República de Colombia

Gobernación de Santander

PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

PLAN DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN 2019-2022

DIDIER ALBERTO TAVERA AMADO
Gobernador de Santander

JULIO CÉSAR GÓMEZ SUÁREZ
Secretario de las TIC

Bucaramanga, Septiembre de 2019

Título:	Plan de Seguridad y Privacidad de la Información 2019-2022				
Fecha Elaboración	Septiembre de 2019				
Formato	Documento Texto		Lenguaje:		Español
Dependencia:	Secretaría de Las Tecnologías de la Información y Comunicación				
Código:	AP-TIC-PL-02	Versión:	0	Estado:	Terminado
Autor (es):	Secretaría TIC de Santander				
Otros Colaboradores:	Jhon Jairo Jiménez Álvarez: c.jhjimenez@santander.gov.co Ingeniero de Sistemas - M.Sc. en Tecnologías de la Información y las Comunicaciones Yoham Efrén Rojas González: c.yrojas@santander.gov.co Ingeniero Electrónico – Especialista en Telecomunicaciones Juan Sebastián Rodríguez Mejía: c.jurodriguez@santander.gov.co Ingeniero Industrial				
Revisó	Ing., Julio Cesar Gómez Suárez Secretario de las TIC				
Aprobó:	Comité Institucional de Gestión y Desempeño				
Ubicación:	Secretaría de Tecnologías de la Información y la Comunicación SETIC – Calle 48 N° 27ª – 48 Santander - Bucaramanga Correo: setic@santander.gov.co Facebook: Setic Santander Twitter: @TICSantander				

Tabla de Contenido

INTRODUCCIÓN

El uso de las tecnologías de la información y las comunicaciones, facilitan la creación de valor en las instituciones, pero es necesaria una adecuada selección e implementación de estas tecnologías, alineadas con la estrategia y la misión para tener éxito.

Desde la Gobernación de Santander, se conciben las tecnologías de la información y las comunicaciones como instrumentos fundamentales para lograr el cumplimiento de los planes y objetivos institucionales; resultado de esta intención de la alta dirección, es la inclusión de los procesos asociados a la gestión de tecnologías de información dentro del proceso de direccionamiento estratégico.

Las Tecnologías de la Información y las Comunicaciones-TIC hacen parte de la planificación estratégica gubernamental/administrativa que permite gestionar y gobernar de manera conjunta y alineada con la estrategia de todo el Departamento de Santander y su Plan de Desarrollo Departamental-PDD “Santander Nos Une” 2016-2019.

La Secretaría de las TIC lidera la planeación estratégica de las tecnologías de la información (TI) acorde con el modelo de negocio (Misión-Visión) del Departamento de Santander, que le permita alcanzar las Metas apuntando a la competitividad y la eficacia de la administración.

Además, desde el área de TI se coordina con la alta dirección (Despacho del Gobernador y Asesores), acciones con el objeto de movilizar los recursos de la forma más eficiente en respuesta a requerimientos estratégicos, de evaluación, misionales y de apoyo definidos en el mapa de procesos de la Gobernación de Santander, de esta forma que se puedan gestionar y controlar las TI.

Tener un buen Gobierno de TI, constituye una parte esencial de la gobernanza del Departamento de Santander. Su estructura organizativa y directiva se hace necesaria para asegurar que las Tecnologías de la Información sean soporte para el desarrollo de los Objetivos, Programas y Metas.

El presente documento contiene el plan de seguridad y privacidad de la información para el establecimiento del Sistema de Gestión de Seguridad y Privacidad de la Información de la **GOBERNACIÓN DE SANTANDER**, el cual tomará como referencia el Modelo de Seguridad y Privacidad de la estrategia de Gobierno en Línea y la norma ISO 27001:2013, los cuales proporcionan un marco metodológico basado en buenas prácticas para llevar a cabo la implementación de un modelo de Gestión de Seguridad Digital y Privacidad de la Información en cualquier tipo de organización, lo cual, permite garantizar su efectiva implementación y asegurar su debida permanecía y evolución en el tiempo.

