PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN UNA ENTIDAD DEL SECTOR PÚBLICO BASADO EN LA NTC ISO 27001:2013

GIOVANNI PEDRAZA RODRÍGUEZ

FUNDACIÓN UNIVERSIDAD DE AMÉRICA
FACULTAD DE EDUCACIÓN PERMANENTE Y AVANZADA
ESPECIALIZACIÓN EN GERENCIA DE LA CALIDAD
BOGOTÁ D.C.
2017

PLAN DE IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN EN UNA ENTIDAD DEL SECTOR PÚBLICO BASADO EN LA NTC ISO 27001:2013

GIOVANNI PEDRAZA RODRÍGUEZ

Monografía para optar por el título de Especialista en Gerencia de la Calidad

Orientador

Angélica María Álzate Ibáñez
Magíster, Ingeniera Química

FUNDACIÓN UNIVERSIDAD DE AMÉRICA
FACULTAD DE EDUCACIÓN PERMANENTE Y AVANZADA
ESPECIALIZACIÓN GERENCIA DE LA CALIDAD
BOGOTÁ D.C.
2017

NOTA DE ACEPTACIÓN

_____
_____
_____
_____
_____
_____

_____
Firma del director de la especialización

_____
Firma del calificador

Bogotá D.C., octubre de 2017

Las directivas de la Universidad de América, los jurados calificadores y el cuerpo docente no son responsables por los criterios e ideas expuestas en el presente documento. Estos corresponden únicamente a los autores.

AGRADECIMIENTOS

A Dios por acompañarme e iluminarme con su infinita grandeza el camino de mi vida y en cada una de mis acciones, a mi Esposa e Hijo por su comprensión, amor, respaldo y fuente de motivación y superación para que cada día de nuestras vidas sean mejor.

A todas las personas que hicieron posible la recopilación de la información requerida para elaborar el proyecto; a los funcionarios de la Comisión Nacional del Servicio Civil que me regalaron parte de su tiempo y colaboración para la construcción del documento; y especialmente, a la orientadora Angélica María Álzate Ibáñez, quien brindó su conocimiento y entereza para cumplir con éxito los objetivos propuestos.

DIRECTIVAS DE LA UNIVERSIDAD

Presidente de la Universidad y Rector del claustro:

Dr. Jaime Posada Díaz

Vicerrectora Académica y de Posgrados:

Dra. Ana Josefa Herrera Vargas

Vicerrector de Desarrollo y Recursos Humanos:

Dr. Luis Jaime Posada García Peña

Secretario General:

Dr. Juan Carlos Posada García Peña

Decano de la Facultad de Educación Permanente y Avanzada:

Dr. Luis Fernando Romero Suárez

Director de la Especialización en Gerencia de la Calidad:

Dr. Emerson Mahecha Roa

CONTENIDO

LISTA DE CUADROS

pág.

LISTA DE FIGURAS

GLOSARIO

AMENAZA: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

ANÁLISIS DE RIESGO: elemento de control que permite establecer la probabilidad de ocurrencia de los eventos positivos y/o negativos y el impacto de sus consecuencias, calificándolos y evaluándolos a fin de determinar la capacidad de la entidad pública para su aceptación y manejo. Se debe llevar a cabo un uso sistemático de la información disponible para determinar qué tan frecuentemente pueden ocurrir eventos especificados y la magnitud de sus consecuencias.

CALIDAD: grado en el que un conjunto de características inherentes de un objeto cumple con los requisitos.

COBIT 4.1: *Control Objectives for Information and Related Technology*, creado por *Information Systems Audit and Control Association* (ISACA) (http.isaca.org/). Es un conjunto de buenas prácticas para la gestión de la información. Define cuatro dominios: planificación y organización, adquisición e implementación, entrega y soporte, monitorización y evaluación.

CONFIDENCIALIDAD: la confidencialidad es la propiedad que impide la divulgación de información a personas o sistemas no autorizados. A grandes rasgos, asegura el acceso a la información únicamente a aquellas personas que cuenten con la debida autorización.

CONTRASEÑAS: una contraseña o clave es una forma de autentificación que utiliza información secreta para controlar el acceso hacia algún recurso. La contraseña debe mantenerse en secreto ante aquellos a quien no se le permite el acceso.

DATOS: es una representación simbólica (numérica, alfabética, algorítmica, etc.) de un atributo o variable cuantitativa. Los datos describen hechos empíricos, sucesos y entidades. Es un valor o referente que recibe el computador por diferentes medios. Los datos representan la información que el programador manipula en la construcción de una solución o en el desarrollo de un algoritmo.

DEBILIDAD: se refiere a todos aquellos elementos, recursos, habilidades y actitudes que la empresa ya tiene, y que constituye barreras para lograr la buena marcha de la organización (en este caso un sistema).

DISEÑO: es el resultado final de un proceso, cuyo objetivo es buscar una solución idónea a cierta problemática particular, pero tratando en lo posible de ser práctico y a la vez estético en lo que se hace.

DISPONIBILIDAD: es la característica, cualidad o condición de la información de encontrarse a disposición de quienes deben acceder a ella, ya sean personas,

procesos o aplicaciones. La disponibilidad es el acceso a la información y a los sistemas por personas autorizadas en el momento que así lo requieran.

ESTRATEGIA: es un conjunto de compromisos y actos integrados y coordinados, cuyo objetivo es explotar las competencias y conseguir una ventaja competitiva.

FALLOS: es un estado o situación en la que se encuentra un sistema (formado por dispositivos, equipos, aparatos y/o personas) en el momento que deja de cumplir la función para la cual había sido diseñado. Hay que evitar esta situación siempre que queramos diseñar un sistema altamente fiable, competitivo y fuerte.

FIDELIZACIÓN: fenómeno por medio del cual, un público determinado permanece fiel a la compra de un producto o servicio.

GESTIÓN DE LA CALIDAD: actividades coordinadas para dirigir y controlar una organización con respecto a la calidad.

INFORMACIÓN: conjunto organizado de datos procesados que constituyen un mensaje que cambia el estado de conocimiento del sujeto o sistema que recibe dicho mensaje. La información (ya sea impresa, almacenada digitalmente o hablada), es considerada como un activo dentro de las compañías y se debe proteger por ser de gran importancia.

INTEGRIDAD: es la propiedad que busca mantener los datos libres de modificaciones no autorizadas (no es igual a integridad referencial en bases de datos). A groso modo, la integridad es mantener con exactitud la información tal cual cómo fue generada, sin ser manipulada o alterada por personas o procesos no autorizados.

ITIL: es un marco *Best Practice* que se ha elaborado por los sectores público y privado en el ámbito internacional. En él se describe cómo los recursos de TI deben ser organizados para ofrecer un valor empresarial documentando los procesos, funciones y roles del *IT Service Management* (ITSM).

MEJORA: actividad para optimizar el desempeño.

PHVA: es el ciclo de mejora continua: Planear, Hacer, Verificar y Actuar.

POLÍTICA DE SEGURIDAD: toda intención y directriz expresada formalmente por la Dirección. Su objetivo es proporcionar a la gerencia la guía y soporte para la seguridad de la información, en concordancia con los requerimientos comerciales, las leyes y regulaciones relevantes. Esto debe ser creado de forma particular por cada organización y se debe plasmar en un Documento de la Política de Seguridad de la Información.

PROCEDIMIENTOS: es un conjunto de acciones u operaciones que deben realizarse de la misma forma para obtener siempre el mismo resultado, bajo las mismas circunstancias (por ejemplo: el procedimiento de emergencia).

RIESGO: se define como cualquier impedimento, obstáculo, amenaza o problema que pueda impedirle a la empresa que alcance un objetivo. Se puede ver también como la posibilidad de sufrir un daño o pérdida. Se mide en términos de impacto y de probabilidad de ocurrencia. Adicionalmente, para el caso de las compañías de seguro, se puede definir como el monto que está dispuesto a perder en caso de que se dé una catástrofe.

SGSI: Sistema de Gestión de la Seguridad de la Información, en inglés *Information Security Management System*. Es un conjunto de datos organizados en poder de una entidad, que posean valor para la misma, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail; transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

SISTEMA DE DETECCIÓN DE INTRUSOS: (O IDS de sus siglas en inglés Intrusion Detection System) es un programa usado para detectar accesos no autorizados a un computador o a una red. Estos accesos pueden ser ataques de habilidosos hackers, o de Script Kiddies que usan herramientas automáticas.

SISTEMA INFORMÁTICO: (SI) es un sistema que permite almacenar y procesar información. Es el conjunto de partes interrelacionadas: hardware, software y personal informático.

TIC: Tecnologías de la Información y la Comunicación (TIC).

VULNERABILIDAD: debilidad de un activo o grupo de activos que puede ser aprovechada por una o más amenazas.

RESUMEN

La connotación de seguridad se ha ido ampliando con el tiempo gracias a la inmersión de nuevos sistemas tecnológicos de información. Así mismo, los instrumentos para garantizar el resguardo, la confidencialidad y el tratamiento de la información, se han convertido en estrategias fundamentales para la garantía de la seguridad de las organizaciones públicas y privadas.

Uno de estos instrumentos es la norma ISO 27001, la cual se ha convertido en una importante guía que involucra a los diferentes actores de una entidad en torno a la protección de la información. A la luz de esta norma, el presente trabajo realiza el diseño de un Plan de Implementación de un Sistema de Gestión de la Seguridad de la Información (SGSI) para una entidad colombiana del sector público, que maneja a diario una amplia información de recursos, políticas, documentación y datos personales de los ciudadanos.

La elaboración de este plan comprende el análisis del estado actual de la organización y la evaluación de sus riesgos, así como la implementación del modelo Planear, Hacer, Verificar y Actuar (PHVA), con características procedimentales que apoyan de principio a fin todo el proceso de implantación y facilitan el debido proceso y la continuidad.

El resultado de este diseño será un plan con cronograma de actividades, para que la organización vincule a todo el personal en torno al cumplimiento de la norma, la sensibilización con respecto a la importancia de la seguridad de la información y el desarrollo de actividades por fases que en los tiempos estipulados lograrán tener en pleno funcionamiento el SGSI.

Palabras clave: implementación, seguridad, información, riesgo, análisis, PHVA.

INTRODUCCIÓN

La información en los últimos años se ha definido como uno de los aspectos de mayor relevancia dentro de las organizaciones. Este activo es procesado, dispuesto para intercambio con otros usuarios y conservado a través de redes de datos, equipos informáticos y soportes de almacenamiento, que conforman los “sistemas informáticos”.

Antes de la aparición de estos sistemas, la información era manejada en papel y almacenada en grandes cantidades de archivos físicos que la hacían vulnerable a todos los problemas que conlleva su almacenamiento en cuanto a transporte, acceso y procesamiento.

En la actualidad, el alto volumen y complejidad en el manejo de la información ha llevado al desarrollo de nuevas tecnologías que tienen ventajas como: la digitalización, la reducción de espacio, la disponibilidad, la facilidad en el acceso y hasta la presentación. Pero presenta también riesgos, como la desaparición (ya sea por motivos de robo, pérdida o daños causados por interrupciones en el suministro eléctrico), ataques cibernéticos por intermedio de virus o *hackers*, o físicos: provocados por catástrofes naturales, por ejemplo: incendios, inundaciones, terremotos y accidentes. También está la modificación malintencionada del contenido por parte de empleados o usuarios.

La información es fundamental para la operación de las empresas y los negocios en general. Es por esta razón que su uso se ha incrementado a través de recursos valiosos como la internet y su constante desarrollo de nuevas tecnologías que la hacen accesible, pero también, más vulnerable a perdidas por la materialización de riesgos presentados.

La seguridad en la información va de la mano con los objetivos de las organizaciones que se enfrentan cada día a amenazas y vulnerabilidades. Estas se pueden generar desde el interior o el exterior de la organización, debido a una extensa variedad de fuentes que tienen acceso a información confidencial y que pueden utilizarla de forma perjudicial. Por esto se hace necesario tomar medidas y controles desde el principio, que logren proteger a la entidad de posibles amenazas a sus archivos y documentos informáticos.

Para este riesgo creciente existe una concienciación generalizada a nivel de la alta dirección. Las organizaciones se han ido familiarizando con el hecho de que pueden enfrentarse a una situación de inseguridad que debe ser tratada con profesionalismo y cuidado, para garantizar la disponibilidad, confidencialidad e integridad de la información, como lo indica la norma ISO 27001.

Con base en lo anterior, se generó la necesidad de llevar a cabo este trabajo de investigación, que permitirá proporcionar la información necesaria para elaborar un

Plan de Implementación de un Sistema de Gestión de Seguridad de la Información, en una entidad del sector público, basado en la NTC ISO 27001:2013.

Para ello se realizó una investigación descriptiva con un tipo de estudio cualitativo, en el que se ejecutará como primera medida el desarrollo de un marco teórico con relación al tema propuesto; en segundo lugar se exponen los factores de mayor vulnerabilidad de la empresa seleccionada para el estudio; en tercer lugar se presenta la normatividad exigida para la elaboración y puesta en marcha del plan de implementación a construir, y por último se analizan los resultados obtenidos para ser tenidos en cuenta en la ejecución del Sistema de Gestión de Seguridad de la Información.

OBJETIVOS

OBJETIVO GENERAL

Diseñar un plan para la implementación de un Sistema de Gestión de Seguridad de la Información en una empresa del sector público basado en los requisitos de la norma NTC ISO 27001:2013.

OBJETIVOS ESPECÍFICOS

- Realizar el análisis del contexto organizacional basado en el numeral 4 de la NTC ISO27001:2013 para un sistema de gestión de la seguridad de la información.

- Evaluar los riesgos de la seguridad de la información en una empresa prestadora de servicios de vigilancia del sistema de carrera administrativa basado en el numeral 6.1 de la NTC ISO27001:2013.

- Determinar las actividades y herramientas necesarias dirigidas a la implementación del sistema de gestión de Seguridad de la Información en una empresa del sector público conforme los requisitos de la NTCISO 27001:2013.

1 MARCO TEÓRICO

1.1 SISTEMAS DE GESTIÓN

Las organizaciones, bien sean de naturaleza privada, pública o mixta, se encuentran en la búsqueda del cumplimiento de sus objetivos estratégicos para lograr responder a las demandas del mercado (cada vez más competitivo y globalizado). Su objetivo es lograr buenos resultados empresariales y tener éxito al proveer un producto o un servicio. Esta es la mejor estrategia para subsistir.

Las estrategias administrativas en las organizaciones toman como base algunos modelos o estándares de calidad para hacer un correcto uso de sus sistemas de gestión al establecerlos, documentarlos y mantenerlos, con el fin de optimizar, dirigir y controlar, actividades y recursos en la consecución de sus objetivos.

Por ello, y según las normas ISO 9000, un Sistema de Gestión es un "sistema para establecer la política y los objetivos y para lograr dichos objetivos"[1]. Esta familia de normas, ISO 9000 (9000-9001-9004) orienta y guía para lograr determinar los requisitos y aspectos que debe tener un Sistema de Gestión de Calidad.

- ISO 9000: Brinda los fundamentos para los principios y el vocabulario de un SGC.
- ISO 9001: Especifica los requisitos del cliente y su satisfacción. Sirve como referente para la implementación de un SGC.
- ISO 9004: Guía hacia las buenas prácticas para mantener el SGC.

Para la Fundación Europea para la Gestión de la Calidad (EFQM, por sus siglas en inglés), el sistema de gestión es "un esquema general de procesos y procedimientos que se emplean para garantizar que la organización realiza todas las tareas necesarias paras alcanzar sus objetivos". Este modelo de gestión consta de nueve criterios que se agrupan en dos grandes bloques: (i) Agentes: todos los factores determinantes para la finalidad de la organización, como liderazgo, política y estrategia, personas, recursos alianzas, y procesos. (ii) Resultados: los logros obtenidos por la organización en los clientes, las personas y la sociedad.

Independiente del modelo o sistema de gestión adoptado por la organización, el resultado es una valiosa herramienta para el crecimiento, la toma de decisiones y la mejora de su desempeño.

