Elaboración del estudio preliminar del plan de implementación de la norma ISO - 27001 “Sistemas de gestión de la seguridad de la información”, para el data center de la dirección de sistemas de información de la Gobernación de Santander.

Sergio Arturo Rangel Supelano

Trabajo de investigación presentado como requisito para optar al título de Ingeniero de Sistemas e Informática

Director
Pedro Javier Trujillo Tarazona
Magister en Informática

Codirector:
Herman Ramírez Gómez
Ingeniero de sistemas

Universidad Industrial De Santander
Facultad De Ingeniería Físico-Mecánicas
Escuela de Ingeniería de Sistemas e Informática
Bucaramanga
2021

Agradecimientos

Cómo autor expreso mis agradecimientos a:

Mi Familia, Myriam y Arturo mis padres, María Lyliam mi hermana, por el apoyo incondicional, por el cariño y el afecto que siempre me han expresado.

La Universidad Industrial de Santander y la escuela de Ingeniería de Sistemas por brindarme los conocimientos para ser un próximo Ingeniero de Sistemas, orgulloso de mi Universidad, de mi escuela y de mis profesores.

El Profesor Pedro Javier Trujillo Tarazona, en quien encontré un gran docente, amigo y director, su dedicación en el aula, su aporte y disposición para orientarme a sacar este proyecto adelante han sido fundamentales y valiosos.

El Ingeniero Herman Ramírez Gómez quien, como director de la Dirección de Sistemas de Información de la Gobernación de Santander, abrió las puertas de la dependencia que dirige y brindó su apoyo constante en el desarrollo de este proyecto.

A mis amigos, ellos quienes desde la complicidad de la amistad siempre estuvieron ahí para apoyarme, brindarme su mano amiga y ayudar en muchos momentos de mi vida académica a sacar adelante mi carrera.

Al Partido Liberal Colombiano, quien hoy traza una ruta en mi vida, pues esta organización política me abrió las puertas para ejercer liderazgo dentro de ella y hoy me tiene en cuenta en la construcción de una sociedad más equitativa y justa.

Para todos ellos, mi gratitud perenne.

Contenido

Lista de Tablas

Lista de Figuras

Lista de Apéndices

Ver apéndices adjuntos y pueden ser consultados en la base de datos de la biblioteca UIS

Apéndice A: Ampliación de la Metodología de Base Preliminar del Plan de Implementación de la Norma ISO - 27001: 2013

Apéndice B: Controles Según Los Dominios De La Norma ISO/IEC 27002:2013

Apéndice C Procesos, información, recursos y riesgos

Glosario

ACTIVO DE INFORMACIÓN: Se refiere a todo aquello que posea valor para la organización.

ANÁLISIS DE RIESGO: Hace referencia al estudio de las causas de las posibles amenazas, y los daños y consecuencias que éstas puedan producir.

CONFIDENCIALIDAD: Se trata de una propiedad de la información que pretende garantizar el acceso sólo a las personas autorizadas.

CONTROL: Aspectos de la seguridad de la información que dan apoyo para las acciones de implementación para la reducción del riesgo.

DATA CENTER: Centro de procesamiento de datos que es donde se encuentran los recursos tecnológicos necesarios para el procesamiento de la información de una organización.

DISPONIBILIDAD: Se trata de una propiedad de la información que pretende garantizar estar al alcance de todo proceso o persona que lo requiera en el momento indicado.

ESTUDIO PRELIMINAR: Es el estudio que se hace previamente en referencia a un preámbulo en el proceso de implementación.

EVALUACIÓN: Valoración sobre la estimación en el cumplimiento de los requisitos de la norma.

IMPACTO: Factor del riesgo que indica el nivel de daño que puede causar en las actividades de la organización en el caso que ocurran.

INTEGRIDAD: Se trata de una propiedad de la información que implica su buen estado, exactitud y no corrupción de los datos.

ISO 27001:2013: Estándar internacional para la seguridad de la información. Describe cómo gestionar la seguridad de la información en una organización.

METODOLOGÍA: Indica el proceso a seguir para implementar o llevar a cabo el proceso de SGSI.

PLANIFICAR, HACER, VERIFICAR, ACTUAR: Es el ciclo de mejora continua utilizada como metodología en el proceso de implementación de los sistemas de gestión.

RIESGO: Es la vulnerabilidad a la que está expuesta la información al ser manipulada con fines adecuados.

SEGURIDAD DE INFORMACIÓN: Consiste en la protección de la confidencialidad, integridad y confidencialidad de la información incluyendo el cumplimiento de normas legales.

SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN: Sistema de Gestión que se basa en el análisis de riesgos, estructuración de procesos, creación de políticas y responsabilidades con el fin de proteger los activos de información.

VULNERABILIDAD: Se trata de una propiedad de la información que determina debilidad frente a la seguridad de la información (Diaz, 2012), puede ser aprovechada por una amenaza y generar un riesgo.

Listado de Siglas

ICONTEC: Instituto Colombiano de Normas Técnicas y Certificación.

MINTIC: Ministerio de Tecnologías de la Información y las Comunicaciones

PHVA: Planificar, Hacer, Verificar, Actuar.

SGC: Sistema de Gestión de Calidad.

SGSI: Sistema de Gestión de Calidad de la Información

PETIC: Plan Estratégico de las Tecnologías de la Información y las Comunicaciones.

SETIC: Secretaría de Tecnologías de la Información y las Comunicaciones de Santander.

TIC: Tecnologías de la Información y las Comunicaciones.

MSPI: Modelo de Seguridad y Privacidad de a Información.

IEC: International Electrotechnical Commission

ISO: International Organization for Standardization

MSPI: Modelo de Seguridad y Privacidad de la Información

IDESAN: Instituto Financiero para el Desarrollo de Santander

Resumen

TITULO: ELABORACIÓN DEL ESTUDIO PRELIMINAR DEL PLAN DE IMPLEMENTACIÓN DE LA NORMA ISO 27001 "SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN", PARA EL DATA CENTER DE LA DIRECCIÓN DE SISTEMAS DE INFORMACIÓN DE LA GOBERNACIÓN DE SANTANDER [*]

AUTOR: RANGEL SUPELANO, Sergio Arturo [**]

PALABRAS CLAVES: Sistema de Gestión de Seguridad de la Información. ISO 27001:2013. Activos de Información. Política de Seguridad. Gestión de Riesgos. Gobernación de Santander. Data Center.

DESCRIPCIÓN: La Dirección de Sistemas de Información de la Gobernación de Santander, en su propósito de ofrecer calidad en los servicios que presta su Data Center de acuerdo con lineamientos generales de la Estrategia Gobierno en línea reglamentado parcialmente por La Ley 1341-2009 y, considerando el decreto 2573-2014 (Ministerio de Tecnologías de la Información y las Comunicaciones, 2014) ve la necesidad de iniciar el proceso hacia la certificación ISO 27001:2013. Para ello se realiza este estudio preliminar en el que fue explorada y aplicada la metodología PHVA o de Mejora Continua, la cual es recomendada por la norma ISO 27001, sino también, por modelos establecidos en normas vigentes como los lineamientos de Seguridad y Protección de la Información contemplado en el Modelo de Seguridad y Privacidad como habilitador de la política de Gobierno Digital propuesto por el MinTIC en el año 2021.

Este estudio está compuesto por un esquema que reúne las fases de planificar, hacer, verificar y actuar, estableciendo compromisos y liderazgo necesarios por la entidad, así como políticas de seguridad, acciones de soporte, evaluación de desempeño, comunicación y documentación pertinente. Se adjunta una relación de la infraestructura del Data Center y un análisis de los riesgos que pueden perjudicar el buen funcionamiento del mismo. Finalmente, se anexan documentos que contiene controles según los dominios de la norma.

El desarrollo de una propuesta de implementación es un primer paso para desplegar los requerimientos que deben cumplirse en la implementación y certificación en una norma ISO – 27001 por consiguiente, las dimensiones de este proyecto de grado fueron acotadas al alcance real del autor y los recursos disponibles. Igualmente, fue lograda una recopilación de información y aplicación de la misma con el objetivo de elaborar una base inicial para la implementación de la ISO 27001:2013 en el Data Center de la entidad.

---

[*] Proyecto de Grado

[**] Facultad de Ingenierías Físico Mecánicas. Escuela de Ingeniería de Sistemas e Informática. Director de Proyecto: Mg en Informática Pedro Javier Trujillo Tarazona. Codirector: Ingeniero de Sistemas Herman Ramírez Gómez

Abstract

TITULO: PRELIMINARY STUDY DEVELOPMENT OF THE IMPLEMENTATION PLAN FOR ISO 27001 "MANAGEMENT SYSTEM INFORMATION SECURITY" FOR THE DATA CENTER OF THE INFORMATION SYSTEM MANAGEMENT IN THE GOVERNMENT OF SANTANDER*

AUTHOR: RANGEL SUPELANO, Sergio Arturo**

KEYWORDS: Management system information security. Information assets. Security policy. Risk management. Data Center. Information system management.

DESCRIPTION: The Information Systems Directorate of the Government of Santander, in its purpose of offering quality in the services it provides its Data Center in accordance with general guidelines of Online Government Strategy partially regulated by Law 1341-2009 and, Considering Decree 2573-2014 (Ministry of Information and Communication Technologies, 2014). We see the need to start the process towards ISO 27001: 2013 certification. For this, this preliminary study is carried out in which PDCA or Continuous Improvement methodology was explored and applied, which is endorsed not by the same ISO 27001 standard and by models established in current regulations. These models refer to the Information Security and Protection guidelines contemplated in the Security and Privacy Model as an enabler of the Digital Government policy proposed by the MinTIC in the year 2021.

This study is made up of a scheme that brings together the plan, do, check, and act phases, establishing the necessary commitments and leadership on for the entity, as well as security policies, support actions, performance evaluation, communication, and pertinent documentation. Attached is a list of the Data Center infrastructure and an analysis of the risks that may impair its proper functioning. Finally, documents containing controls according to the domains of the standard.

The development of an implementation proposal is a first step to deploy the requirements that must be met in the implementation and certification in an ISO - 27001 standard, therefore, the dimensions of this degree project were limited to the real scope of the author and the resources. available. Likewise, a compilation of information and its application was achieved with the aim of elaborating an initial base for the implementation of ISO 27001: 2013 in the entity's Data Center.

* Minor Degree Project

** Faculty of Physic and Mechanic Engineering. School of System Engineering. Project Director: MCs on Computer Science Pedro Javier Trujillo Tarazona. Codirector: System Engineer Herman Ramírez Gómez

Introducción

La información en una organización es un bien de pertenencia exclusiva, no debe ser manipulada ni estar al alcance de agentes externos, procesos o personas no interesadas y de ser posible debe lograr el objetivo de alcanzar los más altos niveles de confidencialidad, disponibilidad e integridad. El objetivo de la ISO 27001 es prevenir y evitar que la información llegue a manos indeseadas que puedan dar uso inadecuado a la información de la organización o de las personas que ella la integran.

Dado que en cualquier organización la información es su principal activo, frecuentemente se encuentra en estado de vulnerabilidad porque requiere ser consultada y manipulada por cualquier agente que haga parte de esta y necesite de su uso para fines organizacionales. Es por ello, que se requiere de la implementación de un Sistema de Gestión de Seguridad de la Información, para reducir al mínimo cualquier acto indebido que de mal uso o dañe la información.

Siendo la Gobernación de Santander, entidad del orden estatal, una organización que maneja grandes volúmenes de información, y que a su vez, por ser de carácter público, contiene información que debe ser de libre consulta para cualquier ciudadano. La Seguridad de la Información le permitirá implementar un esquema que salva guarde los principios de confidencialidad, seguridad y resguardo adecuado de la información.

La Dirección de Sistemas de Información a través del Data Center, es el principal responsable del procesamiento y almacenamiento de información dentro de la entidad, y tiene como objetivo implementar la norma ISO 27001:2013 para dar cumplimiento a la Ley 1581 de 2012 Protección de Datos Personales y lograr dar un manejo adecuado y eficiente a la información que resguarda.

En este trabajo, se describe un estudio preliminar del Sistema de Gestión de Seguridad de la Información ISO 27001 en concordancia con las necesidades en torno de la seguridad de la información para el Data Center bajo la administración de la Dirección de Sistemas de Información de la Secretaría de las TIC de la Gobernación de Santander, teniendo en cuenta los requisitos planteados por la norma ISO 27001:2013.

En el marco teórico se presentan diferentes postulados que sustentan la metodología de este proyecto de investigación, es decir, se dan a conocer conceptos y propósitos de la seguridad de la información, su funcionamiento y a su vez la normativa que determina las directrices a seguir. Esta normativa no sólo provee actividades de mejora a las prácticas que se deben llevar a cabo en este caso en un Data Center, sino suministra los requerimientos que se deben cumplir para lograr una certificación internacional como lo es la Norma ISO 27001: 2013. Con base en ello es posible desplegar todo el estudio preliminar para dar el paso inicial en la transformación del Data Center de la Gobernación de Santander en pro de lograr un excelente funcionamiento del mismo que permita sobre todo brindar un servicio que sea congruente con las actividades del ente estatal para con la comunidad santandereana.

