PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LAS UNIDADES TECNOLÓGICAS DE SANTANDER

Presentado Por:

Coordinador Recursos Informáticos

UNIDADES TECNOLOGICAS DE SANTANDER

BUCARAMANGA, OCTUBRE DE 2019

Tabla de contenido

1. OBJETIVO

Establecer los lineamientos, optimización e implementación de la Política de Seguridad y Privacidad de la Información, que permitan, medir, prevenir y atender la atención de riesgos en la seguridad y privacidad de la información en las Unidades Tecnológicas de Santander.

2. ALCANCE

El presente documento describe el Plan de Seguridad y Privacidad de la información, alineado con los objetivos, metas, procesos, procedimientos y estructura organizacional, de tal forma que se asegure la confidencialidad, integridad y disponibilidad los componentes de información.

Esta política de seguridad y privacidad de la información aplica a todas las dependencias de las Unidades Tecnológicas de Santander.

La información que se genera en cada uno de los procesos de la entidad es muy relevante para el logro de las metas y objetivos institucionales, garantizando la integridad, disponibilidad y confidencialidad de los activos de información de las Unidades Tecnológicas de Santander.

Estas políticas de seguridad y privacidad de la información aplican para todos los servidores públicos, contratitas, pasantes, administrativos, estudiantes y visitantes de las Unidades Tecnológicas de Santander y deben ser de obligatorio cumplimiento.

3. TERMINOS Y DEFINICIONES

Amenaza: Causa potencial de un incidente no deseado, que puede provocar daños a un sistema o a la institución.

Aceptación de riesgo: Decisión informada de asumir un riesgo concreto.

Activos de información: Los activos de información son los recursos del Sistema de Seguridad de la Información, relacionados con el procesamiento,

almacenamiento y salvaguarda de la información de la institución y que soportan los procesos necesarios para la continuidad de las operaciones.

Confidencialidad: Propiedad de la información de no ponerse a disposición o ser revelada a destinatarios no autorizados. La información debe ser accedida sólo por aquellas personas a las que se ha concedido acceso como una necesidad legítima para la realización de sus funciones.

Control: Las políticas, los procedimientos, las prácticas y las estructuras institucionales concebidas para mantener los riesgos de seguridad de la información por debajo del nivel de riesgo asumido.

Datos Abiertos: Son todos aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan

Datos Personales: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables. (Ley 1581 de 2012, art.3).

Riesgo de seguridad de la información: Posibilidad de que una amenaza concreta que pueda aprovechar una vulnerabilidad para causar una pérdida o daño en un activo de información; estos daños consisten en la afectación de la confidencialidad, integridad o disponibilidad de la información. Cuando la amenaza se convierta en una oportunidad se debe tener en cuenta en el beneficio que se genera. También se puede generar riesgo positivo en la seguridad de la información por el aprovechamiento de oportunidades y fortalezas que se presenten.

Riesgo Positivo: Posibilidad de ocurrencia de un evento o situación que permita optimizar los procesos y/o la gestión institucional, a causa de oportunidades y/o fortalezas que se presentan en beneficio de la entidad.

Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos, preservando.

4. POLITICA INSTITUCIONAL UNIDADES TECNOLOGICAS DE SANTANDER

Para las Unidades Tecnológicas de Santander la información constituye un activo valioso para la gestión, control y toma de decisiones de todas sus actividades misionales.

Política Corporativa de Seguridad de la Información En las UNIDADES TECNOLÓGICAS SANTANDER la información es un activo fundamental para la prestación de sus servicios y la toma de decisiones eficientes, razón por la cual existe un compromiso expreso de protección de sus propiedades más significativas como parte de una estrategia orientada al fortalecimiento institucional, la administración de riesgos y la consolidación de una cultura de seguridad. Consciente de sus necesidades actuales, las UNIDADES TECNOLÓGICAS SANTANDER implementa un modelo de gestión de seguridad de la información como la herramienta que permite identificar y minimizar los riesgos a los cuales se expone la información, ayuda a la reducción de costos operativos y financieros, establece una cultura de seguridad y garantiza el cumplimiento de los requerimientos legales, contractuales, regulatorios vigentes.