---

[1] VILLANUEVA Isabel; SÁNCHEZ Juan y PASTOR, Óscar. Elicitación de requisitos en sistemas de gestión orientados a procesos. Trabajo subvencionado por el proyecto Destino Mec Nº TIN 2004-03534. Universidad Politécnica. España, 2005, p. [3-48].

1.2 SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Un Sistema de gestión de seguridad de la información (SGSI), según la norma UNE-ISO/IEC 27001, es "una parte del sistema de gestión general, basada en un enfoque de riesgo empresarial, que se establece para crear, implementar, operar, supervisar, revisar, mantener y mejorar la seguridad de la información"[2]. El sistema propicia que la organización evite operar intuitivamente y tome el control de los sistemas de información y de la información manejada dentro de la entidad.

Según Sánchez[3]., el objetivo principal que tiene una organización al hacer la implementación de un SGSI, es identificar los riesgos para gestionar los controles pertinentes con el fin de mantener la integridad, confidencialidad y disponibilidad de la información Cabe aclarar que un SGSI no garantiza la seguridad en un 100% porque pueden surgir imprevistos. Sin embargo, logrará gestionar y minimizar los riesgos y el impacto de una forma estructurada y documentada.

Como afirma el portal Iso27000.es[4]: Un Sistema de Gestión de Seguridad de la Información provee a las organizaciones un proceso de mejora continua que asegura la correcta gestión de los riesgos en materia de seguridad, y permite la participación constante de todos los miembros de la organización en cada uno de sus momentos: planeación, definición, identificación e implementación de controles y medidas orientadas a salvaguardar la seguridad de los activos de información de la organización.

Este proceso busca salvaguardar el llamado Triángulo de Seguridad de la Información, cuyas aristas fundamentales son la confidencialidad, la disponibilidad y la integridad. La primera hace referencia a la garantía de que el usuario de la información sea legítimo, la segunda, a que la información pueda ser manipulada en el momento en que se necesita, y la integridad asegura la fiabilidad de la información.

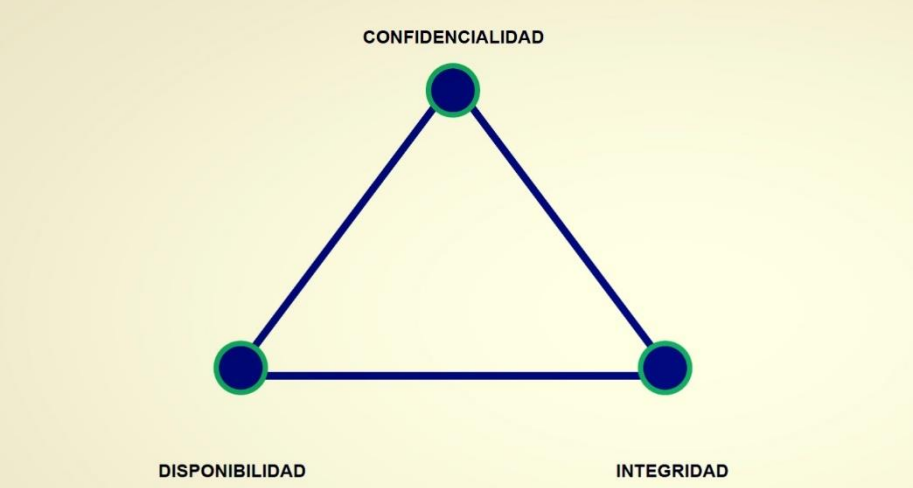
---

[2] ÁLVAREZ, Ana y FERNÁNDEZ, Luis. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para Pymes. Madrid: AENOR, 2012, p. [3].

[3] SÁNCHEZ Shirley Alexandra. Importancia de implementar el SGSI en una empresa certificada BASC. Bogotá: Universidad Militar Nueva Granada, 2014, p. [22].

[4] ISO 2700.ES. Integrar normas y sistemas. [sitio web]. España. Sec. Serie 27k. [Consultado 17, agosto, 2017]. Disponible en: http://www.iso27000.es/iso27000.html.

Figura 1. Triángulo de Seguridad de la Información



Fuente: IT IS SKULL. triángulo de la Seguridad de la Información [sitio web]. s.l. aec. Content [Consultado 18, agosto,2017]. Disponible en: https://www.it-skull.com/2-seguridad-de-la-informacion-que-es/6-triangulo-de-la-seguridad-de-la-informacion.html.

1.2.1 Serie ISO 27000

La norma ISO/IEC 27000 es un conjunto de estándares internacionales, desarrollados para proporcionar un marco de seguridad de la información. Aunque para este caso se utilizará la norma ISO 27001:2013, que es la norma certificable para Colombia, a continuación se mencionan las normas que conforman la serie y que aparecen publicadas en el portal ISO 27000[5]:

- ISO/IEC 27000: publicada el 1 de mayo de 2009, fue revisada en una segunda edición de 1 de diciembre de 2012, su tercera edición se publicó el 14 de enero de 2014 y una cuarta en febrero de 2016. Esta norma brinda una visión general de las normas que componen la serie 27000.

- ISO/IEC 27001: fue publicada el 15 de octubre de 2005 y revisada el 25 de septiembre de 2013. Es la norma principal de la serie porque contiene los requisitos del sistema de gestión de seguridad de la información.

- ISO/IEC 27002: apareció 1 de Julio de 2007, es el nuevo nombre de ISO 17799:2005, manteniendo 2005 como año de edición. Es una guía de buenas prácticas que describe los objetivos del control y controles recomendables en seguridad de la información, aunque no es certificable.

[5] ISO 2700.ES. Integrar normas y sistemas. [sitio web]. España. Sec. Serie 27000. [Consultado 17, agosto, 2017]. Disponible en: http://www.iso27000.es/iso27000.html.

ISO/IEC 27003: fue publicada el 1 de febrero de 2010 y actualizada el 12 de abril de 2017. Es una guía de aspectos críticos necesarios para el diseño e implementación con éxito de un SGSI. Tampoco es certificable.

- ISO/IEC 27004: publicada el 15 de diciembre de 2009 y revisada en diciembre de 2016. Es una guía para el desarrollo y uso de métricas y técnicas de medida aplicables para determinar la eficacia de un SGSI. No certificable.

- ISO/IEC 27005: fue publicada en segunda edición el 1 de junio de 2011 (primera edición del 15 de junio de 2008) y proporciona directrices para la gestión del riesgo en la seguridad de la información. No es certificable.

- ISO/IEC 27006: fue publicada en segunda edición el 1 de diciembre de 2011 (primera edición del 1 de marzo de 2007) y revisada el 30 de septiembre de 2015. Contiene los requisitos para la acreditación de entidades de auditoría y certificación de los sistemas de gestión de seguridad de la información.

- ISO/IEC 27007: publicada el 14 de noviembre de 2011. Es una guía de auditoría. Tampoco es certificable.

- ISO/IEC TR 27008: publicada el 15 de octubre de 2011, también es una guía de auditoría. No certificable.

- ISO/IEC 27009: publicada el 15 de junio de 2016. Plasma los requisitos para el uso de la norma ISO/IEC 27001 en cualquier sector. No es certificable.

- ISO/IEC 27010: fue difundida el 20 de octubre de 2012 y revisada el 10 de noviembre de 2015. Es en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012: es aplicable a todas las formas de intercambio y difusión de información sensible, tanto para organizaciones públicas como privadas, y a los intercambios de información y participación, con relación al suministro, mantenimiento y protección de una organización o de la infraestructura crítica de los estados y naciones.

- ISO/IEC 27011: fue publicada el 15 de diciembre de 2008 y revisada en diciembre de 2016. Es una guía de interpretación, implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones.

- ISO/IEC 27013: publicada el 15 de octubre de 2012 y actualizada el 24 de noviembre de 2015. Es una guía de implementación integrada de ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

- ISO/IEC 27014: fue publicada el 23 de abril de 2013. Es en una guía de gobierno corporativo para la seguridad de la información.

- ISO/IEC TR 27015: publicada el 23 de noviembre de 2012. Establece un marco de referencia de SGSI orientada a organizaciones del sector financiero y de seguros.

- ISO/IEC TR 27016: publicada el 20 de febrero de 2014. Es una orientación para valorar aspectos financieros de la seguridad de la información.

- ISO/IEC 27017: publicada el 15 de diciembre de 2015. Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002. Cuenta con controles específicos de estos entornos de nube.

- ISO/IEC 27018: publicada el 29 de Julio de 2014. Es un código de buenas prácticas en controles de protección de datos para servicios de computación en Cloud Computing.

- ISO/IEC TR 27019: fue publicada el 17 de julio de 2013. Es una para el proceso de sistemas de control específicos de la industria de la energía.

- ISO/IEC 27021: se encuentra en desarrollo y contiene los requisitos de las competencias requeridas para los profesionales dedicados a los sistemas de gestión para la seguridad de la información.

- ISO/IEC TR 27023: publicada el 2 de julio de 2015. Es una guía de correspondencias entre las versiones del 2013 de las normas ISO/IEC 27001 y ISO/IEC 27002. No es certificable.

- ISO/IEC 27031: fue publicada el 1 de marzo de 2011 y sirve de orientación para la adecuación de las tecnologías de información y comunicación (TIC) de una organización. No es certificable.

- ISO/IEC 27032: publicada el 16 de julio de 2012, esta norma establece un marco para mejorar el estado de la seguridad cibernética.

- ISO/IEC 27033: está parcialmente desarrollada y está dedicada a la seguridad en redes.

- ISO/IEC 27034: esta norma está parcialmente desarrollada y regula la seguridad de las aplicaciones informáticas.

- ISO/IEC 27035: fue publicada el 17 de agosto de 2011 y brinda un marco para la gestión de incidentes de seguridad en la información.

- ISO/IEC 27036: es una guía en cuatro partes para la seguridad en las relaciones con proveedores.

- ISO/IEC 27037: fue publicada el 15 de octubre de 2012 y brinda directrices para la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales, localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros.

- ISO/IEC 27038: publicada el 13 de marzo de 2014. Brinda una línea base para la seguridad en la redacción digital.

- ISO/IEC 27039: publicada el 11 de febrero de 2015, esta norma sirve de marco para la selección, despliegue y operación de sistemas de detección y prevención de intrusión (IDS/IPS).

- ISO/IEC 27040: fue publicada el 5 de enero de 2015 y es una guía para la seguridad en medios de almacenamiento.

- ISO/IEC 27041: publicada el 19 de junio de 2015, sirve de marco para garantizar la idoneidad y adecuación de los métodos de investigación.

- ISO/IEC 27042: publicada el 19 de junio de 2015, esta norma cuenta con directrices para el análisis e interpretación de las evidencias digitales.

- ISO/IEC 27043: fue publicada el 4 de marzo de 2015 y desarrolla principios y procesos de investigación para la recopilación de evidencias digitales.

- ISO/IEC 27050: fue publicada en noviembre de 2016 y especifica aspectos de la información almacenada en dispositivos electrónicos.

- ISO 27799: fue publicada el 12 de junio de 2008, con una actualización de julio 2016. Es una norma que aporta directrices para apoyar la interpretación y aplicación en el sector sanitario.

Para este caso se utilizará la norma ISO 27001:2013, la cual es la norma certificable para Colombia:

> Publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012 y una tercera edición de 14 de enero de 2014, esta norma proporciona una visión general de las normas que componen la serie 27000, indicando para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implantación de un SGSI, una introducción a los Sistemas de Gestión de Seguridad de la Información, una breve descripción de los pasos para el establecimiento, monitorización, mantenimiento y mejora de un SGSI (la última edición no aborda ya el ciclo Plan-Do-Check-Act para evitar convertirlo en el único marco de referencia para la mejora continua)[6].

1.2.2 Norma ISO 27000

La Organización Internacional de Estandarización (ISO) recoge un gran número de normas en lo que ha llamado la familia ISO/IEC 27000. Estas son un marco de referencia de seguridad que aplica en el ámbito y que proporcionan un marco para la aplicación de mejores prácticas en la gestión de seguridad de la información para cualquier tipo de organización.

[6] Ibíd.

En Colombia, el Instituto Colombiano de Norma Técnicas y Certificaciones (ICONTEC) es el organismo privado sin ánimo de lucro, encargado de normalizar dichos lineamientos "para estar a la vanguardia de información y tecnología"[7].

Las siguientes son algunas de las normas que componen la familia ISO/IEC 27000, que pueden encontrarse en el portal isotools.org y hacen parte del marco teórico que se tendrá en cuenta para efectos de la presente monografía:

- ISO/IEC 27000: Aporta una visión general de los sistemas de gestión de seguridad de la información y establece los términos y definiciones que se utilizan en las diferentes normas de la 27000.

- ISO/IEC 27001: Su última versión es de finales del año 2013 y es la principal norma de la serie 27000, debido a que presenta los requisitos para establecer, implementar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información en las empresas de diferentes tamaños, tipos o naturaleza. Además, incluye los requisitos para la valoración y el tratamiento de riesgos de seguridad de la información[8].

Esta versión 2013 de la norma, armonizó su estructura con los lineamientos definidos en el Anexo SL de las directivas ISO/IEC, el cual establece que: "Todas las futuras normas de sistemas de gestión tendrán la misma estructura de referencia, texto básico idéntico, así como términos y definiciones comunes. Aunque la estructura de referencia no se puede modificar, se pueden añadir sub-cláusulas y texto específico de la disciplina"[9].

Esta estructura de la nueva ISO27001:2013 significa un gran avance para las organizaciones, porque ahora pueden articular los sistemas que manejan en diferentes áreas, dentro de un único Sistema Integrado de Gestión, bajo los mismos lineamientos y textos. De esta forma también se facilita su ejecución y socialización al interior de las empresas.

---

[7] INSTITUTO COLOMBIANO DE NORMAS TECNICAS Y CERTIFICACIÓN – ICONTEC -. Quiénes somos. [sitio web]. Bogotá D.C. CO. Sec. Inicio . [Consultado 18, agosto, 2017]. Disponible en: http://www.icontec.org/NC/QS/Paginas/Qui.aspx.

[8] ISOTOOLS. La Familia de Normas ISO 27000. [sitio web]. Bogotá D.C. CO. Sec. Inicio. [Consultado 18, agosto, 2017]. Disponible en: https://www.isotools.org/2015/01/21/familia-normas-iso-27000.

[9] BSI GROUP. ISO / IEC 27001 Gestión de la seguridad de la información. [sitio web]. Reino Unido. [Consultado 17, agosto, 2017]. Disponible en : https://www.bsigroup.com/LocalFiles/esES/Documentos%20-tecnicos/Revisiones%20ISO/ISO%209001/BSI-Anexo%20SL-ISO-9001-2015.pdf.

1.2.3 Estándares ISO 27000

1.2.3.1 ISO 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares. Como dicen los fundamentos[10], la norma ISO 27000 es certificable posterior a una auditoría. Para tal fin las organizaciones deben contar con un Sistema de Gestión de Seguridad de la Información (SGSI) y este debe estar implementado como mínimo con tres meses de antelación.

En la auditoría se toman en cuenta puntos como la política de seguridad (que debe incluir los objetivos y estar alineada a la gestión del riesgo en general), la asignación de responsabilidades de seguridad (en la que se señalan tareas específicas para cada persona), la formación y capacitación para la seguridad (en la que se demuestra la conciencia del personal con la seguridad de la información), el registro de incidencias de seguridad (que determina los controles y las respuesta a incidentes), la gestión de continuidad del negocio (que revisa que el objetivo del sistema no se pierda por el camino), la salvaguarda de registros de la organización (en donde se revisa que los registros cumplan con las propiedades de confidencialidad, integridad y disponibilidad), la protección de datos personales (como parte de la información total de la organización) y los derechos de propiedad intelectual (que garantizan que la organización tenga las licencias y permisos para el uso de software).

La auditoría se realiza en tres fases: la pre-auditoría, que es opcional pero de gran ayuda para obtener información sobre el estado de la organización, y la primera y segunda fase, que tardan máximo seis meses y consisten en analizar la documentación, destacar cualquier falla de la norma, revisar las políticas y las exclusiones según la Declaración de Aplicabilidad. El resultado de estas dos fases es el informe de la auditoría. Una vez se hayan tomado las acciones correctivas (en caso de que sea necesario) y de haberse verificado, el auditor emite un informe favorable que se traduce en la certificación ISO 27001.