Como metodología se aplicó y se propone el seguimiento del ciclo de mejora continua PHVA descrito en al norma ISO 27001-2013 y especialmente descritos en 14 pasos descritos en el capítulo 4 Desarrollo del Proyecto. En este capítulo también se incluyen: Identificación de las partes interesadas y reconocimiento de la infraestructura tecnológica del Data Center.

Se encuentran plasmados en el estudio preliminar descripción de la plataforma tecnológica del Data Center, identificación de seguridad y agentes comprometidos, análisis de la matriz de riesgos, recopilación de la información y el estudio preliminar.

El estudio preliminar de un proyecto de estandarización de prácticas y requerimientos para el cumplimiento y certificación en una Norma ISO – 27001 funciona como un paso previo a la planificación de cualquier proyecto, de allí nacen los objetivos y el alcance del proyecto de mejora. Se constituye como una primera aproximación en la cual se determina a modo de diagnóstico el estado actual del objeto de estudio, en este caso el estado de los recursos, procesos e infraestructura del Data Center de la Gobernación de Santander. Teniendo dicho diagnóstico se plantea una mejora con base en los requerimientos y directrices de la Norma ISO - 27001 para contrarrestar los riesgos o problemas que se identifican con ayuda del análisis del diagnóstico inicial.

El estudio preliminar entrega tres productos que consisten en una metodología (Apéndice A) basada en la teoría de PHVA con la cual se pretenden contrarrestar los riesgos analizados teniendo en cuenta los procesos, la infraestructura y la información que se encuentra

documentado en otro producto de este estudio preliminar (Apéndice C) y finalmente, se produce los controles que permiten una evaluación constante de la metodología propuesta (Apéndice B).

1. Especificaciones del proyecto

1.1. Título del proyecto

Elaboración del estudio preliminar del plan de implementación de la Norma ISO 27001 "Sistemas de Gestión de la Seguridad de la Información", Para el Data Center de la Dirección de Sistemas de Información de la Gobernación de Santander.

1.2. Justificación

La Gobernación de Santander ha venido haciendo esfuerzos para manejar los estándares planteados por el programa de "Gobierno en Línea" (Colombia, n.d.) de la Presidencia de la República que es el Portal del Estado Colombiano que unifica el acceso a la información, trámites y servicios de las entidades del Estado, para facilitar el acceso a trámites y servicios, y de ahí se trazan los lineamientos de la digitalización y sistematización de los procesos gubernamentales y administrativos de todas las entidades territoriales, y en consecuencia a esto, la Dirección de Sistemas de Información de la Gobernación de Santander quiere dar un paso adelante en cuanto al manejo de la seguridad de la información que administra en su Data Center.

Por tal motivo la Secretaría de las TIC de la administración departamental, ha desarrollado actividades que buscan reforzar la seguridad de la Información resguardada en el Data Center a su cargo, información que es consultada, gestionada y modificada por diferentes entes

involucrados con el departamento de Santander, haciéndose necesario el diseño de un plan de implementación de la norma ISO 27001 con el fin de que el Data Center que se encuentra bajo la tutela de la Dirección de Sistemas de Información, avance en el mejoramiento de Sistemas de Gestión de la Seguridad de la Información (SGSI).

Para la entidad, será un apoyo contar con el estudio preliminar, porque servirá como punto de partida a la implementación de la norma, porque la metodología determina que se tiene y que hay que hacer para cumplir con los requisitos que establece la norma ISO 27001:2013, lo que permitirá ingresar a un nivel organizacional competitivo, con información protegida y segura.

1.3. Definición del problema

Cada vez hay más conciencia sobre la importancia de la seguridad de la información en las organizaciones, todas ellas sin importar que tipo de organización sea, el rol que desempeñe en la sociedad o el sector económico al cual pertenezca, todas están en común acuerdo sobre la seguridad de la información de sus organizaciones.

Según el estándar Internacional ISO/IEC 17799 “la información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita ser protegido adecuadamente.” por eso se hace necesario la realización de un sistema de gestión de seguridad de la información con el fin de salvaguardar los intereses de la información que la entidad resguarda en su Data Center, información que en ocasiones su publicación puede vulnerar la ley de protección de datos personales.

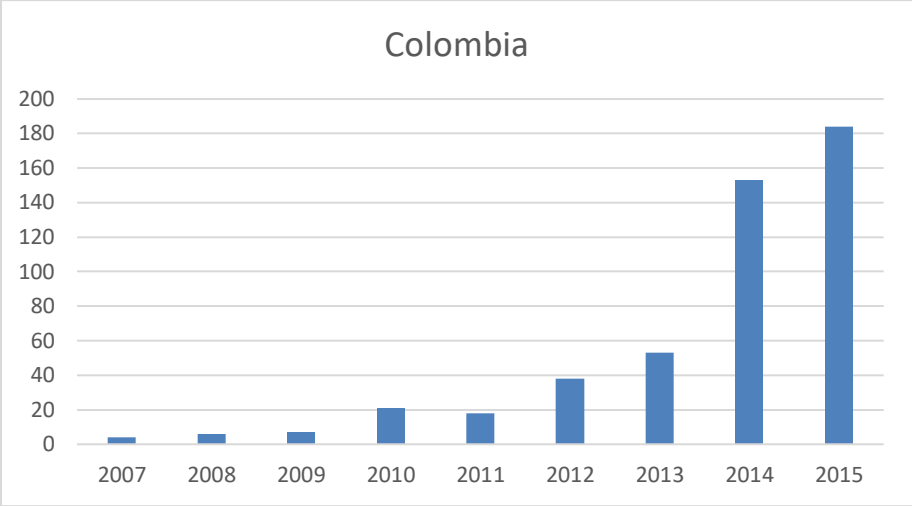
Dentro del plan de Acción de la Secretaría de las TIC está contemplada la implementación de una política de seguridad de la información, adelantado en su propósito en el Plan Estratégico de Tecnologías de la Información y las comunicaciones PETIC, y que contribuye en el cumplimiento de requisitos contemplados por la norma ISO 27001:2013.

El objetivo del estudio preliminar se cumple a cabalidad, porque se hace un diagnóstico sobre los requisitos de la norma, los procesos y plataforma tecnológica del Data Center y queda plasmado en un documento que servirá de apoyo en el proceso de implementación, el documento contiene:

- La definición total de los procesos manejados por el Data Center e información resguardada en el mismo.
- La infraestructura tecnológica del Data Center.
- La metodología obtenida del diagnóstico de los requisitos de la norma ISO 27001:2013 incluido el instructivo de implementación de controles del Apéndice A.

Figura 1

Evolución de Certificados ISO/IEC 27001 en Colombia. Elaboración Propia



Nota: Datos tomados de las encuestas realizadas anualmente por la entidad ISO. (ISO, 2015)

1.4. Alcance

El producto al que se desea llegar con este estudio preliminar para la aplicación de la Norma ISO – 27001: 2013 consiste en el diagnóstico del estado actual del Data Center de la Gobernación de Santander y con base en ello elaborar una metodología alineada a lo dictado por la Norma ISO – 27001:2013, cumpliendo los requisitos de Seguridad de la Información propuestos por ella apegándose a la normativa vigente que busca optimizar los procesos y servicios que brinda esta importante dependencia de dicha entidad gubernamental. Dicha estudio preliminar incluye una identificación de riesgos, una metodología basada en el ciclo PHVA y recomendaciones de acuerdo a la implementación de controles.

1.5. Objetivos

1.5.1. Objetivo general

Elaborar el estudio preliminar de el plan de implementación de la norma ISO 27001 Sistemas de Gestión de la Seguridad de la Información para el Data Center de la Dirección de Sistemas de Información de la Secretaría de las TIC de la Gobernación de Santander con el fin de que este sea implementado posteriormente para garantizar el cumplimiento de las leyes y regulaciones establecidas en materia de gestión de la información.

1.5.2. Objetivos específicos

- Proponer una metodología base que será un punto de partida para la implementación del SGSI para el Data Center de la Dirección de Sistemas de Información de la Gobernación de Santander en concordancia con la norma ISO 27001:2013.
- Identificar procesos, información e infraestructura que se relacionen con el funcionamiento del Data Center de la Dirección de Sistemas de Información de la Secretaría de las TIC de la Gobernación de Santander, para definir los alcances de la norma ISO 27001:2013.
- Identificar riesgos relacionados a los procesos, información e infraestructura manejada en el Data Center de la Dirección de Sistemas de Información de la Gobernación de Santander en concordancia con la norma ISO 27001:2013.
- Estructurar el estudio preliminar del plan de implementación de la norma ISO 27001:2013 en el Data Center de la Dirección de Sistemas de Información de la Secretaría de las TIC de la Gobernación de Santander que le sirva a la Dirección de

Sistemas de Información de la Secretaría de las TIC de la Gobernación como herramienta para identificar documentación necesaria para la posterior implementación de la norma ISO 27001:2013.

1.6. Metodología de la investigación

Durante el propósito del desarrollo del proyecto fue necesario el uso de técnicas de diagnóstico como reuniones con el Director de Sistemas de Información de la Secretaría de las TIC y el contratista asignado a la administración del Data Center.

Como primer punto en el desarrollo del proyecto, fue el estudio y entendimiento de la norma ISO 27001:2013, revisión y conocimiento a cabalidad del alcance y objetivo que ella plantea y la interpretación con respecto a las ventajas de la implementación de la norma, uno de los propósitos para el dominio de la norma se llevó a cabo en una exposición realizada en la asignatura Auditoría de Sistemas en el segundo semestre de 2014 bajo la orientación del profesor Luis Carlos Gómez Flórez.

Se llevó a cabo el análisis de los documentos de la dependencia suministrados por el director, como el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC, Análisis de riesgos de la infraestructura tecnológica y el Plan de contingencia, para extraer información sobre sus características, inferir aspectos importantes sobre la cultura organizacional y conocer detalladamente los procesos que maneja el Data Center.

El conocimiento de la información contemplada en estos documentos, sirvió para identificar los objetivos que la implementación de estos cumplirá con base a los requisitos de la norma, y así dejarlos plasmados en el estudio preliminar.

Con el acompañamiento y asesoría del administrador del Data Center, se realizó el levantamiento de la información concerniente a la infraestructura tecnológica, procesos e inventario de sistemas de información que se relacionan con el funcionamiento del Data Center.

La revisión de la documentación generada en el desarrollo del proyecto por parte del Director de Sistemas de Información fue fundamental para lograr alcanzar los objetivos planteados en el proyecto. Adicionalmente fueron usadas las directrices propuestas por el Modelo de Seguridad y Privacidad de la Información (MSPI) que hace parte como habilitador transversal de la política de Gobierno Digital, documento diseñado por el MINTIC; el cual está alineado con la Norma ISO – 27001:2013 y de acuerdo a las buenas prácticas pertinentes a la seguridad de la información y a la legislación relacionada con la protección de la información como lo es la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública.

2. Gobernación de Santander – Secretaría de tecnologías de la información y las comunicaciones

La Gobernación de Santander, "de acuerdo con el Artículo 298 de la actual Constitución Política de Colombia, es una entidad territorial que goza de autonomía para la administración de los asuntos seccionales y la planificación y promoción del desarrollo económico y social dentro de su territorio en los términos establecidos por la Constitución y las leyes. Los departamentos ejercen funciones administrativas, de coordinación, de complementariedad de la acción municipal, de intermediación entre la Nación y los municipios y de prestación de los servicios que determinen la Constitución y las leyes". (Departamento Administrativo Nacional de Estadística - DANE, 2014)

"La Gobernación de Santander contempla como objetivo primordial mejorar la calidad de vida de los santandereanos fomentando la competitividad, fortaleciendo la ciencia y la tecnología y recuperando la infraestructura vial, entre otros, vitales para el desarrollo y la proyección del departamento". (Gobernación de Santander, 2012)

2.1. Plan estratégico

2.1.1. Misión

"La Secretaría de las Tecnologías de la Información y las Comunicaciones tiene como misión crear, fomentar, dirigir, apropiar y administrar el ecosistema digital departamental, basado en el fortalecimiento de la productividad de la región, a través de la interconexión digital,

que permita contar con información oportuna y confiable para la toma de decisiones y el cumplimiento de todas las misiones del ecosistema digital del departamento de Santander". (SETIC, 2015) (Misión modificada recientemente).

