República de Colombia

Gobernación de Santander

MANUAL DE POLÍTICAS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

MANUAL DE POLÍTICAS 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:	Manual de Políticas de Seguridad Digital y Privacidad de la Información				
Fecha Elaboración	Septiembre de 2019 Modificado				
Formato	Documento Texto		Lenguaje:		Español
Dependencia:	Secretaría de Las Tecnologías de la Información y Comunicación				
Código:	AP-TIC-MA-01	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

La Gobernación de Santander identifica la información como un componente indispensable en la conducción y consecución de los objetivos definidos por la estrategia de la Entidad, la rápida evolución del entorno técnico requiere que las Entidades del Estado adopten un conjunto mínimo de controles de seguridad para proteger su información y sistemas de información. El propósito de la Política de Seguridad y Privacidad de la Información es proporcionar una visión general de los requisitos de seguridad digital y se describen los controles en el lugar o los previstos para cumplir esos requisitos.

Este documento describe las políticas y normas de seguridad de la información definidas por la Gobernación de Santander. Para la elaboración del mismo, se toman como base la normatividad, recomendaciones del Modelo de Seguridad y Privacidad propuesto por el Ministerio de las TIC y demás regulaciones aplicables, la norma ISO 27001:2013 y las recomendaciones del estándar ISO 27002:2013.

Las políticas incluidas en este manual se constituyen como parte fundamental del Modelo Integrado de Planeación y Gestión de la Gobernación de Santander y se convierten en la base para la implementación de los controles, procedimientos y estándares necesarios.

La seguridad de la información es una prioridad para la Gobernación de Santander y por tanto es responsabilidad de todos velar por que no se realicen actividades que contradigan la esencia y el espíritu de cada una de estas políticas.

2. OBJETIVO

El objetivo de este documento es establecer las políticas en seguridad digital y privacidad de la información de la Gobernación de Santander, con el fin de regular la protección, calidad y gestión de la información en la Entidad.

3. ALCANCE

El alcance de esta política es contrarrestar el incremento de las amenazas informáticas que afecten significativamente, y afrontar retos en aspectos de seguridad cibernética.

En materia de Seguridad Digital, el Documento CONPES 3854 de 2016 incorpora la Política Nacional de Seguridad Digital coordinada por la Presidencia de la República, para orientar y dar los lineamientos respectivos a las Entidades.

En el orden nacional, en los Comités Sectoriales de Gestión y Desempeño se darán las directrices para su implementación. Además, la articulación en materia de Seguridad Digital estará a cargo del enlace sectorial de seguridad digital quien será el encargado de rendir

cuentas al Coordinador Nacional de Seguridad Digital acerca de la implementación de la Política Nacional de Seguridad Digital en el respectivo sector.

De otro lado, en el Comité Institucional de Gestión y Desempeño se debe articular los esfuerzos, recursos, metodologías y estrategias para asegurar la implementación de la política. Para ello, se debe designar un responsable de Seguridad Digital que también es el responsable de la Seguridad de la Información en la Entidad. Desde el Ministerio de las Tecnologías de la Información y las Comunicaciones - Min TIC se desarrollarán los lineamientos para que las Entidades territoriales definan la figura del enlace de Seguridad Digital territorial para la implementación de la política de Seguridad Digital, así como las instancias respectivas para la articulación con el Coordinador Nacional de Seguridad Digital.

4. DEFINICIONES

Activo de información: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos de negocios de la Entidad y, en consecuencia, debe ser protegido.

Acuerdo de Confidencialidad: es u documento en los que los servidores públicos de la Gobernación de Santander o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de la Entidad, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.

Análisis de riesgos de seguridad digital: proceso sistemático de identificación de fuentes, estimación de impactos y probabilidades y comparación de dichas variables contra criterios de evaluación para determinar las consecuencias potenciales de pérdida de confidencialidad, integridad y disponibilidad de la información.

Autenticación: es el procedimiento de comprobación de la Entidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.

Capacity Planning: es el proceso para determinar la capacidad de los recursos de la plataforma tecnológica que necesita la Entidad para satisfacer las necesidades de procesamiento de dichos recursos de forma eficiente y con un rendimiento adecuado.

Centros de cableado: son habitaciones donde se deberán instalar los dispositivos de comunicación y la mayoría de los cables. Al igual que los centros de cómputo, los centros de cableado deben cumplir requisitos de acceso físico, materiales de paredes, pisos y techos, suministro de alimentación eléctrica y condiciones de temperatura y humedad.

Centro de cómputo: es una zona específica para el almacenamiento de múltiples computadores para un fin específico, los cuales se encuentran conectados entre sí a través de una red de datos. El centro de cómputo debe cumplir ciertos estándares con el fin de garantizar los controles de acceso físico, los materiales de paredes, pisos y techos, el suministro de alimentación eléctrica y las condiciones medioambientales adecuadas.

Cifrado: es la transformación de los datos mediante el uso de la criptografía para producir datos ininteligibles (cifrados) y asegurar su confidencialidad. El cifrado es una técnica muy útil para prevenir la fuga de información, el monitoreo no autorizado e incluso el acceso no autorizado a los repositorios de información.

Confidencialidad: es la garantía de que la información no está disponible o divulgada a personas, Entidades o procesos no autorizados.

Control: es toda actividad o proceso encaminado a mitigar o evitar un riesgo. Incluye policías, procedimientos, guías, estructuras organizacionales y buenas prácticas, que pueden ser de carácter administrativo, tecnológico, físico o legal.

Criptografía: es la disciplina que agrupa a los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.

Custodio del activo de información: es la unidad organizacional o proceso, designado por los propietarios, encargado de mantener las medidas de protección establecidas sobre los activos de información confiados.

Derechos de Autor: es un conjunto de normas y principios que regulan los derechos morales y patrimoniales que la ley concede a los autores por el solo hecho de la creación de una obra literaria, artística o científica, tanto publicada o que todavía no se haya publicado.

Disponibilidad: es la garantía de que los usuarios autorizados tienen acceso a la información y a los activos asociados cuando lo requieren.

Equipo de cómputo: dispositivo electrónico capaz de recibir un conjunto de instrucciones y ejecutarlas realizando cálculos sobre los datos numéricos, o bien compilando y correlacionando otros tipos de información.

Guías de clasificación de la información: directrices para catalogar la información de la Entidad y hacer una distinción entre la información que es crítica y aquella que lo es menos o no lo es y, de acuerdo con esto, establecer diferencias entre las medidas de seguridad a aplicar para preservar los criterios de confidencialidad, integridad y disponibilidad de la información

Hacking ético: es el conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

Incidente de Seguridad: es un evento adverso, confirmado o bajo sospecha, que haya vulnerado la seguridad de la información o que intente vulnerarla, sin importar la información afectada, la plataforma tecnológica, la frecuencia, las consecuencia, el número de veces ocurrido o el origen (interno o externo).

Integridad: es la protección de la exactitud y estado completo de los activos.

Inventario de activos de información: es una lista ordenada y documentada de los activos de información pertenecientes a la Entidad.

Licencia de software: es un contrato en donde se especifican todas las normas y cláusulas que rigen el uso de un determinado producto de software, teniendo en cuenta aspectos como: alcances de uso, instalación, reproducción y copia de estos productos.

Medio removible: es cualquier componente extraíble de hardware que sea usado para el almacenamiento de información; los medios removibles incluyen cintas, discos duros removibles, CD, DVD y unidades de almacenamiento USB, entre otras.

Perfiles de usuario: son grupos que concentran varios usuarios con similares necesidades de información y autorizaciones idénticas sobre los recursos tecnológicos o los sistemas de información a los cuales se les concede acceso de acuerdo con las funciones realizadas. Las modificaciones sobre un perfil de usuario afectan a todos los usuarios cobijados dentro de él.

Propiedad intelectual: es el reconocimiento de un derecho particular en favor de un autor u otros titulares de derechos, sobre las obras del intelecto humano. Este reconocimiento es aplicable a cualquier propiedad que se considere de naturaleza intelectual y merecedora de protección, incluyendo las invenciones científicas y tecnológicas, las producciones literarias o artísticas, las marcas y los identificadores, los dibujos y modelos industriales y las indicaciones geográficas.

Propietario de la información: es la unidad organizacional o proceso donde se crean los activos de información.

Recursos tecnológicos: son aquellos componentes de hardware y software tales como: servidores (de aplicaciones y de servicios de red), estaciones de trabajo, equipos portátiles, dispositivos de comunicaciones y de seguridad, servicios de red de datos y bases de datos, entre otros, los cuales tienen como finalidad apoyar las tareas administrativas necesarias para el buen funcionamiento y la optimización del trabajo al interior de la Gobernación de Santander.

Registros de Auditoría: son archivos donde son registrados los eventos que se han identificado en los sistemas de información, recursos tecnológicos y redes de datos de la Entidad. Dichos eventos pueden ser, entre otros, identificación de usuarios, eventos y acciones ejecutadas, terminales o ubicaciones, intentos de acceso exitosos y fallidos, cambios a la configuración, uso de utilidades y fallas de los sistemas.

Responsable por el activo de información: es la persona o grupo de personas, designadas por los propietarios, encargados de velar por la confidencialidad, la integridad y disponibilidad de los activos de información y decidir la forma de usar, identificar, clasificar y proteger dichos activos a su cargo.

Servidor público: El servidor público tiene un contrato de trabajo, se trata de un trabajador oficial y su régimen legal será el establecido en el contrato de trabajo, la convención colectiva, el pacto colectivo o en el reglamento interno de trabajo, y por lo no previsto en ellos en la Ley 6 de 1945, al Decreto 2127 de 1945 y demás normas que lo modifican o adicionan; si por el contrario, el servidor público fue vinculado mediante una relación legal y reglamentaria a un empleo de libre nombramiento y remoción o a un cargo de carrera administrativa sea por concurso o provisional, tiene la calidad de empleado público y su régimen legal será el establecido en las normas para empleados públicos.

SGSI: Sistema de Gestión de Seguridad de la Información.

Sistema de información: es un conjunto organizado de datos, operaciones y transacciones que interactúan para el almacenamiento y procesamiento de la información que, a su vez, requiere la interacción de uno o más activos de información para efectuar sus tareas. Un sistema de información es todo componente de software ya sea de origen interno, es decir desarrollado por la Gobernación de Santander o de origen externo ya sea adquirido por la Entidad como un producto estándar de mercado o desarrollado para las necesidades de ésta.

Sistemas de control ambiental: son sistemas que utilizan la climatización, un proceso de tratamiento del aire que permite modificar ciertas características del mismo, fundamentalmente humedad y temperatura y, de manera adicional, también permite controlar su pureza y su movimiento.

Software malicioso: es una variedad de software o programas de códigos hostiles e intrusivos que tienen como objeto infiltrarse o dañar los recursos tecnológicos, sistemas operativos, redes de datos o sistemas de información.

Terceros: todas las personas, jurídicas o naturales, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

Vulnerabilidades: son las debilidades, hoyos de seguridad o flaquezas inherentes a los activos de información que pueden ser explotadas por factores externos y no controlables por la Entidad (amenazas), las cuales se constituyen en fuentes de riesgo.

5. POLÍTICA GLOBAL DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

En la Gobernación de 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 a la continuidad del negocio, la administración de riesgos y la consolidación de una cultura de seguridad digital.

Consciente de las necesidades actuales, la Gobernación de Santander define una política de seguridad digital y privacidad de la información como herramienta para minimizar los riesgos a los cuales se expone la información, apuntando a la reducción de costos operativos y financieros, estableciendo una cultura de seguridad digital y garantizando el cumplimiento de los requerimientos legales, contractuales y regulatorios.

Los servidores públicos, personal externo, proveedores y todos aquellos que tengan responsabilidades sobre las fuentes, repositorios y recursos de procesamiento de la información de la Gobernación de Santander, deben adoptar los lineamientos contenidos en el presente documento y en los documentos relacionados con él, con el fin de mantener la confidencialidad, la integridad y asegurar la disponibilidad de la información.

La Política Global de Seguridad Digital de la Gobernación de Santander se encuentra soportada por políticas, normas y procedimientos específicos los cuales guiarán el manejo adecuado de la información de la Entidad. Adicionalmente, se establecerán políticas específicas de seguridad de la información las cuales se fundamentan en los dominios y objetivos de control del Anexo A de la norma internacional ISO 27001:2013.

El Comité Institucional de Gestión y Desempeño, con el apoyo del líder u oficial de seguridad digital, tendrán la potestad de modificar la Política Global o las Políticas Específicas de Seguridad Digital y Privacidad de la Información de acuerdo con las necesidades de revisión establecidas periódicamente o a la aplicabilidad de las mismas.

6. COMPROMISO DE LA ALTA DIRECCIÓN

El Comité Institucional de Gestión y Desempeño de la Gobernación de Santander aprueba esta Política de Seguridad Digital y Privacidad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de políticas eficientes que garanticen la seguridad de la información de la Entidad, dando cumplimiento al Decreto 612 de 2018 que reglamenta la integración de los planes institucionales y estratégicos al plan de acción por parte de las Entidades del Estado.

La Alta Dirección de la Gobernación de Santander demuestran su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad Digital contenidas en este documento.
- La promoción activa de una cultura de seguridad.
- Facilitar la divulgación de este manual a todos los servidores públicos, personal externo y proveedores de la Entidad.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de seguridad digital.
- La verificación del cumplimiento de las políticas aquí mencionadas.

7. SANCIONES PARA LAS VIOLACIONES A LAS POLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

El incumplimiento a la Política de Seguridad Digital y Privacidad de la Información se gestiona a través de procedimientos administrativos que puede repercutir en procesos disciplinarios, judiciales y procesos administrativos según las circunstancias de modo, tiempo, lugar y gravedad de la falta.

Por lo anterior, se hace necesario que las violaciones a la Política de Seguridad Digital y Privacidad de la Información sean clasificadas, con el objetivo de aplicar medidas correctivas conforme con los niveles de clasificación definidos (integridad, disponibilidad y confidencialidad) y mitigar posibles afectaciones contra la seguridad de la información.

8. POLÍTICAS DE LA ORGANIZACIÓN DE LA SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

Cada rol y responsabilidad para la seguridad digital y privacidad de la información se define mediante el plan de seguridad digital y privacidad de la información.

La Gobernación de Santander deberá estructurar el sistema de gestión de seguridad digital que incluya las orientaciones, definiciones y revisiones para su administración liderado por el comité de seguridad de la información, el cual se deberá crear al interior de la Entidad.

A cada servidor público, personal externo y proveedor se le asignará una responsabilidad en el sistema de gestión de seguridad digital y las mismas se podrán reflejar en el presente documento.

La gestión de los riesgos y la evaluación del riesgo residual es responsabilidad de los líderes de procesos con el apoyo de la dirección de sistemas integrados de gestión.

8.1. Política de la estructura organizacional de seguridad digital y privacidad de la Información

La Gobernación de Santander establecerá un esquema de seguridad de la información en donde existan roles y responsabilidades definidos que consideren actividades de administración, operación y gestión de la seguridad de la información.

8.1.1. Normas que rigen para la estructura organizacional de seguridad digital y privacidad de la información

Normas dirigidas a: LA ALTA DIRECCIÓN

- Definir y establecer los roles y responsabilidades relacionados con la seguridad de la información en niveles directivo y operativo.

- Revisar y aprobar las Políticas de Seguridad Digital y Privacidad de la Información contenidas en este documento.
- Definir y aprobar el presupuesto para seguridad digital.
- Promover activamente una cultura de seguridad de la información en la Entidad.
- Facilitar la divulgación de las Políticas de Seguridad Digital y Privacidad de la Información a todos los servidores públicos de la Entidad y al personal provisto por terceras partes.
- La Alta Dirección y la Secretaría General asigna los recursos, la infraestructura física y el personal necesario para la gestión de la seguridad digital.

Normas dirigidas a: EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- Presentar y actualizar ante el Comité Institucional de Gestión y Desempeño y de la Gobernación de Santander, el plan de acción para la administración de los riesgos de seguridad digital y la metodología para la clasificación de la información, según lo considere pertinente.
- Analizar los incidentes de seguridad digital que le son escalados al Comité y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.
- Verificar el cumplimiento de las Políticas de seguridad Digital y Privacidad de la Información aquí mencionadas.

Normas dirigidas a: EL RESPOSABLE DE LA SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

- Debe liderar la generación de lineamientos para gestionar la seguridad de la información de la Gobernación de Santander y el establecimiento de controles técnicos, físicos y administrativos derivados de análisis de riesgos de seguridad.
- Debe validar y monitorear de manera periódica la implementación de los controles de seguridad establecidos.

Normas dirigidas a: LA OFICINA DE CONTROL INTERNO

- Debe ejecutar revisiones totales o parciales de los procesos o áreas que hacen parte del alcance y/o procesos relacionados con la gestión de seguridad digital, con el fin de verificar la eficacia de las acciones correctivas cuando sean identificadas no conformidades.
- Debe informar a las áreas responsables los hallazgos de las auditorías.

Normas dirigidas a: SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Debe asignar las funciones, roles y responsabilidades, a sus servidores públicos[1] para la operación y administración de la plataforma tecnológica de la Gobernación de Santander. Dichas funciones, roles y responsabilidades deben encontrarse debidamente documentadas.