Posterior a la certificación, es importante llevar a cabo un seguimiento a través de auditorías semestrales o anuales. De esta forma se garantizará que el SGSI se use en la organización. Además, la certificación debe ser renovada cada tres años, siguiendo las fases anteriormente mencionadas.

Para esta labor es importante señalar que existen tres tipos de auditores, es decir, personas que comprueban que el SGSI de una organización esté correctamente

[10] LADINO, Martha; VILLA, Paula y LÓPEZ, Ana. Fundamentos de ISO 27001 y su aplicación en las empresas. En: *Scientia et technica.* Pereira. No. 47 (abril, 2011), p. [334-339].

diseñado e implementado. El primero es el auditor interno, que pertenece a la organización y la mantiene alerta para la auditoría de certificación; el segundo es el auditor de cliente, que audita en nombre de un cliente de la empresa; y el tercero es el auditor independiente, que audita como una parte imparcial, dirigido a lograr la certificación. Vale la pena aclarar que el auditor debe disponer de certificación de competencias profesionales para desempeñar la labor.

Por otra parte, aunque el proceso de certificación es largo, complejo y costoso, aplica puntos clave en materia de seguridad. Aquí Ladino, M.I., Villa, P.A., y María, A. L.[11] brindan algunas recomendaciones para implementar un sistema de seguridad en la organización, que harán el proceso más fácil y económico:

- La alta dirección debe tener conocimiento del sistema y de los riesgos a los que se expone la organización de no contar con un SGSI.
- La organización debe identificar todos los activos relacionados con la información: equipos, aplicaciones y la misma información.
- La empresa debe fomentar una cultura de seguridad en todos los miembros: La seguridad no solo puede quedar plasmada en el papel.
- Los expertos del área de seguridad (jefe de área y su equipo) deben identificar amenazas y debilidades que puedan afectar a los activos críticos. Así será más fácil determinar los riesgos y su frecuencia.
- La organización debe tener presente que es imposible controlar todos los riesgos. Así que es importante que definan un nivel aceptable de riesgo, es decir, cuáles pueden asumir porque no generan un impacto tan negativo en el trabajo de la entidad.
- Posterior al diseño del sistema de seguridad, se debe promover la capacitación de las personas que trabajan en la organización y proveer los equipos necesarios para garantizar la seguridad.
- Y para que la implementación sea efectiva, se requiere hacer seguimiento y control a los procesos y hallazgos, de tal forma que exista una retroalimentación que permita mejorar el SGSI e identificar nuevos riesgos.

1.2.3.2 ISO 27001:

Como afirman MANJÓN-CABEZA, M., & MARÍA, J.12, esta es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y

[11] Ibíd.

[12] MANJÓN CABEZA, José María. Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013. Universidad Oberta de Catalunya. Barcelona, 2015.

describe cómo gestionar la seguridad de la información en una empresa. Su nombre completo es ISO/IEC 27001:2013.
La primera revisión se publicó en 2005 y fue desarrollada con base a la norma británica BS 7799-2. ISO 27001. Esta puede ser implementada en cualquier tipo de organización y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización.

La certificación de esta norma da la seguridad de que se ha dado cumplimiento a una norma que se ha convertido en la principal en el ámbito mundial para la seguridad de la información.

> Es un estándar para la seguridad de la información, y fomenta la importancia de entender los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información, implementar y operar controles para manejar los riesgos de la seguridad de la información, monitorear y revisar el desempeño y la efectividad de SGSI y mejoramiento continuo en base a la medición de los objetivos[13].

Con relación a su origen, Parra afirma que[14]: La British Standards Institution (BS) promulgó en 1995 la norma BS 7799-1, en la que dio a conocer algunas prácticas para ayudar a las empresas británicas a administrar la seguridad de la información. Las recomendaciones aún no daban opción de certificación; pero en 1998, una segunda parte de esta misma publicación, estableció los requisitos a cumplir para tener un Sistema de Gestión de Seguridad de la Información certificable. Las dos publicaciones fueron revisadas en el año 2000 por la Organización Internacional para la Estandarización (ISO) dando lugar a la norma británica ISO 17799. La versión BS 7799 del año 2002 incluyó la acreditación de empresas por una entidad certificadora en Reino Unido y en otros países.

En el año 2005, Estándar ISO 27001 se convirtió en la norma principal de la serie, dando a conocer los requisitos del Sistema de Gestión de Seguridad de la Información. En el año 2007 surge la Estándar ISO 27002:2005 y una nueva versión de la ISO 270001:2007, la cual es conocida en Chile como NCh-ISO27001, en España como UNE-ISO/IEC 27001:2007, en Colombia como NTC-ISO-IEC 27001, en Venezuela como Fondo norma ISO/IEC 27001, en Argentina como IRAM-ISO

[13] GIRALDO, Luis. Análisis para la implementación de un sistema de gestión de la seguridad de la información según la norma ISO 27001 en la empresa Servidoc S.A. Universidad Nacional Abierta y a Distancia. Cali. Especialización en Seguridad Informática. 2016.

[14] PARRA, Julieth. Elaboración de un plan de implementación de la norma ISO/IEC 27001: 2013 en una empresa prestadora de servicios de acueducto y alcantarillado. Universidad Oberta de Catalunya. Barcelona, 2015.

IEC,c 27001, en México como NMX-I-041/02-NYCE y en Uruguay como UNIT-ISO/IEC 27001[15].

Posteriormente, en el año 2013, la nueva versión de la ISO 27001 presenta cambios en la estructura, la forma de evaluar y el tratamiento a los riesgos. En el 2014 aparece la versión ISO 27002, que se actualizó con base en los cambios de la norma ISO 27001:2013.

1.3 MARCO LEGAL

Ley 23 de 1982: Reglamenta todas las generalidades sobre las normas que protegen los derechos de autor para cualquier obra científica, literaria u artística.

Ley 44 de 1993: Modifica y adiciona la ley 23 de 1982.

Ley 527 de 1999: Se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones.

Documento Conpes 3072 de 2000: Agenda de conectividad programa presidencial para la identificación de las necesidades de información, computacional y social en Colombia.

Decreto 1747 de 2000 artículo 9: La entidad deberá contar con un equipo de personas, una infraestructura física y tecnológica y unos procedimientos y sistemas de seguridad, tal que puedan generar las firmas digitales propias y todos los servicios para los que soliciten autorización.

Ley 962 de 2005: ley Anti-tramites, tiene como objetivo facilitar las relaciones de los particulares con la administración pública.

Ley 1151 de 2007 artículo 6: El cual especifica la intención del estado en promover la implementación progresiva del software en las entidades públicas y la inclusión digital.

Decreto 1151 de 2008: Reglamenta los lineamientos de gobierno en línea y empieza a implementar la ley anti- trámites.

Ley Estatutaria 1266 de 2008 “Habeas Data”, que regula el manejo de la información de las personas recopiladas y almacenadas en bases de datos de terceros, en especial la información de carácter financiero, crediticio, comercial, de servicios y la proveniente de terceros países.

[15] Ibíd.

Ley 1273 de 2009: Dicta disposiciones para preservar integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones.

Documento Conpes 3650 de 2010: Implementa la agenda de conectividad.

Ley 1450 de 2011 art. 227: Administración de bases de datos de acceso permanente, seguro y confiable.

Ley 1450 de 2011 art. 230: Establece el cumplimiento de la estrategia de gobierno en línea que será liderada por el Mintic.

Ley 1450 de 2011 art. 232: Haciendo uso de las tecnologías y las comunicaciones ofrecer una oportuna, eficiente y eficaz prestación de servicio en la gestión de las entidades.

Decreto 2693 de 2012: Definir lo lineamientos, plazos términos para garantizar el máximo aprovechamiento de las tecnologías de la información y las comunicaciones con el fin de contribuir con la construcción de un estado más eficiente más transparente y participativo que preste mejores servicios con la colaboración de toda la sociedad. Utilizar lineamientos o estándares internacionales.

Ley Estatutaria 1581 de 2012: Por la cual se dictan disposiciones generales para la protección de datos personales. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

1.4 EL CICLO DE MEJORA CONTINUA

También conocido como ciclo PDCA (del inglés plando-check-act), el ciclo de mejora continua o PHVA (Planificar-Hacer-Verificar-Actuar), también es conocido como Ciclo de Deming por ser Edwards Deming su creador[16].

Actualmente es la herramienta gerencial más utilizada en la gestión de los sistemas de calidad. En la gran mayoría de las organizaciones del mundo se ha podido demostrar la mejora continua obtenida en los niveles de eficacia y eficiencia de cada

[16] PDCA HOME. Ciclo PDCA (Planificar, Hacer, Verificar y Actuar). [sitio web]. España. [Consultado 16, agosto, 2017]. Disponible en: https://www.pdcahome.com/5202/ciclo-pdca/.

uno de sus procesos. La planeación de recursos y las actividades (planear), la realización de lo planeado (hacer), analizar y medir si se obtuvo lo que se planeó (verificar), y determinar las mejoras o correcciones a lo realizado (actuar); son las principales características. Empezar nuevamente el proceso en procura de una mejora, siempre va en sentido ascendente y sin un final determinado. Estas son las etapas de este ciclo[17]:

- **Planear (P)**: consiste en gestionar el riesgo a través de políticas, objetivos, procesos, procedimientos y metas, para mejorar la seguridad de la información y contar con indicadores de resultados que permitan establecer la forma de cumplir los objetivos de la organización.

- **Hacer (H)**: Significa ejecutar las tareas como se propusieron en el plan y contar con las evidencias del trabajo. Para el cumplimiento de la ejecución es fundamental el entrenamiento previo del personal.

- **Verificar (V)**: Consiste en comparar los resultados con las metas propuestas en la etapa de planeación.

- **Actuar (A)**: Se detectan los desvíos y se toman las medidas para evitarlos a través de acciones correctivas y preventivas. Esta etapa se realiza con base en los resultados de las auditorías internas y la revisión realizada por la dirección.

1.4.1.1 Ventajas y desventajas del ciclo PHVA (planear, hacer, verificar, actuar)

Dentro de sus principales ventajas están[18]:

- Obtención de la mejora en corto plazo con resultados visibles.
- Reducción en costos de fabricación de algunos productos y la prestación de los servicios.

---

[17] MORALES, Rodolfo. Diseño para la implementación de tres dominios de un sistema de gestión en la seguridad de la información basada en la norma ISO 27001 e ISO 27002, para el área de software de la procesadora nacional de alimentos Pronaca. Maestría en Gerencia de Redes y Telecomunicaciones. Universidad de las Fuerzas Armadas ESPE. Ecuador, 2015.

[18] ISO TOOLS. ¿En qué consiste el ciclo PHVA de mejora continua? [sitio web]. Colombia. [Consultado 16, agosto, 2017]. Disponible en: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua.

- Incrementa la productividad de la organización y la enfoca a un mejor grado de competitividad.
- Detecta y elimina los procesos repetitivos.

Y las desventajas[19]:

- El mejoramiento deberá hacerse a todas las áreas de la organización y no centrarse en una sola**, porque se podrá perder la perspectiva de interrelación** existente entre las distintas áreas de la organización.

- Es un cambio importante para toda la organización, lo que conllevará a inversiones bastante importantes en los recursos, tanto en infraestructura como en humano.

1.4.1.2 Cómo se aplica

Este es un ejemplo basado en los anteriores conceptos y en el aporte sobre ciclo que hacen Manuel García, Carlos Quispe y Luis Ráez[20]: si una persona desea conocer algún lugar del mundo en el exterior, lo primero que hace es mirar que opciones tiene y conque recursos cuenta, de esta forma se decide por un sitio en especial (Planificar), y que lo puede lograr ahorrando durante todo el año hasta sus próximas vacaciones, de esta forma se va de paseo (hacer).

Después de su regreso comienza a hacer balances de todo lo que disfrutó de sus vacaciones en términos del incremento de su satisfacción con respecto a otras vacaciones, de los nuevos lugares que conoció, cuán lejos logro llegar a fin de compararlos con los ya visitados y que no estaban tan lejanos de su lugar de residencia y por ende no tan placenteros (verificar). Con estos balances, decide ahorrar un poco más para futuros viajes (actuar).

1.4.1.3 Cómo se trabaja en las organizaciones

La mejora continua de los procesos puede lograrse aplicando el concepto de PHVA en cualquier nivel de la organización y en cualquier tipo de proceso, ya que está directamente asociado con la planificación, implementación, control y mejora del desempeño. El concepto es aplicable en procesos estratégicos de la alta dirección, como en las actividades operativas[21].

---

[19] Ibid.

[20] GARCÍA, Manuel, QUISPE, Carlos y Ráez, Luis; Mejora continua de la calidad de los procesos, Industrial Data. Vol 5. Número 1. Universidad Nacional Mayor de San Carlos. Lima, Perú. 2003.

Sobre la importancia dice Durango[22] que la utilización continua del PHVA brinda una solución que permite mantener la competitividad de los productos y servicios, mejorar la calidad, reducir los costos mejorar la productividad, aumentar la participación en el mercado y la supervivencia de la empresa, así como proveer nuevos puestos de trabajo y aumenta la rentabilidad de la organización.

1.4.1.4 Ciclo de mejora continua alineado a la norma ISO 27001:2013

Aunque la norma ISO 27001 en su versión 2013, no tiene la sección de "Enfoque basado en procesos" que apareció en la versión 2005, la nueva estructura de esta versión se puede armonizar con el ciclo de mejora continua. Este proceso pretende generar mayor flexibilidad al momento de seleccionar un modelo de mejora continua del Sistema de Gestión de Seguridad de la Información. En la figura 2 se presenta el ciclo de mejora continua para alinearlo posteriormente a la norma.

Figura 2. Ciclo de mejora continua alineado a la norma ISO 27001:2013

Fuente: WELIVESECURITY. Publicada ISO 27000:2013, cambios en la norma para gestionar la seguridad de la información. [sitio web]. [Consultado 18, agosto, 2017]. Disponible en: http://www.welivesecurity.com/la-es/2013/10/09/publicada-iso-270002013-cambios-en-la-norma-para-gestionar-la-seguridad-de-la-informacion/

[21] Ibíd.

[22] DURANGO, José. Ciclo PHVA. [sitio web]. Colombia. [Consultado 16, agosto, 2017]. Disponible en: http://www.escolme.edu.co/almacenamiento/oei/tecnicos/ppios_admon/contenido_u3_2.pdf.

se evidencia la relación que existe entre las fases del ciclo de la mejora continua "PHVA" (planear, hacer, verificar y actuar) y la estructura de capítulos y numerales de la norma ISO 27001:2013:

Cuadro 1. Fases PHVA vs Estructura ISO 27001:2013

Fase PHVA	ISO 27001:2013
PLANEAR	4. Contexto de la organización. 5. Liderazgos. 6. Planificación. 7. Soporte.
HACER	8. Operación.
VERIFICAR	9. Evaluación de desempeño.
ACTUAR	10.Mejora.

Fuente: SGSI. Blog especializado en Sistemas de Gestión de Seguridad de la Información. [basada en sitio web]. [Consultado 18, agosto, 2017]. Disponible en: http://www.pmg-ssi.com/2015/06/iso-27001-ciclo-de-deming/

Por lo anterior, de aquí en adelante se llevará a cabo una explicación de la estructura que plantea la norma de acuerdo a las fases PHVA, teniendo en cuenta el capítulo respectivo de este en la misma.

Fase: PLANEAR en la norma ISO 27001:2013

Según la norma ISO 27001:2013[23]: en esta fase se debe comenzar por realizar un análisis de las cuestiones externas e internas de la organización y del contexto en el que se mueve, con el fin de incluir las necesidades y expectativas de las partes interesadas en el alcance del SGSI.

Una parte importante de esta primera fase es el liderazgo[24], que como menciona la NTC, establece las responsabilidades y compromisos de la alta dirección con al Sistema de Gestión de Seguridad de la Información y la necesidad de definir una política de seguridad adecuada y específica para el propósito de la organización. Desde esta fase debe asegurarse la asignación de los recursos para el SGSI y las responsabilidades de todos los involucrados.