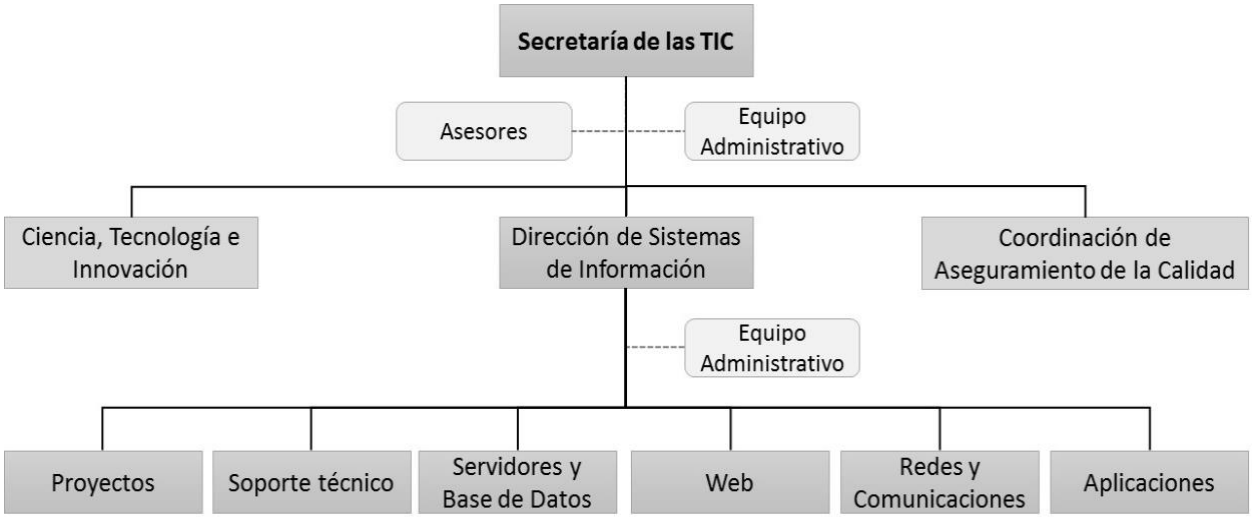
2.1.2. Visión

"La Secretaría tiene como proyección ser para el 2021 la Secretaría de Tecnologías de la Información y Comunicaciones de referencia en la Administración Departamental y Nacional, pautada en el avance y promoción de las TIC por su liderazgo en los índices de implementación del ecosistema digital nacional". (SETIC, 2015) (Visión modificada recientemente).

2.1.3. Estructura Organizacional

Figura 2.

Organigrama Secretaría de Tecnología de la Información y las Comunicaciones.



Nota: Basado en el organigrama de la entidad

2.1.4. Objetivo general

"La Secretaría de las TIC se encarga de incentivar el desarrollo de infraestructura, contenidos y aplicaciones, así como la ubicación estratégica de terminales y de equipos que beneficien realmente a los ciudadanos al acceder a las aplicaciones tecnológicas en todo el departamento". (Santander S. d., 2015).

2.2. Dirección de sistemas de información

Dentro de la Secretaría de Tecnología de la Información y las Comunicaciones, se encuentra la Dirección de Sistemas de Información, a cargo de un profesional en Ingeniería de Sistemas como director; esta dependencia tiene a cargo la administración del Data Center.

Figura 3

Data Center de la Secretaría de Tecnología de la Información y las Comunicaciones

Nota: Imagen tomada de la Portada del Video institucional y de presentación del Data Center

https://www.youtube.com/watch?v=W0BP11JWxWU

2.2.1. Propósito Principal

"Dirigir todo lo concerniente a la preparación, coordinación y formulación de políticas y programas en temas relacionados con la aprobación y desarrollo de las tecnologías de la información en el Departamento". (Santander S. d., 2015).

2.2.2. Funciones Esenciales

- "Liderar la formulación de políticas y planes de desarrollo informático de acuerdo con las necesidades de las dependencias y el avance tecnológico.
- Fomentar, evaluar, desarrollar e implementar el sistema de información de la Gobernación de Santander, planeando las políticas y lineamientos para la adquisición de la infraestructura de hardware, software y telecomunicaciones requerida por las secretarías e institutos descentralizados.
- Garantizar la oportunidad y calidad en los servicios de mantenimiento y actualidad de los equipos de red y base de datos.
- Evaluar periódicamente el funcionamiento de la estructura tecnológica del departamento, proponiendo los ajustes necesarios para mejorar la gestión administrativa y adaptarla a la normatividad vigente y a las innovaciones tecnológicas.
- Realizar las demás funciones que le asigne el superior inmediato, relacionadas con el cargo que desempeña". (Santander S. d., 2015)**.**

2.3. Coordinador de aseguramiento de la calidad

2.3.1. ***Propósito Principal***

"Velar por la sostenibilidad de los procesos y procedimientos de la Secretaría de las TIC en los sistemas integrados de gestión adoptados por la Gobernación de Santander". (Santander S. d., 2015)

2.3.2. Funciones Esenciales

- "Dirigir las actividades necesarias en la Secretaría de las TIC para establecer, documentar, implementar, mantener y mejorar los sistemas de gestión de la Gobernación de Santander.
- Planear y coordinar las auditorías internas y externas que evalúan la conveniencia, adecuación, eficacia y efectividad de los sistemas de gestión adoptados por la Gobernación de Santander.
- Dirigir las acciones de mejora de los procesos de la secretaría de las TIC en los sistemas de gestión de la Gobernación de Santander.
- Informar a la alta dirección sobre el desempeño de los sistemas de gestión adoptados por la Gobernación de Santander.
- Orientar, revisar y aprobar la documentación generada en la Secretaría de las TIC en la implementación, mantenimiento, y mejora de los sistemas de gestión de la Gobernación de Santander.
- Realizar las demás funciones que le asigne el superior inmediato, relacionadas con el cargo que desempeña". (Santander S. d., 2015)

3. Marco teórico

3.1. Sistema de gestión de seguridad de la información

Uno de los principales objetivos de una empresa ya establecida o una que comienza, es el éxito que quiere tener, que proyecta y que día a día busca con esmero durante todas las actividades y productos que realiza.

Cada una debe mantenerse al día con respecto a los avances tecnológicos y adaptarse a los cambios a los que el mundo está expuesto día tras día, en un mundo donde los conceptos ahora son globalizados y la competencia ya no es local si no mundial. Es así, como las empresas se interesan por tener presencia en la web y la sistematización de su información y en muchas ocasiones de sus procesos para el buen funcionamiento de cualquier organización y deben tener prioridad por la seguridad de la información.

"El modelo ISO 27001 define a un SGSI como "La parte del sistema de gestión global, basada en una orientación a riesgo de negocio, para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la seguridad de la información"". (Alexander, 2007, p. 19)

"La norma ISO 27001 define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información". (EPPS Services Ltd. para negocios electrónicos y consultoría comercial., n.d.)

La norma ISO 27002 establece los controles que se deben adoptar en la organización con el fin de implementar el sistema de gestión de seguridad de la información. (EPPS Services Ltd. para negocios electrónicos y consultoría comercial., n.d.).

3.1.1. Seguridad de la información

"Se entiende por información todo aquel 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.

La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización." (Free Website Template By: PriteshGupta.com, 2012)

La información que posee cualquier empresa sea privada o pública, es un valioso recurso porque con ello obtiene conclusiones importantes para determinar productos y servicios que favorezcan su competitividad en el campo deseado; en este caso, la información gubernamental es importante, contiene información que legalmente es pública por ser una entidad del estado, y por tal motivo hay que protegerla de todo tipo de manipulación mal intencionada, sin llegar nunca a ocultar la información.

Para tal motivo, las entidades deben identificar qué información es imprescindible para su correcto funcionamiento y determinar los riesgos a la exposición de información y buscar la manera de disminuir el riesgo al que se expone la información que debe ser visible.

3.1.2. Fundamentos

"Para garantizar que la seguridad de la información es gestionada correctamente se debe identificar inicialmente su ciclo de vida y los aspectos relevantes adoptados para garantizar su C-I-D:

- Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados.
- Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.
- Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran." (Free Website Template By: PriteshGupta.com, 2012)

3.1.3. Ventajas

- "Mejorar continuamente la gestión de la seguridad de la información.
- Disminuir el riesgo, con la consiguiente reducción de gastos asociados.
- Reducir la incertidumbre por el conocimiento de los riesgos e impactos asociados.
- Aumento de la rentabilidad, derivado de un control de los riesgos.
- Garantizar la confidencialidad, integridad y disponibilidad de la información sensible.
- Garantizar la continuidad del negocio.
- Aumento de la competitividad por la mejora de la imagen corporativa
- Incremento de la confianza de las partes interesadas.
- Cumplir la legislación vigente referente a seguridad de la información.
- Aumentar las oportunidades de negocio.

- Reducir los costos asociados a los incidentes.
- Mejorar la implicación y participación del personal en la gestión de la seguridad.
- Mejorar los procesos y servicios prestados.” (Excellence, n.d.)

3.1.4. Norma ISO 27001:2013

“ISO 27001 es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

ISO 27001 se ha convertido en la principal norma a nivel mundial para la seguridad de la información y muchas empresas han certificado su cumplimiento; aquí se puede ver la cantidad de certificados en los últimos años”: (EPPS Services Ltd. para negocios electrónicos y consultoría comercial., n.d.)

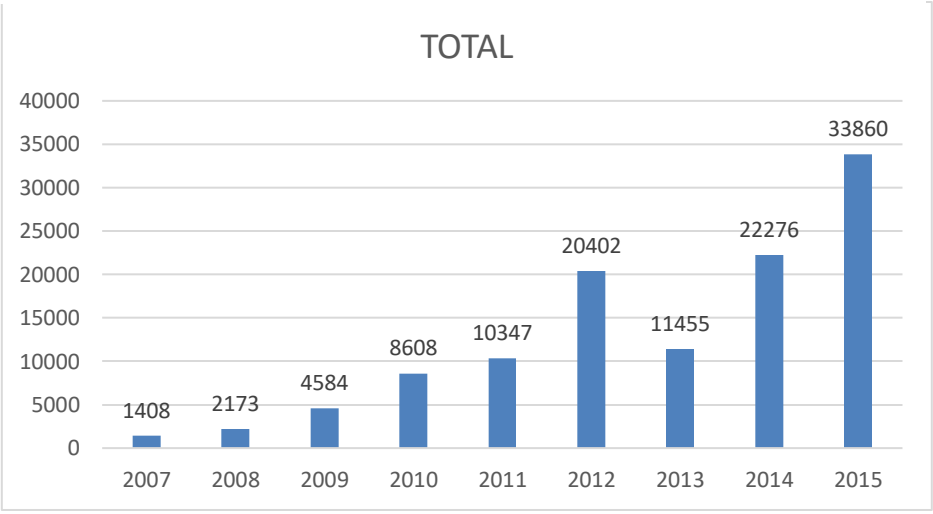
3.1.5. Norma ISO 27002:2013

ISO/IEC 27002:2013 establece los lineamientos para implementar los controles que se indican en la ISO/IEC 27001:2013 de 114 controles incluidos en 14 dominios que tienen como función principal la de reducir los riesgos de seguridad de la información, conociendo de forma precisa todos los activos que posee y manteniendo una base sólida de la administración de sus riesgos.

La norma ISO/IEC 27002:2013 indica como generar la tabla de controles por medio de la cual la organización establece cuales son de su uso y cuáles no, identificándolos a través de un análisis de riesgo que proporcione información valiosa sobre los activos que pueden dividirse en recursos de información, recursos de software, activos físicos y servicios. (EPPS Services Ltd. para negocios electrónicos y consultoría comercial., n.d.).

Figura 4

Cantidad de Certificados Emitidos por la entidad ISO. Elaboración Propia.



Nota: Datos tomados Encuesta ISO sobre generación de certificaciones de la norma para sistemas de gestión ISO – 27001 (ISO, 2015)

3.1.6. Normas y regulaciones relacionadas

Tabla 1.

Identificación de las principales normativas colombianas que rigen los procesos de implementación de sistemas de gestión de seguridad de la información.