Normas dirigidas a: TODOS LOS USUARIOS

- Los servidores públicos, personal externo y proveedores que realicen funciones en o para la Gobernación de Santander, tienen la responsabilidad de cumplir con las políticas, normas, procedimientos y estándares referentes a la seguridad digital y privacidad de la información.

8.2. Políticas para uso de dispositivos móviles

La Gobernación de Santander proveerá las condiciones para el manejo de los dispositivos móviles (teléfonos, inteligentes y tabletas, entre otros) institucionales y personales que hagan uso de servicios de la Entidad. Así mismo, velará porque los servidores públicos hagan un uso responsable de los servicios y equipos proporcionados por la Entidad.

8.2.1. Normas para uso de dispositivos móviles

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIONES

- Debe investigar y probar las opciones de protección de los dispositivos móviles institucionales y personales que hagan uso de los servicios provistos por la Gobernación de Santander.

- Establecer las configuraciones aceptables para los dispositivos móviles institucionales o personales que hagan uso de los servicios provistos por la Gobernación de Santander.

- Establecer un método de bloqueo (por ejemplo; contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios.

- Activar la opción de cifrado de la memoria de almacenamiento de los dispositivos móviles institucionales haciendo imposible la copia o extracción de datos si no se conoce el método de desbloqueo.

---

[1] Funcionario vinculado de libre nombramiento y remoción, carrera administrativa, provisional o contratista de la Gobernación de Santander.

- Configurar la opción de borrado remoto de información en los dispositivos móviles institucionales, con el fin de eliminar los datos de dichos dispositivos y restaurarlos a los valores de fábrica, de forma remota, evitando así divulgación no autorizada de información en caso de pérdida o hurto.

- Definir una solución de copias de seguridad para la información contenida en los dispositivos móviles institucionales de la Gobernación de Santander; dichas copias deben acogerse al procedimiento de copias de respaldo de la información.
- Instalar un software de antivirus tanto en los dispositivos móviles institucionales. como en los personales que hagan uso de los servicios provistos por la Gobernación de Santander.

- Activar los códigos de seguridad de la tarjeta SIM para los dispositivos móviles institucionales antes de asignarlos a los usuarios y almacenar estos códigos en un lugar seguro.

Normas dirigidas a: TODOS LOS USUARIOS

- Evitar usar los dispositivos móviles institucionales en lugares que no les ofrezcan las garantías de seguridad física necesarias para evitar pérdida o robo de estos.

- La modificación de las configuraciones de seguridad de los dispositivos móviles institucionales será bajo su responsabilidad, no deberá desinstalar el software provisto con ellos al momento de su entrega.

- Evitar la instalación de programas desde fuentes desconocidas; se deben instalar aplicaciones únicamente desde los repositorios oficiales de los dispositivos móviles institucionales.

- Cada vez que el sistema de sus dispositivos móviles institucionales notifique de una actualización disponible, aceptar y aplicar la nueva versión.

- Evitar hacer uso de redes inalámbricas de uso público, así como deben desactivar las redes inalámbricas como WIFI, Bluetooth, o infrarrojos en los dispositivos móviles institucionales asignados.

- Evitar conectar los dispositivos móviles institucionales asignados por puerto USB a cualquier computador público, de hoteles o cafés internet, entre otros.

- No deben almacenar videos, fotografías o información personal en los dispositivos móviles institucionales asignados.

- Preservando el derecho fundamental a la intimidad. las actividades realizadas con los dispositivos móviles institucionales o los activos de información institucionales

podrán ser monitoreadas siguiendo los procedimientos administrativos de la Gobernación de Santander o los definidos por la normatividad vigente.

8.3. Política para uso de conexiones remotas

La Gobernación de Santander establecerá las circunstancias y requisitos para el establecimiento de conexiones remotas a la plataforma tecnológica de la Entidad; así mismo, suministrará las herramientas y controles necesarios para que dichas conexiones se realicen de manera segura.

8.3.1. Normas para uso de conexiones remotas

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Aprobar las conexiones remotas a la plataforma tecnológica de la Gobernación de Santander en los formatos existentes.
-
- Implantar los métodos y controles de seguridad para establecer conexiones remotas hacia la plataforma tecnológica de la Gobernación de Santander.

- Restringir las conexiones remotas a los recursos de la plataforma tecnológica; únicamente se deben permitir estos accesos a personal autorizado y por periodos de tiempo establecidos, de acuerdo con las funciones desempeñadas.

- Monitorear los accesos de conexiones remotas a la plataforma tecnológica y alertar sobre potenciales amenazas internas y externas de acceso no autorizado a la información o recursos.

- Suministrar el soporte, mantenimiento y actualización del hardware y software empleado para realizar las conexiones remotas.

- Verificar la efectividad de los controles aplicados sobre las conexiones remotas a los recursos de la plataforma tecnológica de la Gobernación de Santander de manera permanente.

Normas dirigidas a: LA OFICINA DE CONTROL INTERNO

- Dentro de su autonomía y con el apoyo de la Secretaría de Tecnologías de la Información y las Comunicaciones, podrá realizar auditorías sobre los controles implantados para las conexiones remotas a la plataforma tecnológica de la Gobernación de Santander.

Normas dirigidas a: TODOS LOS USUARIOS

- Contar con las aprobaciones requeridas para establecer dicha conexión a los dispositivos de la plataforma tecnológica de la Gobernación de Santander y deben acatar las condiciones de uso establecidas para dichas conexiones.

- Los usuarios únicamente deben establecer conexiones remotas en computadores previamente identificados y, bajo ninguna circunstancia, en computadores públicos o de uso compartido, de hoteles o cafés internet, entre otros.

9. POLÍTICAS DE SEGURIDAD DEL PERSONAL

9.1. Política relacionada con la vinculación de servidores públicos

La Gobernación de Santander reconoce la importancia que tiene el talento humano para el cumplimiento de sus objetivos misionales y, con el interés de contar con el personal mejor calificado, garantizará que la vinculación de nuevos servidores públicos se realizará siguiendo un proceso formal de selección, acorde con la legislación vigente, el cual estará orientado a las funciones y roles que deben desempeñar los servidores públicos en sus cargos.

9.1.1. Normas relacionadas con la vinculación de servidores públicos

Normas dirigidas a: LA SECRETARIA GENERAL

- Realizar las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo en la Gobernación de Santander, antes de su vinculación definitiva.

- Certificar que los servidores públicos de la Gobernación de Santander firmen un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad Digital y Privacidad de la Información; estos documentos deben ser anexados a los demás documentos relacionados con la ocupación del cargo y los demás documentos que integrarán la hoja de vida institucional del servidor público.

Normas dirigidas a: LOS SUPERVISORES DE CONTRATO, ESTRUCTURADORES DE ESTUDIOS PREVIOS, SECRETARIOS, DIRECTORES Y JEFES DE OFICINA

- Asegurar la existencia de Acuerdos y/o Cláusulas de Confidencialidad y de la documentación de Aceptación de Políticas para el personal provisto por terceras partes, antes de otorgar acceso a la información de la Gobernación de Santander.

- Especificar las responsabilidades del personal propuesto por el proponente durante el proceso de contratación.

Normas dirigidas a: EL PERSONAL PROVISTO POR TERCERAS PARTES

- Firmar un Acuerdo y/o Cláusula de Confidencialidad y un documento de Aceptación de Políticas de Seguridad digital y Privacidad de la Información, antes de que se les otorgue acceso a las instalaciones y a la plataforma tecnológica.

- Garantizar el cumplimiento de los Acuerdos y/o Cláusulas de Confidencialidad y aceptación de las Políticas de Seguridad Digital y Privacidad de la Información de la Gobernación de Santander.

- Proveer el personal de acuerdo con los perfiles definidos en los contratos suscritos con la Gobernación de Santander.

9.2. Política aplicable durante la ejecución del empleo

La Gobernación de Santander en su interés por proteger su información, fomenta la cultura de la seguridad digital y la gestión de riesgos durante el desarrollo de las funciones de los servidores públicos, ejecutando jornadas de capacitación, sensibilización y promulgando la presente política.

Todos los servidores públicos de la Gobernación de Santander deben ser cuidadosos de no divulgar información confidencial en lugares públicos, en conversaciones o situaciones que pongan en riesgo la seguridad y el buen nombre de la Entidad.

9.2.1. Normas aplicables durante la vinculación de servidores públicos y personal provisto por terceros

Normas dirigidas a: LA ALTA DIRECCIÓN

- Promover el fortalecimiento de la cultura en seguridad digital para el uso adecuado de la información y así afianzar la confianza con los usuarios, servidores públicos y terceras partes.

Normas dirigidas a: LA DIRECCIÓN DE SISTEMAS INTEGRADOS DE GESTIÓN – SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Establecer los principios y lineamientos para promover la cultura de seguridad digital que incluye actividades de difusión, capacitación y concientización tanto al interior de la Entidad como frente a usuarios y terceros.

- Formular y coadyuvar en la ejecución y actualización del programa de capacitación, sensibilización y toma de conciencia en seguridad digital, políticas, procedimientos y controles de ingeniería social para los servidores públicos y contratistas.

Normas dirigidas a: LA SECRETARÍA GENERAL

- Aplicar las medidas administrativas de la Gobernación de Santander cuando se identifiquen violaciones o incumplimientos a las políticas de seguridad digital.

- Convocar a los servidores públicos, temporales y contratistas, a capacitaciones y eventos programados como parte del programa de sensibilización en seguridad digital.

- Proveer los recursos para la ejecución de las capacitaciones y llevar el registro de la asistencia a dichas capacitaciones y eventos, y tomar las acciones correctivas por la falta de asistencia no justificada.

Normas dirigidas a: TODOS LOS USUARIOS

- Cumplir con las políticas y controles de seguridad, de acuerdo con la normatividad vigente, aplicable a la Gobernación de Santander.

- Asistir a las capacitaciones y jornadas de educación y formación que programe la Gobernación de Santander en materia de seguridad digital con el fin de adquirir las competencias necesarias para el debido manejo de la información.

9.3. Política de desvinculación, permisos, licencias, vacaciones o cambio de funciones de los servidores públicos y personal provisto por terceros

La Gobernación de Santander asegurará que sus servidores públicos y el personal provisto por terceros serán desvinculados o reasignados para la ejecución de nuevas funciones de una forma ordenada, controlada y segura.

9.3.1. Normas para la desvinculación, permisos, licencias, vacaciones o cambios de funciones de los servidores públicos y personal provisto por terceros

Normas dirigidas a: LASECRETARÍA GENERAL

- Realizar el proceso de desvinculación, licencias, vacaciones o cambio de funciones de los servidores públicos de la Gobernación de Santander llevando a cabo los procedimientos y ejecutando los controles establecidos para tal fin.

Normas dirigidas a: LOS SUPERVISORES DE CONTRATO, SECRETARIOS, DIRECTORES Y JEFES DE OFICINA

- Monitorear y reportar de manera inmediata la desvinculación o cambio de funciones de los servidores públicos o personal provisto por terceras partes.

10. POLÍTICAS DE GESTIÓN DE ACTIVOS DE INFORMACIÓN

10.1. Política de responsabilidad por los activos de información

La Gobernación de Santander como propietario de la información física, así como de la información generada, procesada, almacenada y transmitida con su plataforma tecnológica, otorgará responsabilidad a las áreas sobre sus activos de información, asegurando el cumplimiento de las directrices que regulen el uso adecuado de la misma.

La información, archivos físicos, los sistemas, los servicios y los equipos (ej. estaciones de trabajo, equipos portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos y fases, entre otros) son propiedad de la Gobernación de Santander y se proporcionan a los servidores públicos y terceros autorizados, para cumplir con los propósitos de la Entidad.

Toda la información sensible de la Gobernación de Santander, así como los activos donde estos se almacenan y se procesan deben ser asignados a un responsable, inventariados y posteriormente clasificados, de acuerdo con los requerimientos y los criterios que determine la Entidad.

10.1.1. Normas de responsabilidad por los activos de información

Normas dirigidas a: LOS PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

Secretarios de Despacho, directores, Jefes de Oficina y Coordinadores de Grupos de la Gobernación de Santander, deben actuar como propietarios de la información física y electrónica de la Entidad, para lo cual deben:

- Designar, autorizar o revocar el acceso a la información y a los recursos tecnológicos.
- Recibir los recursos tecnológicos asignados a sus colaboradores cuando estos se retiran de la Gobernación de Santander o son trasladados de área.
- Generar un inventario de dichos activos para los procesos que lideran, acogiendo las indicaciones de las Guía para la Clasificación de Activos de Información, así mismo, deben mantenerlo actualizado.
- Monitorear periódicamente la validez de los usuarios y sus perfiles de acceso a la información.
- Ser conscientes que los recursos de procesamiento de información de la Gobernación de Santander, se encuentran sujetos a auditorías por parte de la Oficina de Control Interno y a revisiones de cumplimiento por parte de la Dirección de Sistemas Integrados de Gestión.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Es la propietaria de los activos de información correspondientes a la plataforma tecnológica de la Gobernación de Santander y, en consecuencia, debe asegurar su apropiada operación y administración.

- Autoriza la instalación, cambio o eliminación de componentes de la plataforma tecnológica de la Gobernación de Santander.

- Establecer, operar y mantener las configuraciones adecuadas para los recursos tecnológicos, con el fin de preservar la seguridad digital y hacer un uso adecuado de ellos.

- Preparar las estaciones de trabajo fijas y/o portátiles de los servidores públicos y de hacer entrega de las mismas.

- Recibir los equipos de cómputo para su reasignación o disposición final, y generar copias de seguridad digital de la información de los servidores públicos que se retiran o cambian de funciones, cuando le es formalmente notificado.

Normas dirigidas a: EL RESPONSABLE DE LA SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN – LA DIRECCIÓN DE SISTEMAS INTEGRADOS DE GESTIÓN

- Realizar un análisis de riesgos de seguridad digital de manera periódica, sobre los procesos de la Gobernación de Santander.

- Definir las condiciones de uso y protección de los activos de información, tanto los tecnológicos como aquellos que no lo son.

- Realizar revisiones periódicas de los recursos de la plataforma tecnológica y los sistemas de información de la Gobernación de Santander.

Normas dirigidas a: SECRETARIOS, DIRECTORES, JEFES DE OFICINA Y COORDINADORES DE GRUPOS

- Los Secretarios, Directores, Jefes de Oficina y Coordinadores de Grupos, o quien ellos designen, deben autorizar a sus servidores públicos el uso de los recursos tecnológicos, previamente preparados por la Secretaría de Tecnologías de la Información y las Comunicaciones.

Normas dirigidas a: TODOS LOS USUARIOS

- Los recursos tecnológicos de la Gobernación de Santander provistos a servidores públicos y personal suministrado por terceras partes, tienen como único fin llevar a

cabo las funciones de la Entidad; por consiguiente, no deben ser utilizados para fines personales o ajenos a este.

- La utilización de equipos fijos o móviles o software de propiedad personal para realizar funciones propias de la Gobernación de Santander, será de exclusiva responsabilidad del servidor público el cual deberá gestionar la debida autorización para acceder a los servicios tecnológicos de la Entidad mediante el mecanismo establecido para tal fin por la Secretaría de Tecnologías de la Información y las Comunicaciones.

- Hacer uso adecuado y eficiente de los recursos tecnológicos para el cumplimiento de las funciones asignadas.

- En el momento de desvinculación o cambio de funciones, los servidores públicos deben realizar la entrega de su puesto de trabajo a el Secretario, Director, Jefe de Oficina o Coordinador de Grupo o quien este delegue; así mismo, deben encontrarse a paz y salvo con la entrega de los recursos tecnológicos y otros activos de información suministrados en el momento de su vinculación.

10.2. Política de clasificación y manejo de la información

La Gobernación de Santander definirá los niveles más adecuados para clasificar su información de acuerdo con su sensibilidad, y generará una Guía de Clasificación de los Activos de Información para que los propietarios de la misma la cataloguen y determinen los controles requeridos para su protección.

Toda la información de la Gobernación de Santander debe ser identificada, clasificada y documentada de acuerdo con las guías de Clasificación de la Información establecidas por el Comité de Seguridad de la Información.

Una vez clasificada la información, la Gobernación de Santander proporcionará los recursos necesarios para la aplicación de controles en busca de preservar la confidencialidad, integridad y disponibilidad de la misma, con el fin de promover el uso adecuado por parte de los servidores públicos y personal provisto por terceras partes que se encuentre autorizado y requiera de ella para la ejecución de sus actividades.

10.2.1. Normas para la clasificación y manejo de la información

Normas dirigidas a: EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- Recomendar los niveles de clasificación de la información propuestos con el apoyo de la Dirección de Sistemas Integrados de Gestión y la Guía de Clasificación de los Activos de Información de la Gobernación de Santander para que sean aprobados por el Comité Institucional de Gestión y Desempeño.

Normas dirigidas a: EL RESPONSABLE DE LA SEGURIDAD DIGITAL – LA DIRECCIÓN DE SISTEMAS INTEGRADOS DE GESTIÓN – EL GRUPO DE GESTIÓN DOCUMENTAL

- Definir los niveles de clasificación de la información para la Gobernación de Santander, de acuerdo con los lineamientos normativos.

- Socializar y divulgar la Guía de Clasificación de los Activos de Información a toda la Entidad.