[23] INSTITUTO COLOMBIANO DE NORMAS TÉCNICAS Y CERTIFICACIÓN. NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001. NTC-ISO-IEC 27001:2013. Bogotá D.C.: El Instituto, 2006.

[24] Ibíd., p. 2-3.

En esta fase[25] se establece toda la valoración, los riesgos de la seguridad y los objetivos para el tratamiento de los riesgos.

Fase HACER en la norma ISO 27001:2013

En la operación de la norma ISO 27001:2013[26], se señala que la organización debe planificar, implementar y controlar todos los procesos necesarios para cumplir los objetivos y requisitos de seguridad. En esta fase se lleva a cabo el tratamiento de los riesgos de la seguridad de la información, asegurando contar con todas las evidencias y registros necesarios.

Fase VERIFICAR en la norma ISO 27001:2013

En la Evaluación del desempeño[27], se definen claramente los requerimientos para evaluar de forma periódica el desempeño de la seguridad de la información y eficacia del sistema de gestión de seguridad de la información. De tal forma que la organización pueda dar continuidad a procesos o definir nuevas rutas para la mejora continua de la seguridad de la información.

Fase ACTUAR en la norma ISO 27001:2013

Según la Norma Técnica Colombiana NTC-ISO/IEC 27001[28], la mejora de los procesos se establece para mejorar del Sistema de Gestión de Seguridad de la Información, que a partir de las no-conformidades que ocurran, se generan al interior de las organizaciones. Estas entidades deben establecer acciones más efectivas para solucionarlas y evaluar la necesidad de nuevas operaciones, para eliminar las causas de la no conformidad y evitar su repetición.

1.5 BS 7799-2

La norma BS 7999 se origina en Inglaterra a mediados de 1995 y fue promulgada por la entidad British Standards Institution, con el objetivo de brindar buenas prácticas en seguridad. En 1998 se publica la norma BS 7792, que fue derivada de

[25] Ibíd., p. 4-6.

[26] Ibíd., p. 8-9.

[27] Ibíd., p. 9-11.

[28] Ibid. p. 11-12.

la primera y tiene como beneficios: mejorar el desempeño, reducir el riesgo y ser más sustentable.

Al respecto, la Global Information Assurance Certification Paper dice[29]:

> Esta norma específica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización. Especifica los requisitos para la implementación de los controles de seguridad adaptados a las necesidades de las organizaciones individuales o partes de ellas.
>
> El SGSI está diseñado para garantizar controles de seguridad adecuados y proporcionados que protejan adecuadamente los activos de información y brinden confianza a los clientes ya otras partes interesadas. Esto puede traducirse en mantener y mejorar la ventaja competitiva, el flujo de caja, la rentabilidad, el cumplimiento legal y la imagen comercial.

1.6 ANTECEDENTES

A partir de la revisión de la literatura, es posible encontrar diferentes estudios realizados en torno al objeto de estudio, que sirven como referente para el desarrollo de la monografía. Existen diferentes autores, informes, revistas científicas, leyes, decretos, resoluciones, cartillas, trabajos de grado, libros públicos o privados y artículos indexados.

De acuerdo al autor Manjón-Cabeza,[30]: esta tesis de grado tiene como objeto el desarrollo de un análisis para la implantación de un Sistema de Gestión de Seguridad de la Información dentro de una organización ficticia pero aplicable a cualquier tipo y ubicada en cualquier parte del mundo. Su desarrollo fue seguido por las directrices establecidas en la norma ISO 27001 y sus resultados fueron: el análisis contextual del SGSI, estudio de las normas ISO 27001 y 27002, análisis y diagnóstico de la empresa, determinación del sistema de gestión documental, tratamiento de riesgos, propuesta de proyectos y determinación de auditorías de control.

---

[29] Global Information Assurance Certification Paper. Information security management system (BS7799-2:2002) implementation overview. [sitio web]. Estados Unidos. [Consultado en 17, agosto, 2017]. Disponible en: https://www.giac.org/paper/gsec/3740/information-security-management-system-bs-7799-2-2002-implementation-overview/105976.

[30] MANJÓN-CABEZA, José María. Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013. Universidad Oberta de Catalunya. Barcelona, 2015.

A su vez Porras León, R. A.[31], establece una metodología para la adecuada implantación de un Sistema de Gestión de Calidad basado en la Norma ISO 9001:2008, en las instituciones del sector público ecuatoriano, considerando sus características particulares. El estudio se basa en el análisis de experiencias en implementación de este tipo de sistemas, para lo cual se recopila información histórica, se realiza un análisis comparativo y se identifican factores claves en la implementación de entrevistas con partes relacionadas, teniendo como resultado la documentación de una metodología con las mejores prácticas.

Mientras que Sarria Cuéllar, M. [32] tiene como objetivo el proponer un diseño de modelo de un sistema de gestión de seguridad de la información, mediante la metodología de la norma ISO/IEC 27001:2013. Sus resultados fueron: determinación del campo contextual de la empresa, implementación de la metodología de la norma ISO 27001 (planear, hacer, verificar, actuar), tratamiento de los riesgos, diseño de un modelo de SGSI, diseño de implementación del SGSI y plan de contingencia de la empresa.

Por su parte, Arévalo, J. G., Bayona, R. A., Bautista, R., & Willmer, D.[33] exploraron la actividad productiva en una zona de Santander, mediante una investigación descriptiva que les permitiera obtener los resultados de debilidades empresariales en temas como por ejemplo la información, para proponer el uso de herramientas de análisis de sistemas de información, usando la norma ISO 27001:2005.

En el estudio de Solarte, F., Rosero, E. & del Carmen Benavides, M.[34] desarrollaron una metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001.

---

[31] ARROYO, Flavio y PORRAS, Ronald. Estudio metodológico para la implementación de un sistema de gestión de calidad basado en Norma ISO 9001:2008, aplicable para Instituciones del Sector Público Ecuatoriano. Trabajo presentado como requisito parcial para la obtención del Grado de Magíster en Sistemas Integrados de Gestión. Instituto de Investigación y Posgrado. Universidad Central del Ecuador. Quito, 2016, p. [35].

[32] ARÉVALO, José; BAYONA, Ramón y RICO, Willmer. Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. En: Revista Tecnura. Abril-agosto, 2015, p. [123-134].

[33] Ibíd.

[34] SARRIA, Mercedes. Diseño de un modelo de un sistema de gestión de seguridad de la información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001: 2013. Tesis de grado para optar por el título: Especialista En Seguridad Informática. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Florencia, 2015.

El artículo tiene como objetivo desarrollar habilidades en los ingenieros de sistemas, que les permitan conducir proyectos de diagnóstico, para la implementación e implantación de sistemas de seguridad de la información – SGSI alineado con el estándar ISO/IEC 27001 y el sistema de control propuesto en la norma ISO/IEC 27002,los resultados son los de una experiencia aplicando las fases de auditoría y la metodología de análisis y evaluación de riesgos con el diseño y aplicación de diversos instrumentos como cuestionarios aplicados a los administradores, clave de seguridad, entrevistas al personal del área informática y usuarios de los sistemas, pruebas de intrusión y testeo. Posteriormente se aplica una lista de chequeo basada en la norma, para verificar la existencia de controles de seguridad en los procesos organizacionales. Finalmente y de acuerdo a los resultados del análisis y evaluación de los riesgos, se proponen los controles de seguridad para que sean integrados hacia el futuro dentro de un SGSI que responda a las necesidades de seguridad informática y de la información acorde a sus necesidades[35].

[35] SOLARTE, Francisco; ROSERO, Edgar y BENAVIDES, Mirian. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. En: Revista Tecnológica-ESPOL. Diciembre, 2015, vol. 28, No 5.

2 . DISEÑO METODOLÓGICO

2.1 TIPO DE INVESTIGACIÓN

Se realizó un estudio de tipo cualitativo descriptivo, que partió del resultado de investigaciones ya realizadas, para resolver el problema a tratar: cómo diseñar un plan para la implementación de un SGSI en una empresa del sector público, bajo la norma ISO 27001:2013.

2.2 FUENTES DE INFORMACIÓN

Se analizó la información obtenida por los proyectos de implementación de SGSI de otros autores que se encuentran en internet, como las bases de datos suscritas por la Universidad de América y de acceso libre; además de material de tipo bibliográfico, libros, revistas y la norma que se encuentra disponible en el ICONTEC. A continuación se relacionan las actividades detalladas según su objetivo:

2.3 ACTIVIDADES DETALLADAS

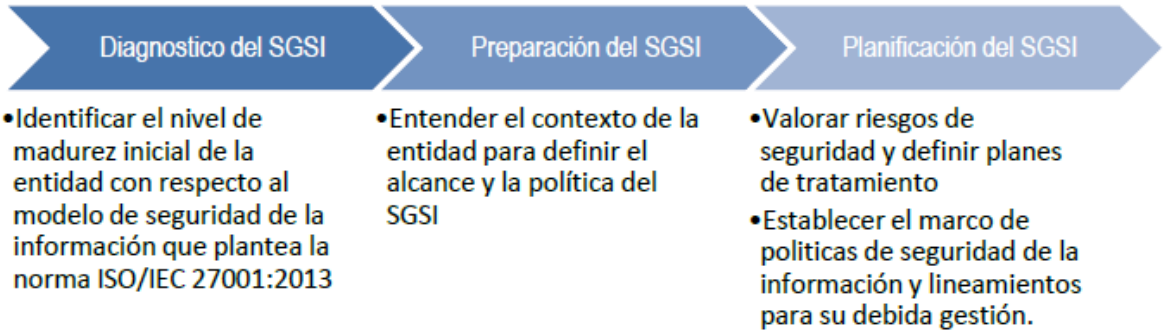
Cuadro 2. Relación de objetivos específicos y actividades

Objetivo especifico	Actividades
Realizar el análisis del contexto organizacional basado en el numeral 4 de la NTC ISO27001:2013 para un sistema de gestión de la seguridad de la información.	1. Consulta de la norma
Evaluar los riesgos de la seguridad de la información en una empresa prestadora de servicios de vigilancia del sistema de carrera administrativa basado en el numeral 6.1 de la NTC ISO27001:2013.	2. Definir los requerimientos de la norma.
Determinar las actividades y herramientas necesarias dirigidas a la implementación del sistema de gestión de Seguridad de la Información en una empresa del sector público conforme los requisitos de la NTCISO 27001:2013	3. Establecer alcance del SGSI. 4. Establecer las políticas y objetivos del SGSI. 5. Definir el enfoque organizacional para la valoración de los riesgos. 6. Definir los controles aplicables.

Fuente: elaborado por el autor.

Para lograr lo planteado dentro del diseño del Sistema de Gestión de Seguridad de la entidad, se proponen las actividades en la figura siguiente:

Figura 3. Fases para el diseño del SGSI



Fuente: GUZMÁN C.A. Diseño de un sistema de gestión de seguridad de la información. Trabajo de grado. Instituto Politécnico Gran Colombiano. [sitio web]. [Consultado 18, agosto, 2017]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/654/ProyectodeGradoSGSI-IGM-CarlosGuzmanFINAL.pdf?sequence=1&isAllowed=y

3 EMPRESA CASO DE ESTUDIO

3.1 GENERALIDADES

La organización seleccionada para el caso de estudio fue la Comisión Nacional del Servicio Civil (CNSC), entidad que hace parte del Sistema Técnico de Administración de Personal del Estado, que ejerce la función pública y la carrera administrativa. “La carrera administrativa es un sistema técnico de administración de personal que tiene por objeto garantizar la eficiencia de la administración pública y ofrecer igualdad de oportunidades para el acceso al servicio público, la capacitación, la estabilidad en los empleos y la posibilidad de ascenso”[36].

Para alcanzar estos objetivos: el ingreso, la permanencia y el ascenso en los empleos de carrera administrativa se utiliza la metodología del mérito; en el que aspectos como la raza, la religión, el sexo, la filiación política o las consideraciones de otra índole, no puedan tener influencia en la elección del personal[37].

La CNSC parte del principio de igualdad en la oportunidad y el mérito para lograr profesionalizar o estabilizar el empleo público, buscando lograr la eficiencia y el buen servicio a la sociedad. Además, también es el organismo encargado de regular los deberes y derechos de la administración y el funcionario. Por esta razón, el sistema busca verificar la honestidad del servidor público, a través de la regulación de sus deberes y derechos, apoyándose en funcionarios expertos.

Su historia se remonta a 1938 cuando se hizo la primera regulación de la carrera administrativa. En ese entonces un informe dio a conocer la experiencia de la en esta área, y arrojó resultados desalentadores: las personas consultadas (como sindicatos, empleados, supervisores y hasta el público en general) opinaban que resultaba inoperante y no cumplía su finalidad.

Del 100% de los empleados gubernamentales, un poco menos del 3% había ingresado a la carrera administrativa desde que empezó, y de este porcentaje apenas el 2,8% lo había hecho con un examen. El restante lo logró con algún tipo de beneficio recibido, por ejemplo: cumplir dos años de servicio o la obtención de un certificado de buena conducta.

---

[36] COLOMBIA. CONGRESO DE LA REPÚBLICA. Ley 443. (11, junio, 1998). Por la cual se expiden normas sobre carrera administrativa y se dictan otras disposiciones. Bogotá D.C., p. [1].

[37] Comisión Nacional del Servicio Civil. [sitio web]. Colombia. [Consultado 16, agosto, 2017] Disponible en: https://www.cnsc.gov.co/.

Llegó a demostrarse que había disposiciones que protegían al empleado ante alguna destitución por motivos políticos, y esto fue aprovechado por muchos para mantener en sus cargos a aquellos ineficientes e incompetentes; lo que originó que en muchos sectores se viera la carrera administrativa con desconfianza y no como una prueba de esfuerzo y mérito individual.

En la Colombia del siglo XX, la perspectiva jurídica política de la carrera administrativa no tenía un horizonte claro. El tratamiento que se le daba, estaba relacionado con el clientelismo de tipo partidista y el pago de cuotas políticas para el reconocimiento personal.

En 1957 los partidos políticos Liberal y Conservador se pusieron de acuerdo para diseñar e implementar un sistema de carrera. El acuerdo fue firmado por Benidorm, Sitges, Alberto Lleras y Laureano Gómez, dando origen al plebiscito que limitaba la facultad del presidente electo en la elección y despido de los empleados del gobierno y creaba una carrera más seria y con un buen grado de especialización de los empleados contratados, para manejar los negocios públicos.

En la reforma a nuestra Carta Magna de 1958, se elevó la carrera administrativa al plano constitucional, instituyendo que las inclinaciones políticas de los ciudadanos no podrían ser un obstáculo para acceder a un cargo público de carrera administrativa, ni para ser destituido.

> Con la expedición de la Ley 19 de 1958, se crearon, entre otros, el Departamento Administrativo del Servicio Civil, la Escuela de Administración Pública, la Sala de Consulta y Servicio Civil del Consejo de Estado, que dieron un sentido más técnico a las obligaciones del Estado con respecto a la administración de personal[38].

Con el sistema de nombramiento y provisión de empleo se tomó un nuevo rumbo, pues la facultad constitucional del presidente para nombrar y cambiar a los funcionarios, se limitó a aquellos que fuesen políticos de confianza o de agencia presidencial.

En 1960 se expide el Decreto-Ley 1732, en el que se categorizan los empleos en: libre nombramiento y carrera administrativa, y se establece el método técnico de elección de funcionarios basado en la igualdad y el mérito personal. La experiencia no fue muy satisfactoria, porque que su ejecución en el ámbito nacional fue parcial y en el plano territorial fue marginada; debido a que no se le dio la misma importancia en cada uno de los niveles. Esto sucedió tanto en las funciones como la asignación presupuestal. A esto se le suma la demanda burocrática de los grupos políticos que exigían la inclusión de personal de su interés en la nómina oficial.

---

[38] GONZÁLEZ, Efrén. La Carrera Administrativa: experiencias y perspectivas. En: Revista Administración y Desarrollo. Escuela Superior de Administración Pública. 2010, No. 25, p. [13-42].