El proceso de análisis de riesgos de los activos de información es el soporte para el desarrollo de las Políticas de Seguridad de la Información y de los controles y objetivos de control seleccionados para obtener los niveles de protección esperados en las UNIDADES TECNOLÓGICAS SANTANDER; este proceso será liderado de manera permanente por la Oficina de Recursos Informáticos. Esta política será revisada con regularidad como parte del proceso de Infraestructura y Logística, o cuando se identifiquen cambios en la Institución, su estructura, sus objetivos o alguna condición que afecten la política, para asegurar que sigue siendo adecuada y ajustada a los requerimientos identificados.

4.1 PARAMETROS DE LA POLITICA

- **PROPIEDAD DE LA INFORMACIÓN:** Las Unidades Tecnológicas de Santander tiene la propiedad absoluta de la información generada y gestionada en la institución por parte de los servidores, contratistas y docentes, garantizada en acuerdos de confidencialidad y manejo de la información para garantizar el buen uso de acuerdo a sus funciones y obligaciones en las labores operativas y de conservación de las misma, sin perjuicio para la Institución de perder la propiedad de la Información.

- **GESTION DE ACTIVOS DE INFORMACION:** Se entenderá cómo activo de información, todo documento u archivo físico, electrónico o digital, que tiene valor para el ejercicio propio de la misión de la Institución, para lo cual el Grupo de Recursos Informáticos será la responsable de Inventariar los activos de información según su categoría y uso, determinando el proceso

responsable y los posibles riesgos asociados al manejo de estos activos, protegiéndolos según la determinación de los planes de riesgos que se establezcan pare este fin.

- **CONTROL DE ACCESO**: Las Unidades Tecnológicas de Santander, por medio de la oficina de Recursos Informáticos establecerán los controles de acceso a la información necesarios en los equipos, sistemas de información, redes internas y otros activos de información que lo requieran.

- **ADMINISTRACION DE REDES Y EQUIPOS:** Los equipos de cómputo, sistemas de almacenamiento y procesamiento de datos, redes de datos son herramientas de apoyo para la ejecución de labores de servidores y contratistas tanto administrativos cómo académicos, por lo tanto, la Oficina de Recursos Informáticos, cómo administradora de la infraestructura tecnológica dispondrá de los lineamientos necesarios para garantizar la disponibilidad, soporte y mantenimiento de los equipos y redes de la Institución.

- **USO DE SOFTWARE Y SISTEMAS DE INFORMACION, CORREO ELECTRONICO Y USO DE INTERNET:** Todos los funcionarios tanto de planta como contratista de la Institución son responsables del buen uso del software, sistemas de información, correo electrónico y uso del internet, respetando la legalidad del software, evitando instalar software no licenciado en los equipos, todas las herramientas de correo electrónico, internet que provee o delega la Institución deberá sólo ser usado con fines institucionales evitando cualquier uso de interés personal.

- **RESPONABILIDADES:** Todos los funcionarios tantos de planta como contratista de la Institución a los cuales les sean asignados usuarios de acceso a sistemas de Información, tendrán el uso y resguardo de los mismos, asumiendo la responsabilidad de los roles y permisos de dicho usuario y contraseña asignada, evitando su préstamo, divulgación y uso indebido de los activos de información a los cuales tenga acceso.

- **SEGURIDAD FISICA DE LA INFORMACION:** Las Unidades Tecnológicas de Santander mediante la oficina de Recursos Informáticos determinará las áreas donde reposen los activos de información, planteando planes para impedir el acceso no autorizado, evitar robo, pérdida, daño entre otros que puedan afectar la integridad de los activos de información, sistemas de procesamiento y comunicaciones de la institución.