- Monitorear con una periodicidad establecida la aplicación de la Guía de Clasificación de los Activos de Información.

- Asesorar en el inventario y clasificación de los activos de información de la Gobernación de Santander a las diferentes dependencias.

- Consolidar el Inventario y Clasificación de Activos de Información y asegurar su aprobación y publicación en el Portal Web – Ley de Transparencia.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Proveer, ejecutar y monitorear los controles técnicos establecidos en la Guía de Clasificación de los Activos de Información y normas legales de acuerdo con la clasificación de la información.

- Administrar el almacenamiento, respaldo, resguardo y pruebas de las cintas de Backus y otros medios de almacenamiento.

- Administrar el almacenamiento y resguardo de los documentos físicos de la Entidad.

Normas dirigidas a: EL RESPONSABLE DE LA SEGURIDAD DIGITAL – LA DIRECCIÓN DE SISTEMAS INTEGRADOS DE GESTIÓN

- Asesorar en la definición de los controles de acuerdo con el nivel de clasificación de los activos de información.

Normas dirigidas a: EL GRUPO DE GESTIÓN DOCUMENTAL

- Utilizar los medios de los cuales está dotada para realizar adecuadamente la disposición final de la documentación física y electrónica con base en lo establecido y dispuesto en las Tablas de Retención Documental de la Gobernación de Santander, con el fin de evitar la reconstrucción de la misma, acogiéndose a procedimiento establecido para tal fin.

- La información física y electrónica de la Gobernación de Santander debe tener un período de almacenamiento que puede ser dictaminado por requerimientos legales o misionales; este período debe ser indicado en las tablas de retención documental y cuando se cumpla su período de retención, debe aplicarse su disposición final de acuerdo con la normatividad aplicable.

- La Coordinación de Archivo debe administrar el contrato de almacenamiento y resguardo de las cintas de Backus, otros medios de almacenamiento y documentos físicos de la Gobernación de Santander con el proveedor del servicio.

- Administrar el almacenamiento y resguardo de los documentos físicos y electrónicos de archivo de la Gobernación de Santander.

Normas dirigidas a: EL PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Con el apoyo del grupo de gestión documental y el responsable de la seguridad digital, generar un inventario de activos de información para los procesos que lideran, así como la clasificación de acuerdo con la Guía para la clasificación de los Activos de Información establecida, la cual está basada en las Tablas de Retención Documental de la Gobernación de Santander.

- Ejecutar y monitorear los controles de resguardo de la información de acuerdo con la Guía para el manejo de los activos información.

Normas dirigidas a: TODOS LOS USUARIOS (SERVIDORES PÚBLICOS Y PERSONAL PROVISTO POR TERCERAS PARTES)

- Acatar los lineamientos Guía de Clasificación de Activos de Información para el acceso, divulgación, almacenamiento, copia, transmisión, etiquetado y eliminación de la información contenida en los recursos tecnológicos, así como de la información física de la Gobernación de Santander.

- Impedir el acceso no autorizado a información impresa, digitalizada o almacenada en puestos de trabajo cuando quedan desatendidos.

- Mantener los puestos trabajos libres de documentos y medios de almacenamiento utilizados para el desempeño de las funciones cuando se finaliza la jornada laboral.

- Aplicar los controles de seguridad definidos por la Entidad para la preservación de la confidencialidad, integridad y disponibilidad de los activos de información tanto en estaciones de trabajo como en ambientes de procesamientos en nube de datos.

- Los usuarios deben tener en cuenta estas consideraciones cuando impriman, escaneen, saquen copias y envíes faxes: verificar las áreas adyacentes a impresoras, escáneres, fotocopiadoras y máquinas de fax para asegurarse que no quedaron documentos relacionados o adicionales; así mismo, recoger de las

impresoras, escáneres, fotocopiadoras y máquinas de fax, inmediatamente los documentos confidenciales para evitar su divulgación no autorizada.

10.3. Política para uso de tokens de seguridad

La Gobernación de Santander proveerá las condiciones de manejo de los tokens de seguridad para los procesos que los utilizan y velará porque los servidores públicos hagan un uso responsable de estos.

10.3.1. Normas para uso de tokens de seguridad

Normas dirigidas a: LAS ÁREAS USUARIAS DE TOKENS DE SEGURIDAD

- Cada área usuaria de tokens de seguridad debe asignar un funcionario administrador de los mismos con la potestad para autorizar las solicitudes de acceso.

Normas dirigidas a: LOS ADMINISTRADORES DE LOS TOKENS DE SEGURIDAD

- Procesar las solicitudes de dichos tokens según los requerimientos de cada Entidad proveedora de éstos y adjuntar la documentación necesaria.
- Recibir los tokens y realizar la activación necesaria en los respectivos portales o sitios de uso para poder realizar operaciones por medio de ellos.
- Crear los usuarios y perfiles en cada portal o sitio de uso, según las actividades a realizar por cada funcionario creado.
- Entregar a los servidores públicos designados los usuarios y seriales de los dispositivos que le son asignados para su uso, formalizando la entrega por medio de acta y tula (o sobre) de seguridad para custodia de los mismos.
- Avisar a las Entidades emisoras en caso de robo o pérdida de estos con el fin de efectuar el bloqueo respectivo y la reposición de los mismos.
- Realizar el cambio de estos, cuando se presente mal funcionamiento, caducidad, cambio de funciones o cambio del titular, reportando a la entidad emisora y devolviendo los dispositivos asignados.

Normas dirigidas a: LOS USUARIOS DE TOKENS DE SEGURIDAD

- Contar con una cuenta de usuario en los portales o sitios de uso de los mismos; dichos tokens harán parte del inventario físico de cada usuario a quien se haya asignado.

- Devolver el token asignado en estado operativo al administrador de los tokens cuando el vínculo laboral con la Gobernación de Santander se dé por terminado o haya cambio de cargo, para obtener la paz y salvo, el cual será requerido para legalizar la finalización del vínculo con la entidad.

- Cada usuario de los portales o sitios de uso de los tokens debe tener su propio dispositivo, el cual es exclusivo, personal e intransferible, al igual que la cuenta de usuario y la contraseña de acceso.

- El almacenamiento de los tokens debe efectuarse bajo estrictas medidas de seguridad, en la tula o sobre asignado para cada token, dentro de caja fuerte o escritorios con llave al interior de las áreas usuarias, de tal forma que se mantengan fuera del alcance de terceros no autorizados.

- Prevenir su daño por contacto con líquidos, sustancias químicas, fuego o agentes que los puedan dañar (polvo, fuentes de calor extremo, campos magnéticos fuertes, etc.

- No realizar modificaciones físicas al dispositivo como cambio de baterías, apertura, grabación o borrado de datos.

- Los usuarios deben responder por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como servidores públicos de la Gobernación de Santander. En caso de que suceda algún evento irregular con los tokens los usuarios deben asumir la responsabilidad administrativa, disciplinaria y económica.

- Almacenar de manera segura el token mientras no está en uso o cuando está desatendido el puesto de trabajo.

- Notificar al administrador de los tokens en caso de robo, pérdida, mal funcionamiento o caducidad para que este a su vez, se comuniquen con las entidades emisoras de dichos tokens.

- Mantener en secreto las claves de uso del token. Utilizar servicios de soporte únicamente de personal autorizado por los administradores de los tokens.

- Asumir la responsabilidad por las transacciones electrónicas que se efectúen con la cuenta de usuario, clave y el token asignado, en el desarrollo de las actividades como servidores públicos de la Gobernación de Santander.

- Asumir la responsabilidad administrativa, disciplinaria y económica en caso de uso no autorizado o irregularidad con los tokens asignados.

10.4. Política de uso de periféricos y medios de almacenamiento

El uso de periféricos y medios de almacenamiento en los recursos de la plataforma tecnológica de la Gobernación de Santander será reglamentado por la Secretaría de Tecnologías de la Información y las Comunicaciones, considerando las funciones realizadas por los servidores públicos y su necesidad de uso.

10.4.1. Normas uso de periféricos y medios de almacenamiento

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Implantar los controles que regulen el uso de periféricos y medios de almacenamiento en la plataforma tecnológica de la Gobernación de Santander, de acuerdo con los lineamientos y condiciones establecidas.

- Monitorear el uso de periféricos y medios de almacenamiento en la plataforma tecnológica y las estaciones de trabajo de la Gobernación de Santander.

- Mantener el inventario de servidores públicos y personal provisto por terceros autorizados y habilitados para dar uso de dispositivos de almacenamiento con sus respectivos soportes.

- Generar los lineamientos para el uso de los medios de almacenamiento de la Entidad, ya sea cuando son dados de baja o reasignados a un nuevo usuario.

- Autorizar y mantener actualizado los derechos de uso de periféricos o medios de almacenamiento en la plataforma tecnológica de la entidad de acuerdo con el perfil del cargo del funcionario solicitante.

Normas dirigidas a: LOS SECRETARIOS, DIRECTORES, JEFES DE OFICINA Y COORDINADORES DE GRUPOS

- Realizar el inventario de los dispositivos de almacenamiento removibles.

- Reportar al responsable de la seguridad digital y privacidad de la información, los usuarios del área a su cargo que tienen habilitados permisos para acceso a dispositivos de almacenamiento removibles en sus estaciones de trabajo.

Normas dirigidas a: TODOS LOS USUARIOS (SERVIDORES PÚBLICOS Y PERSONAL PROVISTOS POR TERCERAS PARTES)

- Cumplir las condiciones .de uso de los periféricos y medios de almacenamiento establecidos por el responsable de la seguridad digital y privacidad de la información.

- No modificar la configuración de periféricos y medios de almacenamiento establecidos por la Secretaría de Tecnologías de la Información y las Comunicaciones.

- Custodiar los medios de almacenamiento institucionales asignados.

- No utilizar medios de almacenamiento personales en la plataforma tecnológica de la Gobernación de Santander.

10.5. Política de borrado seguro

La Gobernación de Santander vela porque se realice borrado seguro en los dispositivos que contengan información pública reservada o pública clasificada, tanto para personal de planta, provisionalidad y contratistas, cuando se apliquen las siguientes acciones al dispositivo:

- Reasignar a otro servidor público.
- Enviar a bodega.
- Cambiar del dispositivo.
- Devolver por terminación de vínculo contractual.
- Reparar por parte del proveedor o un tercero.
- Regresar al proveedor por fin de contrato de suministro.
- En caso de hurto del dispositivo

10.5.1. Normas de política de borrado seguro

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

Definir el mecanismo de borrado o método de disposición final de acuerdo con el tipo de dispositivo, contemplando:

- Evidenciar del borrado o disposición final.

- Impedir la recuperación de la información del medio a través de controles de cifrado.

- Seleccionar de manera apropiada los servicios de borrado o destrucción por terceros en caso de contratación del servicio.

11. POLÍTICAS DE CONTROL DE ACCESO

La Gobernación de Santander en busca de garantizar un adecuado control de acceso a sus activos de información, ha definido las políticas para garantizar un adecuado control de acceso a los sistemas; para ello se implementan mecanismos de control para acceder a la red, sistemas operativos, bases de datos, sistemas de información y en general a todo elemento que de alguna forma acceda a información de carácter público reservado o publico clasificado, cuyo origen sea la Gobernación de Santander. De igual manera, implementa procedimientos para la asignación de privilegios de acceso a los sistemas.

El acceso a los sistemas de información y activos de información está determinado por el principio de mínimo privilegio necesario para el cumplimiento de las funciones asignadas a trabajadores de planta, provisionalidad y contratistas.

El acceso a la información contempla el establecimiento de permisos específicos para leer, escribir, modificar, borrar o ejecutar utilidades que procesen información institucional.

11.1. Política de acceso a redes y recursos de red

La Secretaría de Tecnologías de la Información y las Comunicaciones de la Gobernación de Santander, como responsable de las redes de datos y los recursos de red de la entidad, propende porque dichas redes sean debidamente protegidas contra accesos no autorizados a través de mecanismos de control de acceso lógico y físicos monitoreados y con capacidad de generar alertas.

11.1.1. Normas de acceso a redes y recursos de red

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Establecer el procedimiento y los controles de acceso a los ambientes de producción, pruebas y desarrollo de los sistemas de información, redes de datos y los recursos de red de la Gobernación de Santander.

- Asegurar que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

- Asegurar que las redes inalámbricas de la Gobernación de Santander cuenten con métodos de autenticación y cifrado que eviten accesos no autorizados.

- Asignar credenciales de acceso a los diferentes sistemas de forma separada, garantizando la segregación de tareas y limitando la autorización de acceso solo a la información indispensable para la ejecución de las funciones asignadas.

- Establecer en conjunto con el responsable de la seguridad digital y la dirección de Sistemas Integrados de Gestión, los controles para la identificación y autenticación

de los usuarios provistos por terceras partes en las redes o recursos de red de la Gobernación de Santander, así como velar por la aceptación de las responsabilidades sobre uso de activos, acuerdos de confidencialidad y las Políticas de Seguridad Digital y Privacidad de la Información.

- Monitorear, alertar y reportar actividades anómalas respecto al acceso y uso de los datos en los sistemas de información, redes de datos y los recursos de red de la Gobernación de Santander a los responsables de los procesos de dichos sistemas de información.

- La Secretaría de Tecnologías de la Información y las Comunicaciones con la solicitud de cuentas de usuario debidamente aprobada por el jefe de área a la cual pertenece el solicitante y la validación del responsable de la seguridad digital y privacidad de la información, debe crear, modificar, bloquear o eliminar cuentas de usuarios sobre las redes de datos, los recursos tecnológicos y los sistemas de información administrados, acorde con el procedimiento establecido.

- Configurar los equipos de cómputo de usuario final que se conecten o deseen conectarse a las redes de datos de la Gobernación de Santander para que cumplan con todos los requisitos o controles para autenticase en ellas.

Normas dirigidas a: LOS DESARROLLADORES (INTERNOS Y EXTERNOS)

- Los desarrolladores deben, a nivel de los aplicativos, restringir acceso a archivos de configuración u otros recursos, a direcciones URL protegidas, a funciones protegidas, a credenciales, a servicios, a información de las aplicaciones, a atributos y políticas utilizadas por los controles de acceso y a la información relevante de la configuración, solamente a usuarios autorizados.

Normas dirigidas a: EL RESPONSABLE DE LA SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

- Validar la creación o modificación de las cuentas de acceso a las redes o recursos de red de la Gobernación de Santander.

Normas dirigidas a: LOS SECRETARIOS, JEFES DE OFICINAS, DIRECTORES, Y COORDINADORES DE GRUPOS

- Solicitar la creación, modificación, bloqueo y eliminación de cuentas de usuario, para los servidores públicos que laboran en sus áreas, acogiéndose al procedimiento establecido para tal fin.

Normas dirigidas a: TODOS LOS USUARIOS

- Diligenciar el formato de creación de cuentas de usuario y realizar los trámites de solicitud antes de contar con acceso lógico por primera vez a la red de datos de la Gobernación de Santander.

- Informar oportunamente a la Secretaría de Tecnologías de la Información y las Comunicaciones y al Líder de Proceso sobre cualquier inconveniente, ya sea por exceso o falta de permisos, para acceder a la información.

- Utilizar las redes y servicios de comunicación de la Gobernación de Santander únicamente para el cumplimiento de las funciones asignadas evitando usos no autorizados o en beneficio propio.

11.2. Política de administración de acceso de usuarios

La Gobernación de Santander establecerá privilegios para el control de acceso lógico de cada usuario o grupo de usuarios a las redes de datos, los recursos tecnológicos y los sistemas de información de la entidad. Así mismo, velará porque los servidores públicos y el personal provisto por terceras partes tengan acceso únicamente a la información necesaria para el desarrollo de sus funciones y porque la asignación de los derechos de acceso esté regulada por normas y procedimientos establecidos para tal fin.

11.2.1. Normas de administración de acceso de usuarios

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Establecer un procedimiento formal para la administración de los usuarios en las redes de datos, los recursos tecnológicos y sistemas de información de la entidad, que contemple la creación, modificación, bloqueo o eliminación de las cuentas de usuario.

- Verificar periódicamente los controles de acceso de los usuarios, con el fin de revisar que éstos tengan acceso permitido únicamente a aquellos recursos de red y servicios de las plataformas tecnológicas para los que fueron autorizados.

Normas dirigidas a: OFICIAL DE SEGURIDAD DIGITAL

- Solicitar periódicamente a la Secretaría de Tecnologías de la Información y las Comunicaciones los registros y seguimientos a las actividades sobre los sistemas de información por parte de usuarios con permisos elevados (administrador, root, etc.), para analizarlos y de esta forma, analizar los riesgos a los que se están exponiendo los sistemas de información y recursos de red de la Gobernación de Santander, con las actividades de dichos usuarios.

- Revisar periódicamente los controles de acceso a los recursos tecnológicos y sistemas de información con el fin de verificar que los usuarios tengan acceso permitido únicamente a aquellos recursos de red y servicios de las plataformas tecnológicas para los que fueron autorizados.

11.3. Política de responsabilidades de acceso de los usuarios

Los usuarios de los recursos tecnológicos y los sistemas de información de la Gobernación de Santander realizarán un uso adecuado y responsable de dichos recursos y sistemas, salvaguardando la información a la cual les es permitido el acceso.