La expedición del Decreto 2400 de 1968, durante el gobierno de Carlos Lleras Restrepo, introdujo la reforma administrativa donde se descentralizó la selección a las unidades de personal de cada organismo. El estatuto para funcionarios de carrera pasó a un reglamento de administración de personal y nuevamente se hizo a un lado en el plano territorial, pues se interpretó que era aplicable al nacional.

Fue hasta 1973 que se reglamentó la carrera administrativa, debido a la existencia del fenómeno del clientelismo que convivía con los administradores de la política del momento, y la cada vez mayor importancia del nivel territorial, que se tomaba menos en cuenta por su poca representación fiscal en el Producto Interno Bruto (PIB) de la nación, como en la tributación nacional.

Después de 10 años se decreta nuevamente bajo la condición de que sea implementada gradualmente. Fue así como la carrera administrativa creció secuencialmente debido al gran número de cargos provisionales. Posteriormente, sale a la luz pública la Ley 61 de 1987 y determina los empleos de libre nombramiento y remoción. Los demás empleos que regula -por un concepto residual- son los de carrera administrativa y la insubsistencia, la carrera diplomática y consular, el retiro, entre otros.

En la última década del siglo XX con la reforma a la Constitución Nacional, se promulgaron leyes y decretos complementarios que adoptaron códigos y normas, creando sistemas relativos a la carrera administrativa y a un régimen procedimental para actuaciones administrativas entre autoridades del sistema y de la función pública.

En 1998 se promulga la Ley 489, llamada también Estatuto Básico de Organización y Funcionamiento de la Administración Pública, y para agosto de 1999 se promulga el Decreto 1444, por medio del cual se reestructura el Departamento Administrativo de la Función Pública y se le asigna la responsabilidad de fijar políticas en gestión del talento humano, en torno de todas sus prácticas administrativas[39].

Actualmente, el régimen de carrera administrativa es regulado por la Ley 909 de 2004, con la que se buscó mejorar las falencias señaladas, con apoyo en la jurisprudencia desarrollada por la Corte Constitucional, en la que se otorgó plena autonomía a la Comisión Nacional del Servicio Civil, creando los acuerdos de gestión entre los nominadores y los cargos de gerencia pública, así como la posibilidad de organizar concursos de meritocracia para algunos cargos de libre

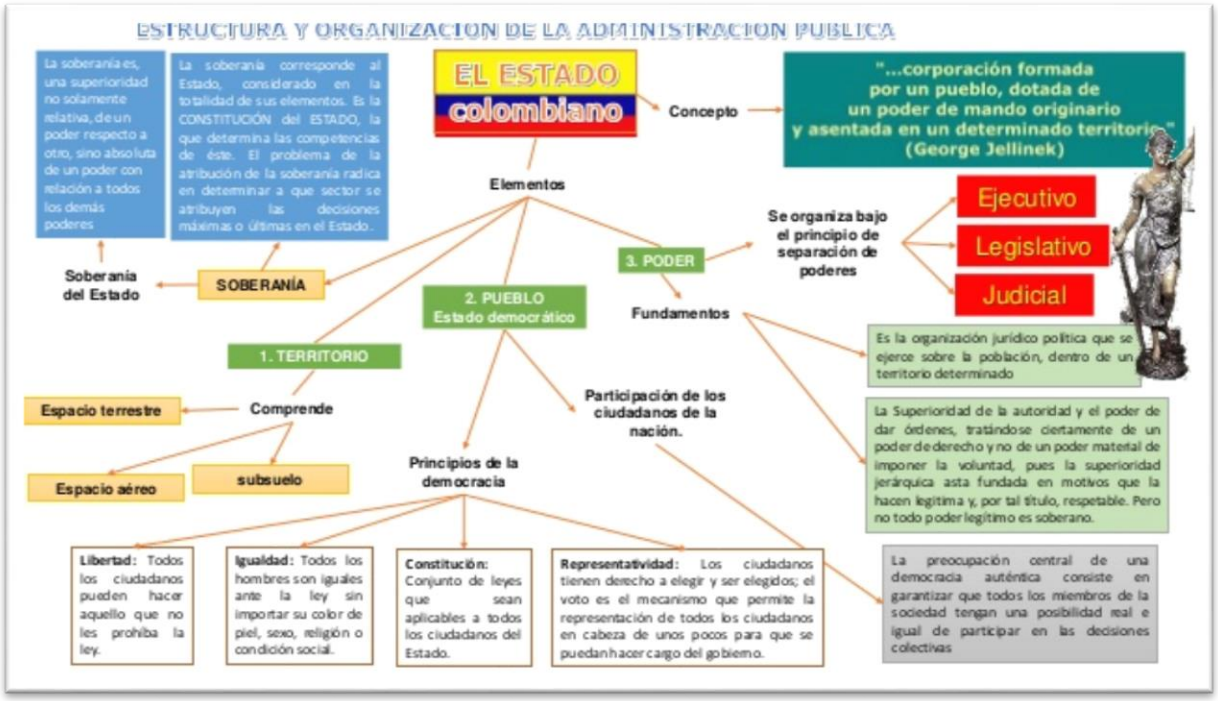
[39] Comisión Nacional del Servicio Civil. [sitio web]. Colombia. [Consultado 16, agosto, 2017] Disponible en: https://www.cnsc.gov.co/.

nombramiento y remoción[40].

De igual manera, se determinó el tiempo máximo de seis años para comisionar a servidores de carrera en cargos de libre nombramiento y remoción. En el documento se consagró también el respeto a los derechos de maternidad, estado de gestación, discapacidad y desplazamiento, entre otros. Además fijó los procedimientos para las distintas etapas de los concursos públicos de méritos, a partir de la convocatoria y expresó las causales de retiro de los servidores de carrera[41].

A continuación se presenta la estructura de la administración pública en el país que regula la Comisión y la estructura orgánica por la que vela (figuras 6 y 7):

Figura 4. Estructura y organización de la administración pública

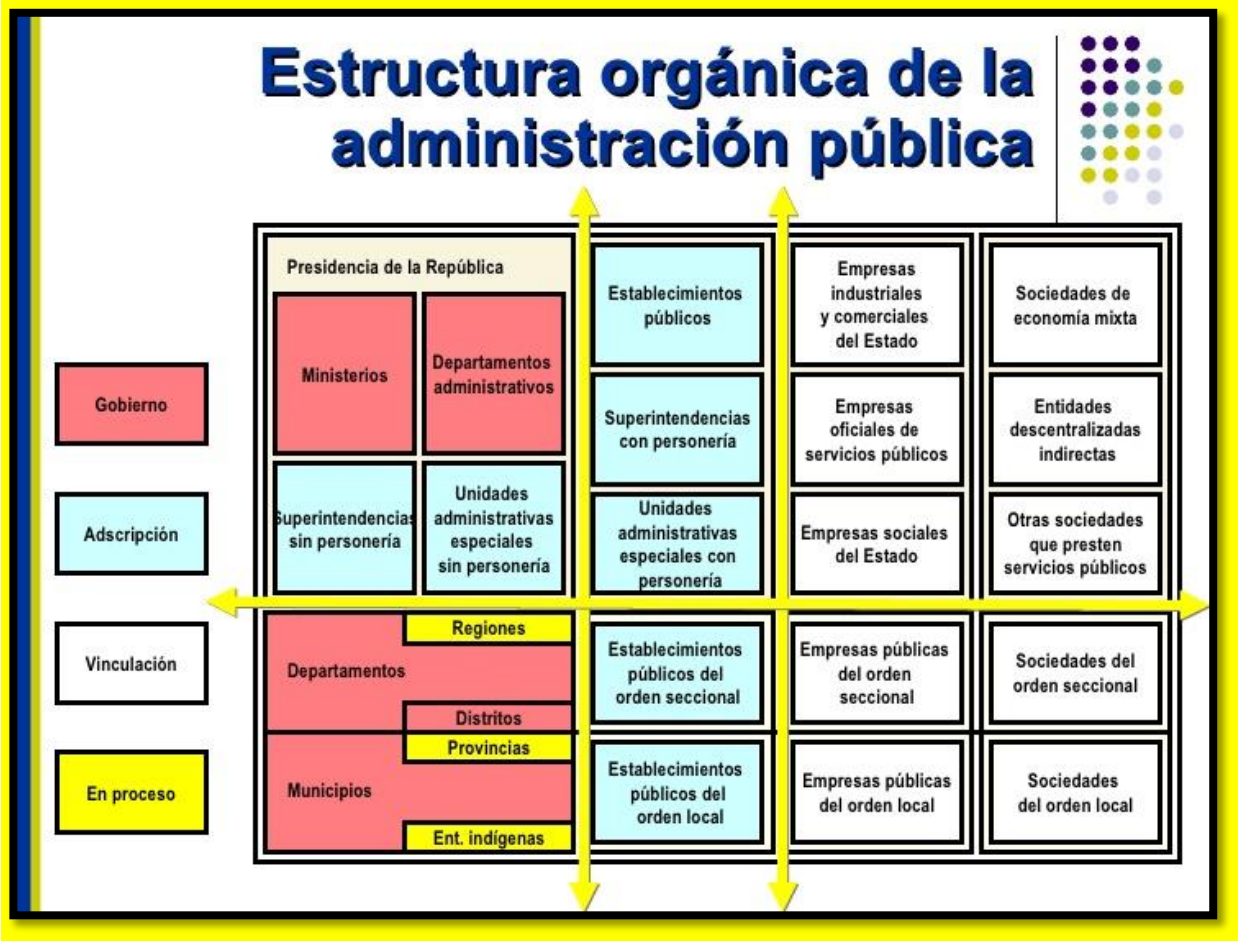


Fuente: GÓMEZ HENRY. Estructura y organización de la administración pública. [sitio web] [Consultado en 18, agosto 2017]. Disponible en: https://es.slideshare.net/HenrryGmezAlbernia/estructura-y-organizacin-de-la-administracin-pblica-mapa-conceptual.

[40] Ibíd.

[41] Ibíd.

Figura 5. Estructura orgánica de la administración pública



Fuente: QUICENO JAIME. Estructura orgánica de la administración pública. [sitio web]. ¨[Consultado en 18, agosto 2017]. Disponible en: https://es.slideshare.net/jaimequiceno/la-funcin-administrativa.

3.2 PROBLEMÁTICA DE LA ENTIDAD

La CNSC cuenta con una base de datos e información de entidades, empleados y ciudadanos, amplia y completa. Dentro de sus archivos se encuentran todas las convocatorias realizadas y por realizar, la información de las comisiones de personal, evaluaciones de desempeño laboral la normatividad relacionada con los concursos, jurisprudencia y doctrina, los datos de las universidades acreditadas con la comisión, así como un gran archivo de publicaciones, seminarios capacitaciones, informes de gestión y de encuestas, manuales y certificaciones.

Adicionalmente, la entidad maneja los datos personales de todos los ciudadanos aspirantes a la carrera administrativa del país y las listas de elegibles para cualquier

cargo público, a la que puede acceder cualquier entidad del Estado para proveer su planta.

Tomando en cuenta lo anterior. Se observa la necesidad de generar e implementar un sistema para la protección de la información, que garantice la seguridad de los datos sensibles y confidenciales que se encuentran vulnerables a pérdida o alteración.

Además, la implementación de un sistema de seguridad de la información en este tipo de entidades públicas, se hace necesaria no solo para garantizar una buena práctica para el manejo de su información, sino para buscar el cumplimiento a leyes gubernamentales, como la Ley de Transparencia y el Acceso a la Información Pública, y la Ley de Protección de Datos, que hacen parte de la Estrategia de Gobierno en Línea.

4 . ANÁLISIS CONTEXTO ORGANIZACIONAL

Teniendo en cuenta que la norma ICONTEC ISO 27001:2013 señala la importancia de dar a conocer los factores internos y externos de la organización en estudio, porque estos pueden afectar o ser afectados por el establecimiento del Sistema de Gestión de Seguridad de la Información a implementar, se presenta el contexto de la organización, la cual está contenida en el capítulo 4 de la norma ISO 27001:2013, en donde se busca establecer las situaciones internas y externas, que son pertinentes para la seguridad de la información.

4.1 CONOCIMIENTO DE LA ORGANIZACIÓN

4.1.1 Naturaleza de la entidad

La Comisión Nacional del Servicio Civil –CNSC- es una entidad autónoma del más alto nivel en la estructura del Estado Colombiano. Tiene personería jurídica, autonomía administrativa, patrimonial y técnica, y también es independiente de todas las ramas del poder público.

Según el artículo 130 de la Constitución Política de Colombia es "responsable de la administración y vigilancia de las carreras de los servidores públicos, excepción hecha de las que tengan carácter especial"[42].

"Su misión se encuentra orientada a posicionar el mérito y la igualdad en el ingreso y desarrollo del empleo público; velar por la correcta aplicación de los instrumentos normativos y técnicos que posibiliten el adecuado funcionamiento del sistema de carrera; y generar información oportuna y actualizada, para una gestión eficiente del sistema de carrera administrativa"[43].

4.1.2 Misión y visión de la entidad

A continuación se presenta la visión y la misión de esta organización, recuperada de su portal WEB oficial[44]:

[42] COLOMBIA. CONSEJO SUPERIOR DE LA JUDICATURA, SALA ADMINISTRATIVA. Constitución Política de Colombia de 1991. Actualizada con los actos legislativos a 2015. Corte Constitucional de Colombia. Bogotá, 2015, p. [138].

[43] Comisión Nacional del Servicio Civil. [sitio web]. Colombia. [Consultado 16, agosto, 2017] Disponible en: https://www.cnsc.gov.co/.

[44] Ibíd.

4.1.2.1 Misión

"Garantizar a través del mérito, que las entidades públicas cuenten con servidores de carrera competentes y comprometidos con los objetivos institucionales y el logro de los fines del Estado".

4.1.2.2 Visión

"Ser reconocida en el 2018 como la Entidad que en el Estado Colombiano garantiza de manera efectiva la Carrera Administrativa, con adecuada capacidad institucional y posicionada como la autoridad técnica en la materia".

4.1.3 Objetivos a desarrollar por la entidad

Los objetivos estratégicos de la Comisión Nacional del Servicio Civil, se determinaron en la formulación del Plan Estratégico aprobado para el periodo 2015 - 2018 por la Sala Plena, en Sesión celebrada el 30 de abril de 2015[45].

1. Fortalecer y aumentar el proceso de acreditación de las universidades e instituciones de educación superior en términos técnicos.
2. Aumentar y hacer más eficientes los procesos de selección por mérito del Sistema de Carrera Administrativa.
3. Fortalecer el Sistema de Evaluación del Desempeño Laboral como herramienta de gestión determinante para la permanencia de los servidores públicos y el desarrollo de la Carrera Administrativa.
4. Afianzar el Registro Público de Carrera Administrativa como el sistema único de información de las novedades sucedidas dentro del sistema de carrera administrativa.
5. Unificar y divulgar las normas y doctrina del Sistema de Carrera Administrativa.
6. Fortalecer los mecanismos de vigilancia para la correcta y efectiva aplicación de las normas de carrera administrativa y los lineamientos que imparta la CNSC.
7. Fortalecer y aumentar la capacidad de gestión institucional de la Comisión Nacional del Servicio Civil[46].

