República de Colombia

Gobernación de Santander

MANUAL DE POLÍTICAS ESPECÍFICAS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1. INTRODUCCIÓN

En la actualidad, la información es uno de los activos más valiosos de cualquier entidad. A medida que las tecnologías de la información se integran cada vez más en los procesos de una Entidad, se vuelve importante establecer lineamientos claros para el control y la protección de estos activos, especialmente en cuanto a la confidencialidad, integridad y disponibilidad de la información.

La transformación digital trae a las Entidades numerosos beneficios, como la mejora en la eficiencia operativa y la toma de decisiones basada en datos. Sin embargo, también ha incrementado los riesgos asociados al uso de la información, incluyendo amenazas en el ciberespacio, la pérdida de datos y accesos no autorizados. Por lo tanto, es esencial implementar políticas robustas de seguridad digital y privacidad que no solo protejan la información, sino que también garanticen la continuidad del negocio y la confianza de los ciudadanos en los servicios ofrecidos por la Entidad.

Este documento ofrece una visión general de los requisitos de Seguridad Digital y Privacidad de la Información que deben cumplirse en el Departamento de Santander. Estos lineamientos están diseñados para asegurar que todas las dependencias del Departamento de Santander adopten prácticas seguras en el manejo de su información, fomentando una cultura de seguridad que minimice riesgos y promueva la responsabilidad compartida entre todos los usuarios de la Entidad. Al seguir estas políticas, buscamos proteger la información con alto nivel de sensibilidad y asegurar que los servicios proporcionados sean confiables y resilientes frente a posibles amenazas.

2. OBJETIVO

Establecer las Políticas de Seguridad Digital y Privacidad de la Información para el Departamento de Santander con el fin preservar la confidencialidad, integridad y disponibilidad de la información y de los activos asociados, fortaleciendo así los procesos de la Entidad en un entorno de confianza digital de acuerdo a los lineamientos establecidos por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) a través del Modelo de Seguridad y Privacidad de la Información (MSPI).

3. ALCANCE Y APLICABILIDAD

Este Manual de Políticas de Seguridad Digital y Privacidad de la Información abarca los aspectos de privacidad, acceso, autenticación, mantenimiento y divulgación relacionados con cualquier activo de información. Estas políticas son de cumplimiento y aplicación obligatoria para todo el personal, proveedores, contratistas y aplicaciones tecnológicas vinculadas al Departamento de Santander.

4. DEFINICIONES

Activo de información: Son datos o conocimientos que, debido a su importancia para las actividades del Departamento de Santander, se consideran bienes valiosos que deben ser protegidos. Según la norma ISO/IEC 27001, se define como "conocimientos, datos o información que una organización o entidad valora y, por lo tanto, debe proteger". Los activos de información pueden existir en forma física, como archivos impresos, libros, personas y CDs, o en forma lógica, como aplicaciones, bases de datos, archivos en Word, Excel, PDF, fotografías y videos.

Administradores y operadores de los sistemas y servicios de información: Personas responsables de administrar, controlar, supervisar y garantizar la operatividad y funcionalidad de los sistemas y servicios informáticos.

Ambiente de Desarrollo: Entorno tecnológico establecido puntualmente para proporcionar servicios integrales al desarrollo y elaboración de código fuente para la implementación de sistemas y servicios de información.

Ambiente de Producción: Entorno tecnológico establecido para la operación diaria de los sistemas y servicios de información de cara a los Usuarios del Departamento de Santander.

Ambiente de Pruebas: Entorno tecnológico establecido para la ejecución de pruebas a los sistemas y servicios de información.

Amenaza [Según ISO 27000]: Causa potencial de un incidente no deseado, que puede provocar daños a la información, a un sistema o a la Entidad, por ejemplo, un incendio, una inundación, deficiencia en el suministro de energía o algún usuario malintencionado.