11.3.1. Normas de responsabilidades de acceso de los usuarios

Normas dirigidas a: TODOS LOS USUARIOS

- Los usuarios de la plataforma tecnológica, los servicios de red y los sistemas de información de la Gobernación de Santander deben hacerse responsables de las acciones realizadas en los mismos, así como del usuario y contraseña asignados para el acceso a estos.

- Los servidores públicos no deben compartir sus cuentas de usuario y contraseñas con otros servidores públicos o con personal provisto por terceras partes.

- Los servidores públicos y personal provisto por terceras partes que posean acceso a la plataforma tecnológica, los servicios de red y los sistemas de información de la entidad deben acogerse a lineamientos para la configuración de contraseñas implantados por la entidad.

- Utilizar las cuentas de usuario únicamente para el desarrollo de las funciones asignadas.

- Informar oportunamente a la Secretaría de Tecnologías de la Información y las Comunicaciones y al Líder de Proceso sobre cualquier inconveniente con los accesos de usuario, ya sea por exceso o falta de permisos, para acceder a la información.

11.4. Política de uso de altos privilegios y utilitarios de administración

La Secretaría de Tecnologías de la Información y las Comunicaciones de la Gobernación de Santander velará porque los recursos de la plataforma tecnológica y los servicios de red de la entidad sean operados y administrados en condiciones controladas y de seguridad, implementando y operando los controles para el monitoreo, alerta temprana y automática de actividades de los usuarios administradores, poseedores de los más altos privilegios sobre la plataforma tecnológica y servicios.

11.4.1. Normas de uso de altos privilegios y utilitarios de administración

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, LOS ADMINISTRADORES DE LOS RECURSOS TECNOLÓGICOS Y SERVICIOS DE RED

- Otorgar los privilegios para administración de recursos tecnológicos, servicios de red y sistemas de información sólo a aquellos servidores públicos designados para dichas funciones.

- Establecer cuentas personalizadas con altos privilegios para cada uno de los administradores de los recursos tecnológicos, servicios de red y sistemas de información.

- Verificar y asegurar que los administradores de los recursos tecnológicos y servicios de red no tengan acceso a sistemas de información en producción.

- Restringir las conexiones remotas a los recursos de la plataforma tecnológica solo a personal debidamente autorizado y solo para las funciones asignadas.

- Implementar líneas bases de aseguramiento a los sistemas de información y tecnologías, de acuerdo con la arquitectura definida para cada para los mismos.

- Establecer los controles para que los usuarios finales de los recursos tecnológicos, los servicios de red y los sistemas de información no tengan instalados en sus equipos de cómputo utilitarios que permitan accesos privilegiados a dichos recursos, servicios o sistemas.

- Generar y mantener actualizado un listado de las cuentas administrativas de los recursos de la plataforma tecnológica.

- Validar que las políticas de contraseñas establecidas sobre la plataforma tecnológica, los servicios de red y los sistemas de información son aplicables a los usuarios administradores; así mismo, debe verificar que el cambio de contraseña de los usuarios administradores acoja el procedimiento definido para tal fin.

- Revisar periódicamente la actividad de los usuarios con altos privilegios en los registros de auditoría de la plataforma tecnológica y los sistemas de información.

Normas dirigidas a: TODOS LOS USUARIOS

- No utilizar herramientas o software que permitan evadir los controles de seguridad de los recursos tecnológicos y servicios de red.

11.5. Política de control de acceso a sistemas de información y aplicativos

La Gobernación de Santander vela porque todos los usuarios se identifiquen en los sistemas de información y recursos tecnológicos, se autentiquen con credenciales únicas y las autorizaciones se otorguen conforme a los niveles de acceso a la información. Se registran los accesos exitosos y fallidos a los sistemas de información y tecnologías con el fin de identificar y alertar posibles amenazas de accesos y cambios no autorizados.

11.5.1. Normas de control de acceso a sistemas y aplicativos

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Establecer ambientes separados a nivel físico y lógico para desarrollo, pruebas y producción, contando cada uno con su plataforma, servidores, aplicaciones, dispositivos y versiones independientes de los otros ambientes, evitando que las actividades de desarrollo y pruebas puedan poner en riesgo la integridad de la información de producción.

- Asegurar que los usuarios utilicen diferentes perfiles para los ambientes de desarrollo, pruebas y producción.

- Establecer el procedimiento y los controles de acceso a los ambientes de producción de los sistemas de información.

- Asegurar que los desarrolladores internos o externos, posean acceso limitado y controlado a los datos y archivos que se encuentren en los ambientes de producción.

- Controlar el acceso al código fuente de los programas, sistemas de información o software desarrollado por la Gobernación de Santander solo al personal autorizado y llevar control de los cambios autorizados a código fuente.

- Definir en conjunto con la dirección de Sistemas de Información los lineamientos para la configuración de contraseñas que se apliquen sobre la plataforma tecnológica, los servicios de red y los sistemas de información de la Gobernación de Santander, incluyendo longitud, complejidad, cambio periódico, control histórico, bloqueo por número de intentos fallidos en la autenticación y cambio de contraseña en el primer acceso además de otros definidos en buenas prácticas o identificados por la Gobernación de Santander.

Normas dirigidas a: LOS DESARROLLADORES (INTERNOS Y EXTERNOS)

- Asegurar que los sistemas de información construidos exijan autenticación para todos los recursos y operaciones ejecutadas con el software.

- Certificar que no se almacenen contraseñas, cadenas de conexión u otra información pública clasificada y pública restringida en texto claro y que se implementen controles de integridad de dichas contraseñas.

- Establecer los controles de autenticación que eviten la visualización de contraseñas.

- Desarrollar el software siguiendo estándares de desarrollo seguro.

- Implementar en el software controles que eviten múltiples intentos de autenticación fallida.

- Implementar en el software controles que obliguen al usuario a cambiar la contraseña por defecto en el primer ingreso.

Normas dirigidas a: LOS SECRETARIOS, DIRECTORES, JEFES DE OFICINA Y COORDINADORES DE GRUPO

- Definir los perfiles de usuario a los sistemas de información, de manera conjunta con la Secretaría de Tecnologías de la Información y las Comunicaciones.

- Velar por la asignación controlada de privilegios de acceso, modificación, revocación a los sistemas de información bajo su responsabilidad.

- Monitorear periódicamente los perfiles definidos en los sistemas de información bajo su responsabilidad y los privilegios asignados a los usuarios que acceden a ellos.

- Verificar y ratificar semestralmente todas las autorizaciones sobre sus recursos tecnológicos.

12. POLÍTICA DE TELETRABAJO

La Gobernación de Santander garantizará la seguridad digital cuando se haga uso de los recursos tecnológicos y activos de información, autorizadas por la Gobernación de Santander para el desarrollo de las actividades de teletrabajo realizadas según lo establecido en la Ley 1221 de 2008, Decreto 884 de 2012 y demás normas que las adicione, compile, modifique o sustituya.

La Gobernación de Santander realizará un análisis de riesgos que permite identificar, proteger y proporcionar los mecanismos de control adecuados para la protección de sus activos de información cuando se autorizan actividades de teletrabajo.

Antes de realizar cualquier actividad de teletrabajo, la Gobernación de Santander definirá con la Alta Dirección, el alcance de las actividades a desarrollar estableciendo como mínimo, el horario, los activos de información a acceder, los sistemas de información y los servicios requeridos para el desarrollo de las actividades de teletrabajo.

13. POLÍTICAS DE CRIPTOGRAFÍA

La Gobernación de Santander velará por proteger la información pública clasificada y pública reservada mediante mecanismos de cifrado al momento de ser transferida o transmitida a terceras partes. Las claves de acceso a sistemas de información y sistemas operacionales se almacenan en forma cifrada para preservar su confidencialidad.

13.1. Política de controles criptográficos

La Gobernación de Santander velará porque la información de la entidad, clasificada como reservada o restringida, será cifrada al momento de almacenarse y/o transmitirse por cualquier medio.

13.1.1. Normas de controles criptográficos

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Almacenar, transferir y/o transmitir la información digital calificada como clasificada y reservada, por el dueño de la información, bajo técnicas de cifrado fuerte con el propósito de proteger su confidencialidad e integridad.

- Aplicar con base en buenas prácticas de la industria mecanismos de verificación de integridad de la información con herramientas de cifrado.

- Mantener activos y documentados los controles sobre el ciclo de vida de las llaves criptográficas incluidas la generación, almacenamiento, archivo, recuperación, distribución, retiro y destrucción de las mismas.

- Verificar que las llaves de cifrado solo puedan ser utilizadas para una sola función, (firma electrónica o cifrado de datos, autenticación, etc.), nunca para varias funciones o sean reutilizadas. Como caso especial, se acepta el uso de la misma llave de cifrado para elementos que ofrecen más de un servicio criptográfico, por ejemplo: una llave de firma digital puede ser utilizada, para tener integridad, autenticidad y no repudio.

- Definir la vigencia durante la cual son válidas las llaves criptográficas fechas, periodo después del cual son desactivadas.

- En los casos en los que existan solicitudes de entes de control, organismos de seguridad del Estado u órdenes judiciales, la información cifrada puede ser puesta a disposición en forma no cifrada previa autorización del comité de seguridad de la información y el líder y/o oficial de seguridad digital.

- Definir las directrices y herramientas de software que se utilizarán para implementar técnicas de cifrado de información en los desarrollos de software.

- Autorizar el uso de herramientas de cifrado en los desarrollos de software cuando han sido aprobados por estándares conocidos de la industria.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Verificar que las normas sobre controles criptográficos se ejecuten y apliquen adecuadamente con frecuencia anual.

14. POLÍTICAS DE SEGURIDAD FISICA Y MEDIOAMBIENTAL

14.1. Política de áreas seguras

La Gobernación de Santander proveerá la implementación y velará por la efectividad de los mecanismos de seguridad física y control de acceso que aseguren el perímetro de sus instalaciones en todas sus sedes. Así mismo, controlará las amenazas físicas externas e internas y las condiciones medioambientales de sus oficinas.

Todas las áreas destinadas al procesamiento o almacenamiento de información sensible, así como aquellas en las que se encuentren los equipos y demás infraestructura de soporte a los sistemas de información y comunicaciones, se consideran áreas de acceso restringido.

Se considera áreas restringidas las siguientes: Tesorería, Oficina de Control Interno, Centros de Cómputo, Centro de Cableado, Centro de Monitoreo y Vigilancia, Archivo y Gestión Documental, Contratación, Recursos Físicos – Bodega, Despacho del Gobernador.

14.1.1. Normas de áreas seguras

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Autorizar y gestionar el acompañamiento permanente de los visitantes a las áreas de procesamiento de información y centros de comunicaciones.

- Registrar el ingreso de los visitantes al centro de cómputo y a los centros de cableado que están bajo su custodia, en una bitácora ubicada en la entrada de estos lugares de forma visible.

- Descontinuar o modificar de manera inmediata los privilegios de acceso físico al centro de cómputo y los centros de cableado que están bajo su custodia, en los eventos de desvinculación o cambio en las funciones de un funcionario autorizado.

- Proveer las condiciones físicas y medioambientales necesarias para garantizar la protección y correcta operación de los recursos de la plataforma tecnológica

ubicados en el centro de cómputo, que deben ser monitoreados de manera permanente.

- Propender en conjunto con la Coordinación de Recursos Físicos, que las áreas de carga y descarga de equipos de cómputo se encuentren aisladas del centro de cómputo y otras áreas de procesamiento de información.

Normas dirigidas a: LOS SECRETARIOS, DIRECTORES, JEFES DE OFICINA Y COORDINADORES DE GRUPO

- Velar mediante monitoreo por la efectividad de los controles de acceso físico y equipos de vigilancia implantados en su área.

- Autorizar los ingresos temporales a sus áreas, evaluando la pertinencia del ingreso; y definir los responsables del registro y supervisión de los ingresos autorizados a sus áreas.
- Velar porque las contraseñas de sistemas de alarma, cajas fuertes, llaves y otros mecanismos de seguridad de acceso a sus áreas solo sean utilizados por los servidores públicos autorizados y, salvo situaciones de emergencia u otro tipo de eventos que por su naturaleza lo requieran, estos no sean transferidos a otros servidores públicos de la entidad.

Normas dirigidas a: LA SECRETARÍA GENERAL

- Proporcionar los recursos necesarios para ayudar a proteger, regular y velar por el perfecto estado de los controles físicos implantados en las instalaciones de la Gobernación de Santander.

- Identificar mejoras a los mecanismos implantados y, de ser necesario, la implementación de nuevos mecanismos, con el fin de proveer la seguridad física de las instalaciones de la entidad.

- Almacenar y custodiar los registros del sistema de control de acceso a las instalaciones de la Gobernación de Santander.

- Asegurar la efectividad de los mecanismos de seguridad física y control de acceso al centro de cómputo, centros de cableado y demás áreas de procesamiento de información o carga y despacho.

- Verificar que los centros de cableado que están bajo su custodia, se encuentren separados de áreas que tengan líquidos inflamables o que corran riesgo de inundaciones e incendios.

- Controlar el acceso a las áreas del despacho del gobernador e implementar mecanismos que permitan la separación de éstas, de las áreas de almacenamiento o procesamiento de información.

- Verificar que el cableado se encuentra protegido con el fin de disminuir las intercepciones o daños.

- Asegurar que las funciones de mantenimiento de redes eléctricas, de voz y de datos, sean realizadas por personal idóneo y apropiadamente autorizado e identificado; así mismo, se debe llevar control de la programación de los mantenimientos preventivos.

Normas dirigidas a: TODOS LOS USUARIOS (SERVIDORES PÚBLICOS Y PERSONAL PROVISTO POR TERCERAS PARTES)

- Los ingresos y salidas del personal de la Gobernación de Santander deben ser registrados; por consiguiente, los servidores públicos y personal provisto por terceras partes deben cumplir completamente con los controles físicos implantados.

- Los servidores públicos deben portar el carnet que los identifica como tal, en un lugar visible mientras se encuentren en las instalaciones de la entidad; en caso de pérdida del carnet de acceso a las instalaciones, deben reportarlo a la mayor brevedad posible.

- Aquellos servidores públicos o personal provisto por terceras partes para los que aplique, en razón del servicio prestado, deben utilizar prendas distintivas que faciliten su identificación.

- Los servidores públicos de la Gobernación de Santander y el personal provisto por terceras partes, no deben intentar ingresar a áreas a las cuales no tengan autorización.

14.2. Política de seguridad para los equipos institucionales

La Gobernación de Santander para evitar la pérdida, robo o exposición al peligro de los recursos de la plataforma tecnológica de la entidad que se encuentren dentro o fuera de sus instalaciones, proveerá los recursos que garanticen la mitigación de riesgos sobre dicha plataforma tecnológica.

14.2.1. Normas de seguridad para los equipos institucionales

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Proveer los mecanismos y estrategias necesarios para proteger la confidencialidad, integridad y disponibilidad de los recursos tecnológicos, dentro y fuera de las instalaciones de la Gobernación de Santander.

- Generar y aplicar estándares de configuración segura para los equipos de cómputo de los servidores públicos de la Gobernación de Santander y configurar dichos equipos acogiendo los estándares generados.

- Establecer las condiciones que deben cumplir los equipos de cómputo de personal provisto por terceros, que requieran conectarse a la red de datos de la entidad y verificar el cumplimiento de dichas condiciones antes de conceder a estos equipos acceso a los servicios de red.

- Aislar los equipos de áreas sensibles, como Tesorería para proteger su acceso de los demás usuarios de la red de la Gobernación de Santander.

Normas dirigidas a: EL RESPONSABLE DE LA SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

- Debe evaluar y analizar los informes de verificación de equipos de cómputo de las diferentes áreas de la Gobernación de Santander, en particular de las áreas sensibles.

Normas dirigidas a: LA SECRETARIA GENERAL

- Revisar los accesos físicos en horas no hábiles a las áreas donde se procesa información.

- Restringir el acceso físico a los equipos de cómputo de áreas donde se procesa información sensible.

- Velar porque la entrada y salida de estaciones de trabajo, servidores, equipos portátiles y demás recursos tecnológicos institucionales de las instalaciones de la Gobernación de Santander cuenten con la autorización documentada y aprobada.

- Velar porque los equipos que se encuentran sujetos a traslados físicos fuera de la Gobernación de Santander, cuenten con un seguro suministrado por una aseguradora debidamente registrada y acreditada en Colombia.

Normas dirigidas a: TODOS LOS USUARIOS

- La Secretaría de Tecnologías de la Información y las Comunicaciones es la única área autorizada para realizar movimientos y asignaciones de recursos tecnológicos; por consiguiente, se encuentra prohibida la disposición indebida que pueda hacer cualquier servidor público de los recursos tecnológicos de la entidad.

- Las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos asignados a los servidores públicos y personal provisto por terceras partes deben acoger las instrucciones técnicas que proporcione la Secretaría de Tecnologías de la Información y las Comunicaciones.

- Cuando se presente una falla o problema de hardware o software en una estación de trabajo u otro recurso tecnológico propiedad de la Gobernación de Santander, el usuario responsable debe informar a la Mesa de Ayuda en donde se atenderá o escalará al interior de la Secretaría de Tecnologías de la Información y las Comunicaciones, con el fin de realizar una asistencia adecuada. El usuario no debe intentar solucionar el problema.