4.1.4 Estructura organizacional

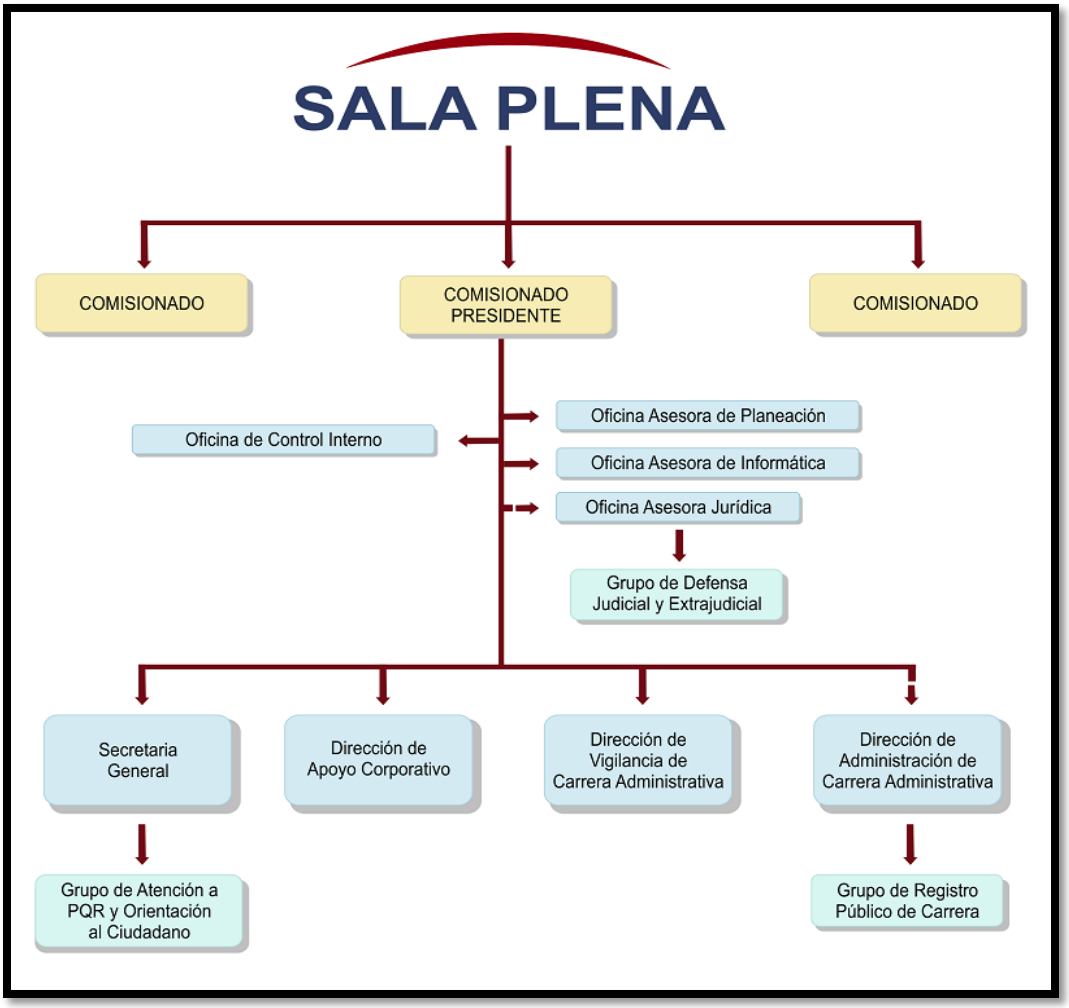
La Sala Plena de la Comisión Nacional del Servicio Civil (CNSC) se encuentra conformada por tres comisionados de los cuales uno es el presidente y de quien hacen parte las oficinas de Control Interno, la asesora de Planeación, la asesora de Informática y la Jurídica (esta a su vez cuenta con un grupo de defensa judicial y extrajudicial).

[45] Ibíd.

[46] Ibíd.

Posteriormente, en el orden jerárquico se encuentran la Secretaría General, la Dirección de Apoyo Corporativo y las direcciones de Vigilancia y Administración de la Carrera Administrativa. De la Secretaría General depende el grupo de atención a PQRS (preguntas, quejas, reclamos y sugerencias) y de la Dirección Administrativa de Carrera Administrativa depende el grupo de Registro Público de Carrera. (Ver figura 8).

Figura 6. Estructura organizacional



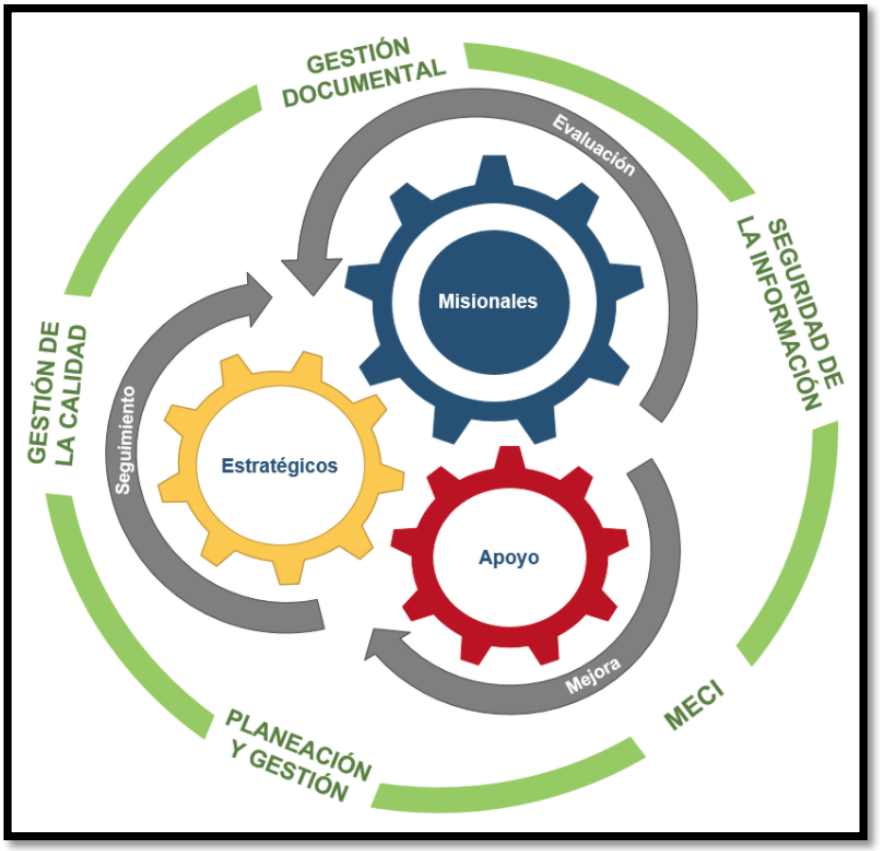
Fuente: COMISIÓN NACIONAL DEL SERVICIO CIVIL. Estructura organizacional. [sitio web]. [Consultado 18, agosto, 2017]. Disponible en: https://www.cnsc.gov.co/index.php/institucional/estructura-organizacional/estructura-organica

4.1.5 Sistema Integrado de Gestión

La gestión de la CNSC está orientada a la atención efectiva a los grupos de interés. En la siguiente figura, se evidencia cómo se encuentran interrelacionados los

elementos que la Comisión utiliza en su gestión diaria para la optimización del desempeño institucional y la alineación de los sistemas de gestión documental, gestión de la calidad, planeación y gestión, MECI y Seguridad de la Información:

Figura 7. Sistema Integrado de Gestión



Fuente: COMISIÓN NACIONAL DEL SERVICIO CIVIL. Direccionamiento estratégico. [sitio web]. [Consultado 18, agosto, 2017]. Disponible en: https://www.cnsc.gov.co/index.php/institucional/direccionamiento-estrategico/sistema-integrado-de-gestion

4.1.6 Guía de Gestión de Riesgos

La Guía de Gestión de Riesgos está incluida en uno de los procesos estratégicos de la Comisión y busca establecer, implementar y mantener controlados los Riesgos de la entidad. Su alcance inicia con la identificación de los riesgos y termina con la implementación y evaluación de los controles.
En general lo que se busca con la Guía de Gestión de Riesgos, dentro de la entidad es forjar un adecuado Modelo de Gestión de Seguridad de la Información, debido a

que tiene a su cargo la responsabilidad de la gestión de riesgos de la entidad, seguridad de la información y el plan de Continuidad de la entidad[47].

De acuerdo a lo anterior, es importante resaltar cada una de las actividades en riesgo que han motivado la realización del presente texto, las cuales serán detalladas más adelante, por lo pronto es importante resaltar por medio de un mapa de riesgos cuales son los puntos más susceptibles. (Ver figura 10).

Figura 8. Mapa de Riesgos

COMISIÓN NACIONAL DEL SERVICIO CIVIL

Mapa de Riesgos

No.	Tipo	proceso	Riesgo	Causa	Consecuencia	Probabilidad	Impacto	Valoración del Riesgo	Controles	Impacto después del control			Responsable por implementar el tratamiento	Monitoreo y Revisión
										Probabilidad	Impacto	Valoracion del riesgo		
1	Corrupción	Control Interno Disciplinario	Promover, inducir y/o provocar actuaciones administrativas atendiendo intereses personales a cambio de obtener un beneficio personal.	Interes procesal Interés económico. Amenazas	Fallos no ajustados a los lineamientos legales.	2	6	8	Capacitaciones en materia preventiva y en codigo de etica	2	3	5	Profesional Especializado Responsable de Control Interno	Permanente
2	Operativo	Control Interno Disciplinario	Violación del debido proceso	Fugas de información Incumplimiento de los terminos Desconocmiento de las normas Ilegalidad sustancial	Absolución del disciplinado. Desgaste administrativo. Ampliación de términos	3	3	6	Reserva de las actuaciones procesales Vigilancia de las normas prestablecidas Capacitaciones en normas vigentes y jurisprudencia	2	2	4	Profesional Especializado Responsable de Control Interno	Permanente

Fuente: COMISIÓN NACIONAL DEL SERVICIO CIVIL. Direccionamiento estratégico. [sitio web]. [Consultado 18, agosto, 2017]. Disponible en: https://www.cnsc.gov.co/index.php/institucional/direccionamiento-estrategico/sistema-integrado-de-gestion/category/437-control-interno-disciplinario#

4.1.7 Áreas críticas de la entidad

Después de efectuar el análisis de riesgos en las diferentes áreas de la entidad, se determinó que hay dos oficinas que administran con frecuencia información considerada de alta sensibilidad y en las que existe un peligro inminente de vulnerabilidad:

- **Área de Informática:** es la encargada de brindar soporte en las tecnologías de la información, gestionar y mantener infraestructuras del equipo de cómputo instalado en la entidad, haciendo el mantenimiento adecuado y apoyando en la gestión de software de la organización.

[47] GUZMÁN, Carlos. Diseño de un sistema de gestión de seguridad de la información. Trabajo de Grado. Especialización en Seguridad de la Información. Institución Universitaria Politécnico Gran Colombiano. Facultad de Ingeniería y Ciencias Básicas. Bogotá, 2015.

- **Área de recepción de Correspondencia**: recibe, clasifica, registra y entrega documentos de origen interno y externo, gestionando la información entre las diferentes áreas.

5 . ANÁLISIS Y EVALUACIÓN DE RIESGOS

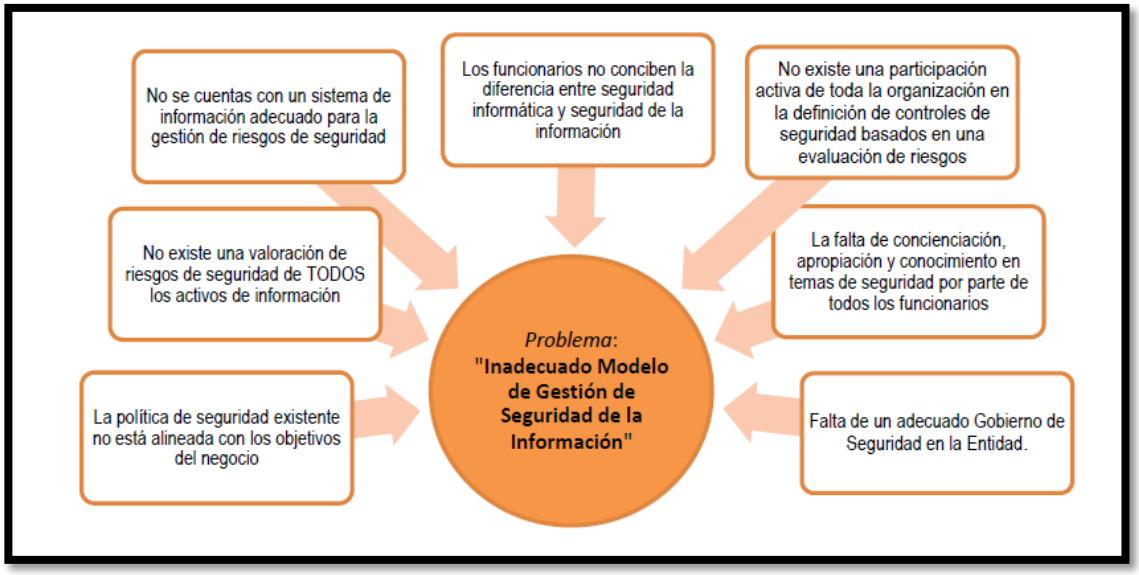
Con base en la anterior metodología planteada, en este capítulo se presenta el análisis de riesgos del SGSI de una empresa del sector público, en concordancia con la norma ISO 27001:2013, que define el enfoque de evaluación de riesgos.

Los resultados obtenidos son comparables y repetibles, para evitar que sean falsos o subjetivos y determinan los activos de la organización que tienen mayor valor, sus amenazas, las vulnerabilidades y el impacto que podría suponer una pérdida de confidencialidad, integridad y disponibilidad para cada activo.

5.1 DIAGNÓSTICO SITUACIÓN PROBLEMA

Teniendo en cuenta los resultados del análisis del estado de la seguridad de la entidad en estudio, y encontrando soporte en un autor consultado, se logró la identificación de las situaciones que afectan la seguridad. La figura 11 ilustra la situación problema:

Figura 94. Identificación de la situación problema



Fuente: GUZMÁN C.A. Diseño de un sistema de gestión de seguridad de la información. Trabajo de grado. Instituto Politécnico Gran Colombiano. [sitio web]. [Consultado 18, agosto, 2017]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/654/ProyectodeGradoSGSI-IGM-CarlosGuzmanFINAL.pdf?sequence=1&isAllowed=y

5.1.1 Grupos de interés

Los grupos de interés, son aquellas partes internas y externas de una entidad, que se encuentran interesadas en la organización. Dichas partes pueden ser naturales

o jurídicas y son tomadas en cuenta por su interacción con la entidad en el pleno ejercicio de sus funciones.

Estos grupos de interés se ven afectados directa o indirectamente, y positiva o negativamente, a causa de las políticas seguridad en la información que implemente la entidad en estudio.

A continuación, en el cuadro 3, se presentan los posibles grupos de interés que manifiestan interés directo, explícito y comprometido, con los propósitos del Sistema de Gestión de Seguridad de la Información:

Cuadro 3. Partes de interés interno y externa en función del SGSI

Grupos de interés Interno	Detalle
Alta Directiva	Mostrará liderazgo y compromiso con los objetivos pertenecientes a la Seguridad de la Información de la entidad.
Comité de Seguridad	Apoyo directo a la junta directiva y a la Presidencia de la entidad, en control, seguimiento e implementación de las políticas SGSI.
Jefe de Informática	Responsable de la seguridad informática y continuidad tecnológica de la entidad.
Gestión del desarrollo y talento humano	Garante de la seguridad de la información, antes, durante y después de la vinculación de los funcionarios. Responsable de las capacitaciones.
Jefe de Jurídica	Garantiza el cumplimiento de la normatividad vigente.
Colaboradores	Responsables del tratamiento de los datos personales de los titulares vinculados de alguna forma con la entidad.
Grupos de interés Externos	**Descripción**
Accionistas	Pueden tratarse de: la Nación, entidades públicas de orden nacional, departamentos, personas naturales o jurídicas, nacionales o extranjeras y organismos internacionales.
Gobierno	Establece el marco normativo del funcionamiento de la entidad.
Beneficiarios	Son las personales naturales o jurídicas encargadas de ejecutar los proyectos de la entidad.
Entes de control externo	Entes de vigilancia y control encargados de supervisar las actividades de la entidad.

Proveedores	Encargados de prestar servicios a la entidad.

Fuente: Elaborado por el autor, apoyado en Guzmán C.A. Diseño de un sistema de gestión de seguridad de la información. Trabajo de grado. Instituto Politécnico Gran Colombiano. Bogotá. 2015.

5.1.2 Enfoque organizacional para la valoración de los riesgos

Con el propósito de asegurar que el diseño del Sistema de Gestión de Seguridad de la Información alcance los objetivos propuestos, se llevó a cabo el análisis y la determinación de los riesgos más altos dentro de la organización. De igual manera se tuvo en cuenta el enfoque organizacional para relacionarlos y generarles valor.