Centros de procesamiento de datos: Es la instalación encargada del procesamiento sistematizado de datos e información. Este procesamiento se realiza mediante el uso de computadoras (hardware) y programas (software) necesarios para cumplir con dicha tarea. En el Departamento de Santander, el DataCenter está a cargo de la Dirección de Sistemas de Información.

Ciclo de vida de un activo: Comprende todas las actividades realizadas sobre un activo de información desde su creación hasta su disposición final, asegurando su uso adecuado a lo largo de su existencia.

Cifrado: Proceso que convierte texto legible en texto ilegible mediante algoritmos matemáticos. Se utiliza para proteger la confidencialidad de la información crítica para la entidad.

ColCERT: es el Grupo de Respuesta a Emergencias Cibernéticas de Colombia, encargado de coordinar la Ciberseguridad y Ciberdefensa a nivel nacional. Está integrado dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su principal objetivo es coordinar acciones para proteger la infraestructura crítica

del Estado colombiano ante emergencias de Ciberseguridad que puedan comprometer la seguridad nacional y la defensa del país.

Comité Institucional de Gestión y Desempeño: es un órgano creado en el Departamento de Santander según el Decreto 494 de 2018. Su función principal es dirigir, coordinar y ejecutar las acciones y estrategias para implementar, operar, desarrollar, evaluar y dar seguimiento al modelo integrado de planeación y gestión, conocido como MIPG, a nivel institucional.

Confidencialidad: Esta propiedad asegura que la información solo esté disponible y sea revelada a individuos, entidades o procesos autorizados. En seguridad digital, proteger la confidencialidad implica evitar que personas no autorizadas accedan a la información.

Contraseña: Es una forma de autenticación privada compuesta por números, letras y caracteres especiales. Permite al usuario acceder a una computadora, archivo o programa específico.

CSIRT: Centro de respuesta para incidentes de seguridad en tecnologías de la información: Ofrece acompañamiento y apoyo a entidades estatales mediante un portafolio de servicios. Su objetivo es mejorar los procesos de seguridad de la infraestructura tecnológica, gestionar incidentes cibernéticos y fomentar la conciencia en seguridad digital.

Custodio del activo de información: Es responsable de administrar y aplicar los controles de seguridad definidos por el dueño o propietario del activo. Esto incluye realizar copias de respaldo (backups), gestionar privilegios de acceso, modificación y borrado, identificar posibles incidentes relacionados con el activo, entre otras funciones.

Disponibilidad: Esta propiedad asegura que la información sea accesible y utilizable por usuarios autorizados cuando sea necesario. En seguridad digital, proteger la disponibilidad implica garantizar que la información esté disponible para usuarios autorizados cuando lo necesiten.

Dispositivo móvil: Es un dispositivo electrónico portátil capaz de almacenar y procesar información. Comparte funciones similares a los dispositivos de uso fijo, como trabajo en red, acceso a Internet, correo electrónico y gestión de archivos. Para fines de este documento, se consideran dispositivos móviles: computadoras portátiles, teléfonos móviles, tabletas, entre otros.

Dispositivos de almacenamiento externo: Son dispositivos utilizados para almacenar volúmenes de información fuera de la computadora principal. Ejemplos de estos dispositivos incluyen memorias USB, discos duros externos, CDs, DVDs, entre otros.

Dueño o propietario del activo de información: Se refiere a la persona responsable de la gestión de un activo de información. Este individuo debe garantizar que el activo esté protegido adecuadamente y debe conocer su valor, sensibilidad y relevancia para la entidad. En el Departamento de Santander, esta responsabilidad se delega a los cargos con roles directivos.

Evento de Seguridad de la información: Actividad que indica cualquier ocurrencia relacionada con los activos o el entorno que indique un posible compromiso de las políticas o la falla de los controles.

Firma Digital: En la transmisión de mensajes telemáticos y gestión de documentos electrónicos, la firma digital es un método criptográfico que vincula la identidad de una persona o equipo informático con el mensaje o documento.