5. OBJETIVOS DEL SISTEMA DE GESTION DE SEGURIDAD DE LA INFORMACION

- Definir y formalizar los elementos normativos sobre los temas de protección de la información.
- Establecer los mecanismos de aseguramiento físico y digital, para fortalecer la confidencialidad, integridad, disponibilidad, legalidad, confiabilidad de la información.
- Generar y divulgar una cultura sobre seguridad de la información a los funcionarios públicos, contratistas, comunidad, proveedores y demás partes interesadas en las Unidades Tecnológicas de Santander

6. COMITÉ DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

El Sistema de Gestión de Seguridad de la Información de la Unidades Tecnológicas de Santander se está formalizando con el proceso de Gestión de Sistemas de Información donde se integrará el Comité de Seguridad de la Información que será integrado por los funcionarios de cada uno de los procesos de la Unidades Tecnológicas de Santander. Quedando conformado así:

La entidad debe definir mediante un acto administrativo (Resolución, circular, decreto, entre otros) los roles y las responsabilidades de seguridad de la información en los diferentes niveles (Directivo, De procesos y Operativos) que permitan la correcta toma de decisiones y una adecuada gestión que permita el cumplimiento de los objetivos de las Unidades Tecnológicas de Santander. Creando el Comité.

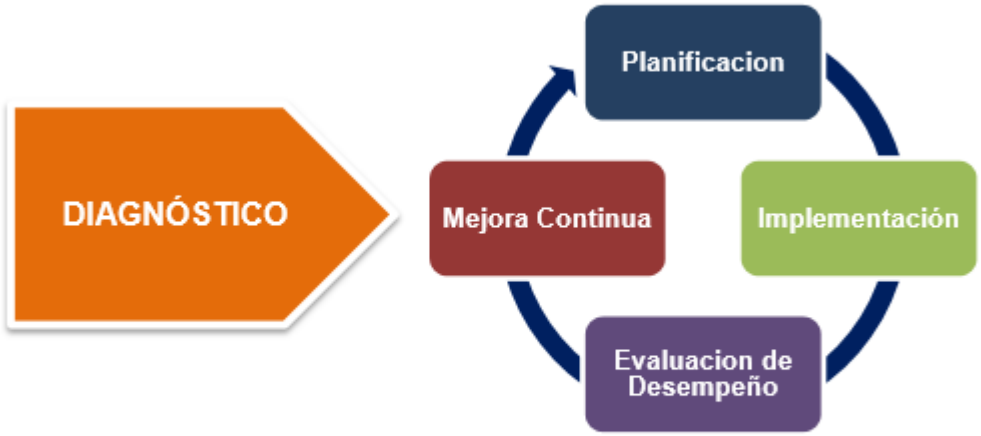
CATEGORIA	PROCESO	FUNCIONARIO
	CONCEJO DIRECTIVO	1
	CONCEJO ACADEMICO	1
ESTRATEGICOS	PLANEACION NSTITUCIONAL	1
	COMUNICACIÓN INTITUCIONAL	1
	SEGUIMIENTO Y CONTROL	1
MISIONALES	DOCENCIA	1
	INVESTIGACION	1
	PROYECION SOCIAL	1
APOYO	BIENESTAR INSTITUCIONAL	1
	COMPRAS Y SUMINISTROS	1
	ADMINISTRACIONES Y MATRICULAS	1
	GESTION JURIDICA	1
	GESTION DOCUMENTAL	1
	GESTION CONOCIMIENTO	1
	GESTION FINANCIERA	1
	GESTION TALENTO HUMANO	1
	INFRAESTRUCTURA LOGISTICA	1
	INTERNACIONALIZACION	1
	SOPORTE DE SISTEMA DE GESTION	1
EVALUACION	CONTROL DE EVALUACION	1

7. PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACION.

El modelo de seguridad y privacidad de la información contempla un ciclo de operación que consta de cinco (5) fases, las cuales permiten que las Unidades Tecnológicas de Santander puedan gestionar adecuadamente la seguridad y privacidad de sus activos de información.