En la valoración se tuvieron en cuenta los criterios de alto y medio, puesto que el nivel bajo no representa igualdad de riesgo.

En el siguiente cuadro se relacionan los activos de información y los niveles de criticidad:

Cuadro 4. Valoración de riesgos según el enfoque organizacional

Activo de información	Nivel de criticidad	Contener y/o activo seleccionado para valoración de riesgos
Área administración de plataforma.	Alto	Área administración de plataforma.
Computadores, administradores	Alto	
Registro de incidentes de seguridad.	Alto	Bases de datos.
Usuarios	Alto	
Computadores de escritorio usuarios.	Medio	Computadores.
Dispositivos de red.	Alto	Cuartos de rack.
Cuartos de comunicaciones.	Medio	
Centro Principal de Procesamiento.	Alto	Data Center del proveedor.
Servidores de administración.	Alto	
Servidores de aplicaciones.	Alto	
Servidores de bases de datos.	Alto	
Plataforma de Correo.	Medio	
Solución de backup.	Medio	
Datos de autenticación.	Alto	Directorio activo.
Identidad del usuario.	Alto	
Log de evento de seguridad.	Alto	Log de eventos.
Correo electrónico.	Medio	Plataforma de correo.

Portátiles	Medio	Portátiles
Red LAN.	**Alto**	Red LAN.
Red WIFI corporativa.	**Alto**	
Red WIFI invitados.	Medio	
Red WAN.	**Alto**	Red WAN.
Directorio activo.	**Alto**	Servidores de administración.
File Server.	**Alto**	
Herramienta de virtualización.	**Alto**	
Sistema de control de acceso.	Medio	
Sistema de grabación de llamadas.	Medio	
Aplicativo de nómina.	Medio	Servidores de aplicaciones.
Aplicativo WEB transaccional.	Medio	
Página WEB.	Medio	
Bases de datos.	**Alto**	Servidores de bases de datos.
Sistema gestor base de datos.		Servidores de bases de datos.

Fuente: Elaborado por el autor, apoyado en Guzmán C.A. Diseño de un sistema de gestión de seguridad de la información. Trabajo de grado. Instituto Politécnico Gran Colombiano. Bogotá. 2015.

5.2 CONTROLES APLICABLES

En el cuadro 5 se identifican cuáles son los medios de seguridad que se pueden aplicar, para lograr una justa ejecución del SGSI:

Cuadro 5. Controles aplicables

Control	Justificación
Políticas de seguridad	
Distribución de la dirección para la gestión dela seguridad de la información.	Es necesario tener una actualización permanente del uso de las políticas actualizadas de acuerdo a los requerimientos del gobierno y de la norma.
Revisión de las políticas para la seguridad dela información.	
Organización de la seguridad de la información.	
Organización Interna	La organización debe estar en torno a la seguridad de la información, deberán existir responsables para cada una de las actividades de información y así mismo, encargados de la comunicación con las autoridades correspondientes en caso de un incidente.
Roles y responsabilidades.	
Contacto con las Autoridades.	
Política de restricción para dispositivos móviles.	Existe información que puede ser extraída usando las cámaras de celulares.

Control	Justificación
Seguridad de los Recursos Humanos.	
Antes, durante y después de asumir el empleo.	La organización debe establecer la información de la cual son responsables los empleados, contratistas o usuarios, comprobando que todo lo dicho y suministrado por este, sea legal y confiable.
Seguridad en las comunicaciones	
Seguridad de los servicios de red.	La organización debe mantener la plena seguridad de que la información compartida a sus trabajadores y usuarios por su sensibilidad, estará protegida. Por esta razón deberán existir acuerdos firmados de confidencialidad sobre la información sobre la cual se está teniendo acceso.
Transferencia de información.	
Políticas y procedimientos de transferencia de información.	
Acuerdos de confidencialidad o de no divulgación.	
Cumplimiento	Se mantendrán controles sobre las políticas, procesos y demás, que tengan relación con la seguridad de la información. Por otra parte, se mantendrá una actualización periódica de la misma, siempre teniendo en cuenta los cambios de la organización y la información que se procesa.
Requisitos legales y contractuales.	
Protección de registros.	
Privacidad y protección de información de datos. Personales	
Cumplimiento con las políticas y normas de seguridad.	

Fuente: Elaborado por el autor, apoyado en Guzmán C.A. Diseño de un sistema de gestión de seguridad de la información. Trabajo de grado. Instituto Politécnico Gran Colombiano. Bogotá. 2015.

5.3 PLANEACIÓN DEL SGSI

Para dar cumplimiento a los objetivos planteados, la norma ISO 27001 propone como primer paso definir el alcance del SGSI, ya que al realizar una definición adecuada, se facilita la tarea de estructurar los pasos más importantes que cubren toda la organización. A continuación se define el alcance del sistema de gestión.

5.3.1 Definición del alcance del SGSI

En las reuniones sostenidas con el grupo de Gobierno en Línea -el cual es el equipo de trabajo encargado por parte de la Comisión Nacional del Servicio Civil para definir

los esfuerzos en la implementación del SGSI- se definieron dos aspectos: el primero es el cumplir los requerimientos que establece la norma ISO\IEC 27001:2013 en su numeral 4.3: Determinación del Alcance del Sistema de Gestión de Seguridad de la Información[48]; y el segundo: alcanzar lo planteado en la presentación del anteproyecto, en el cual se manifestaba que: "El proyecto referente se desarrollará en el término de seis meses, describirá el diseño de un plan para la implementación de un SGSI y estará dirigido a todas las personas vinculadas con las tecnologías de la información directa e indirectamente de cualquier entidad prestadora de servicios de vigilancia del Sistema de Carrera Administrativa del sector público, cubriendo la primera fase de la implementación, la planeación del sistema, utilizando como base la NTC ISO 27001:2013".

5.3.2 Políticas y objetivos del SGSI

5.3.2.1 Políticas del SGSI

- La creación de un Comité de Seguridad de la Información, el cual será responsable de la revisión, mantenimiento y mejora del SGSI.

- Se definirán los controles para la protección de la información contra accesos no autorizados; los cuales deberán garantizar la tranquilidad requerida por los usuarios.

- Por su parte los funcionarios y/o contratistas tendrán la responsabilidad de proteger la información a la cual tengan acceso, para que esta no se pierda, se filtre, se altere o tenga un uso inadecuado.

- Se llevarán a cabo auditorías y controles periódicos sobre el SGSI.

5.3.2.2 Objetivos del SGSI

- Aportar para que exista un fuerte incremento en la transparencia de la gestión pública, permitiendo al ciudadano tener conocimiento de la gestión del Estado.

- Suscitar a la ciudadanía hacer uso de los medios electrónicos, habilitando nuevos canales de consulta para la solución de problemas, toma de decisiones y control social. Con ello se generará mayor confianza y seguridad en ellos.

- Mejorar las condiciones de competitividad y tranquilidad de los usuarios tanto internos como externos, permitiendo que todos los servicios sean acordes y respondan a las necesidades de los ciudadanos y de las mismas entidades.

[48] Instituto Colombiano de Normas Técnicas y Certificación. Norma Técnica NTC-ISO/IEC COLOMBIANA 27001. NTC-ISO-IEC 27001:2013. El Instituto. Bogotá, 2006, p. [1-2].

6 . PLAN DE IMPLEMENTACION DEL SISTEMA DE SEGURIDAD DE LA INFORMACION

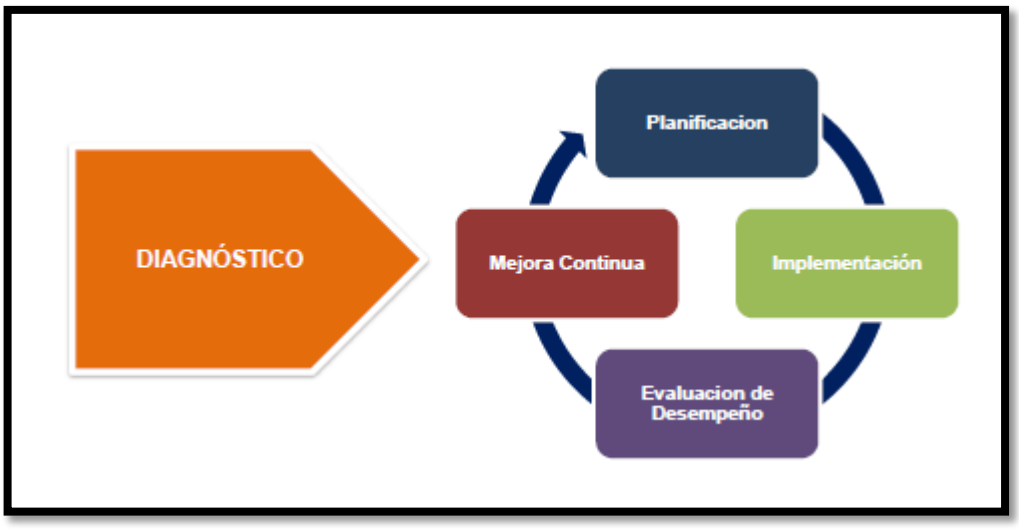
6.1 FASES DE IMPLEMENTACIÓN

Basados en la metodología descrita por las guías del modelo de seguridad y privacidad de la información del Ministerio de Tecnologías de la Información y las Comunicaciones -Min tic-, las cuales alinean los requerimientos de la norma ISO/IEC 27001:2013 y la Estrategia de Gobierno en Línea para la planeación del Sistema de Gestión de Seguridad de la Información, se han logrado establecer las siguientes fases para el desarrollo del proyecto:

6.1.1 FASE I - DIAGNÓSTICO

Es el desarrollo de las actividades de aplicación de la herramienta incluida dentro del modelo, para lograr identificar el estado actual de la entidad con respecto a los controles que se llevan a cabo dentro de la entidad para proteger la información. La figura 4 esquematiza el proceso:

Figura 10. Diagrama de diagnóstico



Fuente: MINTIC. Modelo de Seguridad y Privacidad de la Información [sitio web]. [Consultado 18, agosto, 2017] Disponible en: https:/www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf Bogotá.

El análisis del diagnóstico permitirá conocer:

- El estado actual de la gestión de seguridad y privacidad de la información al interior de la entidad.
- Identificar el nivel de madurez de seguridad y privacidad de la información en la entidad.

- Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.

6.1.2 FASE II – PREPARACIÓN

Son todas las actividades necesarias para establecer los lineamientos y directrices del sistema de seguridad de la información, corresponden a.

- Realizar el análisis contextual de todos los factores externos e internos que son pertinentes al sistema y que puedan afectar o se afectados en su implementación.
- Definir el alcance del sistema, determinando los límites y la aplicabilidad.
- Definir la política del sistema.
- Definir la estructura organizacional de la entidad que determinará los roles y responsabilidades con el sistema.

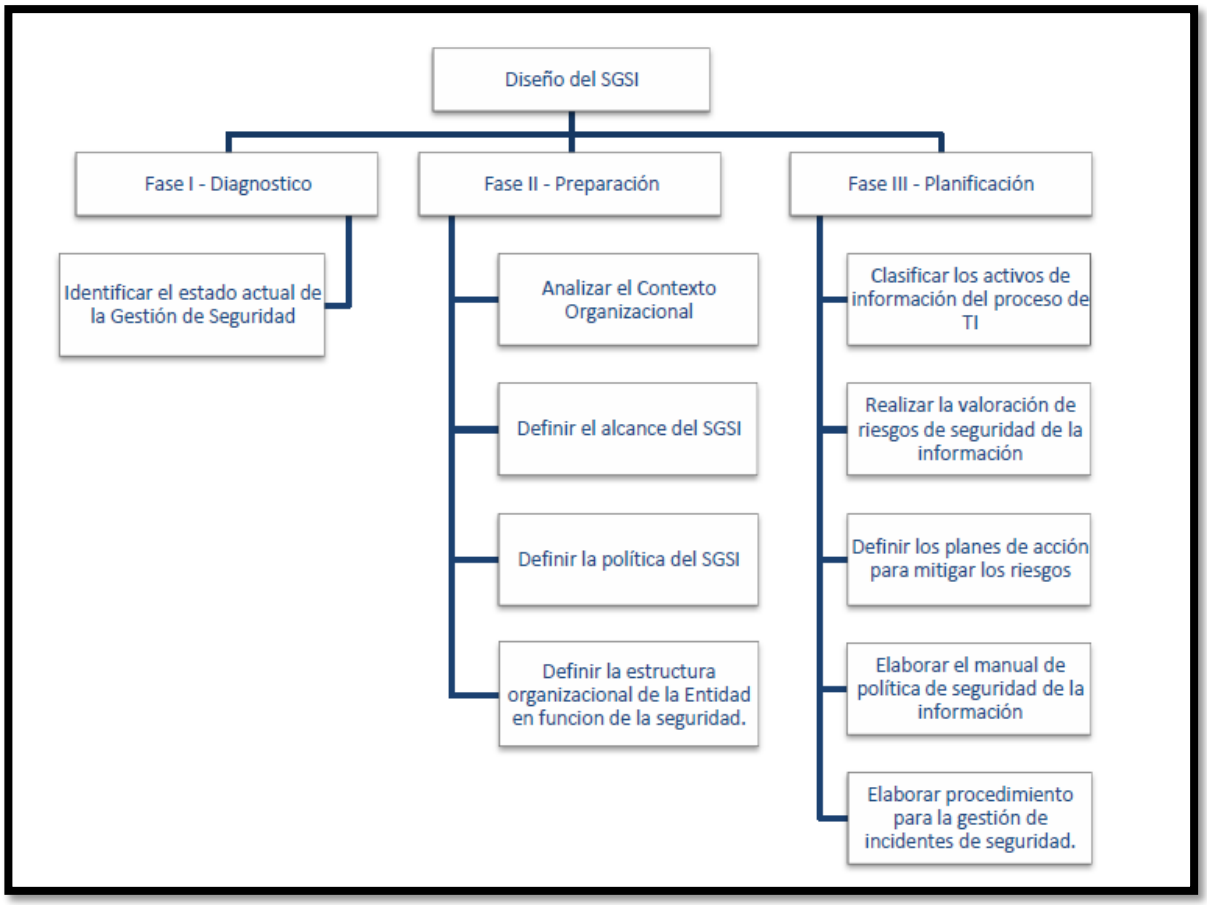
6.1.3 FASE III – PLANIFICACIÓN

Son todas las actividades que permiten asegurar el cumplimento de todos los objetivos propuestos del sistema y corresponden a:

- La realización del inventario de activos.
- Determinación de los riesgos y metodología para tratarlos.

La figura 5 esquematiza los pasos a seguir en el diseño del SGSI de la organización:

Figura 11. Fases para el diseño del SGSI de la entidad



Fuente: GUZMÁN C.A. Diseño de un sistema de gestión de seguridad de la información. Trabajo de grado. Instituto Politécnico Gran Colombiano. [sitio web]. [Consultado 18, agosto, 2017]. Disponible en: http://repository.poligran.edu.co/bitstream/handle/10823/654/ProyectodeGradoSGSI-IGM-CarlosGuzmanFINAL.pdf?sequence=1&isAllowed=y

6.2 HERRAMIENTAS PARA LA IMPLEMENTACIÓN DEL SGSI

Con base en las fases planteadas, se propone la realización de cuatro periodos o etapas, en los que además de dar cumplimiento a la norma NTCISO 27001:2013, se da cumplimiento al Decreto 2573 de 2014, “Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en Línea” y al Decreto 1078 de 2015 “Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones".

La primera etapa desarrolla la primera fase del diagnóstico, la segunda hace parte de la segunda fase de preparación y la tercera y cuarta hacen parte de la fase de planificación.

En el cuadro 6 se propone un cronograma de actividades que permitirán determinar los momentos y herramientas necesarias, dirigidas a la implementación del Sistema de Gestión de Seguridad de la Información en la CNSC, conforme los requisitos de la NTCISO 27001:2013. Posteriormente se explicará el objetivo y desarrollo de dichas actividades.