Incidente de seguridad digital y privacidad de la información: Se refiere a uno o más eventos de seguridad digital que comprometen las operaciones de la entidad y la seguridad de la información que maneja. A diferencia de un simple evento, un incidente tiene el potencial de afectar negativamente a la entidad y comprometer la seguridad de su información.

Información pública clasificada: Se refiere a la información que, aunque está en poder o custodia de un sujeto obligado en su calidad de tal, pertenece al ámbito propio, particular y privado o semi-privado de una persona natural o jurídica. Su acceso puede ser negado o exceptuado, siempre que se trate de circunstancias legítimas y necesarias y se respeten los derechos particulares o privados consagrados en el artículo 18 de la Ley 1712 de 2014. Para el Departamento de Santander, se entiende como información pública clasificada aquella que se genera y procesa diariamente y que puede ser compartida libremente con otros procesos internos de la entidad.

Información pública reservada: Se refiere a la información que, aunque está en poder o custodia de un sujeto obligado, es exceptuada del acceso público debido al daño que podría causar a intereses públicos. Esto debe cumplir con los requisitos establecidos en el artículo 19 de la Ley 1712 de 2014. Para el Departamento de Santander, la información pública reservada es aquella que, por su nivel de confidencialidad, solo puede ser accedida por un grupo reducido de personas. Esta información puede generarse en el día a día, pero no puede ser compartida libremente con otros procesos internos de la entidad ni con la ciudadanía, a menos que un requerimiento legal lo obligue.

Información pública: Es toda información que un sujeto obligado genere, obtenga, adquiera, o controle en su calidad de tal; para efectos del Departamento de Santander, es la información que por su nivel de confidencialidad u obligación legal puede ser compartida a toda la ciudadanía.

Integridad: Esta propiedad asegura la exactitud y estado completo de los activos. En seguridad digital, proteger la integridad de la información implica garantizar que solo sea modificada por usuarios autorizados cuando sea necesario.

Internet: Conjunto de redes conectadas, que utilizan el protocolo TCP/IP para comunicarse entre sí, a través de ellas, se tiene acceso a servicios digitales en el ciberespacio.

Ley 1712 de 2014: Ley de transparencia y del derecho de acceso a la información pública nacional, busca regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

Llaves criptográficas: Son códigos o algoritmos generados automáticamente. Su principal función es asociar la identidad de una persona o equipo informático a un documento o privilegio específico.

Malware: Se refiere a código malicioso o programas diseñados para causar daños o infiltrarse de manera no autorizada en sistemas o servicios de información.

No Repudio: No repudio es un atributo utilizado para demostrar la participación de un emisor al transmitir mensajes de datos. Este concepto asegura que se pueda verificar con certeza quién envió un mensaje, sin que el emisor pueda posteriormente negar haberlo enviado.

Política: Es un documento que contiene instrucciones que son obligatorias y que guían la manera como una Entidad debe prevenir, proteger y manejar sus riesgos relacionados.

Registro de eventos: Es el registro de todas las actividades que se ejecuten sobre los Sistemas y servicios de información.

Responsable del Usuario: Este rol corresponde a los funcionarios que tienen la responsabilidad en el Departamento de Santander, como el Gobernador, los Secretarios de Despacho, los directores y los Jefes de Oficina o Dependencia. Para los contratistas, el responsable incluye al Gobernador, Secretarios de Despacho, Directores, Jefes de Oficina o Dependencia, o al Supervisor de Contrato.

Servicios de almacenamiento en la nube: Son servicios donde los datos se almacenan, gestionan y respaldan de manera remota, generalmente en servidores alojados en la nube y administrados por un proveedor de servicios, como por ejemplo, OneDrive.

Servidores públicos: Persona que trabaja para el estado, desempeñando funciones públicas en beneficio del estado y la comunidad.

Servidor: Es una computadora que comparte recursos con otras computadoras conectadas a través de una red. Su principal función es proporcionar servicios tecnológicos a los usuarios.