- La instalación, reparación o retiro de cualquier componente de hardware o software de las estaciones de trabajo, dispositivos móviles y demás recursos tecnológicos de la Gobernación de Santander, solo puede ser realizado por el personal de la Secretaría de Tecnologías de la Información y las Comunicaciones, o personal de terceras partes autorizado por dicha Secretaría.

- Bloquear sus estaciones de trabajo en el momento de abandonar su puesto de trabajo.

- Apagar las estaciones de trabajo u otros recursos tecnológicos en horas no laborables o cuando se deban ausentar por largos periodos de su puesto de trabajo.

- Los equipos de cómputo, en ninguna circunstancia, deben ser dejados desatendidos en lugares públicos o a la vista, en el caso de que estén siendo transportados.

- Los equipos de cómputo deben ser transportados con las medidas de seguridad apropiadas, que garanticen su integridad física.

- Los equipos portátiles siempre deben ser llevados como equipaje de mano y se debe tener especial cuidado de no exponerlos a fuertes campos electromagnéticos.

- En caso de pérdida o robo de un equipo de cómputo de la Gobernación de Santander, se debe informar de forma inmediatamente al líder del proceso para que se inicie el trámite interno y se debe poner la denuncia ante la autoridad competente.

- Asegurar que sus escritorios se encuentran libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y, que estos sean almacenados bajo las protecciones de seguridad necesarias.

- No almacene documentos con información confidencial en la pantalla del escritorio.

15. POLITICAS DE SEGURIDAD EN LAS OPERACIONES

La Gobernación de Santander vela por la protección de operaciones y el procesamiento de la información, ello incluye la gestión de capacidad, gestión de cambios, controles contra código malicioso, respaldo de la información, registro de eventos, protección de la información de registro, registro del administrador y operadores, sincronización de relojes, instalación de softwares en sistemas operativos, gestión de vulnerabilidades técnicas,

restricción sobre la instalación de software y controles de auditorías de sistemas de información.

La seguridad en las operaciones debe ser documentada y con las responsabilidades asignadas.

15.1. Política de asignación de responsabilidades operativas

La Secretaría de Tecnologías de la Información y las Comunicaciones, encargada de la operación y administración de los recursos tecnológicos que apoyan los procesos de la Gobernación de Santander, asignará funciones específicas a sus servidores públicos, quienes deben efectuar la operación y administración de dichos recursos tecnológicos, manteniendo y actualizando la documentación de los procesos operativos para la ejecución de las actividades. Así mismo, velará por la eficiencia de los controles implantados en los procesos operativos asociados a los recursos tecnológicos con el objeto de proteger la confidencialidad, la integridad y la disponibilidad de la información manejada y asegurará que los cambios efectuados sobre los recursos tecnológicos, serán adecuadamente controlados y debidamente autorizados.

La Secretaría de Tecnologías de la Información y las Comunicaciones proveerá la capacidad de procesamiento requerida en los recursos tecnológicos y sistemas de información de la Entidad, efectuando proyecciones de crecimiento y provisiones en la plataforma tecnológica con una periodicidad definida.

La Secretaría de Tecnologías de la Información y las Comunicaciones proveerá y ejecutará los controles de seguridad informática y ciberseguridad a fin de resguardar los servicios tecnológicos y la información.

15.1.1. Normas de asignación de responsabilidades operativas

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Elaborar y actualizar la documentación de procedimientos relacionados con la operación y administración de la plataforma tecnológica de la Gobernación de Santander a través de la Secretaría de Planeación.

- Poner a disposición de sus servidores públicos manuales de configuración y operación de los sistemas operativos, firmware, servicios de red, bases de datos y sistemas de información que conforman la plataforma tecnológica de la Gobernación de Santander de acuerdo con las funciones asignadas al usuario.

- Proveer los recursos necesarios para la implementación de controles que permitan la separación de ambientes de desarrollo, pruebas y producción, teniendo en cuenta consideraciones como: controles para el intercambio de información entre los ambientes de desarrollo y producción, la inexistencia de compiladores, editores o

fuentes en los ambientes de producción y un acceso diferente para cada uno de los ambientes.

- Realizar estudios sobre la demanda y proyecciones de crecimiento de los recursos administrados (Capacity Planning) de manera periódica, con el fin de asegurar el desempeño y capacidad de la plataforma tecnológica. Estos estudios y proyecciones deben considerar aspectos de consumo de recursos de procesadores, memorias, discos, servicios de impresión, anchos de banda, internet y tráfico de las redes de datos, entre otros.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Emitir concepto y generar recomendaciones acerca de las soluciones de seguridad seleccionadas para herramientas colaborativas y sistemas de información de la entidad.

15.2. Política de protección frente a software malicioso

La Gobernación de Santander proporcionará los mecanismos necesarios que garanticen la protección de la información y los recursos de la plataforma tecnológica en donde se procesa y almacena, adoptando los controles necesarios para evitar la divulgación, modificación o daño permanente ocasionados por el contagio de software malicioso.

Además, proporcionará los mecanismos para generar cultura de seguridad entre sus servidores públicos y personal provisto por terceras partes frente a los ataques de software malicioso.

15.2.1. Normas de protección frente a software malicioso

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Proveer herramientas tales como antivirus, antimalware, antispam, antispyware, entre otras, que reduzcan el riesgo de contagio de software malicioso y respalden la seguridad de la información contenida y administrada en la plataforma tecnológica de la Gobernación de Santander y los servicios que se ejecutan en la misma.

- Asegurar que el software de antivirus, antimalware, antispam y antispyware cuente con las licencias de uso requeridas, certificando así su autenticidad y la posibilidad de actualización periódica de las últimas bases de datos de firmas del proveedor del servicio.

- Garantizar que la información almacenada en la plataforma tecnológica sea verificada por el software de antivirus, incluyendo la información que se encuentra contenida y es transmitida por el servicio de correo electrónico.

- Asegurar que los usuarios no puedan realizar cambios en la configuración del software de antivirus, antispyware, antispam, antimalware.

- Garantizar que el software de antimalware y antispam, posea las últimas actualizaciones y parches de seguridad para evitar que sean explotadas ciertas vulnerabilidades.

Normas dirigidas a: TODOS LOS USUARIOS

- No cambiar o eliminar la configuración del software de antimalware y antispam definida por la Secretaría de Tecnologías de la Información y las Comunicaciones.

- Asegurar que los archivos adjuntos de los correos electrónicos descargados de internet o copiados de cualquier medio de almacenamiento, provienen de fuentes conocidas y seguras para evitar el contagio de virus informáticos y/o instalación de software malicioso en los recursos tecnológicos.

- Ante sospechas o detección de alguna infección por software malicioso deben notificar a la mesa de ayuda, para que, a través de ella, la Secretaría de Tecnologías de la Información y las Comunicaciones tome las medidas de control correspondientes.

- Evitar abrir correos de fuentes desconocidas y publicidad engañosa

15.3. Política de copias de respaldo de la información

La Secretaría de Tecnologías de la Información y las Comunicaciones certificará la generación de copias de respaldo y almacenamiento de la información considerando las medidas de contingencia, seguridad y necesidades del negocio y proporciona los recursos necesarios, los procedimientos y mecanismos para la realización de estas actividades.

Así mismo, la Gobernación de Santander velará porque los medios magnéticos que contienen la información crítica sean almacenados en una ubicación diferente a las instalaciones donde se encuentra dispuesta. El sitio externo donde se resguarden las copias de respaldo debe contar con los controles de seguridad física y medioambiental apropiados.

Las copias de respaldo deberán cumplir con las características de completitud, exactitud y restauración.

15.3.1. Normas de copias de respaldo de la información

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Proveer los procedimientos para la generación, restauración, almacenamiento y tratamiento para las copias de respaldo de la información, velando por su integridad y disponibilidad.

- Disponer de los recursos necesarios para permitir la identificación de los medios de almacenamiento, la información contenida en ellos y la ubicación física de los mismos para permitir un rápido y eficiente acceso a los medios que contienen la información resguardada.

- Ejecutar los procedimientos para realizar pruebas de recuperación a las copias de respaldo, para así comprobar su integridad y posibilidad de uso en caso de ser necesario.

- Definir las condiciones de transporte o transmisión y custodia de las copias de respaldo de la información que son almacenadas externamente.

- Definir en conjunto con el oficial de seguridad digital, las estrategias para la generación, retención y rotación de las copias de respaldo de los activos de información.

Normas dirigidas a: LOS SECRETARIOS, DIRECTORES, JEFES DE OFICINA Y COORDINADORES DE GRUPO

- Identificar las funciones críticas que contienen la información a ser respaldada y almacenada.

15.4. Política de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información.

La Gobernación de Santander realizará monitoreo permanente del uso que dan los servidores públicos y el personal provisto por terceras partes, a los recursos de la plataforma tecnológica y los sistemas de información de la entidad. Además, velará por la custodia de los registros de auditoría cumpliendo con los periodos de retención establecidos para dichos registros.

La Secretaría de Tecnologías de la Información y las Comunicaciones y el responsable de la seguridad digital y privacidad de la información definirán la realización de monitoreo de los registros de auditoría sobre los aplicativos donde se opera los procesos misionales de la Gobernación de Santander.

Los logs de los eventos generados por los componentes informáticos, capturan y retienen con base en criticidad de los sistemas y el valor de los datos, aspectos relevantes para la revisión periódica en beneficio de identificar posibles anomalías, generar alertas tempranas conducentes a reconstruir operaciones sensibles y tomar acciones en lo pertinente a la gestión de riesgos en la Gobernación de Santander.

Los registros de auditoría requieren de condiciones de preservación similares a las establecidas para los datos y operaciones que los generan y ser consistentes con los criterios de respaldo y recuperación fundamentados en los requerimientos de retención de la información.

Los logs deben tener mecanismos de seguridad y control administrativo resistentes a ataques para evitar la adulteración de los mismos, también deben generar las capacidades suficientes para detectar y grabar eventos significativos en aspectos de seguridad de información (control a través de un detector de intrusos para los archivos de configuración y logs).

15.4.1. Normas de registro de eventos y monitoreo de los recursos tecnológicos y los sistemas de información

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Habilitar los registros de auditoría y sistemas de monitoreo de la plataforma tecnológica administrada, acorde con los eventos a auditar.

- Velar por la integridad y disponibilidad de los registros de auditoría generados en la plataforma tecnológica y los sistemas de información de la Gobernación de Santander. Estos registros deben ser almacenados y solo deben ser accedidos por personal autorizado.

- Definir un usuario con privilegios únicamente para administración y control de los logs, adicionalmente, dicho usuario debe realizar el correspondiente seguimiento y revisiones periódicas.

- Establecer los registros de auditoría en los recursos tecnológicos y los sistemas de información considerando los estándares de desarrollo seguro para registros de auditoría.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – OFICIAL DE SEGURIDAD DIGITAL

- Determinar los períodos de retención de los registros (logs) de auditoría de los recursos tecnológicos y los sistemas de información de la Gobernación de Santander.

- Definir y ejecutar las tareas de revisión de logs de eventos.

Normas dirigidas a: LOS DESARROLLADORES (INTERNOS Y EXTERNOS)

- Implementar en los desarrollos de software, los controles necesarios para generar y garantizar la integridad los registros (logs) de auditoría de las actividades

realizadas por los usuarios finales y administradores en los sistemas de información desarrollados.

- Implementar en los desarrollos de software mecanismos para registrar en los logs de auditoría eventos como: fallas de validación, intentos de autenticación fallidos y exitosos, fallas en los controles de acceso, intento de evasión de controles, excepciones de los sistemas, funciones administrativas y cambios de configuración de seguridad, entre otros.

Normas dirigidas a: LOS ADMINISTRADORES DE SISTEMAS DE INFORMACIÓN E INFRAESTRUCTURA TECNOLÓGICA

- Los administradores de aplicaciones deben habilitar y generar logs de auditoría en las aplicaciones en la periodicidad establecida.

- Los administradores de sistemas operativos deben habilitar y generar en la periodicidad establecida los logs de auditoría del sistema operativo.

- Los administradores de bases de datos deben habilitar y generar logs en la periodicidad establecida sobre las bases de datos y tablas para los campos que manejen información clasificada y reservada.

- Los administradores de seguridad perimetral deben generar y revisar en la periodicidad establecida los reportes generados por la plataforma e identificar intentos de accesos no autorizados con su correspondiente cantidad de eventos, origen y tipo de evento (firewall, ips, waf, rdp, vpn, acceso a plataformas de gestión, otros componentes tecnológicos para la seguridad y telecomunicaciones).

- Los administradores de consola de antivirus deben revisar los reportes generados por la plataforma e identificar anomalías en cada uno de los servidores y estaciones de trabajo generando un consolidado de amenazas identificadas.

- Los coordinadores de infraestructura son responsables de recopilar y revisar los resultados de los reportes generados por los administradores de base de datos, aplicaciones, sistema operativo, consola de antivirus y correo electrónico con la finalidad de presentar al comité de seguridad de la información propuestas de acciones y formular ajustes necesarios para la solución de las alarmas o incongruencias identificadas.

- Los administradores de sistemas de información e infraestructura tecnológica deben configurar el envío de logs de auditoría generados al correlacionador de eventos para su revisión.

15.5. Política de control al software operativo

La Gobernación de Santander revisa la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de pruebas periódicas de vulnerabilidades, a fin de realizar la corrección sobre los hallazgos arrojados por dichas pruebas, de acuerdo con los criterios establecidos. La Secretaría de Tecnologías de la Información y las Comunicaciones y el oficial de seguridad digital, conformarán el Comité de Vulnerabilidades encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

15.5.1. Normas de control al software operativo

Normas dirigidas a: SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Establecer responsabilidades para controlar la instalación del software operativo, que interactúen con el procedimiento de control de cambios existente en la Gobernación de Santander.

- Asegurar que el software operativo instalado en la plataforma tecnológica de la Gobernación de Santander cuenta con soporte de los proveedores.

- Conceder accesos temporales y controlados a los proveedores para realizar las actualizaciones sobre el software operativo, así como monitorear dichas actualizaciones.

- Validar los riesgos que genera la migración hacia nuevas versiones del software operativo.

- Asegurar el correcto funcionamiento de sistemas de información y herramientas de software que se ejecutan sobre la plataforma tecnológica cuando el software operativo es actualizado.

- Considerar los requisitos del negocio para la gestión de cambios sobre el software operacional.

- Establecer las restricciones y limitaciones para la instalación de software operativo en los equipos de cómputo de la entidad.

- Mantener un inventario del software implementado, así como sus respectivas versiones y niveles de soporte por parte del proveedor.

15.6. Política de gestión de vulnerabilidades

La Gobernación de Santander, a través de la Secretaría de Tecnologías de la Información y las Comunicaciones y el responsable de la seguridad digital y privacidad de la información, revisará periódicamente la aparición de vulnerabilidades técnicas sobre los recursos de la plataforma tecnológica por medio de la realización periódica de pruebas de

vulnerabilidades, con el objetivo de realizar la corrección sobre los hallazgos arrojados por dichas pruebas. Estas áreas conformarán el Comité de vulnerabilidades encargado de revisar, valorar y gestionar las vulnerabilidades técnicas encontradas.

15.6.1. Normas para la gestión de vulnerabilidades

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Adelantar los trámites correspondientes para la realización de pruebas de vulnerabilidades y hacking ético con una periodicidad establecida, por un ente independiente al área objeto de las pruebas, con el fin de garantizar la objetividad del desarrollo de las mismas.

- Generar los lineamientos y recomendaciones para la mitigación de vulnerabilidades, resultado de las pruebas de vulnerabilidades y hacking ético.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Revisar y hacer seguimiento a la aparición de nuevas vulnerabilidades técnicas y reportar a los administradores de la plataforma tecnológica y los desarrolladores de los sistemas de información, con el fin de que se evalúe las acciones necesarias para corregir las mismas de acuerdo con los criterios definidos en el procedimiento, de Pruebas de Vulnerabilidad.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – EL OFICIAL DE SEGURIDAD DIGITAL

- Evaluar los resultados de las pruebas de vulnerabilidades y hacking ético y definir acciones para su resolución de hallazgos.

- Revisar las acciones ejecutadas para la resolución de vulnerabilidades técnicas y autorizar su cierre definitivo, en la Matriz de Vulnerabilidades. herramientas tecnológicas para su identificación.

15.7. Política de auditorías a sistemas de información

Las actividades de auditoría sobre los activos de información e infraestructura tecnológica se controlan para reducir el impacto sobre las operaciones del negocio y preservar la seguridad digital. Estas actividades son planificadas y acordadas con la Secretaría de Tecnologías de la Información y las Comunicaciones.

El acceso a sistemas de información y datos son acordados y controlados con el responsable del activo de información.

El alcance de las pruebas técnicas de auditoría se acuerda y controla con el responsable del activo de información.

El acceso diferente a solo lectura se autoriza para copias aisladas de los activos de información y se realiza borrado seguro una vez se ha finalizado la auditoría o en su defecto se establece protección apropiada en caso de necesidad de mantenerlos como documentación de prueba de auditoría.

Las pruebas de auditoría que puedan afectar disponibilidad en la prestación de servicios se realizan fuera del horario laboral.

15.7.1. Normas de política de auditorías a sistemas de información

Normas dirigidas a: SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Brindar apoyo técnico al responsable de la auditoría para facilitar las actividades planificadas.