2. OBJETIVOS

2.1. Objetivo General

Establecer un Plan de Privacidad y Seguridad de la Información que apoye la implementación del manual de Política de Seguridad Digital y Privacidad de la Gobernación de Santander, acorde a los requerimientos del modelo de seguridad y privacidad de la información (MSPI) de la Política de Gobierno Digital, los requerimientos del negocio y en cumplimiento de las disposiciones legales vigentes.

2.2. Objetivos Específicos

1. Definir las etapas del plan de seguridad de privacidad de la información de la Gobernación de Santander en el primer semestre del 2019, a partir de autodiagnóstico de la entidad, con el fin de establecer la estrategia de seguridad digital.
2. Implementar controles de seguridad y privacidad de la información en la vigencia 2019-2022 mediante un cronograma que defina los responsables y fechas estimadas de cumplimiento.
3. Evaluar el nivel de implementación de la política de seguridad y privacidad de la información en la Gobernación de Santander en la vigencia 2019-2022, cumpliendo en un 100% con la ejecución de actividades e implementación de los controles de seguridad de la información.

3. METODOLOGÍA PARA LA IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD DIGITAL

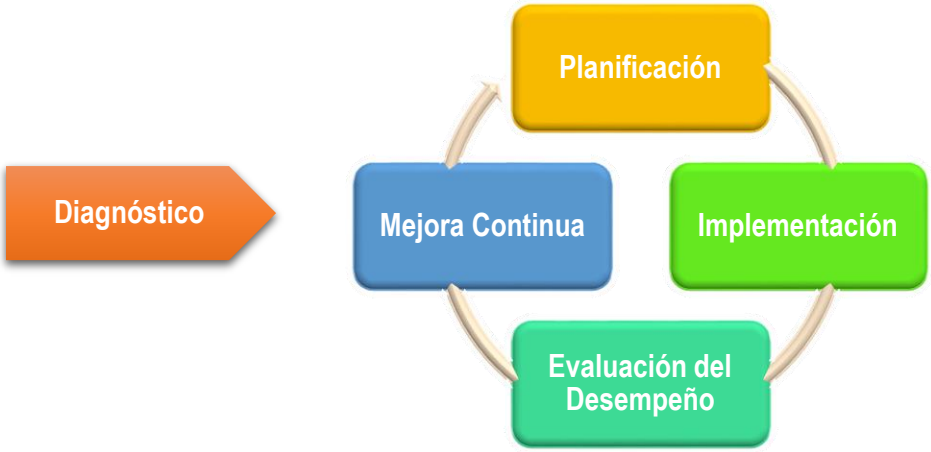
3.1. Ciclo de Operación

En el presente capitulo se explica el ciclo de operación que la Gobernación de Santander implementará para el Modelo de Seguridad y Privacidad de la Información de la Política de Seguridad Digital y Privacidad de la Información.

La metodología contempla, en su ciclo de operación cinco (5) etapas, las cuales permiten que la Gobernación de Santander pueda gestionar adecuadamente la seguridad y privacidad de sus activos de información[1]

Esquema 1. Ciclo de Operación del Modelo de Seguridad Digital y Privacidad de la Información

[1] https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf



Diagnóstico: Permite identificar el estado actual de la Gobernación de Santander con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información.

Planificación (Planear): En esta etapa se establecen los objetivos a alcanzar y las actividades del proceso a controlar mediante la implementación de políticas, así como los indicadores de medición para controlar y cuantificar los objetivos.

Implementación (Hacer): En esta etapa se ejecuta el plan establecido que consiste en realizar las acciones necesarias para lograr el cumplimiento de la política de seguridad digital y privacidad de la información.

