, de igual manera se debe tener en cuenta que el compromiso de los funcionarios va íntimamente ligado al éxito de dicha implementación.

9. RECOMENDACIONES

Uno de los factores críticos en la implementación de cualquier tipo de sistema, es el sostenimiento del mismo, ya que en muchos casos las empresas posterior a dicho proceso no realizan el debido seguimiento y control, por lo tanto es necesario planear estrategias que sean adecuadas para mitigar que el Sistema se caiga como lo son; la programación periódica de capacitaciones, auditorías, revisiones por parte de la dirección, evaluación regular de los riesgos, mantener actualizado los planes de seguridad y llevar un registro de los eventos o acciones entre otros, los cuales puedan causar impacto en la eficacia y rendimiento del SGSI.

El proceso de implementación de un SGSI es algo muy importante, no se trata de realizan la contratación de una empresa o agente consultor para la ejecución de un contrato mas, no es un proceso aislado, ya que no generaría ningún interés, es de carácter colectivo e institucional por lo cual es fundamental que para la planificación y diseño del SGSI contar con la cooperación de todos los funcionarios de la organización, de esta manera lograr una buena definición del alcance, políticas, evaluaciones de riesgos, identificación de amenazas, vulnerabilidades e impactos entre otras, dando como resultado un proceso totalmente transparente, participativo y que no se convierta en un requisito mas por cumplir en la entidad.

La realización de jornadas de concientización periódicas para el personal del INFOTEP con respecto a la seguridad de información son bases fundamentales para la mejora del sistema, de tal manera que todos los empleados de la institución, conozcan la importancia y las efectos del no seguir los lineamientos de seguridad en el día a día.

Buscar mecanismos para dar a conocer las responsabilidades de los diferentes grupos de interés con respecto a la iniciativa de seguridad de la información.

Es necesario contar con el suficiente recurso humano al igual que establecer un rol de “Oficial de Seguridad de Información” dentro del INFOTEP para el monitoreo y cumplimiento de las políticas y controles establecidos por la alta gerencia al igual que la realización de ejercicios de escritorio para comprobar los controles establecidos dentro del SGSI.

10. BIBLIOGRAFIA

Aldana de Vega, Luz Ángela, Álvarez Builes, María Patricia, Bernal Torres, César Augusto. 2011. Administración por calidad. México: Alfaomega Grupo Editor.

Álvarez Marañón, Gonzalo, Pérez García, Pedro Pablo. 2004. Seguridad informática para empresas y particulares. España: McGraw-Hill España.

Centro de investigación de las Telecomunicaciones - CINTEL. Modelo de Seguridad de la Información para la estrategia de Gobierno en línea. Bogotá, D.C., Diciembre de 2011.

Centro de Investigación de las Telecomunicaciones - CINTEL. Anexo 1: Organigrama Modelo y SASIGEL - Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C., Diciembre de 2011.

Centro de Investigación de las Telecomunicaciones - CINTEL. Anexo 3: Estratificación de Entidades - Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C., Diciembre de 2011.

Centro de Investigación de las Telecomunicaciones - CINTEL. Anexo 5: Formato Políticas SGSI - Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C., Diciembre de 2011.

Centro de Investigación de las Telecomunicaciones - CINTEL. Anexo 7: Metodología de Clasificación de los Activos - Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C., Diciembre de 2011.

Centro de Investigación de las Telecomunicaciones - CINTEL. Anexo 8: Controles y lineamientos de seguridad - Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C., Diciembre de 2011.

Centro de Investigación de las Telecomunicaciones - CINTEL. Anexo 14: Fase hacer - Modelo de seguridad de la información para la estrategia de gobierno en línea 2.0. Bogotá, D.C., Diciembre de 2011.

Ciclo PDCA, Recuperado de la web: http://datateca.unad.edu.co/contenidos/233003/modulo/modulo-233003-online/151_ciclo_pdca__edward_deming.html.

Escrivá Gascó, Gema, Romero Serrano, Rosa María, Ramada, David Jorge. 2013. Seguridad informática. España: Macmillan Iberia, S.A. P 210.

GOBIERNO EN LÍNEA (2014). Que es Gobierno en Línea. Recuperado de: http://vive.gobiernoenlinea.gov.co/

Gómez Fernández, Luis, Andrés Álvarez, Ana. 2012. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. España: ENOR - Asociación Española de Normalización y Certificación. P 24.

ICONTEC. (2014) Quienes Somos. Recuperado de: http://www.icontec.org/index.php/es/nuestra-compania/nuestra-compania

INFOTEP. (2014) Reseña histórica. Recuperado de: http://infotep.edu.co/images/pdf/resena_historica_infotep.pdf

INTECO (2013). Fases del SGSI. Recuperado de www.inteco.es/Formacion/SGSI/Conceptos_Basicos/Fases_SGSI

ISO (2013). ISO 27000. Recuperado de http://www.iso27000.es/download/doc_iso27000_all.pdf

ISO 27001:2005 Tecnología de la Información – Técnicas de seguridad – Sistemas de seguridad de la información - Requerimientos.

ISO/IEC 27001 (2014). for Small Businesses - Practical advice. Recuperado de http://www.iso.org/iso/news.htm?refid=Ref1365

MINTIC, 2012. Metodología para la implementación del Modelo Integrado de Planeación y Gestión.

Moreno, F. 2009. La ISO/IEC 27005 en la búsqueda de información más segura. Normas y Calidad. ICONTEC. Cuarta edición. P 28 – 32.

Norma Técnica Colombiana NTC/ISO 27001. (2006-03-22). Sistema de Gestión de la Seguridad de la Información. Requisitos.

Norma Técnica Colombiana NTC/ISO 27002. (2007-11-16). Código de práctica para la Gestión de la seguridad de la Información.

Norma Técnica Colombiana NTC/ISO 27005. (2009-08-19). Gestión de Riesgos en la seguridad de la Información.

NTC-ISO/IEC 27002, Tecnología de la información. Código de práctica para la gestión de la seguridad de la información. P 10 - 11

Stonebumer, G. NIST. (2002). Risk management guide for information technology systems. Recuperado de http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

Toro, M. 2011. Plan de seguridad de la información ISO 27002 Vs COBIT. Normas y Calidad. ICONTEC. Cuarta edición. P 26 – 28.