Sistema Operativo: Es un programa o conjunto de programas que permiten gestionar los recursos de hardware y software de una computadora, servidor o dispositivo móvil. Es fundamental ya que es el encargado de hacer funcionar el hardware.

Sistemas y servicios de información: Son componentes relacionados con las tecnologías de la información y las comunicaciones. Estos pueden ser físicos, como servidores, redes, discos duros, teléfonos, impresoras y computadoras, así como lógicos, como aplicaciones, bases de datos y sistemas operativos.

Terceros: Se refiere a cualquier persona, ya sea jurídica o natural, que no forme parte del Departamento de Santander, pero que tenga algún tipo de relación contractual con la

entidad, como proveedores, contratistas o consultores, y que provean servicios o productos a la misma.

Trabajo en casa: Esta modalidad de trabajo ocasional, diferente al teletrabajo o trabajo remoto, permite a los servidores públicos o trabajadores del sector privado realizar temporalmente sus funciones o actividades laborales fuera de su ubicación habitual.

Usuarios: Se considera usuario a cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo que acceda a los activos de información del Departamento de Santander. Esto incluye a funcionarios de carrera administrativa y de libre nombramiento, temporales, practicantes, contratistas, personal de empresas proveedoras de servicios y aplicaciones que utilicen servicios o información de la entidad, ya sea en formato físico o digital.

Virus: Es un tipo de software malicioso diseñado para alterar el funcionamiento normal de una computadora. Los virus reemplazan programas ejecutables sin la autorización ni el conocimiento del usuario.

Vulnerabilidad [Según ISO 27000]: Debilidad de un activo o control que puede ser explotada por una o más amenazas.

5. COMPROMISO DE LA ALTA DIRECCIÓN

En el Departamento de Santander, la alta dirección la representa el Comité Institucional de Gestión y Desempeño, encargado de guiar la implementación y operación del Modelo Integrado de Planeación y Gestión (MIPG). Este comité aprueba las Políticas de Seguridad Digital y Privacidad de la Información, demostrando su compromiso y apoyo para diseñar e implementar prácticas efectivas que aseguren la seguridad digital y la privacidad de la información de la entidad.

La Alta Dirección del Departamento de Santander demuestra su compromiso a través de:

- La revisión y aprobación de las Políticas de Seguridad Digital y Privacidad de la Información.
- La promoción activa de una cultura de seguridad.
- La divulgación de este manual a todos los servidores públicos, personal externo y proveedores de la Entidad.
- El Apoyo a la gestión de riesgos de seguridad digital y protección de los activos de información críticos.
- El aseguramiento de los recursos adecuados para implementar y mantener las políticas de Seguridad Digital y Privacidad de la Información.
- Aprobación y seguimiento a los procedimientos, planes, programas, proyectos, estrategias y herramientas necesarios para la implementación interna del presente manual de políticas de Seguridad Digital y Privacidad de la Información.
- La verificación del cumplimiento de las políticas aquí mencionadas.

6. CUMPLIMIENTO DE LAS POLÍTICAS

El incumplimiento de las Políticas de Seguridad Digital y Privacidad de la Información se maneja mediante procedimientos administrativos que pueden resultar en acciones disciplinarias, judiciales o administrativas, dependiendo de la gravedad y las circunstancias de la falta en términos de modo, tiempo y lugar.

En este sentido:

- Todas las violaciones comprobadas a estas políticas por parte de funcionarios públicos serán remitidas a la Oficina de Control Disciplinario del Departamento de Santander.
- En el caso del personal contratista y las empresas proveedoras, se aplicarán investigaciones y sanciones de acuerdo con las cláusulas establecidas en el contrato correspondiente.

7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

A continuación, se presentan las políticas específicas de Seguridad Digital y Privacidad de la Información que son aplicables en el Departamento de Santander y que todos los usuarios deben cumplir:

7.1. PARA LOS ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN

7.1.1. Objetivo

Establecer las funciones y responsabilidades de las dependencias clave en la protección de los activos de información del Departamento de Santander.