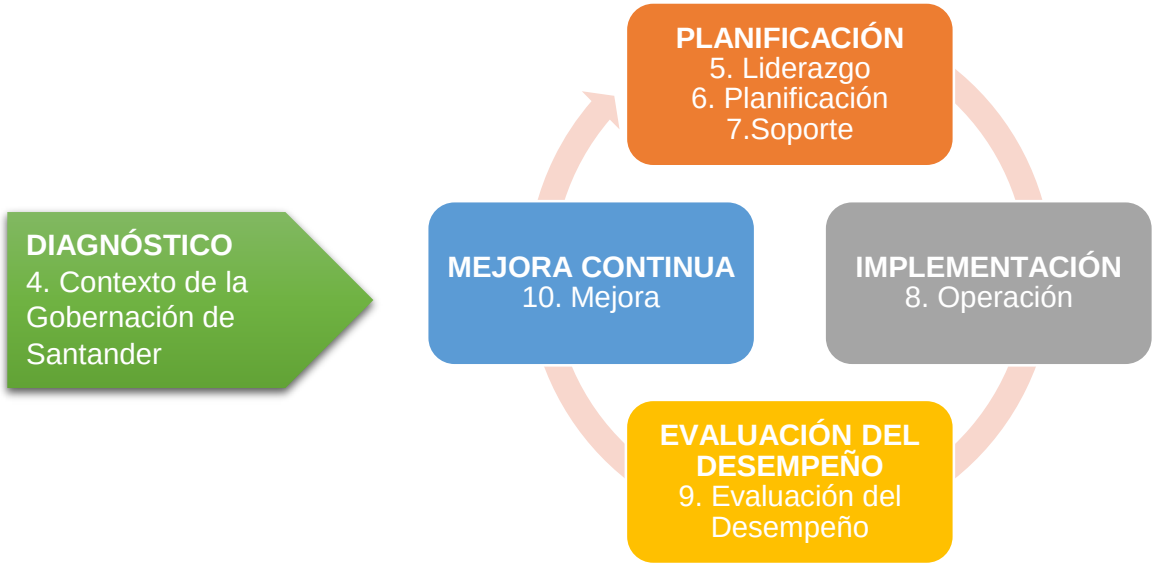
Evaluación de desempeño (Verificar): Una vez implementada la política de seguridad digital y privacidad de la información, se establece un periodo de prueba para verificar el correcto funcionamiento de las acciones ejecutadas y su estado de cumplimiento.

Fase Mejora Continua (Actuar): Se analizan los resultados de las políticas implementadas y el nivel de incumplimiento de los objetivos definidos, con el fin de analizar las cusas de las desviaciones y generar los respectivos planes de mejora.

3.2. ALINEACION NORMA ISO 27001:2013 VS CICLO DE OPERACION

Debido a que la norma ISO 27001:2013 no determina un modelo de mejora continua (PHVA) como requisito para estructurar los procesos del Sistema de Gestión de Seguridad de la Información, la nueva estructura de esta versión se puede alinear con el ciclo de mejora continua de los modelos de gestión de la siguiente forma:

Esquema 2. Alineación Norma ISO 27001:2013 con el Ciclo de Operación del Modelo de Seguridad y Privacidad de la Información



Contextualización de las fases según la norma ISO 27001:2013:

- **Diagnóstico:** En el capítulo 4 **"Contexto de la organización"** de la norma, se determina la necesidad de realizar un análisis en el entorno externo e interno de la Gobernación de Santander y de su contexto, con el propósito de incluir las necesidades y expectativas de las partes interesadas de la Entidad en el alcance del SGSI.

- **Planeación**: En el capítulo 5 **"Liderazgo"**, se establece las responsabilidades y compromisos de la Alta Dirección respecto al Sistema de Gestión de Seguridad de la Información (SGSI) y entre otros aspectos, la necesidad de que la Alta Dirección establezca una política de seguridad de la información adecuada al propósito de la Gobernación de Santander y asegure la asignación de los recursos para el SGSI y que las responsabilidades y roles pertinentes a la seguridad de la información se asignen y comuniquen.

  En el capítulo 6 **"Planeación"**, se establece los requerimientos para la valoración y tratamiento de riesgos de seguridad y para la definición de objetivos viables de seguridad de la información y planes específicos para su cumplimiento.