Norma Vigente	**Descripción**
Ley 1341 de 2009	Esta Ley define los principios y los conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones –TIC. Por ejemplo, en el artículo 2 se disponen los principios orientadores que determinan que la investigación, el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones son una política de Estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los Derechos Humanos inherentes y la inclusión social. Puntualmente en el numeral 8 de este artículo se establece que todas las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las TIC con el fin lograr la prestación de servicios eficientes a los ciudadanos para lo cual el Gobierno dará a conocer los mecanismos y condiciones que garantizan este objetivo entre los cuales se destacan los plazos, términos y prescripciones para la implementación de infraestructura y actualización de la misma y con la

Norma Vigente	Descripción
	información completa los medios y los instrumentos tecnológicos.
Ley 1581 de 2012	Es una Ley bastante conocida como la Ley de Habeas Data en esta se dictan las disposiciones generales para la protección de datos personales, 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. Desarrolla unos principios que versan sobre protección de datos personales de carácter general entre los cuales se destaca el principio de seguridad que hace referencia que cuando en lo que respecta a la información personal contenida en bases de datos y la resultante de las consultas que realicen los usuarios, se incorporen las medidas técnicas necesarias para garantizar la seguridad de los registros, a fin de evitar su adulteración, pérdida, consulta o uso no autorizado.
Decreto 1078 de 2015	En este decreto se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, El objeto de este decreto es compilar la normatividad vigente expedida por el Gobierno Nacional mediante las facultades reglamentarlas conferidas por el numeral 11 del artículo 189 de la Constitución Política al Presidente de la República para la cumplida ejecución de las leyes en el sector de Tecnologías de la Información y las Comunicaciones. Puntualmente hace referencia a los elementos, lineamientos, componentes y objetivos transversales de La Política de Gobierno Digital que permitirán el

Norma Vigente	Descripción
	logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC siempre proponiendo una optimización de las funciones del estado y su relación con la sociedad.
Decreto 1083 de 2015	Es un decreto que está relacionado casi en su totalidad con los lineamientos, directrices y objetivos del Sector de La Función Pública, para lo cual son tenidos en cuenta las TIC como elemento importante a través del establecimiento de un Plan de Seguridad y Privacidad de la Información el cual comprende todas aquellas actividades que contribuyen a la protección de la información.
Decreto 2106 de 2019	Más conocido como Decreto Anti-trámite, tiene por objeto simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la Administración Pública, bajo los principios constitucionales y legales que rigen la función pública, con el propósito de garantizar la efectividad de los principios, derechos y deberes de las personas consagrados en la Constitución mediante trámites, procesos y procedimientos administrativos sencillos, ágiles, coordinados, modernos y digitales.
Resolución número 00500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital

4. Desarrollo del proyecto

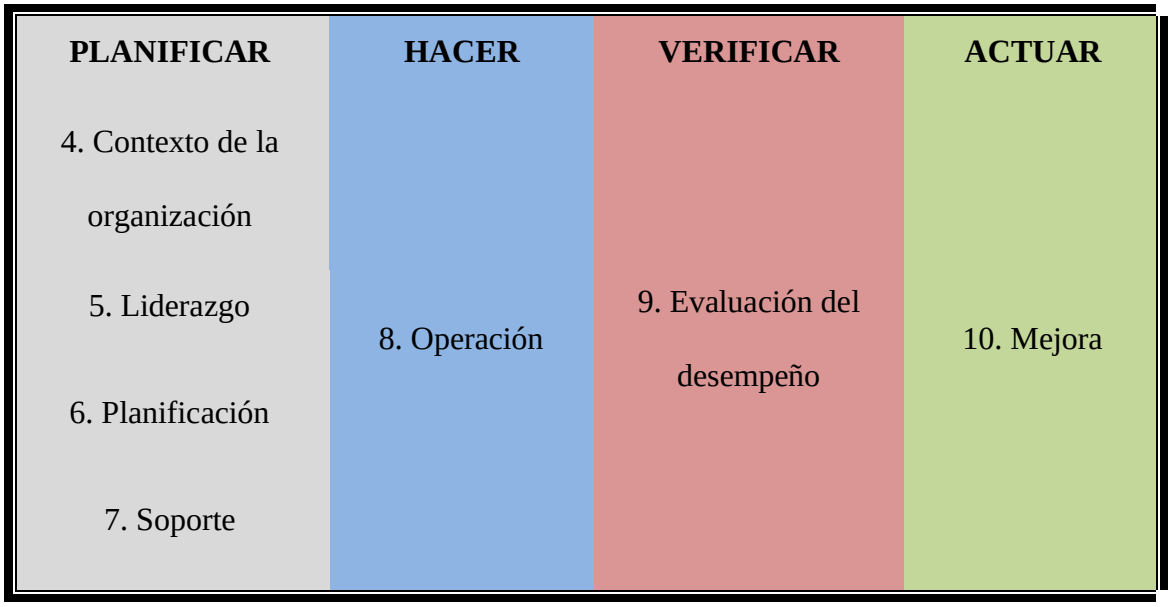
4.1. Metodología basada en el ciclo de mejora continua

La información necesaria para el cumplimiento del objetivo está documentada como estudio preliminar y metodología de implementación como una herramienta de apoyo a la Dirección de Sistemas de Información de acuerdo al modelo de implementación de la norma ISO 27001:2013 Sistemas de Gestión de Seguridad de la Información.

En toda organización en proceso de certificación es fundamental el uso del PHVA (Planificar, Hacer, Verificar, Actuar) ciclo de mejora continua:

Figura 5.

Ciclo de Mejora Continua



Nota: Basado en el Modelo de Edwards Deming, PDCA Cycle: Plan, Do, Check, Act.

- **Planificar:** Establecer los objetivos y procesos necesarios como metas para alcanzarlas de conformidad con los requisitos de la organización y de la norma.
- **Hacer:** Implementar los procesos, recoger datos para alcanzar los objetivos.
- **Verificar:** Realizar seguimiento y medir los procesos evaluando los resultados de los procesos ejecutados en relación con las políticas, objetivos, requisitos e identificando las NO conformidades y reportando los resultados alcanzados.
- **Actuar:** Realizar acciones, tomar medidas correctivas para lograr el cumplimiento de las metas y promover la mejora continua del desempeño de los procesos.

El diagnóstico sobre la situación actual, el levantamiento de información sobre los procesos o sistemas de información y la infraestructura tecnológica que tienen relación con el Data Center, fueron la clave principal para poder realizar el estudio preliminar sobre la norma ISO 27001:2013 y así proponer una metodología que pueda ser usada como herramienta en el propósito de implementación y certificación.

El estudio se fundamenta en la actualización 2013, que ha sido basada y mejorada con respecto a la norma ISO 27001:2005 y determina los requisitos que la organización, en este caso, el Data Center de la Dirección de Sistemas de Información de la Secretaría de las TIC de la Gobernación de Santander, debe cumplir para establecer con éxito su proceso de certificación ISO 27001, también se hace referencia a la norma ISO 27002:2013 que establece como implementar los controles de la norma ISO/IEC 27001:2013 generando un mayor aseguramiento de los activos de información y una mejor gestión del riesgo. Para este proyecto de investigación se ha elaborado un Apéndice B *Controles Según Los Dominios De La Norma ISO/IEC*

27002:2013 en el cual se detallan los controles que permiten establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI dentro de la organización en este caso la Gobernación de Santander garantizando la aplicación de las medidas de seguridad informática adecuadas que permitan el acceso a la información solo al usuario indicado y a los recursos indicados establecidos en nuestro plan de gestión.

4.2. Metodología de implementación

La implementación de la norma ISO - 27001 es un proceso continuo y extenso en el cual se involucran diferentes fases que buscan establecer un conjunto de acciones preventivas en función de la seguridad de la información que dispone una organización y las oportunidades de mejora que puedan verse involucradas. Estas fases se componen de diversas actividades sistemáticas las cuales están definidas a continuación para el contexto del manejo seguro del Data Center de la Gobernación de Santander.

A partir del ciclo PHVA se propone un conjunto de doce actividades principales que se detallan en la Tabla 1 y las cuales son: lograr un compromiso administrativo, establecer una política pública, definir un alcance, establecer una planificación, planificar acciones de soporte, operaciones, verificaciones a partir de la evaluación del desempeño y optimizaciones aplicadas a lo largo del tiempo. Dicha metodología se relaciona en el Apéndice A *Ampliación de la Metodología de Base Preliminar del Plan de Implementación de la Norma ISO- 27001: 2013*. Sin embargo en la siguiente tabla se definen de manera resumida las acciones que hacen parte de cada una de las fases del ciclo de Mejora Continua.

Tabla 2.

Cuadro resumen de las acciones principales en la propuesta de implementación de la Norma ISO-27001 SGSI

CUADRO RESUMEN DEL PROCESO DE IMPLEMENTACIÓN SGSI	
Acción	**Descripción**
1. Lograr un Compromiso Administrativo	En primer lugar debe surgir un compromiso por parte de la Dirección de Sistemas de Información que permita garantizar el talento humano, tecnológico y económico para iniciar el proceso de implementación de SGSI.
2. Establecer como Política Pública.	Establecer la implementación de un SGSI requiere de todo el apoyo administrativo de una entidad, y ello conlleva a que sea una Política Pública de la entidad llevarlo a cabo, para con ello poder garantizar su cumplimiento mediante la apropiación de recursos que permitan adquirir el talento humano y el recurso físico necesario para su posterior implementación.
3. Definir un Alcance	Determinar el cumplimiento de parámetros legales y políticas de obligatorio cumplimiento como Habeas Data, Gobierno en Línea, etc. que la implementación del SGSI garantiza.
4. Definir la Política de SGSI	La política del SGSI es el documento que sirve de Columna Vertebral de todo el proceso de Implementación, debe contemplar los aspectos básicos de la norma aterrizados en el entorno del Data Center. (Aspectos mencionados anteriormente).

CUADRO RESUMEN DEL PROCESO DE IMPLEMENTACIÓN SGSI

Acción	Descripción
5. Analizar Riesgos	Es una de las partes más importantes de la norma, en esta parte se identifican los aspectos relacionados con la norma, se detallan los activos, factores de vulnerabilidad, amenazas, consecuencias y formalidades en los posibles hallazgos. Siempre debe haber resultados de la evaluación de riesgos que permitan definir el nivel de seguridad de la información.
6. Elaborar la Declaración de Aplicabilidad	Es el documento que consolida toda la política de SGSI, define justificadamente los controles aplicables y no aplicables en el Data Center, los objetivos alcanzados y descripción de la implementación de controles.
7. Definir el Plan de Riesgo	Define como se implementan los controles de la Declaración de Aplicabilidad, los roles de quienes intervienen en ello y como se llevará acabo tanto técnica como presupuestalmente, sin este plan no se podrá saber cuál es el siguiente paso.
8. Evaluar la Medición de Controles	Identificar los indicadores que permitan medir la eficiencia y eficacia de los controles de la Declaración de Aplicabilidad para poder determinar si se está o no cumpliendo con los objetivos de la implementación del SGSI y cuál es su índice de aplicabilidad.

CUADRO RESUMEN DEL PROCESO DE IMPLEMENTACIÓN SGSI

Acción	Descripción
9. Implementar la Declaración de Aplicabilidad	Es la actividad más dispendiosa de toda la metodología, aquí se ponen en ejecución los puntos anteriormente definidos basados en los controles, donde seguramente habrá que generar cambios en la organización tanto de hábitos como de conductas con respecto al manejo de la información que pueden inicialmente generar resistencia, prevención y algo de caos organizacional.
10. Capacitar y Socializar	Para poder sortear de la mejor manera el punto anterior es imperativo la capacitación y concientización del talento humano que tendrá que ver con la aplicación de controles, saber qué hacer en determinados casos, conocer la importancia de la norma, dar a conocer las políticas, el plan de riesgo, los mecanismos de medición, etc. La no aplicabilidad de este punto puente poner en riesgo la implementación y el éxito del SGSI.
11. Poner en Marcha el SGSI y Supervisarlo.	Es la puesta en marcha de los 10 puntos anteriores y la profundización de la implementación de los mismos, es aquí donde los responsables del cumplimiento del SGSI están supervisando los indicadores de medición, la implementación adecuada de la ISO 27001 y saber cuáles tareas se están llevando adecuadamente y cuales no dentro del esquema que involucra al Data Center y crear registros para poder evaluar.
12. Realizar Auditoría Interna	Todo proceso administrativo tiene su auditoría interna, y esta no es la excepción, desde el momento en que se convierte en una política pública dentro de la organización hay que establecer que está bien y que está mal,

CUADRO RESUMEN DEL PROCESO DE IMPLEMENTACIÓN SGSI

Acción	Descripción
	medirlo, hacerlo saber y corregirlo. La identificación de hallazgos no es para sancionar administrativamente sino al contrario, debe servir como un modelo de mejora continua dentro de la organización.
13. Designar Dirección	La cabeza administrativa del Data Center es el responsable de saber el estado real del SGSI, contempla la obligación de saber el nivel de conformidad en la aplicación de la norma de todas las personas que en ella intervienen, su grado de compromiso y la ejecución de las tareas establecidas dentro de los parámetros anteriormente definidos, la dirección basada en su supervisión determina los pasos que se deben dar.
14. Activar Promoción y Prevención	La razón de la implementación de la norma es hacer que las no conformidades sean corregidas, que los factores de riesgo y vulnerabilidad sean evitados en lo posible, y establece las medidas correctivas o preventivas a aplicar. Se debe solucionar el problema y evitar que se repita.

4.3. Identificación de las partes interesadas

Las partes interesadas en un proyecto pueden estar vinculadas a personas naturales o jurídicas que se ven afectadas en mayor o menor proporción con las acciones de alguna organización. En el proceso de identificar estas partes interesadas fueron encontradas diferentes dependencias de la Gobernación de Santander e Institutos descentralizados que se podrían

beneficiarse o afectarse por una decisión, actividad o resultado de este proyecto; a continuación en la Tabla 3 se relacionan los principales interesados en el desarrollo de esta propuesta de implementación:

Tabla 3

Dependencias interesadas en el desarrollo del proyecto

Dependencia	**Edificio Central de**	**Externo**
Asamblea Departamental		x
Casa de Participación		x
Despacho del Gobernador	x	
Forest (Sistema Documental)	x	
IDESAN		x
Prensa	x	
Secretaría de Agricultura y		x
Secretaría de Cultura y Turismo		x
Secretaría de Desarrollo	x	
Secretaría de Educación	x	
Secretaría de Hacienda	x	
Secretaría de Planeación	x	
Secretaría de Salud		x
Secretaría de la Mujer	x	
Secretaría de Transporte e Infraestructura	x	
Secretaría de Vivienda		x
Secretaría del Interior	x	
Secretaría General	x	
Secretaría Tecnologías de la	x	x

4.4. Reconocimiento de la infraestructura tecnológica del Data Center

La infraestructura tecnológica del Data Center consta de 9 Servidores en funcionamiento, incorporados en un complejo habitacional adecuado y óptimo para su uso, seguro y dotado con todos los sistemas de seguridad física para así convertirlo en un Data Center, seguro, eficiente, competitivo y accesible. Aquí se detalla la configuración de los 9 servidores que componen el Data Center.