7.1.2. Alcance

Aplicable a todos los usuarios involucrados en todas las actividades de operación, gestión y administración de la Seguridad Digital y Privacidad de la Información en el Departamento de Santander.

7.1.3. Descripción

A continuación, se establecen los lineamientos para la asignación de responsabilidades para la Seguridad Digital y Privacidad de la Información:

De la Alta Dirección:

- Aprobar las modificaciones o las nuevas Políticas de Seguridad Digital y Privacidad de la Información como muestra de compromiso y apoyo al diseño e implementación de políticas eficientes que aseguren la seguridad de la información de la Entidad.
- Definir y establecer roles y responsabilidades relacionados con la Seguridad Digital y Privacidad de la Información a nivel directivo y operativo.
- Autorizar el uso de metodologías y procesos específicos para la seguridad de la Información.
- Fomentar activamente una cultura de Seguridad Digital y Privacidad de la Información en la Entidad.
- Aprobar la asignación de recursos, infraestructura física y personal que se requiera para el cumplimiento y la gestión de la Seguridad Digital y Privacidad de la Información.
- Proponer ajustes y mejoras en materia de Seguridad Digital y Privacidad de la Información para la Entidad.

De los Usuarios:

- Conocer, cumplir y difundir las políticas, normas, procedimientos y estándares relativos a la Seguridad Digital y Privacidad de la Información.

- Mantener en estricta confidencialidad la información a la que se tenga acceso y abstenerse de compartirla o modificarla sin autorización.
- Acceder únicamente a la información para la cual se cuente con los permisos necesarios y que sea indispensable para el desempeño de sus funciones.
- Informar cualquier incidente o evento de seguridad que ocurra durante el ejercicio de sus funciones.
- Participar en sesiones de capacitación sobre Seguridad Digital y Privacidad de la Información organizadas por la Entidad.
- Aplicar los controles que sean establecidos para la Gestión de Riesgos de Seguridad Digital.
- Utilizar exclusivamente los medios proporcionados por el Departamento de Santander para el manejo de la información institucional, abstenerse de utilizar cuentas personales de correo electrónico, almacenamiento en la nube u otros medios similares.

De la Dirección de Gobierno Digital:

- Establecer, implementar, mantener y mejorar continuamente toda la documentación relacionada con la gestión de Seguridad Digital y Privacidad de la Información del Departamento de Santander.
- Garantizar la actualización de las políticas según las necesidades y requisitos de la Entidad.
- Asesorar la gestión de riesgos y la implementación de controles de seguridad digital en las dependencias pertinentes.
- Gestionar el respaldo de la alta dirección para cumplir los principios y objetivos que apoyen la administración y desarrollo de iniciativas sobre gestión de seguridad digital y privacidad de la información.
- Asesorar, guiar y capacitar a los Usuarios de los procesos en buenas prácticas de Seguridad Digital y Privacidad de la Información.
- Mantener comunicación con autoridades y grupos de interés especializados (como colCERT, CSIRT) para reportar incidentes de Seguridad Digital y Privacidad de la Información.

7.2. PARA EL USO DE DISPOSITIVOS MÓVILES Y EL TRABAJO EN CASA

7.2.1. Objetivo

Proteger la información del Departamento de Santander almacenada o accesible desde dispositivos móviles, previniendo la infección o distribución de malware mediante su uso; asegurando la seguridad, integridad y confidencialidad de la información manejada a través de conexiones remotas a los recursos informáticos y la infraestructura tecnológica de la Entidad.

7.2.2. Alcance

Esta política se aplica a todos los usuarios que, mediante el uso de dispositivos móviles institucionales o personales, acceden a información del Departamento de Santander por iniciativa propia o debido a las funciones específicas de su cargo o a obligaciones

contractuales que requieren acceso remoto a los recursos informáticos y la infraestructura tecnológica de la Entidad.