Cuadro 6. Cronograma de actividades

Fase	Actividad	Número de meses	Responsable
Diagnóstico	Identificación inicial a través de la evaluación de *hardware* y *software*	6	Alta Dirección
	Identificación de brechas por medio de encuestas		Grupos de interés interno
Preparación	Análisis de información recopilada	6	Comité de Seguridad
	Socialización del sistema a grupos de interés.	6	Gestión del Desarrollo y Talento Humano
Planificación	Clasificación de los activos	6	Colaboradores y Gestión del Desarrollo y Talento Humano
	Valoración de riesgos		
	Definición de planes de acción		
	Elaboración del manual para la política de seguridad		
	Elaboración del procedimiento de gestión de incidentes de seguridad		
	Monitoreo y medición del sistema		
	Revisión de resultados		

Fuente: elaborado por el autor, apoyado en Guzmán C.A. Diseño de un sistema de gestión de seguridad de la información. Trabajo de grado. Instituto Politécnico Gran Colombiano. Bogotá. 2015.

6.2.1 Primera etapa

Se desarrolla durante dieciocho meses, corresponde al 40 % del total de la articulación del sistema y consta de:

a. Identificación inicial: comprende el desarrollo del diagnóstico, el cual se realizará bajo el criterio de definición actual de la situación de la entidad y la identificación de las brechas, su alcance en términos poblacionales, vinculará a todo el personal de la entidad, aunque con un compromiso más constante por parte de la Alta Dirección.

Para dicha identificación se trabajará con los grupos de interés interno, que a su vez designarán unos colaboradores con quienes se evaluarán los procesos, las funciones específicas del personal, el *hardware* y *software* con el que cuenta la organización, así como la calidad y pertinencia de los mismos con los objetivos de la entidad y del Plan de Implementación del Sistema de Seguridad de la Información.

La identificación de brechas incluye la aplicación de encuestas que faciliten la recopilación de información que evalúe los siguientes elementos:

- Infraestructura física, accesos de la entidad y ambiente (accesos, barreras, cableado, equipos, aire acondicionado, planta de emergencia).

- Lógico (actualización de servidores, pruebas de intrusión, ingeniería social).

- Metodológico (políticas, procedimientos, normas, estándares que se utilicen en la entidad).

- Definición del nivel de madurez (se realiza a través de una autoevaluación que obtiene información de la estructura organizacional, el nivel de gestión de la seguridad de la información y las políticas, controles y métricas existentes).

En esta primera identificación es fundamental el compromiso de la Alta Dirección con la destinación de los espacios y el personal humano que facilitará la recopilación detallada de la información material e inmaterial de la organización.

Responsables: Grupos de interés interno.

Tiempo: seis meses.

b. Definición del marco de seguridad y privacidad de la entidad: esta etapa analiza la información recopilada para obtener el contexto organizacional. Se definen roles y responsabilidades, se prepara el inventario de activos de información, se analizan los riesgos y controles, así como la documentación de procedimientos para el manejo de la información, y se definen los indicadores para medir el cumplimiento de los controles.

   En esta etapa se evaluará la madurez de la seguridad, haciendo una revisión detallada de las políticas y procesos vigentes en la entidad, la organización actual de la seguridad en la información, los espacios físicos que garantizan la seguridad y la privacidad de los datos y las relaciones que se establecen con los grupos de interés externos.

   Responsable: Comité de Seguridad.

   Tiempo: seis meses.

c. Socialización del sistema a todos los servidores públicos, dando a conocer las ventajas y beneficios de esta buena práctica de seguridad. Dentro de esta labor el grupo de interés de Gestión del Desarrollo y Talento Humano será de gran ayuda en la generación de mensajes relacionados con la seguridad de la información y la elaboración de campañas dirigidas a todo el personal, para sembrar por una parte la necesidad de implementar el Plan y por otra: la motivación para participar constantemente, no solo con el aporte en la recopilación de la información, sino con el conocimiento de los servidores públicos en la optimización e implementación de nuevos procesos.

   La socialización debe realizarse desde los primeros seis meses de la etapa, con el objetivo de que el personal se sienta parte del sistema y contribuya de forma entusiasta. Los servidores, además de ser incluidos como grupos de interés internos, serán los encargados de revisar los resultados del informe diagnóstico que deberá presentar el auditor de la mano de la Alta Dirección. Del éxito de la primera etapa dependen las siguientes.

   Responsable: Gestión del Desarrollo y Talento Humano.

   Tiempo: Los 18 meses de la primera etapa, con énfasis en los últimos seis.

6.2.2 Segunda etapa

Para la segunda etapa se destinarán seis meses y corresponde al 60 % acumulado del total de la articulación del sistema. Durante este tiempo se ponen en marcha todos los procedimientos documentados en la primera etapa. En este momento grupos de interés interno como los colaboradores, deben estar totalmente coordinados con la política a implementar y el alcance del sistema, para sensibilizar a los grupos externos de la entidad. Puesto que será durante esta etapa en la que se modificarán algunos roles y responsabilidades de los servidores públicos frente al sistema, se elaborarán procedimientos técnicos de monitoreo, se establecerán controles y se estandarizarán procesos.

Así mismo, el grupo de interés de Gestión del Desarrollo y Talento Humano debe continuar el trabajo de socialización y sensibilización de los cambios, esta vez generando mensajes para los grupos de interés externos: accionistas, Gobierno, beneficiarios, entes de control externo y proveedores.

Responsable: Colaboradores y Gestión del Desarrollo y Talento Humano.

Tiempo: seis meses.

6.2.3 Tercera etapa

Se realiza de forma paralela a la segunda. Corresponde al 80 % acumulado del total de la articulación del sistema y consiste en el monitoreo constante y la medición del

desempeño del sistema mediante de los indicadores para la adopción de medidas correctivas y de mejora, de acuerdo con los objetivos propuestos.

En la medida en que se vaya implementando el Plan, el equipo evaluador (en el que participa la Alta Dirección) irá documentando el impacto en la organización de la seguridad, los controles de acceso a la información, los procesos en la recopilación y archivo de datos, la seguridad en los sistemas tecnológicos de información, las relaciones con los proveedores y la asimilación de los cambios en los grupos de interés internos y externos.

Esta etapa permite realizar variaciones en el sistema con base en el control, que facilitan una actuación inmediata y no posterior a su implementación. También redefine la estructura organizacional de la entidad en función de la seguridad y el cumplimiento de la norma.

Responsable: Alta Dirección.

Tiempo: seis meses (paralelamente a la anterior etapa).

6.2.4 Cuarta etapa

Corresponde al 100 % de la articulación del sistema. Se refiere revisión de resultados en la gestión de seguridad y privacidad de la información para verificar el desarrollo de todas las acciones propuestas para la mejora y el reinicio del ciclo de mejora continua.

En esta etapa se revisan los registros llevados y los documentos que se relacionan en el cuadro 7. La función de esta cuarta etapa debe repetirse de forma anual para hacer modificaciones a la implementación del plan, con base en los resultados recopilados, así como en las modificaciones que puedan surgir en la norma con el paso del tiempo.

Cuadro 7. Resultados esperados de la implementación

Metas	Resultados
Implementación	Documentos con los riesgos contra la privacidad identificados y las medidas de solución adoptadas a partir de la implementación del Plan de Gestión de Privacidad de la Información.
	Documento que evidencie el registro de las Bases de datos.
	Documento con el índice de información clasificada, reservada, revisada y sus procedimientos ajustados

Fuente: Elaborado por el autor, apoyado en MINTIC. C.A. Modelo de Seguridad y Privacidad de la Información. Bogotá. 2016.

Dentro de las actividades a ejecutar se registran todos los resultados obtenidos, dificultades que se tengan durante la implementación y se realiza la sensibilización y capacitación a los funcionarios y contratistas de la entidad, junto con las modificaciones realizadas y programadas. Aunque es difícil documentar todos los procedimientos operativos de gestión del sistema, la planificación a corto, mediano y largo plazo, ayuda en el proceso.

Para finalizar, se realizan las mediciones de los indicadores definidos en el plan con el objetivo de medir la eficacia a los controles realizados tanto a puntos de control como al establecimiento de las metas que se trazarán para el siguiente año.

Responsable: grupos de interés internos.

Tiempo: un mes (de forma anual).

7 . CONCLUSIONES

El diseño del Plan de Implementación de un Sistema de Gestión de Seguridad de la Información apoyado en los lineamientos de seguridad que dicta la norma ISO/IEC 27001:2013, se considera una herramienta de gran ayuda para identificar los aspectos a tener en cuenta en el momento en el que las organizaciones toman la decisión de establecer un modelo de seguridad de la información. Puesto que, de lograrse el objetivo de la norma ISO, la organización podrá lograr la sostenibilidad del Sistema de Gestión de Seguridad de la Información.

El plan para la implementación de un Sistema de Gestión de Seguridad de la Información en una empresa del sector público basado en los requisitos de la norma NTC ISO 27001:2013 es un proceso dinámico que debe contemplar el análisis del contexto organizacional, además de evaluar los riesgos de la seguridad de la información en dicha empresa. En este proceso, el análisis e identificación de riesgos permitió conocer a profundidad cuáles eran los niveles de vulnerabilidad más altos de la entidad en estudio y así se logró hallar la forma de mitigarlos.

Por otra parte, los planes de manejo y la política de seguridad de la información para la Comisión encausan a la entidad a que sus estados de riesgo se encuentren en un nivel aceptable. Es de reconocer que los sistemas que manejan y políticas como la de privacidad y protección de datos personales, son avances significativos en el camino de salvaguardar la información de la entidad.

Por lo tanto, la implementación del SGSI se considera beneficiosa para la entidad, ya que genera mayor seguridad en los sistemas de información y contribuye a obtener una mejora continua en cada proceso de auditoría interna, todo lo cual aumenta la confianza y mejora de imagen corporativa.

Este trabajo ya cuenta con un avance significativo: el análisis de la entidad, el diseño del Plan de Implementación y el cronograma de actividades. Ahora es fundamental el compromiso de la alta dirección, las áreas que tienen que ver directamente con la producción, uso y administración de la información, así como de los diferentes grupos de interés, para ejecutar en los tiempos señalados cada una de las fases.

8 . RECOMENDACIONES

Se considera fundamental que la Comisión Nacional del Servicio Civil implemente, en el corto plazo (para evitar la desactualización de la información) el Sistema de Gestión de Seguridad de la Información (SGSI), con el cual podrá conseguir mayor confianza y protección de los datos personales de sus usuarios internos y externos.

Adicionalmente es importante generar una labor de capacitación de grupos de interés y sobre todo de las áreas que administran directamente la información, como preparación inicial para la implementación del sistema. De igual forma, es importante sensibilizar al personal de la entidad a través de campañas comunicativas que fortalezcan el sentido de pertenencia con la entidad y al mismo tiempo le permita conocer las recomendaciones y tips de seguridad de la información, con base en los riesgos que puedan presentarse.

Las capacitaciones a futuro también son recomendables para garantizar la actualización constante de los funcionarios en el manejo del Sistema de Gestión de Seguridad de la Información y el cumplimiento de la norma.

BIBLIOGRAFÍA

ÁLVAREZ, Ana y FERNÁNDEZ, Luis. Guía de aplicación de la Norma UNE ISO/IEC 27001 sobre seguridad en sistemas de información para Pymes. Madrid: AENOR, 2012, p. [3].

ARÉVALO, José; BAYONA, Ramón y RICO, Willmer. Implantación de un sistema de gestión de seguridad de información bajo la ISO 27001: análisis del riesgo de la información. En: Revista Tecnura. Abril-agosto, 2015, p. [123-134].

ARROYO, Flavio y PORRAS, Ronald. Estudio metodológico para la implementación de un sistema de gestión de calidad basado en Norma ISO 9001:2008, aplicable para Instituciones del Sector Público Ecuatoriano. Trabajo presentado como requisito parcial para la obtención del Grado de Magíster en Sistemas Integrados de Gestión. Instituto de Investigación y Posgrado. Universidad Central del Ecuador. Quito, 2016, p. [35].

COMISIÓN NACIONAL DEL SERVICIO CIVIL. [sitio web]. Colombia. [Consultado 16, agosto, 2017] Disponible en: https://www.cnsc.gov.co/.

DEMING, William. LA CALIDAD COMO FILOSOFÍA DE GESTIÓN. [sitio web]. [Consultado 16, agosto, 2017]. Disponible en: http://www.pablogiugni.com.ar/william-edwards-deming/.

DURANGO, José. Ciclo PHVA. [sitio web]. Colombia. [Consultado 16, agosto, 2017]. Disponible en: http://www.escolme.edu.co/almacenamiento/oei/tecnicos/ppios_admon/contenido_u3_2.pdf.

GIRALDO, L. 2016. Análisis para la Implementación de un Sistema de Gestión de la Seguridad de la Información según la norma ISO 27001 en la empresa Servidoc S.A. [sitio web]. [Consultado 16, agosto, 2017]. Disponible en: http://hdl.handle.net/10596/6341.

Global Information Assurance Certification Paper. Information security management system (BS7799-2:2002) implementation overview Disponible desde internet en: <https://www.giac.org/paper/gsec/3740/information-security-management-system-bs-7799-2-2002-implementation-overview/105976> [con acceso el 16 de agosto de 2017].

GONZÁLEZ, Efrén. La Carrera Administrativa: experiencias y perspectivas. En: Revista Administración y Desarrollo. Escuela Superior de Administración Pública. 2010, No. 25, p. [13-42].

GUZMÁN, Carlos. Diseño de un sistema de gestión de seguridad de la información. Trabajo de Grado. Especialización en Seguridad de la Información. Institución Universitaria Politécnico Gran Colombiano. Facultad de Ingeniería y Ciencias Básicas. Bogotá, 2015.

LADINO, Martha; VILLA, Paula y LÓPEZ, Ana. Fundamentos de ISO 27001 y su aplicación en las empresas. En: Scientia et technica. Pereira. No. 47 (abril, 2011), p. [334-339].

MANJÓN-CABEZA, José María. Elaboración de un Plan de Implementación de la ISO/IEC 27001:2013. Universidad Oberta de Catalunya. Barcelona, 2015.

MORALES, Rodolfo. Diseño para la implementación de tres dominios de un sistema de gestión en la seguridad de la información basada en la norma ISO 27001 e ISO 27002, para el área de software de la procesadora nacional de alimentos Pronaca. Maestría en Gerencia de Redes y Telecomunicaciones. Universidad de las Fuerzas Armadas ESPE. Ecuador, 2015.

PARRA, Julieth. Elaboración de un plan de implementación de la norma ISO/IEC 27001: 2013 en una empresa prestadora de servicios de acueducto y alcantarillado. Universidad Oberta de Catalunya. Barcelona, 2015.

PDCA HOME. Ciclo PDCA (Planificar, Hacer, Verificar y Actuar). [sitio web]. España. [Consultado 16, agosto, 2017]. Disponible en: https://www.pdcahome.com/5202/ciclo-pdca/.

SÁNCHEZ Shirley Alexandra. Importancia de implementar el SGSI en una empresa certificada BASC. Bogotá: Universidad Militar Nueva Granada, 2014, p. [22].

SARRIA, Mercedes. Diseño de un modelo de un sistema de gestión de seguridad de la información para la empresa social del estado Fabio Jaramillo Londoño mediante la norma ISO/IEC 27001: 2013. Tesis de grado para optar por el título: Especialista En Seguridad Informática. Universidad Nacional Abierta y a Distancia. Escuela de Ciencias Básicas Tecnología e Ingeniería. Florencia, 2015.

SOLARTE, Francisco; ROSERO, Edgar y BENAVIDES, Mirian. Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. En: Revista Tecnológica-ESPOL. Diciembre, 2015, vol. 28, No 5.

VILLANUEVA Isabel; SÁNCHEZ Juan y PASTOR, Óscar. Elicitación de requisitos en sistemas de gestión orientados a procesos. Trabajo subvencionado por el proyecto Destino Mec Nº TIN 2004-03534. Universidad Politécnica. España, 2005, p. [3-48].

ISO TOOLS. ¿En qué consiste el ciclo PHVA de mejora continua? [sitio web]. Colombia. [Consultado 16, agosto, 2017]. Disponible en: https://www.isotools.org/2015/02/20/en-que-consiste-el-ciclo-phva-de-mejora-continua.