  Finalmente, en el capítulo 7 **"Soporte"** se establecen los recursos necesarios para el establecimiento, implementación y mejora continua del SGSI.

- **Implementación**: En el capítulo 8 **"Operación"**, se indica que la Gobernación de Santander debe planificar, implementar y controlar los procesos necesarios para cumplir los objetivos y requisitos de seguridad y llevar a cabo la valoración y tratamiento de los riesgos de la seguridad de la información.

- **Evaluación del Desempeño:** En el capítulo 9 **"Evaluación del desempeño"**, se define los requerimientos para evaluar periódicamente el desempeño de la seguridad de la información y eficacia del SGSI.

- **Mejora Continua:** En el capítulo 10 **"Mejora"**, se establece para el proceso de mejora del SGSI, que a partir de las no-conformidades que ocurran, la Gobernación de Santander debe establecer las acciones para solucionarlas y evaluar la necesidad de acciones para eliminar las causas de la no conformidad con el objetivo de que no se repitan.

3.3. Etapa I: Diagnóstico

Tabla 1. Descripción del Diagnóstico de MSPI

Objetivo	Identificar el estado de la Gobernación de Santander con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Gobierno nacional.

Metas	Actividades / Instrumentos / Resultados
Determinar el **estado actual** de la gestión de seguridad digital y privacidad de la información al interior de la Gobernación de Santander.	**Diagnostico** nivel de cumplimiento de la Gobernación de Santander frente a los objetivos de control y controles establecidos en el **Anexo A** de la norma ISO 27001:2013. **Valoración** estado actual de la gestión de seguridad de la Gobernación de Santander con base en el **Instrumento de Evaluación MSPI de MINTIC**.
Identificar el **nivel de madurez** de seguridad digital y privacidad de la información.	Elaboración del documento **Nivel de Madurez** de seguridad y privacidad de la información, teniendo en cuenta las actividades anteriores de diagnóstico y contemplando lo propuesto en la guía "Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital" del Min. TIC.

Para la recolección de la información, en esta fase se utilizarán mecanismos como:

- Diligenciamiento de cuestionarios con el objetivo de determinar el nivel de cumplimiento de la Gobernación de Santander con relación a los dominios de la norma ISO/IEC 27001:2013.

- Documentación existente en el Sistema de Gestión Integral de la Gobernación de Santander relacionada con la información de las partes interesadas de la entidad y los roles y funciones asociados a la seguridad de la información.

- Fuentes externas, como las guías de autoevaluación, encuesta y estratificación dispuestas por la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones.

3.4. Etapa II: Planificación

Esquema 3. Etapa de planificación del Modelo de seguridad digital y privacidad de la información

Tabla 2. Descripción de la Planificación del MSPI

Objetivo	Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad digital y privacidad de la información, en procura de los resultados que permitan dar cumplimiento a la Política de Seguridad Digital y Privacidad de la Información.