En el presente Modelo de Seguridad y Privacidad de la Información se contemplan 6 niveles de madurez, que corresponden a la evolución de la implementación del modelo de operación. La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que

contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad



Ciclo de operación del Modelo de Seguridad y Privacidad de la Información

7.1 DIAGNOSTICO

7.1.1 Situación Actual

AMBITO	SITUACION ACTUAL
Diagnóstico de seguridad y Privacidad	Las Unidades Tecnológicas de Santander no cuentan con instrumento de evaluación de la implementación del modelo de seguridad y privacidad de la información. Este instrumento de Evaluación cuenta el resultado de identificar el nivel de madurez de la Seguridad y Privacidad de la Información en la entidad, identificar las vulnerabilidades técnicas y administrativas y generar planes de mejoramiento para subsanar dichas vulnerabilidades

	Se ha divulgado la política general de seguridad de la información en las Unidades Tecnológicas de Santander
Plan de Seguridad y privacidad	Se creará y formalizará un comité de seguridad y privacidad de la Información según resolución o acto administrativo de las Unidades Tecnológicas de Santander.
	Es necesario fortalecer los procesos y procedimientos que hacen referencia a la implementación de la seguridad y privacidad de la información en las Unidades Tecnológicas de Santander, actividad que debe ser liderada por la Oficina de Recursos Informáticos, Asesorada por la oficina de Planeación.
	Se deben establecer políticas del tratamiento de riesgos y revisión en un periodo adecuado, reformando el modelo de manejo de incidentes de seguridad para ser elaborado con las especificaciones adecuadas.

8. PLAN DE IMPLEMENTACIÓN DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Teniendo en cuenta la política general de seguridad de la información en las Unidades Tecnológicas de Santander y el Modelo de Operación por Gestiones del Dimensión de Seguridad de la Información se establece el PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN DE LAS UNIDADES TECNOLÓGICAS DE SANTANDER el cual responde a la gobernabilidad de la siguiente manera: Min TIC lidera la política de Gobierno Digital. A continuación, las actividades requeridas para la ejecución del plan:

GESTION	ACTIVIDADES	TAREAS	RESPONSABLES	FECHAS PROGRAMACION
ACTIVOS DE LA INFORMACION	Levantamiento Activos de Información	Socializar la guía de activos de Información	OFICINA DE RECURSO INFORMATICOS	SEP-2019
		Identificar nuevos activos de información en cada dependencia	OFICINA DE RECURSO INFORMATICOS	SEP-2019
		Realizar informe de actualización a los activos de información por alguna de las siguientes novedades: Actualizaciones al proceso al que pertenece el activo, Adición de actividades al proceso, Inclusión de un nuevo activo, Cambios o migraciones de sistemas de información en donde se almacenan o reposan activos de la ubicación ya inventariados.	OFICINA DE RECURSO INFORMATICOS-JEFE PROCESOS DE CADA DEPENDENCIA	SEP-2019
GESTIÓN DE RIESGOS	Actualización de lineamientos de riesgos	Actualizar política y metodología de gestión de riesgos	OFICINA DE RECURSO INFORMATICOS	AGOSTO 2019
	Identificación de Riesgos de Seguridad y Privacidad de la Información, Seguridad Digital	Identificación, Análisis y Evaluación de Riesgos Seguridad y Privacidad de la Información, Seguridad Digital	OFICINA DE RECURSO INFORMATICOS	SEP -2019
	Aceptación de Riesgos Identificados	Aceptación, aprobación Riesgos identificados y planes de tratamiento	OFICINA DE RECURSO INFORMATICOS-PLANEACION	NOV-2019
	Publicación	Publicación Matriz de riesgos a nivel Institucional	PLANEACION	NOV-2019
	Monitoreo y Revisión	Generación, presentación y reporte de indicadores	PLANEACION	NOV-2019
GESTIÓN DE INCIDENTES DE SEGURIDAD	Elaboración de procedimiento de gestión de incidentes de seguridad	Elaboración del procedimiento de gestión de incidentes basados en la ISO 27035	OFICINA DE RECURSO INFORMATICOS	NOV-2019
	Publicar y Socializar el	Publicar el procedimiento de gestión de incidentes	OFICINA DE RECURSO INFORMATICOS	MARZO 2020