- A partir de los resultados de la auditoría gestiona los planes de mejoramiento.

15.8. Política de gestión del cambio

La Gobernación de Santander a través de la Secretaría de Tecnologías de la Información y las Comunicaciones y el oficial de seguridad digital controlan los cambios sobre sus activos de información, instalaciones y sistemas de procesamiento de información. Estas dos áreas conformarán el Comité de control de cambios encargado de revisar, valorar y gestionar los cambios a través de un procedimiento que permite:

- Identificación y registro de los cambios.
- Planificación y prueba de los cambios.
- Valoración del impacto potencial de los cambios.
- Aprobación formal del cambio.
- Verificación de requisitos de seguridad del cambio y de continuidad.
- Comunicación del cambio a las partes pertinentes.
- Actividades de apoyo ante cambios no exitosos o de emergencia.

15.8.1. Normas de políticas de gestión del cambio

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Ejecutar las pruebas técnicas y validar que el solicitante realice las pruebas funcionales de los cambios a aprobar.

- Revisar antes de la ejecución del cambio que el mismo haya sido aprobado por el solicitante y el Comité de control de cambios.

- Catalogar y ejecutar el cambio gestionando los riesgos que puedan afectar la operación.

- Participar en la aprobación de los cambios propuestos al Comité de control de cambios.

- Participar en el seguimiento de los resultados de los cambios ejecutados.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Participar en la evaluación y análisis de impacto del riesgo del cambio.

- Participar en la aprobación de los cambios propuestos al Comité de control de cambios.

- Participar en el seguimiento de los resultados de los cambios ejecutados.

16. POLÍTICAS DE SEGURIDAD EN LAS COMUNICACIONES

Las redes y servicios de comunicaciones, así como las instalaciones que le dan soporte, se gestionarán y controlarán para evitar accesos no autorizados. La información transmitida o transferida mediante redes públicas se salvaguardará a través de controles para prevenir la pérdida de confidencialidad, integridad y la pérdida de disponibilidad de estos.

La conexión de equipo o estaciones de trabajo a las redes de la Gobernación de Santander se controlarán y supervisarán.

16.1. Política de gestión y aseguramiento de las redes de datos

La Gobernación de Santander establecerá, a través de la Secretaría de Tecnologías de la Información y las Comunicaciones los mecanismos de control necesarios para proveer la disponibilidad de las redes de datos y de los servicios que dependen de ellas; así mismo, velará por que se cuente con los mecanismos de seguridad que protejan la integridad y la confidencialidad de la información que se transporta a través de dichas redes de datos.

De igual manera, propenderá por el aseguramiento de las redes de datos, el control del tráfico en dichas redes y la protección de la información reservada y restringida de la Gobernación de Santander.

16.1.1. Normas de gestión y aseguramiento de las redes de datos

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Adoptar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Gobernación de Santander.

- Implementar controles para minimizar los riesgos de seguridad de la información transportada por medio de las redes de datos.

- Identificar los mecanismos de seguridad y los niveles de servicio de red requeridos e incluirlos en los acuerdos de servicios de red, cuando estos se contraten externamente.

- Establecer los estándares técnicos de configuración de los dispositivos de seguridad y de red de la plataforma tecnológica de la entidad, acogiendo buenas prácticas de configuración segura.

- Identificar, justificar y documentar los servicios, protocolos y puertos permitidos por la entidad en sus redes de datos e inhabilitar o eliminar el resto de los servicios, protocolos y puertos.

- Instalar protección entre las redes internas de la Gobernación de Santander y cualquier red externa, que este fuera de la capacidad de control y administración de la entidad.

- Definir los parámetros técnicos requeridos para la conexión segura de los servicios de red, así como las reglas de conexión de seguridad y controles para cifrado de información que circule sobre redes.

16.2. Política de uso del correo electrónico institucional

La Gobernación de Santander, entendiendo la importancia del correo electrónico institucional como herramienta para facilitar la comunicación entre servidores públicos y terceras partes, proporcionará un servicio idóneo y seguro para la ejecución de las actividades que requieran el uso del correo electrónico, respetando siempre los principios de confidencialidad, integridad, disponibilidad y autenticidad de quienes realizan las comunicaciones a través de este medio.

16.2.1. Normas de uso del correo electrónico institucional

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Gestionar el acceso a las cuentas de correo electrónico institucional mediante un procedimiento de asignación/retiros de acceso a los sistemas de información.

- Proveer un ambiente seguro y controlado para el funcionamiento de la plataforma de correo electrónico institucional.

- Adoptar medidas de seguridad que permiten proteger la plataforma de correo electrónico institucional contra código malicioso.

- Establecer mecanismos para el monitoreo y alerta de envío de información calificada como clasificada y clasificada reservada.

- Habilitar los controles que faciliten el etiquetado de la información digital en los servicios de correo electrónico institucional.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Generar las campañas para concientizar a los servidores públicos respecto al uso adecuado y las precauciones que deben adoptar en el intercambio de información calificada como clasifica y clasificada reservada por medio del correo electrónico.

Normas dirigidas a: TODOS LOS USUARIOS

- Usar la cuenta de correo electrónico institucional de manera individual e intransferible y no usar la cuenta de correo electrónico institucional de otro(s) usuarios.

- Usar el servicio de correo, los mensajes y la información contenida en los correos para el desarrollo de las funciones y funciones de cada usuario en apoyo al objetivo misional de la Gobernación de Santander. El correo institucional no debe ser utilizado para actividades personales.

- Los mensajes y la información contenida en los buzones de correo institucional son propiedad de la Gobernación de Santander y cada usuario, como responsable de su buzón, debe mantener solamente los mensajes relacionados con el desarrollo de sus funciones.

- Está prohibido el envío de cadenas de mensajes de cualquier tipo, ya sea comercial, político, religioso, material audiovisual, contenido discriminatorio, pornografía y demás condiciones que degraden la condición humana, vayan en contravía de los derechos humanos y resulten ofensivos para los servidores públicos de la Gobernación de Santander.

- No es permitido en ninguna circunstancia el envío de archivos que contengan extensiones ejecutables o aquellos que puedan afectar sistemas de información o recursos internos o externos, Todos los mensajes enviados deben respetar el estándar de formato e imagen corporativa definidos por la Gobernación de Santander y conservar en todos los casos el mensaje legal corporativo de confidencialidad.

- Todo correo sospechoso debe ser reportado a la Secretaría de Tecnologías de la Información y las Comunicaciones.

- Los servicios colaborativos como One Drive, SharePoint no podrán ser usados para almacenar información personal ni ser utilizados desde redes de Internet externas. Toda excepción es manejada considerando los riesgos y responsabilidades del área solicitante, siguiendo los respectivos procedimientos de solicitud y autorizaciones.

- Todo usuario que produzca, transmita o transfiera información, debe asegurar la adecuada clasificación de la misma y aplicar los parámetros de seguridad señalados por la Gobernación de Santander.

16.3. Política de uso adecuado de internet

La Gobernación de Santander consciente de la importancia del uso de Internet como una herramienta para el desempeño de funciones, proporcionará los recursos necesarios para asegurar su disponibilidad a los usuarios que así lo requieran para el desarrollo de sus actividades diarias en la entidad.

16.3.1. Normas de uso adecuado de internet

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Proporcionar los recursos necesarios para la implementación, administración y mantenimiento requeridos para la prestación segura del servicio de Internet, bajo las restricciones de los perfiles de acceso que se establezcan.

- Diseñar e implementar mecanismos que permitan la continuidad o restablecimiento del servicio de Internet en caso de contingencia interna.

- Monitorear continuamente el canal o canales del servicio de Internet, manteniendo la calidad del servicio para los usuarios.

- Establecer procedimientos e implementar controles para evitar la descarga de software no autorizado, evitar código malicioso proveniente de Internet y evitar el acceso a sitios catalogados como restringidos.

- Generar registros de la navegación y los accesos de los usuarios a Internet, así como establecer e implementar procedimientos de monitoreo sobre la utilización del servicio de Internet.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Generar campañas para concientizar tanto a los servidores públicos, como al personal provisto por terceras partes, respecto a las precauciones que deben tener en cuenta cuando utilicen el servicio de Internet.

Normas dirigidas a: TODOS LOS USUARIOS

- Evitar la descarga de software desde internet, así como su instalación en las estaciones de trabajo o dispositivos móviles asignados para el desempeño de sus funciones.

- Está prohibido por mandato legal, visitar páginas relacionadas con pornografía, drogas, alcohol, web proxys, hacking y/o cualquier otra página que no esté relacionada con las funciones asignadas.
- Hacer uso del mismo en relación con las actividades laborales que así lo requieran.

- Está prohibido el acceso y el uso de servicios interactivos o mensajería instantánea como Hotmail, Facebook, P2P, MSN, Yahoo!, Skype, FTP, HTTP, Net2phone y otros similares, que tengan como objetivo crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias de la Gobernación de Santander.

- Está prohibido la descarga, uso, intercambio y/o instalación de juegos, música, películas, protectores y fondos de pantalla, software de libre distribución, información y/o productos que de alguna forma atenten contra la propiedad intelectual de sus autores, o que contengan archivos ejecutables y/o herramientas que atenten contra la integridad, disponibilidad y/o confidencialidad de la infraestructura tecnológica (hacking), entre otros. La descarga, uso, intercambio y/o instalación de información audiovisual (videos e imágenes) utilizando sitios públicos en Internet debe ser autorizada por el jefe respectivo y la Secretaría de Tecnologías de la Información y las Comunicaciones, o a quienes ellos deleguen de forma explícita para esta función, asociando los procedimientos y controles necesarios para el monitoreo y aseguramiento del buen uso del recurso.

- Está prohibido el intercambio no autorizado de información de propiedad de la Gobernación de Santander, de sus clientes, servidores públicos y proveedores.

16.4. Política de intercambio de información

La Gobernación de Santander asegurará la protección de la información transferida o transmitida con entidades externas y procesos internos, con procedimientos y controles implementados para el intercambio de datos y Acuerdos de Confidencialidad con terceras partes con quienes interactúen con la información.

La información recibida de terceras partes se conservará por un período de tiempo equivalente al de retención de las bases de datos con información personal sobre las cuales

se efectúen actualizaciones, cambios, supresiones con la información fuente, o el tiempo establecido por los requisitos legales aplicables a la Gobernación de Santander.

16.4.1. Normas de intercambio de información

Normas dirigidas a: LA SECRETARIA GENERAL – JURÍDICA – SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- El Grupo de Contratación, en acompañamiento con el oficial de seguridad digital y la Secretaría de Tecnologías de la Información y las Comunicaciones, debe definir los modelos de Acuerdos de Confidencialidad y/o de Intercambio de Información entre la entidad y terceras partes incluyendo los compromisos adquiridos y las consecuencias administrativas, disciplinarias y judiciales por el incumplimiento de dichos acuerdos. Entre los aspectos a considerar se debe incluir la prohibición de divulgar la información entregada por la Gobernación de Santander a los terceros con quienes se establecen estos acuerdos y la destrucción de dicha información una vez cumpla su cometido.

- Establecer con terceras partes, los Acuerdos de Confidencialidad o Acuerdos de intercambio dejando explícitas las responsabilidades y obligaciones legales asignadas a dichos terceros por la divulgación no autorizada de información de beneficiarios de la Gobernación de Santander que les ha sido entregada debido al cumplimiento de los objetivos misionales.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Definir y establecer el procedimiento de intercambio de información con los diferentes terceros que, hacen parte de la operación de la Gobernación de Santander, reciben o envían información de los beneficiarios de la Entidad, que contemple la utilización de medios de transmisión confiables y la adopción de controles, con el fin de proteger la confidencialidad e integridad de la misma.

- Velar porque el intercambio de información de la Gobernación de Santander con Entidades externas se realice en cumplimiento de las Políticas de seguridad para el intercambio de información aquí descritas, los Acuerdos de Intercambio de Información y el procedimiento definido para dicho intercambio de información.

Normas dirigidas a: LOS PROPIETARIOS DE LOS ACTIVOS DE INFORMACION

- Resguardar la información de la Gobernación de Santander o de sus beneficiarios de divulgación no autorizada por parte de los terceros a quienes se entrega, verificando el cumplimiento de las cláusulas relacionadas en los contratos, acuerdos de confidencialidad o acuerdos de intercambio establecidos.

- Asegurar que los datos requeridos de los beneficiarios sólo puedan ser entregados a terceros, previo consentimiento de los titulares de los mismos, salvo en los casos que lo disponga una ley o sea una solicitud de los entes de control.

- Los propietarios de los activos de información, o a quien ellos deleguen, verifican que el intercambio de información con terceros deje registro del tipo de información intercambiada, el emisor y receptor de la misma y la fecha de entrega/recepción.

- Formular los requerimientos de solicitud/envío de información de la Gobernación de Santander por terceras partes, salvo que se trate de solicitudes de entes de control o de cumplimiento de la legislación vigente.

- Asegurar que el Intercambio de información (digital) solamente se realice si se encuentra autorizada y dando cumplimiento a las Políticas de administración de redes, de acceso lógico y de protección de datos personales de la Gobernación de Santander, así como del procedimiento de intercambio de información con terceros.

- Verificar conjuntamente entre el proveedor y el propietario la ejecución de la disposición final de la información suministrada a los terceros, una vez ésta ha cumplido el cometido por el cual fue compartida.

Normas dirigidas a: LASECRETARIA GENERAL – CORRESPONDENCIA

- Operar el procedimiento para el intercambio, de información (medios de almacenamiento y documentos) con terceras partes y la adopción de controles a fin de proteger la información sensible contra divulgación, pérdida o modificaciones.

- Garantizar que todo envío de información física a terceros (documento o medio magnético) utilice únicamente los servicios de transporte o mensajería autorizados por la entidad, y que estos permitan ejecutar rastreo y control de las entregas.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Ofrecer servicios y herramientas, para el cifrado de información pública clasificada o pública reservada, para evitar la divulgación o modificaciones no autorizadas.

Normas dirigidas a: TERCEROS CON QUIENES SE INTERCAMBIA INFORMACIÓN DE LA GOBERNACIÓN DE SANTANDER

- Darle manejo adecuado a la información recibida, en cumplimiento de las Políticas de Seguridad de la entidad, de las condiciones contractuales establecidas y del procedimiento de intercambio de información.

- Realizar la disposición final segura de la información suministrada, una vez ésta cumpla con la función para la cual fue enviada y demostrar mediante acta la realización de las actividades de destrucción.

Normas dirigidas a: TODOS LOS USUARIOS

- No está permitido el intercambio de información clasificada y clasificada reservada de la Gobernación de Santander por vía telefónica.

17. POLÍTICAS DE ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN

La adquisición, desarrollo y mantenimiento de sistemas de información deben incluir buenas prácticas de seguridad digital durante todo el ciclo de vida, los requisitos relacionados con la seguridad digital son incorporados a los sistemas de información tanto nuevos como ya existentes. Los servicios asociados a transacciones electrónicas se protegen para evitar transmisión incompleta, alteración o divulgación no autorizada o enrutamiento errado.

17.1. Política para el establecimiento de requisitos de seguridad

La Gobernación de Santander asegurará que el software adquirido y desarrollado tanto al interior de la entidad, como por terceras partes, cumpla con los requisitos de seguridad y calidad establecidos. Las áreas propietarias de sistemas de información, la Secretaría de Tecnologías de la Información y las Comunicaciones y el Oficial de Seguridad Digital, incluyen requisitos de seguridad en la definición de requerimientos y, posteriormente se aseguran de que estos se encuentren generados a cabalidad durante las pruebas realizadas sobre los desarrollos del software construido. Todos los sistemas de información o desarrollos de software deben tener un área propietaria dentro de la Gobernación de Santander formalmente asignada.

17.1.1. Normas para el establecimiento de requisitos de seguridad

Normas dirigidas a: LOS PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN, SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, OFICIAL DE SEGURIDAD DIGITAL

- Establecer las especificaciones de adquisición o desarrollo de sistemas de información, considerando requerimientos de seguridad digital.

- La Secretaría de Tecnologías de la Información y las Comunicaciones liderará la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos como la estandarización de herramientas de desarrollo, controles de autenticación, controles de acceso y arquitectura de aplicaciones, entre otros.

Normas dirigidas a: DESARROLLADORES (INTERNOS O EXTERNOS)

- Documentar los requerimientos establecidos y definir la arquitectura de software más conveniente para cada sistema de información que se quiera desarrollar, de acuerdo con los requerimientos de seguridad y los controles deseados.

- Certificar que todo sistema de información adquirido o desarrollado utilice herramientas de desarrollo licenciadas.

- Certificar la transmisión de información relacionada con pagos o transacciones en línea a los operadores encargados, por medio de canales seguros.

17.2. Política de desarrollo seguro, realización de pruebas y soporte de los sistemas

La Gobernación de Santander velará porque el desarrollo interno o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se asegurará que todo software desarrollado o adquirido, interna o externamente cuenta con el nivel de soporte requerido por la entidad.