Metas	Actividades / Instrumentos / Resultados
Realizar un análisis de contexto y factores externos e internos de la Gobernación de Santander en torno a la seguridad de la información.	**Realizar** un **Análisis de Contexto** de la Gobernación de Santander entorno a la seguridad de la información teniendo en cuenta el capítulo 4. CONTEXTO DE LA ORGANIZACIÓN de la norma ISO 27001:2013, con el fin de poder determinar las cuestiones externas e internas de la Entidad que son pertinentes para la implementación de la política de seguridad digital y privacidad de la información y la Política de administración del Riesgo en lo concerniente a la seguridad y privacidad de la información.
Definir Roles, Responsables y Funciones de seguridad y privacidad de la información	**Definir los roles y responsabilidades** para la implementación, administración, operación y gestión de la seguridad digital y privacidad de la información e incluirlos en el sistema integrado de calidad de la Gobernación de Santander. **Definir** en la **estructura organizacional** de la Gobernación de Santander la dirección y/o grupo a los que se le asignará los roles y responsabilidades pertinentes a la seguridad de la información. **Crear y/o Nombrar el Oficial de Seguridad Digital** como responsable de la política de seguridad digital y privacidad de la información.
Definir la metodología de riesgos de seguridad de la información	**Definir la Metodología de Valoración de Riesgos de Seguridad Digital**. Integrar la metodología definida con la metodología de riegos gestión y riesgos de corrupción de la Gobernación de Santander.
Elaborar las políticas de seguridad digital y privacidad de la información de la Gobernación de Santander y su plan de implementación.	**Elaborar** el **manual que incluya la política general y las Políticas de Seguridad Digital y Privacidad de la Información**, que corresponde a un documento que contiene las políticas y los lineamientos que se implementaran en la Gobernación de Santander con el objetivo de proteger la disponibilidad, integridad y confidencialidad de la información. Estas políticas deben ser aprobadas por la Alta Dirección y socializadas al interior de la Gobernación de Santander.
Elaborar documentación de operación (formatos de procesos, procedimientos y documentos debidamente definidos y establecidos) del sistema de gestión de seguridad de la información.	**Elaborar** los documentos de operación del sistema de seguridad de la información, cómo mínimo los siguientes: • Declaración de aplicabilidad. • Procedimiento y/o guía de identificación y clasificación de activos de información. • Procedimiento Continuidad del Negocio, Procedimientos operativos para gestión de TI.

	• Procedimiento para control de documentos (SGSI). • Procedimiento para auditoría interna (SGSI). • Procedimiento para medidas correctivas (SGSI). • Procedimiento para la gestión de eventos e incidentes de seguridad de la información. • Procedimiento para la gestión de vulnerabilidades de seguridad de la información.
Identificar y valorar activos de información	**Realizar la identificación y valoración de los activos de información** de la entidad de acuerdo con su nivel de criticidad y con el alcance del SGSI. **Documentar** el inventario de activos de información de la Gobernación de Santander.
Identificar, valorar y tratar los riesgos de seguridad de la información de la entidad	**Realizar la identificación y valoración de los riesgos transversales de seguridad de la información** y definir los respectivos planes de tratamiento. Realizar la valoración de riesgos de seguridad de la información de acuerdo con el alcance del SGSI. **Definir los planes de acción** que incluya los controles a implementar con el objetivo de mitigar los riesgos identificados en el proceso de valoración de riesgos. Para la selección de los controles, se tomará como base los objetivos de control y los controles establecidos en el **Anexo A** de la norma ISO/IEC 27001:2013
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información	**Elaborar** plan anual de capacitación y sensibilización anual de seguridad digital y privacidad de la información.
Establecer Plan de diagnóstico de IPv4 a IPv6.	**Realizar el diagnóstico** para la transición de la entidad de **IPv4 a IPv6**. **Documentar** el Plan de diagnóstico para la transición de IPv4 a IPv6.

3.5. Etapa III: Implementación

Esquema 4. Etapa de implementación del modelo de seguridad digital y privacidad de la información.

Tabla 3. *Descripción de la Etapa de Implementación del MSPI.*

Objetivo	Llevar a cabo la implementación de cada una de las actividades planificadas en la etapa II, para dar cumplimiento a la Política de Seguridad Digital y Privacidad de la Información

Metas	Actividades / Instrumentos / Resultados
Ejecutar el plan de tratamiento de riesgos	**Ejecutar el plan de tratamiento de los riesgos transversales** de seguridad de la información identificados en la etapa de planificación que fue presentado en el **Comité Institucional de Gestión y Desempeño.**
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.	**Ejecutar plan de transición** a IPv6 y elaborar informe de implementación.
Establecer indicadores de gestión de seguridad digital.	**Definir los indicadores** para medir la gestión del modelo de seguridad digital y **establecer** los mecanismos para su medición. Estos indicadores deben permitir verificar la eficacia y efectividad de los controles implementados para mitigar los riesgos de seguridad digital de la Gobernación de Santander.
Implementar procedimiento de gestión de eventos e incidentes de seguridad digital.	**Implementar** el procedimiento y los mecanismos para la **gestión de los eventos e incidentes de seguridad de la información.**
Implementar procedimiento de gestión de vulnerabilidades.	**Implementar** el procedimiento y los mecanismos para la gestión de vulnerabilidades seguridad de la información.
Ejecutar plan de capacitación y sensibilización de seguridad digital y privacidad de la información.	**Ejecutar** el plan anual de capacitación, socialización y sensibilización de seguridad digital y privacidad de la información.
Ejecutar pruebas anuales de vulnerabilidades e intrusión	**Ejecutar** el plan anual de pruebas vulnerabilidades e intrusión con el objetivo de **identificar el nivel de protección de los activos de información** de la Gobernación de Santander.