4.4.1. Configuración servidores

En las siguientes tablas se procede a documentar la información técnica detallada de cada uno de los nueve servidores físicos presentes en el Data Center de la Gobernación de Santander.

Tabla 4

Información Técnica Servidor 1

	Servidor 1	
1	Formato del Servidor RACK o TORRE	RACK
2	Cantidad de Procesadores 1 o 2	2
3	Velocidad del Procesador, Cuantos Cores	2 x 2.393 GHz
4	Cantidad de Memoria RAM	32 GB
5	Cantidad de Discos	2
6	Capacidad de los Discos	300GB
7	Nivel de Arreglo RAID (/0 /1 /5 /6 /10 /60)	1
8	Cantidad de Puertos de Red	4
9	Velocidad de los Puertos de Red	1000 MBS
10	Unidad Óptica Interna, DVD-ROM/DVD-RW	DVD
11	Requiere Fuente de Poder Redundante	TIENE FUENTE
12	Estado/Ciudad en el que se instalara el servidor	BUCARAMANGA
13	Tipo de Soporte (NBD-Básico, Prosupport-Medio, MC-	BASICO
14	Incluye o No Sistema Operativo - Qué Sistema Operativo va	VMWARE
15	Requiere la Instalación del servidor	INSTALADO
16	Otros	OPERAN 4 VM
17	MARCA	DELL
18	MODELO	POWER EDGE 2970

Tabla 5.

Información Técnica Servidor 2

	Servidor 2	
1	Formato del Servidor RACK o TORRE	RACK
2	Cantidad de Procesadores 1 o 2	2
3	Velocidad del Procesador, Cuantos Cores	4 x 2.26 GHz
4	Cantidad de Memoria RAM	64 GB
5	Cantidad de Discos	2
6	Capacidad de los Discos	150 GB
7	Nivel de Arreglo RAID (/0 /1 /5 /6 /10 /60)	1
8	Cantidad de Puertos de Red	4
9	Velocidad de los Puertos de Red	1000 MBS
10	Unidad Óptica Interna, DVD-ROM/DVD-RW	DVD
11	Requiere Fuente de Poder Redundante	TIENE FUENTE
12	Estado/Ciudad en el que se instalara el servidor	BUCARAMANGA
13	Tipo de Soporte (NBD-Básico, Prosupport-Medio, MC-	BASICO
14	Incluye o No Sistema Operativo - Qué Sistema Operativo va	VMWARE
15	Requiere la Instalación del servidor	INSTALADO
16	Otros	OPERAN 2 VM
17	MARCA	DELL
18	MODELO	POWER EDGE R710

Tabla 6

Información Técnica Servidor 3

	Servidor 3	
1	Formato del Servidor RACK o TORRE	RACK
2	Cantidad de Procesadores 1 o 2	2
3	Velocidad del Procesador, Cuantos Cores	4 x 2.26 GHz
4	Cantidad de Memoria RAM	16 GB
5	Cantidad de Discos	2
6	Capacidad de los Discos	150 GB
7	Nivel de Arreglo RAID (/0 /1 /5 /6 /10 /60)	1
8	Cantidad de Puertos de Red	4
9	Velocidad de los Puertos de Red	1000 MBS
10	Unidad Óptica Interna, DVD-ROM/DVD-RW	DVD
11	Requiere Fuente de Poder Redundante	TIENE FUENTE
12	Estado/Ciudad en el que se instalara el servidor	BUCARAMANGA
13	Tipo de Soporte (NBD-Básico, Prosupport-Medio, MC-	BASICO
14	Incluye o No Sistema Operativo - Qué Sistema Operativo va	VMWARE
15	Requiere la Instalación del servidor	INSTALADO
16	Otros	OPERAN 3 VM
17	MARCA	HP
18	MODELO	PROLIANT DL380G5

Tabla 7

Información Técnica Servidor 4

	Servidor 4	
1	Formato del Servidor RACK o TORRE	RACK
2	Cantidad de Procesadores 1 o 2	2
3	Velocidad del Procesador, Cuantos Cores	4 x 2.26 GHz
4	Cantidad de Memoria RAM	16 GB
5	Cantidad de Discos	2
6	Capacidad de los Discos	150 GB
7	Nivel de Arreglo RAID (/0 /1 /5 /6 /10 /60)	1
8	Cantidad de Puertos de Red	4
9	Velocidad de los Puertos de Red	1000 MBS
10	Unidad Óptica Interna, DVD-ROM/DVD-RW	DVD
11	Requiere Fuente de Poder Redundante	TIENE FUENTE
12	Estado/Ciudad en el que se instalara el servidor	BUCARAMANGA
13	Tipo de Soporte (NBD-Básico, Prosupport-Medio, MC-	BASICO
14	Incluye o No Sistema Operativo - Qué Sistema Operativo va	VMWARE
15	Requiere la Instalación del servidor	INSTALADO
16	Otros	OPERAN 5 VM
17	MARCA	HP
18	MODELO	PROLIANT DL380G5

Tabla 8

Información Técnica Servidor 5

	Servidor 5	
1	Formato del Servidor RACK o TORRE	RACK
2	Cantidad de Procesadores 1 o 2	1
3	Velocidad del Procesador, Cuantos Cores	6x1.895 GHz
4	Cantidad de Memoria RAM	32 GB
5	Cantidad de Discos	2
6	Capacidad de los Discos	150 GB
7	Nivel de Arreglo RAID (/0 /1 /5 /6 /10 /60)	1
8	Cantidad de Puertos de Red	4
9	Velocidad de los Puertos de Red	1000 MBS
10	Unidad Óptica Interna, DVD-ROM/DVD-RW	DVD
11	Requiere Fuente de Poder Redundante	TIENE FUENTE
12	Estado/Ciudad en el que se instalara el servidor	BUCARAMANGA
13	Tipo de Soporte (NBD-Básico, Prosupport-Medio, MC-	BASICO
14	Incluye o No Sistema Operativo - Qué Sistema Operativo va	VMWARE
15	Requiere la Instalación del servidor	INSTALADO
16	Otros	OPERAN 4 VM
17	MARCA	LENOVO
18	MODELO	THINKSERVER RB430

Tabla 9

Información Técnica Servidor 6

	Servidor 6	
1	Formato del Servidor RACK o TORRE	BLADE
2	Cantidad de Procesadores 1 o 2	2
3	Velocidad del Procesador, Cuantos Cores	8x1.99 GHz
4	Cantidad de Memoria RAM	128 GB
5	Cantidad de Discos	2
6	Capacidad de los Discos	300 GB
7	Nivel de Arreglo RAID (/0 /1 /5 /6 /10 /60)	1
8	Cantidad de Puertos de Red	4
9	Velocidad de los Puertos de Red	1000 MBS
10	Unidad Óptica Interna, DVD-ROM/DVD-RW	NO
11	Requiere Fuente de Poder Redundante	BLADE
12	Estado/Ciudad en el que se instalara el servidor	BUCARAMANGA
13	Tipo de Soporte (NBD-Básico, Prosupport-Medio, MC-Avanzado)	BASICO
14	Incluye o No Sistema Operativo - Qué Sistema Operativo va a utilizar	VMWARE
15	Requiere la Instalación del servidor	INSTALADO
16	Otros	OPERAN 9 VM
17	MARCA	HP
18	MODELO	PROLIANT BL460 G8

Tabla 10

Información Técnica Servidor 7

	Servidor 7	
1	Formato del Servidor RACK o TORRE	BLADE
2	Cantidad de Procesadores 1 o 2	2
3	Velocidad del Procesador, Cuantos Cores	8x1.99 GHz
4	Cantidad de Memoria RAM	128 GB
5	Cantidad de Discos	2
6	Capacidad de los Discos	300 GB
7	Nivel de Arreglo RAID (/0 /1 /5 /6 /10 /60)	1
8	Cantidad de Puertos de Red	4
9	Velocidad de los Puertos de Red	1000 MBS
10	Unidad Óptica Interna, DVD-ROM/DVD-RW	NO
11	Requiere Fuente de Poder Redundante	BLADE
12	Estado/Ciudad en el que se instalara el servidor	BUCARAMANGA
13	Tipo de Soporte (NBD-Básico, Prosupport-Medio, MC-Avanzado)	BASICO
14	Incluye o No Sistema Operativo - Qué Sistema Operativo va a utilizar	VMWARE
15	Requiere la Instalación del servidor	INSTALADO
16	Otros	OPERAN 5 VM
17	MARCA	HP
18	MODELO	PROLIANT BL460 G8

Tabla 11

Información Técnica Servidor 8

	Servidor 8	
1	Formato del Servidor RACK o TORRE	BLADE
2	Cantidad de Procesadores 1 o 2	2
3	Velocidad del Procesador, Cuantos Cores	8x1.99 GHz
4	Cantidad de Memoria RAM	128 GB
5	Cantidad de Discos	2
6	Capacidad de los Discos	300 GB
7	Nivel de Arreglo RAID (/0 /1 /5 /6 /10 /60)	1
8	Cantidad de Puertos de Red	4
9	Velocidad de los Puertos de Red	1000 MBS
10	Unidad Óptica Interna, DVD-ROM/DVD-RW	NO
11	Requiere Fuente de Poder Redundante	BLADE
12	Estado/Ciudad en el que se instalara el servidor	BUCARAMANGA
13	Tipo de Soporte (NBD-Básico, Prosupport-Medio, MC-Avanzado)	BASICO
14	Incluye o No Sistema Operativo - Qué Sistema Operativo va a utilizar	VMWARE
15	Requiere la Instalación del servidor	INSTALADO
16	Otros	OPERAN 4 VM
17	MARCA	HP
18	MODELO	PROLIANT BL460 G8

Tabla 12

Información Técnica Servidor 9

	Servidor 9	
1	Formato del Servidor RACK o TORRE	BLADE
2	Cantidad de Procesadores 1 o 2	2
3	Velocidad del Procesador, Cuantos Cores	8x1.99 GHz
4	Cantidad de Memoria RAM	128 GB
5	Cantidad de Discos	2
6	Capacidad de los Discos	300 GB
7	Nivel de Arreglo RAID (/0 /1 /5 /6 /10 /60)	1
8	Cantidad de Puertos de Red	4
9	Velocidad de los Puertos de Red	1000 MBS
10	Unidad Óptica Interna, DVD-ROM/DVD-RW	NO
11	Requiere Fuente de Poder Redundante	BLADE
12	Estado/Ciudad en el que se instalara el servidor	BUCARAMANGA
13	Tipo de Soporte (NBD-Básico, Prosupport-Medio, MC-Avanzado)	BASICO
14	Incluye o No Sistema Operativo - Qué Sistema Operativo va a utilizar	VMWARE
15	Requiere la Instalación del servidor	INSTALADO
16	Otros	OPERAN 2 VM
17	MARCA	HP
18	MODELO	PROLIANT BL460 G8

4.5. Plataforma tecnológica de la Gobernación de Santander

4.5.1. Equipos de cómputo

Se enlistan los equipos de cómputo que en su totalidad funcionan en la Gobernación de Santander, de los cuales se encuentran en su totalidad enlazados por red a los servidores del Data Center de la Dirección de Sistemas de Información.