17.2.1. Normas de desarrollo seguro, realización de pruebas y soporte de los sistemas

Normas dirigidas a: LOS PROPIETARIOS DE LOS SISTEMAS DE INFORMACIÓN

- Realizar las pruebas para asegurar que se cumplen con los requerimientos de seguridad establecidos en ambientes de pruebas y producción, utilizando metodologías establecidas para este fin, documentando las pruebas realizadas y aprobando los pasos a producción, considerando nuevos sistemas, nuevas funcionalidades, mantenimientos en aplicaciones construidas internamente, construidas por proveedores, aprovisionadas en la nube o híbrido de las anteriores.

- Aprobar las migraciones entre los ambientes de desarrollo, pruebas y producción de sistemas de información nuevos y/o de cambios o nuevas funcionalidades.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Implementar los controles necesarios para asegurar que las migraciones entre los ambientes de desarrollo, pruebas y producción han sido aprobadas, de acuerdo con el procedimiento de control de cambios.

- Contar con sistemas de control de versiones para administrar los cambios de los sistemas de información de la Gobernación de Santander.

- Asegurar que los sistemas de información adquiridos o desarrollados por terceros, cuenten con un acuerdo de licenciamiento el cual debe especificar las condiciones de uso del software y los derechos de propiedad intelectual.

- Generar metodologías para la realización de pruebas al software desarrollado, que contengan pautas para la selección de escenarios, niveles, tipos, datos de pruebas y sugerencias de documentación.

- Asegurar que la plataforma tecnológica, las herramientas de desarrollo y los componentes de cada sistema de información estén actualizados con todos los parches generados para las versiones en uso y que estén ejecutando la última versión aprobada por el fabricante.

- Asegurar que las aplicaciones y desarrollos se diseñen y construyan en versiones vigentes y estables emitidas por el fabricante respecto a las herramientas, componentes, lenguajes de programación.

- Almacenar las copias de seguridad del código fuente de manera segura previendo riesgos asociados a pérdida de disponibilidad, confidencialidad o integridad.

- Aplicar el procedimiento de control de cambios a los cambios para el software, aplicativos y los sistemas de información de la entidad.

Normas dirigidas a: LOS DESARROLLADORES (INTERNOS O EXTERNOS)

- Considerar y aplicar las buenas prácticas y lineamientos de desarrollo seguro durante todo el ciclo de vida de los mismos sistemas de información.

- Proporcionar un nivel adecuado y oportuno de soporte para solucionar los problemas que se presenten en el software y aplicativos de la Gobernación de Santander.

- Construir los aplicativos de tal manera que efectúen las validaciones de datos de entrada y la generación de los datos de salida de manera confiable, utilizando rutinas de validación centralizadas y estandarizadas.

- Asegurar que los sistemas de información construidos validen la información suministrada por los usuarios antes de procesarla.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Asegurar que las pruebas de seguridad sobre los sistemas de información se realicen de acuerdo con las metodologías definidas, contando con pruebas debidamente documentadas.

17.3. Política para la protección de los datos de prueba

La Secretaría de Tecnologías de la Información y las Comunicaciones de la Gobernación de Santander protegerá los datos de prueba que se entregarán a los desarrolladores, asegurando que no revelan información confidencial de los ambientes de producción.

17.3.1. Normas para la protección de los datos de prueba

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Garantizar que la información a ser entregada a los desarrolladores para sus pruebas se enmascare y no revele información calificada como clasificada y/o reservada de los ambientes de producción.

- Realizar la adecuada disposición final la información de los ambientes de pruebas, una vez éstas han concluido las mismas.

18. POLÍTICAS QUE RIGEN DE LA RELACION CON TERCERAS PARTES

La Gobernación de Santander establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso, conocimiento o relación con los servicios o productos en el marco del contrato cumpla con las políticas, normas y procedimientos de seguridad digital.

18.1. Política de inclusión de condiciones de seguridad en la relación con terceras partes

La Gobernación de Santander establecerá mecanismos de control en sus relaciones con terceras partes, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por las mismas, cumplan con las políticas, normas y procedimientos de seguridad de la información.

Los servidores públicos responsables de la realización y/o firma de contratos o convenios con terceras partes se asegurarán de la divulgación a dichas partes, de las políticas, normas y procedimientos de seguridad de la información de la Gobernación de Santander.

18.1.1. Normas de inclusión de condiciones de seguridad en la relación con terceras partes

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES, JURIDICA Y RESPONSABLE DE SEGURIDAD DIGITAL Y PROVACIDAD DE LA INFORMACIÓN

- Elaborar el modelo de Acuerdo de Confidencialidad y de Intercambio de Información con terceras partes. en dichos acuerdos deberá establecerse una responsabilidad administrativa (procuraduría – contraloría), disciplinaria (control interno) y judicial

(penal, civil o administrativa, incluida la acción de repetición); además deberá existir una tasación anticipada de perjuicios a favor de la Gobernación de Santander.

- Generar un modelo base para los Acuerdos de Niveles de Servicio y requisitos de Seguridad Digital, con los que deben cumplir los proveedores de servicios; dicho modelo, debe ser divulgado a todas las áreas que adquieran o supervisen recursos y/o servicios tecnológicos.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Establecer las condiciones de conexión adecuada para los equipos de cómputo y dispositivos móviles de los terceros en la red de datos de la Gobernación de Santander.

- Establecer las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

- Gestionar los riesgos relacionados con terceras partes que tengan acceso a los sistemas de información y la plataforma tecnológica de la Gobernación de Santander.

- Verificar el cumplimiento de los controles de software base instalado y de licenciamiento de software y hacer extensivos los controles existentes en la red a equipos de cómputo de terceras partes cuando los proveedores que por necesidades o por acuerdos contractuales de la operación, incorporen equipos de cómputo a la red corporativa.

Normas dirigidas a: OFICIAL DE SEGURIDAD DIGITAL

- Evaluar y emitir concepto de los accesos a la información y de los recursos tecnológicos de la entidad requeridos por terceras partes.

- Asesorar en la identificación de los riesgos relacionados con terceras partes.

- Revisar el cumplimiento normativo de seguridad digital en los proveedores.

Normas dirigidas a: LOS SUPERVISORES DE CONTRATOS CON TERCEROS

- Incluir en los contratos el cumplimiento de las normas legales y políticas pertinente al servicio contratado.

- Divulgar a sus proveedores las políticas, normas y procedimientos de seguridad digital de acuerdo con el servicio contratado.

- Asignar permisos al proveedor en los sistemas de información y recursos tecnológicos de acuerdo con las responsabilidades contractuales.

- Verificar el adecuado uso de los recursos tecnológicos y de la información suministrada al proveedor para el desarrollo de las obligaciones del contrato.

- Hacer seguimiento del cumplimiento de las normas legales, políticas, procedimientos y requisitos específicos de seguridad digital por parte del proveedor y reportar su resultado al oficial de seguridad digital.

- Con respecto a seguridad digital, los servidores públicos y personal provisto por terceras partes que por sus funciones hagan uso de la información de la Gobernación de Santander, deben dar cumplimiento a las políticas, normas y procedimientos y recibir la sensibilización o capacitación que determine la Gobernación de Santander en materia de seguridad digital.

18.2. Política de gestión de la prestación de servicios de terceras partes

La Gobernación de Santander propenderá por mantener los niveles acordados de seguridad de la información y de prestación de los servicios de los proveedores, en concordancia con los acuerdos establecidos con estos. Así mismo, velará por la adecuada gestión de cambios en la prestación de servicios de dichos proveedores.

18.2.1. Normas de gestión de la prestación de servicios de terceras partes

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES Y RESPONSABLE DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

- Verificar las condiciones de comunicación segura, cifrado y transmisión de información desde y hacia los terceros proveedores de servicios.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL - SUPERVISORES DE CONTRATOS CON TERCEROS

- Notificar a los proveedores que todos los cambios en los servicios tecnológicos deben ser informados a su correspondiente Supervisor, para que dichos cambios se analicen en comité de control de cambios.

18.3. Política de cadena de suministro

La Gobernación de Santander realizará revisión de seguridad digital a la cadena de suministro de los proveedores que participan en la operación misional de la entidad.

Definirá los requisitos de seguridad digital de la operación realizadas con terceras partes en lo referente a la adquisición de productos y servicios. Exigirá la divulgación de los

requisitos de seguridad a los proveedores a lo largo de la cadena de suministro que éste tenga y a sus colaboradores. Se tendrá formalizado mediante procedimiento la revisión periódica de los requisitos de seguridad de la cadena de suministro. Dentro de la revisión se contempla los componentes de hardware y software crítico para el desarrollo del servicio.

18.3.1. Normas de política de cadena de suministro

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Identificar con el proveedor los componentes de hardware y software crítico para el desarrollo del servicio.

Normas dirigidas a: LOS SUPERVISORES DE CONTRATOS – EL OFICIAL DE SEGURIDAD DIGITAL

- Revisar los requisitos de seguridad de la cadena de suministro de proveedores que participan en la operación misional.

- Revisar el cumplimiento de la divulgación de los requisitos de seguridad de la cadena de suministro de proveedores.

19. POLÍTICAS DE GESTIÓN DE INCIDENTES DE SEGURIDAD

La Gobernación de Santander asegurará la gestión de incidentes de seguridad digital incluyendo la comunicación interna y autoridades competentes de ser necesarias. Se tendrán definidas las responsabilidades a través de procedimientos de gestión de incidentes para asegurar una respuesta eficaz y oportuna.

19.1. Política para el reporte y tratamiento de incidentes de seguridad

La Gobernación de Santander promoverá entre los servidores públicos y personal provisto por terceras partes el reporte de incidentes relacionados con la seguridad de la información y sus medios de procesamiento, incluyendo cualquier tipo de medio de almacenamiento de información, como la plataforma tecnológica, los sistemas de información, los medios físicos de almacenamiento y las personas.

De igual manera, asignará responsables para el tratamiento de los incidentes de seguridad digital, quienes tienen la responsabilidad de aislar, investigar y solucionar los incidentes reportados, tomando las medidas necesarias para evitar su reincidencia y escalando los incidentes de acuerdo con su criticidad. Los responsables con sus respectivas actividades estarán establecidos en el procedimiento de incidentes y en la guía para el manejo de posible delito informático.

La Alta Dirección o a quien delegue, son los únicos autorizados para reportar incidentes de seguridad ante las autoridades; así mismo, son los únicos canales de comunicación autorizados para hacer pronunciamientos oficiales ante entidades externas.

19.1.1. Normas para el reporte y tratamiento de incidentes de seguridad

Normas dirigidas a: LOS PROPIETARIOS DE LOS ACTIVOS DE INFORMACIÓN

- Informar al oficial de seguridad digital, los incidentes de seguridad que identifiquen o que reconozcan su posibilidad de materialización.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Evaluar todos los incidentes de seguridad de acuerdo con sus circunstancias particulares y escalar al comité de seguridad de la información, aquellos en los que se considere pertinente.

- Designar personal calificado, para investigar adecuadamente los incidentes de seguridad reportados, identificando las causas, realizando una investigación exhaustiva, proporcionando las soluciones y finalmente previniendo su recurrencia.

- Generar campañas de concientización a todos los usuarios de la Gobernación de Santander para que conozcan los mecanismos para el reporte de incidentes de seguridad.

- Activar el plan de contingencia tecnológica, de acuerdo con los criterios del manual del plan de continuidad del negocio de la Gobernación de Santander para aquellos incidentes que afecten la disponibilidad y/o integridad de información y de los servicios tecnológicos.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Analizar el incidente con el fin de establecer las posibles causas del mismo, identificando el impacto y ejecutando las acciones para contener el incidente.

- Proponer los planes de mejora e implementar medidas correctivas.

Normas dirigidas a: EL COMITÉ DE SEGURIDAD DE LA INFORMACION

- Analizar los incidentes de seguridad que le son escalados y activar el procedimiento de contacto con las autoridades, cuando lo estime necesario.

Normas dirigidas a: TODOS LOS USUARIOS

- Reportar al oficial de seguridad digital, cualquier evento o incidente relacionado con la información y/o los recursos tecnológicos, para que se registre y se le dé el trámite necesario.

20. POLÍTICAS DE INCLUSIÓN DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

La Gobernación de Santander incorporará las medidas de seguridad digital en sus procesos de gestión de incidentes de continuidad, protegiendo la información de la Entidad.

20.1. Política de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

La Gobernación de Santander responderá ante eventos de contingencia conforme a los escenarios identificados en el Manual de Administración de Plan de Continuidad de Negocio y proporcionará los recursos suficientes para dar una respuesta efectiva y así continuar la operación de procesos críticos, preservando los niveles de seguridad equivalente a los proporcionados en situación normal. La Gobernación de Santander mantendrá canales de comunicación adecuados hacia los servidores públicos, proveedores y partes interesadas ante incidentes de continuidad, normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad digital.

20.1.1. Normas de continuidad, contingencia, recuperación y retorno a la normalidad con consideraciones de seguridad de la información

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Reconocer las situaciones que serán identificadas como emergencia o desastre para la entidad, los procesos o las áreas y determinar cómo se debe actuar sobre las mismas.

- Liderar los aspectos relacionados con la continuidad del negocio y la recuperación ante desastres.

- Realizar el análisis de impacto al negocio y los análisis de riesgos de continuidad para, posteriormente proponer posibles estrategias de recuperación en caso de activarse el plan de contingencia o continuidad, con las consideraciones de seguridad digital a que haya lugar.

- Asegurar la realización de pruebas periódicas del plan de recuperación ante desastres y/o continuidad de negocio, verificando la seguridad digital durante su realización y la documentación de dichas pruebas.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – EL OFICIAL DE SEGURIDAD DIGITAL

- Asegurar un plan de recuperación ante desastres para la infraestructura tecnológica y los procedimientos de contingencia, recuperación y retorno a la normalidad para cada uno de los servicios y sistemas prestados incorporando los controles de seguridad digital.
- Participar activamente en las pruebas de los procedimientos de contingencia y notifica los resultados al comité institucional de gestión y desempeño de la Gobernación de Santander.

20.2. Política de redundancia

La Gobernación de Santander propenderá por la existencia de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad aceptables para la entidad.

20.2.1. Normas de redundancia

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – OFICIAL DE SEGURIDAD DIGITAL

- Analizar y establecer los requerimientos de redundancia para los sistemas de información críticos para la entidad y la plataforma tecnológica que los apoya.

- Realizar pruebas sobre las soluciones de redundancia, para asegurar el cumplimiento de los requerimientos de disponibilidad.

- La Secretaría de Tecnologías de la Información y las Comunicaciones seleccionará las soluciones de redundancia tecnológica adecuadas para los sistemas de información de acuerdo con las necesidades del negocio.

- La Secretaría de Tecnologías de la Información y las Comunicaciones administrará las soluciones de redundancia tecnológica de la Gobernación de Santander.

21. POLÍTICAS DE CUMPLIMIENTO

La Gobernación de Santander velará por la identificación, documentación y cumplimiento de las obligaciones legales estatutarias, de reglamentación y contractuales relacionadas con la seguridad digital, como son: derechos de propiedad intelectual y el uso de software patentado, privacidad y protección de datos personales, transparencia y acceso a la información, requerimientos mínimos de seguridad, calidad y ciberseguridad para entidades vigiladas por la Superintendencia Financiera de Colombia y el marco de seguridad digital emitido por el Ministerio de las Tecnologías y las Comunicaciones – Min. TIC.

Se realizará la verificación de cumplimiento normativo con el fin de identificar posibles falencias de seguridad y optimizar o implementar controles aplicables a la operación, aspecto que es extendido para los proveedores de procesos misionales. El cumplimiento normativo se informará a la Alta Dirección con el fin de dar a conocer su estado y para que orienten la asignación de recursos para la implementación de controles.

21.1. Política de cumplimiento de requisitos legales y contractuales

La Gobernación de Santander propenderá porque el software instalado y el uso de los recursos de la plataforma tecnológica de la entidad, cumplan con los requerimientos legales y de licenciamiento aplicables. En el procedimiento de Inventario de software y hardware y control de software legal se cumplirá con los requisitos legislativos relacionados con los derechos de propiedad intelectual y uso de software patentados.

21.1.1. Normas de cumplimiento con requisitos legales y contractuales

Normas dirigidas a: LASECRETARÍA GENERAL, JURÍDICA

- Los contratos deben Incluir una cláusula donde se exija el registro del software ante la dirección nacional de derechos de autor y el contrato de cesión de derechos patrimoniales de autor, suscrito entre la persona natural y el proveedor propiedad, sobre el bien o servicio adquirido o contratado por la Gobernación de Santander.

- Se deben desarrollar cláusulas de indemnidad con el propósito de asegurar que el proveedor defienda a la entidad en sus derechos ante reclamos sobre infracciones sobre patentes (hardware) o derechos de autor (software). En el supuesto que se compruebe una infracción, deberá asegurarse una solución que no afecte los servicios de la Gobernación de Santander y la definición de los cargos por daños y perjuicios.

- En los contratos con proveedores de desarrollo se debe aclarar los derechos de explotación y propiedad de los desarrollos enumerando los derechos de explotación cedidos: reproducción, distribución, comunicación pública y transformación sobre el resultado del desarrollo a favor de la entidad.

Normas dirigidas a: LASECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Asegurar que todo el software que se ejecuta en la Gobernación de Santander cumpla con los requisitos de derechos de autor y licenciamiento de uso.