DE LA INFORMACIÓN	procedimiento actualizado de incidentes de seguridad de la información Publicar	de Seguridad de la Información.		
		Socializar el procedimiento a los soportes en sitio y Mesa de Servicios, indicando los cambios en el procedimiento	OFICINA DE RECURSO INFORMATICOS	MARZO 2020
		Socializar el procedimiento a los Administrativos, Contratistas, Comunidad Estudiantil de las Unidades Tecnológicas de Santander	TODOS LOS PROCESOS UNIDADES TECNOLOGICAS DE SANTANDER	JUNIO 2020
Gobierno Digital	Gobierno Digital	Actualizar el documento de autodiagnóstico de la entidad en la implementación de Seguridad y Privacidad de la Información.	OFICINA DE RECURSO INFORMATICOS	JUNIO 2020
		Revisar y alinear la documentación del SGSI de las Unidades Tecnológicas de Santander, de acuerdo con la Normatividad vigente.	OFICINA DE RECURSO INFORMATICOS	JUNIO 2020
		Revisar el avance de implementación del Plan de Seguridad Digital en la Entidad	OFICINA DE RECURSO INFORMATICOS	JUNIO 2020
		Reuniones de Socialización de los avances de la implementación del plan de Seguridad Digital y la Estrategia del Modelo de Seguridad y Privacidad de la información	OFICINA DE RECURSO INFORMATICOS	JUNIO 2020

9. MARCO NORMATIVO

- Constitución Política de Colombia. Artículo 15.
- Ley 44 de 1993. Por la cual se modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944 y Decisión Andina 351 de 2015 (Derechos de autor).
- Ley 527 de 1999. Por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- Ley 594 de 2000. Por medio de la cual se expide la Ley General de Archivos.

- Ley 850 de 2003. Por medio de la cual se reglamentan las veedurías ciudadanas
- Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del Hábeas data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.
- Decreto 1008 del 2018. Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
- Resolución 2999 del 2008. Por el cual se adoptan las políticas de seguridad para el manejo de la información y se dictan otras normas para el uso y administración de los bienes y servicios informáticos del Ministerio TIC.
- Resolución 2034 de 2016. Por la cual se adoptó el Modelo de Responsabilidad Social Institucional en el Ministerio TIC.
- Resolución 2007 de 2018. Por la cual se actualiza la política de tratamiento de datos personales del Ministerio/Fondo TIC.
- Resolución 911 de 2018. Por la cual se actualiza el Modelo Integrado de Gestión del MinTIC.
- Resolución 2133 de 2018. Por la cual se establecen las condiciones especiales del Teletrabajo en el Ministerio de Tecnologías de la Información y las Comunicaciones, y se deroga las resoluciones No 3559 y 4950 de 2013, 2313 y 494 de 2014 y 2787 de 2016.
- Resolución 512 de 2019. Por la cual se adopta la Política General de Seguridad y Privacidad de la Información, Seguridad Digital y Continuidad de los servicios del Ministerio/Fondo de Tecnologías de la Información y las Comunicaciones y se definen lineamientos frente al uso y manejo de la información
- CONPES 3701 de 2011. Lineamientos de Política para Ciberseguridad y Ciberdefensa.
- CONPES 3854 de 2016. Política Nacional de Seguridad digital.

VERSION	DESCRIPCIÓN	NUMERO DE SOLICITUD DE CAMBIO	FECHA
01	Emisión Inicial de Documento	N/A	OCTUBRE DE 2019