Tabla 13

Equipos de Cómputo de la Gobernación de Santander

DEPENDENCIA	EQUIPOS
Prensa	2
Forest	9
Asamblea	16
Otro	17
Secretaría de Agricultura y Desarrollo rural	21
Secretaría de Desarrollo	36
Secretaría de Tecnologías de la Información y las Comunicaciones	41
Secretaría de Planeación	57
Secretaría del Interior	59
Secretaría de Transporte e Infraestructura	68
Secretaría de Hacienda	84
Secretaría General	109
Secretaría de Educación	111
Despacho del Gobernador	129
Secretaría de Salud	164
TOTAL	**923**

Nota: Datos tomados de: SETIC - Santander, Plan Estratégico de las Tecnologías de la Información y las Comunicaciones - PETIC 2012 - 2021, Bucaramanga, 2021

4.5.2. Sistemas de información

El Data Center de la Dirección de Sistemas de Información aloja los procesos correspondientes a los siguientes Sistemas de Información:

Tabla 14

Sistemas de Información

No.	SISTEMA DE INFORMACIÓN EN OPERACIÓN	No.	SISTEMA DE INFORMACIÓN EN OPERACIÓN
1	Sistema financiero y administrativo GUANE	12	Portal radicados Despacho del Gobernador
2	SIA (Información hasta el 2013)	13	Portal Seguimiento cuentas
3	Sistema integrado de salud	14	Portal de tramites
4	Nomina	15	Portal de encuentros
5	Portal Chikyapss	16	Portal de inventarios
6	Portal web Gobernación de Santander	17	Sistema SIA Financiero 2005-2013
7	Intranet Gobernación de Santander	18	Pasivocol
8	Portal Sistema plan de igualdad	19	SSEPI
9	Portal Sistema control interno	20	Mesa de ayuda
10	Portal Casa Santander	21	Sistema jurídico
11	Portal SSEPLAT Planeación	22	FOREST Sistema de correspondencia

Nota: Datos tomados de: SETIC - Santander, Plan Estratégico de las Tecnologías de la Información y las Comunicaciones - PETIC 2012 - 2021, Bucaramanga, 2021

4.5.3. Infraestructura de servidores

El Data Center está diseñado para alojar toda la infraestructura de servidores que soporta a los sistemas de Información que apoyan los procesos misionales de la entidad. La Entidad cuenta con un total de 45 servidores, 9 Físicos y 36 Virtuales, los cuales se encuentran alojados en el Data Center que cuenta con las medidas de seguridad físicas y ambientales requeridas para el resguardo de la Información de la Entidad

Tabla 15.

Total de Servidores Virtuales en Operación

TIPO	**SISTEMA OPERATIVO**	**SERVICIO**
VIRTUAL	CENTOS SERVER	DNS PUBLICO 1
VIRTUAL	WINDOWS SERVER 2008	ACTIVE DIRECTORY
VIRTUAL	WINDOWS SERVER 2008	PASIVOCOL
VIRTUAL	WINDOWS SERVER 2008	SIA
VIRTUAL	WINDOWS SERVER 2008	ACTIVE DIRECTORY
VIRTUAL	WINDOWS SERVER 2000	EDUCACION
VIRTUAL	WINDOWS SERVER 2003	SOFTWARE JURIDICA VIEJO
VIRTUAL	WINDOWS SERVER 2008	KASPERSKY SALUD
VIRTUAL	WINDOWS SERVER 2008	ARANDA
VIRTUAL	WINDOWS SERVER 2008	WEBPRINTER
VIRTUAL	WINDOWS SERVER 2008	RENDICION CUENTAS

TIPO	SISTEMA OPERATIVO	SERVICIO
VIRTUAL	WINDOWS XP	TOMCAT
VIRTUAL	WINDOWS SERVER 2008	SALUD SISTEMA INTEGRADO
VIRTUAL	WINDOWS SERVER 2008	SALUD TOMCAT
VIRTUAL	CENTOS SERVER	GUANE
VIRTUAL	CENTOS SERVER	FOREST
VIRTUAL	WINDOWS SERVER 2008	KAV
VIRTUAL	WINDOWS SERVER 2008	WSUS
VIRTUAL	WINDOWS SERVER 2008	SERVIDOR DE ARCHIVOS
VIRTUAL	CENTOS SERVER	DBARANDA
VIRTUAL	CENTOS SERVER	FOREST
VIRTUAL	CENTOS SERVER	FOREST
VIRTUAL	CENTOS SERVER	PORTAL WEB
VIRTUAL	CENTOS SERVER	PORTAL WEB
VIRTUAL	CENTOS SERVER	NAGIOS3
VIRTUAL	WINDOWS SERVER 2012	PLANEACION
VIRTUAL	CENTOS SERVER	PORTAL WEB RESPALDO
VIRTUAL	CENTOS SERVER	SERVIDOR GUANE RESPALDO
VIRTUAL	WINDOWS 2008 SERVER	SNVIDT
VIRTUAL	WINDOWS 2003 SERVER	JURIDICA
VIRTUAL	WINDOWS 2008 SERVER	NOMINA SALIENTE
VIRTUAL	WINDOWS SERVER 2008	ARCGIS

TIPO	SISTEMA OPERATIVO	SERVICIO
VIRTUAL	CENTOS SERVER	GLASSFISH
VIRTUAL	CENTOS SERVER	GUANE
VIRTUAL	CENTOS SERVER	GUANE PRUEBAS
VIRTUAL	CENTOS SERVER	SQL MONITOREO SALA
VIRTUAL	WINDOWS 2008 SERVER	PLANEACION
VIRTUAL	CENTOS SERVER	PLAN DE DESARROLLO

Nota: Datos tomados de: SETIC - Santander, Plan Estratégico de las Tecnologías de la Información y las Comunicaciones - PETIC 2012 - 2021, Bucaramanga, 2021

La infraestructura del Data Center cuenta con un respaldo de energía soportado en dos UPS de 25 KVA más una UPS de 100KVA en el edificio, esto sumado a una planta generadora de energía de emergencia de 45 KVA exclusiva para el Data Center la cual asegura un suministro mínimo de 20 Horas continuas de operación.

4.5.4. Infraestructura de red y comunicaciones

La Gobernación de Santander cuenta con una RED LAN conectada en anillo con Fibra Oscura de terminación de 1GB de velocidad con las sedes remotas para proveer los servicios ofrecidos por la entidad a sus dependencias para su operación. Los componentes de la infraestructura son:

- Dominio Gobsan.Local
- Servicio de direccionamiento automático DHCP

- Servicio de resolución de nombres DNS
- Servicio de antivirus
- Servicios de actualizaciones automáticas De Windows WSUS
- Servicio de internet
- Servicio de Voz IP" (Santander S. d., 2015)

4.6. Identificación de seguridad y agentes comprometidos

Inicialmente se propone una caracterización de procesos operativos que incluyen tanto el capital humano involucrado en ellos, como los equipos y demás aspectos físicos que sean usados. Se realiza esta identificación con el fin de encontrar puntos críticos que puedan representar problemas futuros en la gestión de seguridad de la información del Data Center de la Gobernación Departamental de Santander. Con esta identificación fueron establecidos parámetros que sustentarán de manera inicial un posterior proceso de implementación de la norma. Estos puntos críticos son analizados por medio de una matriz de riesgos propuesta por La Dirección de Sistemas de Información - Secretaría de las TIC Gobernación de Santander presentada en el Apéndice C *Procesos, Información, Recursos y Riesgos* de este proyecto de investigación, dicha matriz es analizada a continuación.

4.7. Análisis de la matriz de riesgos

Durante el año 2018 fue llevado a cabo un análisis de riesgos relacionado a las prácticas informáticas y la infraestructura tecnológica de la Gobernación de Santander. De esta información fue depurada a aquella que no era pertinente y fueron tenidos en cuenta los riesgos

relacionados a diferentes causas tanto físicas como humanos. Cabe resaltar que todos ellos presentan una valoración de moderada a extrema lo que indica una necesidad de intervención oportuna. para lo cual la metodología, prácticas y requerimientos propuestos en la Norma ISO – 27001: 2013 se presentan como una opción que acerca a la Gobernación de Santander al cumplimiento de la normativa vigente que busca proteger la información y aprovechar las TIC para un mejor funcionamiento de las entidades públicas.

4.7.1. Procesos

A continuación se detallarán como algunos procesos pueden considerarse factor de riesgo en las operaciones que se lleven a cabo en el Data Center de la Gobernación de Santander:

- Ingreso de Personal no Autorizado: nuevamente en este ítem es posible identificar como la manipulación del Data Center por personal que no cuenta con el permiso para hacerlo. Para ello se proponen controles de dichos permisos, es decir corroborar constantemente la cantidad de usuarios creados contra los usuarios solicitados. Este riesgo puede conllevar no sólo a pérdidas económicas, sino a acciones legales por el acceso de personas no autorizadas a información importante o delicada.
- Uso inadecuado de la información del Data Center: nuevamente haciendo énfasis en causas relacionadas al personal, pero, este punto se considera bastante grave debido que el uso de la información con intereses particulares conlleva a la pérdida de la credibilidad de la información, daño de la imagen Institucional, sanciones legales y multas. Los controles de mitigación son similares, ya que se propone mantener siempre el acceso restringido al Data Center solo para personas autorizadas, es decir que a través de oficios administrativos sea tramitado su ingreso.

4.7.2. Infraestructura

A continuación se detallarán los riesgos que se encuentran directamente relacionados a la infraestructura del Data Center de la Gobernación de Santander:

- Problemas de Conectividad: principalmente son causados por Problemas en la prestación del servicio de internet y de conectividad por el deterioro en la red de datos. Esto indica la necesidad de optimizar la infraestructura IT del Data Center y exige adicionalmente mantenimientos y monitoreo a la red lógica y física y brindar soporte a través de la Mesa de Ayuda ya que debido a este problema se ralentizan los procesos operativos de la gobernación y por consiguiente, hay pérdidas económicas y de imagen.
- Tecnología Obsoleta: el Data Center presenta una desactualización de los equipos de cómputo y de los sistemas operativos, nuevamente provocando pérdidas económicas en el ejercicio de las actividades de la entidad. Sin embargo, este depende de decisiones administrativas por las cuales el mecanismo de mitigación está relacionado a solicitudes a la Secretaría General para autorizar la adquisición de equipos y software que cumplan con los requerimientos.
- Cortes de energía no programados: es otro de los puntos más críticos de los riesgos, sin embargo la causa no depende de acciones al interior de La Gobernación de Santander, pero su mitigación, sí. Es necesario que se realicen mantenimientos preventivos programados al sistema de respaldo de energía regulado de la entidad ya que es la manera más correcta de evitar la interrupción del servicio y seguido a esto las pérdidas económicas, teniendo en cuenta todo lo que esto conlleva como el daño de equipos por los cambios de tensión y pérdida de información.

4.7.3. Información

A continuación se describirán los riesgos que pueden asumirse en dado caso exista un incorrecto manejo de la información que se encuentre en el Data Center de la Gobernación de Santander:

- Pérdida de la información de los Servidores: es uno de los puntos más críticos de los riesgos evaluados. Representa varias consecuencias como lo son la necesidad de realizar re-procesos, la pérdida de la credibilidad de la entidad, pérdida de la información, interrupción y ralentización de los servicios prestados por la entidad y sanciones legales. Para evitar un colapso por la pérdida de la información se propone llevar a cabo el Backup de los servidores con el fin de salvaguardar la información. La causa principal está relacionada al mal manejo de la información de los servidores, por lo que adicionalmente se propone que la manipulación de los servidores sea solo llevado a cabo por personal autorizado y capacitado.

4.7.4. Lineamientos de prevención de riesgos

A partir de dichos riesgos se desprenden lineamientos clave para salvaguardar la seguridad informática de este sector de la Gobernación de Santander los cuales son resumidos en tabla 16.

Tabla 16.

Lineamientos que deben ser aplicados en los procesos y el personal involucrado con la operación del Data Center teniendo como base los riesgos anteriormente propuestos.

HUMANOS	**FÍSICOS**
Todo miembro de la entidad gubernamental debe mantener la seguridad de la información que resguarda en el Data Center de la Gobernación de Santander, sea propia de la entidad o de agentes externos asociados a la actividad misional de la entidad dando cumplimiento a los criterios de Confidencialidad, Integridad y Disponibilidad. Confidencialidad, dado que se resguardan datos sensibles, Integridad con respecto a la calidad de la información y Disponibilidad para que permita ser consultada en cualquier momento que se requiera.	En los procesos de adquisición de equipos, ya sea mediante compra por parte de la entidad, o alquiler mediante sistemas de outsourcing u otras modalidades que utilice la entidad para adquisición de bienes y servicios tecnológicos se deben plantear y documentar los procedimientos, controles y medidas de seguridad necesarias.
Toda persona natural o jurídica que tenga acceso al Data Center ya se por funciones contractuales o del cargo el cual desempeñe, debe firmar una cláusula de confidencialidad o de no divulgación de la información con fines distintos a los intereses	Los funcionarios y/o Contratistas deben evitar al máximo la utilización de Discos Duros externos, memorias USB, medios magnéticos y otros dispositivos de almacenamiento masivo que permita hacer copias de la información, de ser necesarias su

HUMANOS	FÍSICOS
misionales de la entidad antes de llegar a poder tener acceso a la información resguardada en el Data Center.	utilización evitar dejarlas al alcance de cualquier agente externo a la dependencia y a su vez dejarlas tiradas u olvidadas en sus estaciones de trabajo.
La entidad debe definir roles entre los actores que estarán facultados para la manipulación de la información del Data Center, para así poder facultar quienes tienen dentro de sus facultades atributos para el manejo de la información ya sea para Copiar, publicar, reproducir, destruir, interceptar, modificar etc. antes de otorgar acceso a la información.	Las estaciones de trabajo (Computadores, Servidores y Dispositivos Digitales) que sean herramienta de interacción con la configuración y/o almacenamiento del Data Center deben permanecer siempre bloqueadas y bajo protección cifrada siempre que no se encuentre el funcionario a cargo de la estación de trabajo.
La persona natural o jurídica que se encuentre realizando actividades dentro de la red tecnológica de la administración departamental debe tener prohibido el acceso a la información resguardada en el Data Center y debe incluir dentro de las cláusulas contractuales un ítem que contenga este parámetro.	Realizar jornadas de sensibilización de la información en toda la entidad, para identificar y socializar con todos los miembros de la entidad la información Sensible y que debe ser resguardada en el Data Center.
Se debe estar en una constante revisión y actualización de los perfiles y roles que	El mantenimiento y aseo del Data Center debe estar documentado, elaborando un manual de