- Mantener un inventario con el software y sistemas de información que se encuentran permitidos en las estaciones de trabajo, servidores o equipos móviles de la Gobernación de Santander para el desarrollo de las actividades laborales, así como verificar periódicamente que el software instalado corresponda únicamente al permitido. Este inventario debe contener la evidencia de la propiedad de las licencias.

- Definir controles que garanticen la continuidad en el uso del software bajo el riesgo de desaparición del proveedor.

- Establecer la reserva de los derechos de propiedad intelectual, donde se plasme de forma expresa la reserva de todos los derechos existentes sobre el sitio web institucional.

- Para las aplicaciones Web de la entidad que son ejecutadas de forma remota por los usuarios, no siendo necesaria la descarga o instalación de software alguno en su equipo, se debe aclarar en la licencia de uso una protección tanto a la aplicación, como a los contenidos que son ejecutados a través de la misma.

- Definir e implementar mecanismos que impidan la instalación de software no autorizado por parte de los usuarios finales.

- Vigilar el software instalado por usuarios privilegiados como administradores de los equipos de cómputo y servidores.

Normas dirigidas a: LA OFICINA DE SEGURIDAD DIGITAL

- Emitir concepto de seguridad sobre los sistemas de información de libre distribución con la intención de ser utilizados en la Gobernación de Santander, basados en las especificaciones técnicas del producto y sus debilidades reconocidas en el mercado.

- Sensibilizar a los servidores públicos, temporales y contratista en la instalación y uso de software legal para proteger los derechos de propiedad intelectual y sus acciones disciplinarias en caso de incumplir la normativa.

Normas dirigidas a: TODOS LOS USUARIOS

- Está prohibido instalar software o sistemas de información en sus estaciones de trabajo o equipos móviles suministrados para el desarrollo de sus actividades.

- Cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software.

21.2. Política de privacidad y protección de datos personales

En cumplimiento de la de Ley 1581 de 2012, por la cual se dictan disposiciones para la protección de datos personales, la Gobernación de Santander, a través del oficial de seguridad digital, propenderá por la protección de los datos personales de sus beneficiarios, proveedores y demás terceros de los cuales reciba y administre información.

Se establecerán los términos, condiciones y finalidades para las cuales la Gobernación de Santander, como responsable de los datos personales obtenidos a través de sus distintos canales de atención, tratará la información de todas las personas que, en algún momento, por razones de la actividad que desarrolla la entidad, hayan suministrado datos personales. En caso de delegar a un tercero el tratamiento de datos personales, la Gobernación de

Santander exigirá al tercero la implementación de los lineamientos y procedimientos necesarios para la protección de los datos personales.

21.2.1. Normas de privacidad y protección de datos personales

Normas dirigidas a: LAS AREAS QUE PROCESAN DATOS PERSONALES

- Obtener la autorización para el tratamiento de estos datos con el fin de recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la entidad.

- Asegurar que solo aquellas personas que, por sus funciones, pueden tener acceso a dichos datos.

- Establecer condiciones contractuales y de seguridad a las entidades vinculadas o aliadas delegadas para el tratamiento de dichos datos personales.

- Acoger las directrices técnicas y procedimientos establecidos para el intercambio de estos datos con los terceros delegados, para el tratamiento de dichos datos personales.

- Acoger las directrices técnicas y procedimientos establecidos para enviar a los beneficiarios, proveedores u otros terceros mensajes, a través de correo electrónico y/o mensajes de texto.

Normas dirigidas a: EL RESPONSABLE DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

- Apoyar en la formulación de controles para el tratamiento y protección de los datos personales de los beneficiarios, servidores públicos, proveedores y demás terceros de la Gobernación de Santander de los cuales reciba y administre información.

- Mantener la política de tratamiento de datos personales y sus finalidades relacionadas en la autorización de datos personales vigente, actualizada y alineada con los requisitos legales vigentes.

- Asesorar en la identificación de riesgos relacionados con la privacidad y protección de datos personales a las áreas de la Gobernación de Santander.

- Identificar y reportar incidentes referentes a la protección de datos personales a la Superintendencia de Industria y Comercio.

- Capacitar y sensibilizar en los lineamientos de la ley de protección de datos personales, al personal de la Gobernación de Santander y coordinar la divulgación de estos lineamientos a los proveedores y terceras partes interesadas.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Implantar los controles necesarios para proteger la información personal de los beneficiarios, servidores públicos, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro repositorio y evitar su divulgación, alteración o eliminación sin la autorización requerida.

- Custodiar la base de datos de autorización de datos personales.

Normas dirigidas a: TODOS LOS USUARIOS

- Guardar la discreción correspondiente, o la reserva absoluta con respecto a la información de la entidad o de los beneficiarios, deudores solidarios, servidores públicos y proveedores de cual tengan conocimiento en el ejercicio de sus funciones.

- Aplicar los controles de seguridad definidos por la entidad para el suministro de información de beneficiarios y servidores públicos.

21.3. Política de cumplimiento de ley de transparencia

La Gobernación de Santander garantizará el derecho de acceso a la información pública a través de los canales habilitados por la entidad, excluyendo solo aquella que está sujeta a las excepciones constitucionales, legales y bajo el cumplimiento de los requisitos establecidos en Ley 1712 de 2014 “Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones”.

21.3.1. Normas de cumplimiento de la Ley de Transparencia

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Generar los Instrumentos de Gestión y tramitar su publicación.

Normas dirigidas a: LOS SECRETARIOS, DIRECTORES, JEFES DE OFICINA Y COORDINADORES DE GRUPO

- Actualizar periódicamente la información pública bajo su responsabilidad a través de los procedimientos establecidos en la entidad.

22. POLÍTICA DE SERVICIOS DE COMPUTACIÓN EN LA NUBE

La Gobernación de Santander propenderá por mantener la seguridad de los activos de información de la entidad, cuando se autoriza el uso de servicios de computación en la nube a fin de garantizar la disponibilidad, privacidad, confidencialidad, integridad y cumplimiento de los requisitos legales en materia de protección de información personal.

Esta política se aplicará a los servicios de computación en nube que sean utilizados o contratados por la Gobernación de Santander, así como a los procesos que hagan uso de dichos servicios. La utilización de servicios de computación en la nube con licenciamiento de carácter gratuito o abierto debe ser aprobada por el Comité de Control de Cambios.
En los contratos celebrados con proveedores de servicios de computación en la nube se debe incluir la necesidad de cumplir las políticas de seguridad digital, el cumplimiento de los acuerdos de niveles de servicio, responsabilidades legales y derechos de propiedad intelectual sobre la información, leyes y regulaciones sobre la protección de la información de la entidad e información de carácter personal.

El uso de plataformas internacionales de almacenamiento o procesamiento en la nube para datos de carácter personal deben contar con la autorización del titular de los datos. No se debe almacenar datos personales en servicios de computación en la nube sin la autorización del titular para la transmisión internacional de datos.

22.1. Normas de la Política de Servicios de Computación en la Nube

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Realizar la identificación, valoración y evaluación de los riesgos asociados al uso de servicios de computación en la nube en conjunto con la Secretaría de Tecnologías de la Información y las Comunicaciones.

- Emitir y/o evaluar controles para mitigar los riesgos de seguridad digital cuando se autorice el uso de servicios de computación en la nube para el tratamiento de información institucional, almacenamiento de información personal, protección de secretos comerciales, riesgos legales, técnicos, de continuidad y asociados a la transmisión transfronteriza de información institucional o personal.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Participar en la identificación y tratamiento de riesgos de seguridad digital asociados al uso de computación en la nube.

- Proveer servicios de copia de respaldo para la información de la Gobernación de Santander que está autorizada para almacenamiento en computación en la nube.

- Implementar controles de seguridad digital para preservar los accesos a los servicios de computación en la nube autorizados por la entidad.

- Definir e implementar plan de contingencia para preservar la información almacenada en servicios de computación en la nube.

- Mantener inventario de los servicios de computación en la nube autorizados para uso dentro de las redes corporativas.

- Mantener inventario de los usuarios a los que se les autoriza el uso de servicios de computación en la nube.

- Realizar monitoreo de seguridad digital utilizando las tecnologías de correlación aprovisionadas por la entidad.

- Asegurar que todo servicio de computación en la nube se diseñe, implemente y opere conforme a las políticas de seguridad digital y gestión de riesgo institucional.

Normas dirigidas a: LOS SUPERVISORES DE CONTRATO, SECRETARIOS, DIRECTORES, JEFES DE OFICINA Y COORDINADORES DE GRUPO

- Asegurar la existencia de Acuerdos y/o Cláusulas de Confidencialidad con proveedores de servicios de computación en la nube.

- Especificar responsabilidades sobre el uso de servicios de computación en la nube (almacenamiento y/o procesamiento) del personal a su cargo.

- Asegurar en los contratos que los proveedores disponen de capacidades para demostrar que los servicios ofrecidos cuentan con certificación en ciberseguridad emitida por ente independiente al prestador de servicios.

- Incluir el derecho de auditoría independiente al cumplimiento de seguridad y requisitos legales aplicables a la Gobernación de Santander.

Normas dirigidas a: TODOS LOS USUARIOS

- Cuando se use almacenamiento en la nube, toda información calificada como pública clasificada o pública reservada y toda información de carácter personal, debe permanecer cifrada de acuerdo con las políticas de cifrado institucional, para evitar su divulgación o acceso no autorizados.

- Solicitar ante la Secretaría de Tecnologías de la Información y las Comunicaciones la autorización de uso de servicios de computación en la nube, teniendo en cuenta para ello el uso de guía para la evaluación de necesidades de herramientas de software.

- Utilizar los servicios de computación en nube autorizados, únicamente para el cumplimiento de las funciones asignadas institucionalmente.

- Evitar el uso de servicios de computación en la nube desde equipos de cómputo de uso compartido, inseguros como café internet o centros de alquiler de equipos públicos.

- No almacenar información sujeta a derechos de autor (videos, imágenes, audio, libros, entre otros) en las cuentas de servicios de computación en la nube autorizadas para la Gobernación de Santander.

23. POLITICA DE CIBERSEGURIDAD

La Gobernación de Santander protegerá y asegurará los datos, sistemas y aplicaciones, provenientes y los que viajan, en el ciberespacio que son esenciales para la operación de la entidad, para prevenir, mitigar y disminuir los impactos negativos potenciales de amenazas o ataques cibernéticos mediante los controles tecnológicos, las políticas de seguridad digital, los procedimientos y el trabajo conjunto con entidades de apoyo en ciberseguridad y ciberdefensa.

La gestión de ciberseguridad contempla las etapas de prevención, protección y detección, respuesta y comunicación, recuperación y aprendizaje, las cuales están enfocadas a la adecuada administración de riesgos de ciberseguridad y al mejoramiento continuo de la seguridad digital.

Principios de Ciberseguridad

- Prevención: La gestión de la ciberseguridad es preventiva, para lo cual implementará controles adecuados para velar por la gestión de la ciberseguridad a través de un análisis de riesgos de sus activos de información. La función de prevención admite la capacidad de limitar o contener el impacto de un posible incidente de ciberseguridad.
- Protección y detección: La Gobernación de Santander implementará actividades apropiadas para identificar la ocurrencia de un evento de ciberseguridad.
- Respuesta: Aún con las medidas de seguridad adoptadas, la Gobernación de Santander desarrollará e implementará actividades para mitigar los incidentes relacionados con ciberseguridad y los comunica a los entes competentes.
- Recuperación: Se desarrollará e implementará actividades apropiadas para restaurar cualquier servicio que se haya deteriorado debido a un incidente de ciberseguridad, así como se busca un aprendizaje del mismo a través de un análisis de causa raíz del riesgo.

Lineamientos

- La gestión de la ciberseguridad deberá alinearse con la gestión de las TIC y las estrategias de negocio.
- Los roles y responsabilidades asociadas a la gestión de la ciberseguridad deben estar claramente definidas y aceptadas por los diferentes responsables.
- Los resultados de la gestión de ciberseguridad se deben comunicar a todas las partes interesadas pertinentes incluida la organización interna, organismos de control y terceras partes involucradas.

- La gestión de la ciberseguridad de contribuir a mantener la continuidad de las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel aceptable para la Entidad ante el evento de una interrupción significativa.
- Los procesos de recuperación ante incidentes de seguridad digital deben ser mejorados continuamente mediante las lecciones aprendidas.

Procedimientos

Los procedimientos que apoyan la Gestión de Ciberseguridad son:

- Gestionar riesgos de seguridad de la información.
- Guía metodológica de gestión de riesgos de seguridad de la información.
- Procedimiento para reportar y gestionar incidentes de seguridad de la información.
- Manual de Plan de Continuidad del Negocio.

23.1. Normas de la Política de Ciberseguridad

Normas dirigidas a: EL COMITÉ DE SEGURIDAD DE LA INFORMACIÓN

- Actualizar y presentar ante el comité institucional de gestión y desempeño, las políticas y gestión de ciberseguridad.

- Analizar los incidentes de ciberseguridad que le son escalados y activar el procedimiento de contacto con las autoridades y grupos de interés especial, cuando lo estime necesario.

Normas dirigidas a: EL OFICIAL DE SEGURIDAD DIGITAL

- Elaborar y proponer las políticas de ciberseguridad.

- La ciberseguridad se apoya en los procedimientos de gestión de riesgos e incidentes de seguridad digital, así como del Manual de Plan de Administración de Continuidad del Negocio.

- Monitorear y verificar del cumplimiento de las políticas y procedimientos en materia de ciberseguridad.

- Mediante la ejecución de un programa de capacitación y sensibilización en materia de seguridad digital, la Gobernación de Santander, preparará regularmente a sus servidores públicos y contratistas en temas relacionados con ciberseguridad para mantenerlos actualizados sobre las nuevas ciber amenazas, las políticas de seguridad, los controles, procedimientos y acciones a seguir en caso de incidentes de seguridad digital.

- Mantener actualizado al personal responsable de los riesgos de ciberseguridad para que se mantenga a la vanguardia de las nuevas modalidades de ciberataques que pudieran llegar a afectar a la entidad.

- Identificar, y en la medida de lo posible, medir, los riesgos cibernéticos emergentes que puedan llegar a afectar a la entidad y establecer controles para su mitigación.

- Gestionar los riesgos de ciberseguridad que puedan constituir riesgo cibernético.

- Proponer los controles para mitigar los riesgos que pudieran afectar la seguridad digital.

- Reportar a la alta Dirección y al Comité de Seguridad de la Información, los resultados de las gestiones adelantadas para el tratamiento de los riesgos de ciberseguridad.

- Sugerir anualmente los proyectos y/o presupuestos en materia de seguridad digital.

- Establecer la estrategia de comunicación ante incidentes de ciberseguridad a los Entes de Control.

- Proponer ajustes sus sistemas de gestión de riesgo, de seguridad digital y controles de seguridad como consecuencia de los incidentes presentados.

- Establecer y gestionar los indicadores de la seguridad digital.

- Suministrar los lineamientos para el cumplimiento de obligaciones de terceras partes.

- Informar a los consumidores financieros de la Entidad sobre las medidas de seguridad y recomendaciones que deberán adoptar para su ciberseguridad.

Normas dirigidas a: LA SECRETARÍA DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES

- Implementar, operar y mantener controles para mitigar los riesgos que pudieran afectar la seguridad digital.

- Gestionar la ciberseguridad en los proyectos que impliquen la adopción de nuevas tecnologías.

- Gestionar y documentar la seguridad de la plataforma tecnológica.

- Mantener dentro del plan de continuidad del negocio la respuesta, recuperación, reanudación de la operación en contingencia y restauración ante la materialización de ataques cibernéticos y realiza las respectivas pruebas a dicho plan

- Adoptar los mecanismos necesarios para recuperar los sistemas de información al estado en que se encontraban antes del ataque cibernético.

- Mantener actualizadas y en operación las herramientas y/o servicios que permitan hacer correlación de eventos que puedan alertar sobre incidentes de seguridad.

- Monitorear los canales de atención, volumen transaccional y número de clientes y diferentes fuentes de información tales como sitios web, blogs y redes sociales, con el propósito de identificar posibles ataques cibernéticos contra la Entidad.

- Colaborar con las autoridades que hacen parte del modelo nacional de gestión de ciberseguridad en los proyectos que se adelanten con el propósito de fortalecer la gestión de la ciberseguridad en el sector financiero y a nivel nacional.

- Gestionar las vulnerabilidades de aquellas plataformas que soporten los procesos críticos y que estén expuestos en el ciberespacio.

- Monitorear continuamente la plataforma tecnológica con el propósito de identificar comportamientos inusuales que puedan evidenciar ciberataques contra la Entidad.

- Aplicar el procedimiento de gestión de incidentes cuando se presenten incidentes de seguridad digital, identificando los dispositivos que pudieran haber resultado afectados.

- Preservar cuando sea factible, las evidencias digitales para que las autoridades puedan realizar las investigaciones correspondientes.

Normas dirigidas a: SECRETARIA GENERAL - JURÍDICA

- Incluir en los contratos que se celebren con terceros que harán parte de los procesos operativos, las medidas y obligaciones pertinentes para la adopción y el cumplimiento de políticas para la gestión de los riesgos de seguridad digital.

Normas dirigidas a: SUPERVISORES DE CONTRATOS CON TERCEROS

- Verificar el cumplimiento de las obligaciones y medidas establecidas para la adopción y el cumplimiento de políticas de seguridad digital.

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