3.6. Fase IV: Evaluación y Desempeño

Esquema 5. Etapa de evaluación y desempeño del modelo de seguridad

Tabla 4. Descripción de la Etapa de Evaluación y Desempeño del MSPI.

Objetivo	Evaluar el desempeño y la eficacia del Modelo de Seguridad y Privacidad de la información, a través de instrumentos que permitan determinar la efectividad de la implementación de la Política de Seguridad Digital y Privacidad de la Información.

Metas	Actividades / Instrumentos / Resultados
Ejecución de auditorías de seguridad de la información.	Ejecución de auditorías del modelo de gestión de seguridad y de temas normativos y de cumplimiento de seguridad de la información aplicables a la Gobernación de Santander, de acuerdo con el plan de auditoria revisado y aprobado por la Alta Dirección. Las auditorías internas se deberán llevar a cabo para la revisión del Sistema de Gestión de Seguridad 'SGSI' de la Información implementado en la Gobernación de Santander, con la finalidad de verificar que los objetivos de control, controles, procesos y procedimientos del SGSI cumpla con los requisitos establecidos en la norma ISO 27001:2013 y los del MSPI.
Plan de seguimiento, evaluación y análisis de SGSI.	Elaboración documento con el plan de seguimiento, evaluación y análisis del SGSI revisado y aprobado por el Comité Institucional de Gestión y Desempeño.

3.7. Fase V: Mejora Continua

Esquema 6. Etapa de mejora continua del Modelo de Seguridad.

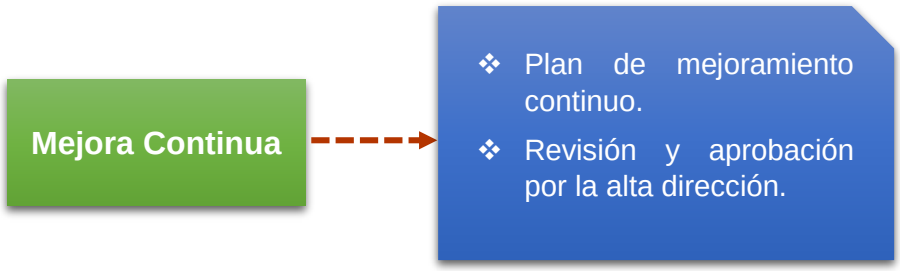


Tabla 5. Descripción de la Etapa de Mejora Continua.

Objetivo	Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad digital y privacidad de la información, que permita realizar el plan de implementación de las acciones de mejora identificadas para el SGSI

Metas	Actividades / Instrumentos / Resultados
Diseñar plan de mejoramiento de Seguridad Digital y Privacidad de la Información	Diseñar el plan de mejoramiento continuo de seguridad digital y privacidad de la información, que permita realizar el plan de implementación de las acciones de mejora identificadas para el Sistema de Gestión de Seguridad de la Información

3.8. Cronograma del Plan de Implementación de Seguridad Digital y Privacidad de la Información

Actividad	2019						2020												2021												2022												COSTO
	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
ETAPA I: DIAGNÓSTICO	Identificar el estado de la Gobernación de Santander con respecto a los requerimientos del Modelo de Seguridad y Privacidad de la Información (MSPI) del Gobierno nacional.																																									$30.000.000
Realizar el diagnostico nivel de cumplimiento de la Gobernación de Santander frente a los objetivos de control y controles establecidos en el **Anexo A** de la norma ISO 27001:2013.																																										
Valoración estado actual de la gestión de seguridad de la Gobernación de Santander con base en el **Instrumento de Evaluación MSPI de MINTIC**.																																										
Elaboración del documento **Nivel de Madurez** de seguridad y privacidad de la información, teniendo en cuenta las actividades anteriores de diagnóstico y contemplando lo propuesto en la guía “Modelo de Seguridad y Privacidad de la Información de la estrategia de Gobierno Digital” del Min. TIC**.**																																										