HUMANOS	FÍSICOS
permiten el acceso a la información de las personas vinculadas al Data Center con el fin de mantener al día y en tiempo real las responsabilidades competentes de cada quien.	acceso y zonas de limpieza e identificar los puntos eléctricos donde se puedan conectar instrumentos ajenos al Data Center para realizar dichas labores.
Se deben realizar actividades de retroalimentación y sensibilización en seguridad de la información entre los actores que intervienen en el Data Center donde se conozcan inquietudes, exposición de utilización de herramientas, soluciones y avances con respecto a las políticas de seguridad de la información.	El ingreso al Data Center debe ser única y exclusivamente electrónica, mediante sistemas biométricos preferiblemente o con la portación de una tarjeta inteligente que identifique quien entra y sale de las instalaciones del Data Center para evitar el ingreso de personas ajenas a esta dependencia.
Todo funcionario que tenga vínculo con el Data Center debe informar cualquier novedad que surja con respecto a las herramientas de seguridad y/o información resguardada para tratar de hacer una actualización con respecto a las herramientas de manejo de información.	La Dirección de Sistemas de información debe realizar las gestiones pertinentes para mantener al día las licencias y software necesarios para la seguridad de los Sistemas de Información, de la red tecnológica y toda su plataforma digital. Se debe inspeccionar el estado físico de los equipos que hacen parte del esquema del Data Center para verificar y garantizar su calidad, eficacia y eficiencia.

4.8. Recopilación de la información

Es el proceso de estudiar y determinar a manera de diagnóstico la información necesaria y los requisitos de los interesados para cumplir con los objetivos del proyecto

Estos aspectos están contemplados en la norma ISO 27001:2013 donde plantea los requisitos para establecer, implementar, operar, realizar seguimiento, auditoría, darle continuidad y mejorar continuamente un SGSI en el contexto de los riesgos que tienen relación al Data Center.

Dentro de la recopilación de la información necesaria para la búsqueda del cumplimiento de los requisitos de la norma, se estudió el Plan Estratégico de Tecnologías de la Información y las Comunicaciones PETIC que está en proceso de elaboración e implementación, documento en el cual se identifica el cumplimiento de requisitos al momento de entrar en cumplimiento el plan estratégico, determina puntos del contexto de la organización, liderazgo, Planificación entre otros.

Al igual que el MSPI o Modelo de Seguridad y Privacidad de la Información que fue determinado por La Resolución 00500 de 2021 el Ministerio de Tecnologías de la Información y las Comunicaciones la cual estableció los lineamientos y estándares para la estrategia de seguridad digital y determinó un modelo de Seguridad y Privacidad de la Información como habilitador de la política de Gobierno Digital, de este documento se toma principalmente la documentación (planillas y formularios) que sirven de apoyo en el control de los procesos y operaciones llevadas a cabo en el Data Center de la Gobernación de Santander. Los pasos definidos en este modelo están detallados en el Apéndice A *Ampliación De La Metodología De*

Base Preliminar Del Plan De Implementación De La Norma ISO- 27001: 2013 como una lista de apoyo a la implementación de la norma que funciona como guía de este proceso.

Igualmente se estudió los documentos, análisis de riesgos de la infraestructura tecnológica y el Plan de contingencia que están en proceso de elaboración e implementación, que igualmente al momento de entrar la implementación de ellos, se identifica el cumplimiento de requisitos planteados por la norma.

En el cumplimiento de los objetivos del proyecto, se hace un levantamiento de información con respecto a la Infraestructura tecnológica del Data Center, y de los procesos y/o sistemas de información que tienen relación y funcionamiento en el Data Center.

4.9. Estudio preliminar

Cumpliendo con el objetivo de elaborar un Estudio Preliminar del Plan de Implementación de la Norma ISO 27001 Para el Data Center de la Dirección de Sistemas de Información, es indispensable la entrega de un documento que detalle y relacione el estudio realizado, cumpliendo con los objetivos planteados en el Plan del Proyecto de Grado.

En el documento queda planteado los aspectos fundamentales a tener en cuenta con respecto al cumplimiento de los requisitos que rige la norma ISO 27001:2013, para lograr con ello avanzar hacia la certificación que a su vez traerá beneficios en los procesos de manejo de información y administración de datos del Data Center, obtener distinción y cumplimientos legales al igual que establecer una cultura de seguridad de la información.

Tabla 17

Cronograma y Estudio Planificar

PLANIFICAR

	Requisitos	Fecha	Se cumplió con:
4. Contexto de la Organización	4.1 Conocimiento de la organización y de su contexto	13 de febrero de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	4.2 Comprensión de las necesidades y expectativas de las partes interesadas	16 de febrero de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	4.3 Determinación del Alcance del SGSI	17 de febrero de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	4.4 Sistema de Gestión de la Seguridad de la Información	18 de febrero de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
5. Liderazgo	5.1 Liderazgo y	24 de febrero	Elaboración de

PLANIFICAR

Requisitos		Fecha	Se cumplió con:
	Compromiso	de 2021	diagnóstico y plantear cumplimiento de requisitos
	5.2 Política	25 de febrero de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	5.3 Roles, Responsabilidades y Autoridades en la Organización	26 de febrero de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
6. Planificación	6.1 Acciones para tratar Riesgos y Oportunidades	2 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	6.2 Objetivos de Seguridad de la Información y planes para lograrlos	3 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos

PLANIFICAR

Requisitos		Fecha	Se cumplió con:
7. Soporte	7.1 Recursos	4 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	7.2 Competencia	5 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	7.3 Toma de Conciencia	9 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	7.4 Comunicación	10 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	7.5 Información Documentada	11 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos

Tabla 18

Cronograma y Estudio Hacer

HACER

	Requisitos	Fecha	Se cumplió con:
8. Operación	8.1 Planificación y Control Operacional	12 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	8.2 Valoración de Riesgos de la Seguridad de la Información	16 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	8.3 Tratamiento de Riesgos de la Seguridad de la Información	17 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos

Tabla 19

Cronograma y Estudio Verificar

VERIFICAR

Requisitos		Fecha	Se cumplió con:
9. Evaluación del Desempeño	9.1 Seguimiento, medición, análisis y evaluación	18 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	9.2 Auditoría Interna	19 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	9.3 Revisión por la Dirección	23 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos

Tabla 20

Cronograma y Estudio Actuar

ACTUAR

	Requisitos	Fecha	Se cumplió con:
10. Mejora	10.1 No conformidades y Acciones correctivas	24 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos
	10.2 Mejora Continua	25 de marzo de 2021	Elaboración de diagnóstico y plantear cumplimiento de requisitos

Para plantear el cumplimiento de los requisitos del ciclo PHVA, al momento de realizar el diagnóstico se tuvo en cuenta los objetivos que cumplirán la implementación del PETIC, de Análisis de Riesgos y Plan de Contingencia. Como soporte del diagnóstico de lo que se tiene y así poder sugerir que se debe hacer. El estudio y realización de este diagnóstico se hizo bajo el esquema de juntas y reuniones individuales entre el autor del proyecto, el Director de Sistemas de Información y el funcionario contratista designado a la administración del Data Center, el resultado de lo obtenido quedó plasmado en la documentación que se entregó al Director de Sistemas de Información.

De esta manera se contribuye complementar los documentos que se encuentran en proceso de elaboración e implementación de tal modo que se tenga en cuenta lo necesario para el cumplimiento de los requisitos de la norma ISO 27001 y así, no entrar en el planteamiento de objetivos innecesarios que no tengan relevancia con la seguridad de la información que es la naturaleza de la creación del Data Center.

La implementación del ciclo PHVA promueve que la práctica de la gestión de seguridad de la información vaya en favor de las oportunidades para que la organización optimice el desempeño de los procesos.

4.10. Cronograma

En la siguiente tabla se detallan las acciones básicas que deben ser llevadas a cabo en una implementación de la Norma ISO – 27001:2013.

Tabla 21

Cronograma del desarrollo del proyecto

Actividad	**Fecha**		**Estado**
	Desde	**Hasta**	
Consulta Bibliográfica, lectura y comprensión de la norma NTC-ISO-IEC 27001 2013-12-11 Norma Técnica Colombiana. (ICONTEC, 2013)	5 de enero de 2021	30 de enero de 2021	Cumplido

Actividad	Fecha		Estado
	Desde	Hasta	
Exposición ISO 27001 en Clase de Auditoria de Sistemas como objetivo del dominio adecuado de la norma.	21 de enero de 2015	21 de enero de 2015	Cumplido
Inventario de infraestructura tecnológica del Data Center.	2 de febrero de 2021	6 de febrero de 2021	Cumplido
Análisis de procesos e Inventario de aplicaciones (Sistemas de Información, Sistemas Operativos, etc.).	9 de febrero de 2021	12 de febrero de 2021	Cumplido
Elaboración de diagnóstico y proponer metodología al cumplimiento de los requisitos del ciclo PHVA: Planificar.	13 de febrero de 2021	11 de marzo de 2021	Cumplido
Elaboración de diagnóstico y proponer metodología al cumplimiento de los requisitos del ciclo PHVA: Hacer.	12 de marzo de 2021	17 de marzo de 2021	Cumplido
Elaboración de diagnóstico y proponer metodología al cumplimiento de los requisitos del ciclo PHVA: Verificar.	18 de marzo de 2021	23 de marzo de 2021	Cumplido
Elaboración de diagnóstico y proponer metodología al cumplimiento de los requisitos del ciclo PHVA: Actuar.	24 de marzo de 2021	25 de marzo de 2021	Cumplido

Actividad	Fecha		Estado
	Desde	Hasta	
Elaboración del documento que contiene el Inventario de la Infraestructura Tecnológica, Inventario de Procesos y Sistemas de Información y la propuesta de metodología como entregable a la Dirección de Sistemas de Información.	27 de marzo de 2021	5 de abril de 2021	Cumplido

4.11. Relación de la propuesta con las regulaciones actuales

En el desarrollo de este trabajo de investigación fueron tenidas en cuenta varias reglamentaciones que en la necesidad de ser cumplidas a cabalidad motivaron la realización de este proyecto. De manera general se puede asegurar que el objetivo de las TIC en el sector de la administración pública hace referencia especialmente al uso de estas como herramientas que permiten un mejor desarrollo de las actividades de las entidades públicas y por consiguiente, posibilitan un mejor servicio a la comunidad. En la Ley 1341 de 2009 que define los principios que orientan el uso de las TIC se determina que El Estado es el responsable de generar investigación, promoción y desarrollo de dichas tecnologías para ser aprovechadas al máximo. En el caso de la Gobernación de Santander con la implementación de la Norma ISO – 27001: 2013 se comenzará de manera gradual una actualización y un fomento de mejores prácticas que mejorarán sustancialmente el manejo del Data Center de esta entidad, aprovechando los servicios que este provee y protegiendo la información que allí es procesada.

Por su parte la implementación de la Norma ISO – 27001: 2013 como bien se ha hecho énfasis tiene como propósito salvaguardar la información, al igual que la Ley 1581 de 2012 la cual su principal propósito es el de proteger los datos personales de todos aquellos que hagan parte de registros, archivos o bases de datos. Para elaborar esta propuesta de implementación de la norma ISO – 27001: 2013 en el Data Center de la Gobernación de Santander fue necesario identificar riesgos que justamente están relacionados a la pérdida o mal manejo de la información, por lo que la estrategia de la norma es ideal para que sean mitigados dichos riesgos en los procesos informáticos llevados a cabo en el Data Center. Es así como también el Data Center de la Gobernación de Santander estaría acoplado a la norma más actual de protección de información llamada Política de Gobierno Digital que estandarizó un modelo de seguridad y privacidad de datos.

Comenzar con la implementación de la Norma ISO – 27001: 2013 también traduce en poner a la entidad al día con los requerimientos, objetivos y componentes de la Política Digital expedida por el Decreto 1078 de 2015 y con el Plan de Seguridad y Privacidad de la Información. Esto principalmente quiere decir que, la actualización y las buenas prácticas provenientes de la Norma ISO – 27001: 2013 generarán una credibilidad y un valor público en la entidad y por consiguiente, mejorará la relación de la entidad con la comunidad a la cual le presta el servicio. Un ejemplo de ello sería el caso del cumplimiento de las normativas anti-trámites en las cuales se propone especialmente que las TIC sean usadas a favor de procesos ágiles que pueden mejorar continuamente desde el contexto IT.