Actividad	2019						2020												2021												2022												COSTO
	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
ETAPA II: PLANIFICACIÓN	Definir la estrategia metodológica, que permita establecer el alcance, objetivos, procesos y procedimientos, pertinentes a la gestión del riesgo y mejora de seguridad digital y privacidad de la información, en procura de los resultados que permitan dar cumplimiento a la política de Seguridad Digital y Privacidad de la Información.																																									$300.000.000

Actividad	2019						2020												2021												2022												COSTO
	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
Realizar un **Análisis de Contexto** de la Gobernación de Santander entorno a la seguridad de la información																																										
Definir los roles y responsabilidades para la implementación, administración, operación y gestión de la seguridad digital y privacidad de la información e incluirlos en el sistema integrado de calidad de la Gobernación de Santander.																																										
Definir en la estructura organizacional de la Gobernación de Santander la dirección y/o grupo a los que se le asignará los roles y responsabilidades pertinentes a la seguridad de la información.																																										
Crear y/o Nombrar el Oficial de Seguridad Digital como responsable de la política de seguridad y priva.																																										

Actividad	2019						2020												2021												2022												COSTO
	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
Definir la metodología de riesgos de seguridad de la información																																										
Elaborar las políticas de seguridad digital y privacidad de la información, con su plan de implementación.																																										
Elaborar documentación de operación del sistema de gestión de seguridad de la información.																																										
I**dentificar y valorar** activos de información																																										
Identificar, valorar y tratar los riesgos de seguridad de la información de la gobernación de santander.																																										
Establecer plan de capacitación, comunicación y sensibilización de seguridad de la información																																										
Establecer Plan de diagnóstico de IPv4 a IPv6.																																										

Actividad	2019						2020												2021												2022												COSTO
	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
FASE III: IMPLEMENTACIÓN	Llevar a cabo la implementación de cada una de las actividades planificadas en la fase II, para dar cumplimiento a la Política de Seguridad Digital y Privacidad de la Información.																																								$2.500.000.000
Ejecutar el plan de tratamiento de riesgos																																									
Ejecutar del plan y estrategia de transición de IPv4 a IPv6.																																									
Establecer indicadores de gestión de seguridad digital.																																									
Implementar procedimiento de gestión de vulnerabilidades.																																									
Ejecutar plan de capacitación y sensibilización de seguridad																																									
Ejecutar pruebas anuales de vulnerabilidades e intrusión																																									
FASE IV: EVAUACIÓN Y DESEMPEÑO	Evaluar el desempeño y la eficacia del Modelo de Seguridad y Privacidad de la información, a través de instrumentos que permitan determinar la efectividad de la implementación de la Política de Seguridad Digital y Privacidad de la Información.																																								$100.000.000
Ejecutar las auditorías de seguridad de la información.																																									
FASE V: MEJORA CONTINUA	Consolidar los resultados obtenidos del componente de evaluación de desempeño, para diseñar el plan de mejoramiento continuo de seguridad digital y privacidad de la información, que permita realizar el plan de implementación de las acciones de mejora identificadas para el SGSI																																								$50.000.000

Actividad	2019						2020												2021												2022												COSTO
	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	1	2	3	4	5	6	7	8	9	10	11	12	
Diseñar plan de mejoramiento de Seguridad Digital y Privacidad de la Información																																										

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**REVISÓ**	**APROBÓ**
0	23/09/2019	Creación del Documento	Secretaría de Tecnologías de la información y comunicaciones Dirección de Sistemas Integrados de Gestión.	Comité Institucional de Gestión y Desempeño