5. Resultados

El primer resultado de este proyecto de investigación fue la promoción de una cultura basada en las mejores prácticas en dependencias que resultan elementos críticos de una organización tal como lo es el Data Center de la Gobernación de Santander. Esta promoción se reflejó en la motivación experimentada desde Dirección de Sistemas de Información y en el entendimiento de la necesidad e importancia de la certificación de la norma ISO-27001:2013 y el cumplimiento de normativas y políticas vigentes relacionadas a la optimización de los recursos TIC en las entidades gubernamentales. Dicha motivación por parte del equipo de trabajo permitió que la dependencia brindara las herramientas necesarias para el desarrollo de este proyecto. Adicionalmente se considera que el compromiso por parte de los directivos y el equipo de trabajo conduce a un proyecto exitoso, por consiguiente, se considera un logro significativo en el desarrollo de este estudio.

La formulación y cumplimiento de los objetivos de este proyecto fueron soportadas por las bases teóricas del proyecto y actividades que se basaron en previos conocimientos adquiridos en la formación del autor en Ingeniería de Sistemas. Dicha base hizo su contribución a través de aportes como la identificación de la infraestructura tecnológica y manejo de la información, los requisitos a cumplir propuestos por la Norma ISO – 27001:2013 y la definición de la documentación y controles que deben ser ejecutados para el buen funcionamiento del Data Center apegado a las directrices suministradas por el SGSI.

Este estudio preliminar provee de herramientas generales para comenzar en el proceso de implementación de la Norma ISO – 27001:2013 lo que implica una serie de productos elaborados que están desglosados en detalle en los Apéndices asociados. En primer lugar fue producido un diagnóstico en el cual fue relevada la infraestructura tecnológica del Data Center incluyendo servidores físicos, servidores virtuales, sistemas operativos, planta eléctrica y equipos de conectividad. A su vez fue determinado un análisis de riesgos basado en la matriz de riesgos elaborada por la dependencia de sistemas de la Gobernación de Santander en la cual fue posible identificar los procesos, información e infraestructura que suponen puntos críticos que en un futuro podrían representar problemas de pérdida o mal manejo de la información, funcionamiento operacional lento y por consiguiente, insatisfacción de los clientes que en este caso al ser una entidad gubernamental haría referencia a la comunidad del departamento de Santander. Esto incurre directamente en el incumplimiento de las normas vigentes que apoyan la política de Gobierno Digital establecidas por el MINTIC (Apéndice C).

Para contrarrestar dichos riesgos se elaboró una metodología que gira fundamentalmente en el ciclo PHVA, la cual inicialmente fue propuesta con el fin de lograr el cumplimiento de todos y cada uno de los requisitos de la Norma ISO – 27001:2013, la cual en una futura implementación será la contribución clave en el proceso acreditación del Data Center de la Gobernación de Santander en el cumplimiento de los requerimientos de seguridad de la información, el cual sería la meta más ambiciosa de este inicio del proyecto (Apéndice A).

Por último, fueron suministrados con base en el Modelo de Seguridad y Privacidad de la Información aquellos controles que contribuyen al monitoreo de la eficacia y productividad de la

implementación del SGSI desarrollada en un futuro. La relación de estos controles también está fundamentada en el ciclo de PHVA que es la base de la teoría de la evaluación de procesos con mejora continua, esto quiere decir que dichos controles y monitoreo son la base para encontrar oportunidades para mejorar constantemente, lo que permite que el Data Center de la Gobernación de Santander se optimice gradualmente según las necesidades de la dependencia a través del tiempo (Apéndice B).

6. Recomendaciones

Se sugiere a la Secretaría de las TIC de la Gobernación de Santander en aras de conformar un equipo adecuado y de calidad para la administración y funcionamiento del Data Center y política de seguridad de la información, vincular en su planta de personal a cuatro funcionarios con los siguientes perfiles:

Tabla 22

Recomendación perfiles a vincular a la planta de personal

Título	Experiencia	Estimación Salarial	Cargo
1 Ingeniero de Sistemas.	Mínima de 1 año	$ 4.700.000	Ingeniero designado al seguimiento del SGSI.
1 ingeniero de Sistemas, Experiencia en Infraestructura TIC o Telemática	Mínima de 2 año	$ 4.700.000	Ingeniero Administrador del Data Center.
1 Ingeniero de Sistemas, Experiencia en Auditoria o afines.	Mínima de 1 año en SGC Certificado por ICONTEC.	$ 4.700.000	Ingeniero designado a la Auditoria Interna del SGSI.
1 Tecnólogo en	Mínima de 1	$ 3.200.000	Tecnólogo de apoyo a la

Título	Experiencia	Estimación Salarial	Cargo
Sistemas, Electrónica o Telecomunicaciones.	año		administración del Data Center.

Al momento de iniciar el proceso de implementación de la norma, se recomienda conformar el comité de seguridad de la información, que lleve a cabo el seguimiento y evaluación al SGSI, estudiar los hallazgos y no conformidades, hacer correcciones y mejoras a implementar, estudio de auditorías y toda necesidad pertinente con el cumplimiento de la norma.

Buscar la continuidad del estudio con la gestión de un proyecto de investigación cuyo propósito sea entregar el de producir un plan completo para llevar a cabo la metodología y los controles de monitoreo propuestos por este estudio preliminar. Para ello será necesario gestionar con la Universidad Industrial de Santander un estudiante de Ingeniería de Sistemas que su proyecto de grado sea la planificación de la implementación del SGSI, de esta manera será posible proveer de un producto más cercano a la acreditación del Data Center de la Gobernación de Santander en la Norma ISO-27001:2013.

Se sugiere adecuar coherentemente con la norma y los lineamientos del MINTIC en la resolución 00500 de 2021, los documentos que actualmente adelanta la secretaría de las TIC de Santander, como el Plan Estratégico de las Tecnologías de la Información y las Comunicaciones – PETIC, Análisis de Riesgos de la Infraestructura Tecnológica y El Plan de Contingencia, en

concordancia con las necesidades planteadas y que en principio ayudan a cumplir requisitos establecidos en la norma.

Se recomienda que la Dirección de Sistemas de Información debe desarrollar y mantener una bitácora para conservar información documentada acerca del proceso de valoración de riesgos de la seguridad de la información, proceso de tratamiento de riesgos de la seguridad de la información, de los objetivos de la seguridad de la información, la información apropiada como evidencia de los resultados de monitoreo y de la medición, evidencias de los resultados de revisiones por la dirección. (Sugerencias tomadas de la norma ISO 27001:2013).

Se sugiere siguiendo con los lineamientos de recomendaciones de la Norma ISO – 27001: 2013 que sea documentada la información que tenga un origen externo y sea necesaria para la planificación y operación del SGSI. Es decir que dicha información se debe identificar y controlar, según sea adecuado. Igualmente se recomienda teniendo en cuenta nuevamente la norma que la organización en este caso la Gobernación de Santander lleve a cabo auditorías internas apegadas a un cronograma, con el fin de proporcionar información acerca del funcionamiento del SGSI con el fin de corroborar su funcionamiento eficaz o la necesidad de implementar mejoras en él. Finalmente, se propone que los procesos, información e infraestructura luego de ser revisados deben incluir las decisiones relacionadas con las oportunidades de mejora continua y cualquier necesidad de cambio en el SGSI.

7. Conclusiones

Con el diagnóstico y la identificación de los procesos, información y procesos ejecutados en el Data Center de la Gobernación de Santander fue posible determinar que la pirámide documental de un SGSI no tiene cumplimiento y necesita de una intervención apegada a la normativa vigente que está relacionada a políticas de mejoramiento de los servicios en función de políticas como Gobierno Digital las cuales tienen base en directrices planteadas como el Modelo de Seguridad y Privacidad de la Información apegado a la Norma ISO – 27001:2013. Los riesgos que necesitan de dicha intervención hacen alusión al posible mal manejo de la información e infraestructura que se encuentra obsoleta, los cuales pueden ser causantes de pérdida de los datos, acceso y uso erróneo de los mismos o ralentización de los procesos y servicios prestados por esta dependencia.

Los riesgos identificados pueden ser contrarrestados a través de la implementación de una metodología basada en el ciclo de Deming o ciclo PHVA (planificar, hacer, verificar y actuar) la cual a su vez está compuesta de una serie de acciones que se basan en las buenas prácticas de un SGSI fundamentado en la Norma ISO – 27001:2013. Dichas acciones incluyen los siguientes lineamientos: lograr un compromiso administrativo, establecer y definir el SGSI como política pública, definir un alcance, analizar riesgos, elaborar la declaración de aplicabilidad, definir el plan de riesgo, evaluar la medición de controles, implementar la declaración de aplicabilidad, capacitar y socializar los involucrados en el manejo del data center, poner en marcha el SGSI y supervisarlo, realizar una auditoría interna, designar el rol de la dirección y activar promoción y prevención de las buenas prácticas en el data center.

Fue posible determinar que la metodología propuesta y los controles que posibilitan una mejora sustancial en el manejo y los servicios prestados por el Data Center no dependen exclusivamente en la creación de software, diseño de base de datos o el análisis de algoritmos, entre otros, sino se basan en componentes que están mayormente relacionados a las buenas prácticas de manejo de la información y la reestructuración de la infraestructura tecnológica del Data Center. Dicha mejora e implementación de la Norma ISO – 27001:2013 basada en una identificación de riesgos corrobora la importancia y la necesidad de implementar un SGSI en la Gobernación de Santander, que se reflejará en el funcionamiento de una dependencia productiva y óptima que posiciona a la entidad gubernamental como una organización competitiva y eficaz en la prestación de servicios a la comunidad. Dicha optimización finalmente, le permite cumplir con lo requerido en las políticas de potenciación de las TIC en las instituciones públicas.

El compromiso decidido y claro de los miembros de una organización como lo es la Gobernación de Santander, hacen que un SGSI obtenga resultados más confiables, reduce los niveles de riesgo y contribuye en el cumplimiento de las políticas de seguridad que se implementen. Para ello fue necesario elaborar previamente a la planificación de una implementación de la Norma ISO – 27001:2013 este estudio preliminar esboza de manera general los puntos críticos a mejorar y tiene como utilidad principal funcionar como herramienta adecuada en la búsqueda del cumplimiento de los requisitos de la norma y lograr cumplir a cabalidad sus propósitos en seguridad de la información.

Referencias Bibliográficas

Alexander, A. G. (2007). *Diseño de un Sistema de Gestión de Seguridad de Información: Óptica ISO 27001:2005* (Primera Edición ed.). Bogotá D.C.: Alfaomega Colombiana S.A.

Colombia, P. d. (s.f.). *Presidencia de la República*. Recuperado el 5 de 04 de 2015, de http://wsp.presidencia.gov.co/Normativa/DAPRE/Paginas/GobiernoEnLinea.aspx

Departamento Administrativo Nacional de Estadística - DANE. (26 de Marzo de 2014). *Pagina Web del DANE*. Recuperado el 26 de Marzo de 2014, de http://www.dane.gov.co/files/inf_geo/4Ge_ConceptosBasicos.pdf

Diaz, S. M. (2012). *Gestion y creación del plan de ejecución del proceso para el proyecto de certificación con la norma ISO 27001:2005 en la FCV.* Bucaramanga: Universidad Industrial de Santander.

EPPS Services Ltd. para negocios electrónicos y consultoría comercial. (s.f.). *27001 Academy*. (EPPS Services Ltd) Recuperado el 18 de Noviembre de 2014, de http://www.iso27001standard.com/es/que-es-la-norma-iso-27001

Excellence, I. T. (s.f.). *ISO Tools Excellence*. (ISO Tools) Recuperado el 06 de 11 de 2014, de http://www.isotools.org/pdfs/Monografico-ISO-27001-ISOTools.pdf

Free Website Template By: PriteshGupta.com. (2012). *El portal de ISO 27001 en Español*. Recuperado el 29 de Marzo de 2014, de http://www.iso27000.es/sgsi.html#section2a

Gobernación de Santander. (2012). *Página Web de la Gobernación de Santander*. Recuperado el 30 de Marzo de 2014, de http://www.santander.gov.co/

ICONTEC. (2013). *Norma Técnica Colombiana NTC-ISO-IEC 27001*. Bogotá: ICONTEC.

Ministerio de Tecnologías de la Información y las Comunicaciones. (12 de Diciembre de 2014). Decreto 2573 de 2014. Bogotá D.C., Colombia.

Santander, S. d. (2015). *Plan Estratégico de las Tecnologías de la Información y las Comunicaciones - PETIC 2012 - 2015.* Bucaramanga: Gobernación de Santander.

Santander, S. d. (2015). *Plan Estratégico de las Tecnologías de la Información y las Comunicaciones - PETIC 2012 - 2015.* Bucaramanga.

SETIC, S. d. (2015). *Setic Santander*. (Gobernación de Santander) Recuperado el 10 de 04 de 2015, de http://seticsantander.gov.co/index.php

ISO. (2015). The ISO Survey of Management System Standard Certifications (2006-2015). ISO/IEC 27001 - Information Technology - Security Techniques - Information Security Management Systems – Requirements. ISO.