7.2.3. Descripción

A continuación, se presentan los lineamientos para el uso de dispositivos móviles propiedad del Departamento de Santander y que sean entregados a los usuarios, se debe:

- Registrar e inventariar todos los dispositivos móviles de manera centralizada.
- Designar un responsable (funcionario, contratista o líder de proceso) para garantizar la protección física y lógica del dispositivo, así como su entrega o devolución a la Entidad.
- Reportar cualquier incidencia con los dispositivos móviles de forma inmediata.
- Implementar bloqueo mediante contraseña u otro método robusto de autenticación.
- Instalar y mantener actualizado un antivirus en los dispositivos.
- Utilizar sistemas operativos obtenidos de canales oficiales o instalados de fábrica.
- Establecer una reutilización o baja segura de los dispositivos, asegurando la eliminación completa y segura de la información sensible previamente almacenada.
- Evitar el almacenamiento de información personal sensible según los términos establecidos en la Ley 1581 de 2012 sobre protección de datos personales.
- Facilitar la revisión del cumplimiento de esta política por parte de la Secretaría de las TIC directamente en los dispositivos móviles propiedad de la Entidad.

Deberes relacionados con el uso de dispositivos móviles personales o proveedores que accedan a la información o utilicen recursos tecnológicos del Departamento de Santander:

El acceso a los recursos y/o servicios TIC desde dispositivos móviles del Departamento de Santander está disponible para cualquier usuario a quien se le haya asignado este privilegio, por ejemplo, el acceso al correo electrónico institucional a través del celular.

El acceso es una decisión voluntaria y propia del usuario y no implica que el Departamento de Santander deba dar soporte técnico o asistencia a los dispositivos móviles personales utilizados para este fin. Por lo tanto, el usuario asume la responsabilidad completa ante el Departamento de Santander por cualquier situación, evento o incidente de seguridad digital que se derive de dicho acceso. Asimismo, si el usuario decide acceder a recursos y/o servicios TIC desde su dispositivo móvil personal, deberá como mínimo:

- Instalar aplicaciones antivirus licenciadas.
- Configurar un bloqueo mediante contraseña u otro método robusto de autenticación.
- Evitar almacenar información sensible o datos personales del Departamento de Santander en dispositivos móviles personales o de proveedores.
- Cumplir estrictamente con todos los numerales definidos en este documento para los dispositivos móviles personales o de proveedores que accedan a la información del Departamento de Santander.

Para el trabajo desde casa:

Al momento que un usuario por alguna razón deba realizar trabajo desde casa, este debe:

- Establecer y asegurar un entorno seguro y controlado para evitar el acceso de personas ajenas a la Entidad a la información del Departamento de Santander.
- Permitir la auditoría técnica de los equipos de cómputo utilizados para el trabajo en casa.
- Solicitar acceso remoto o VPN a los recursos tecnológicos del Departamento de Santander, en caso de ser necesario, a la Dirección de Sistemas de Información y obtener el visto bueno del secretario del área correspondiente.
- Garantizar el uso de la información accedida y gestionada de forma remota conforme a las funciones del cargo o a las obligaciones contractuales.
- Mantener la seguridad mínima en la red de internet utilizada para la conexión remota, evitando el uso de redes públicas.
- Mantener actualizado el antivirus en todos los dispositivos utilizados para el trabajo remoto.
- Bloquear la pantalla cada vez que el usuario se ausente temporalmente de su puesto de trabajo.
- Resguardar y almacenar la información propiedad del Departamento de Santander en los recursos tecnológicos proporcionados por la entidad, evitando el uso de dispositivos de almacenamiento externo o servicios gratuitos de almacenamiento en la nube (como Dropbox, Google Drive, WeTransfer o similares).
- Compartir y almacenar información del Departamento de Santander exclusivamente a través de los servicios de almacenamiento en la nube y/o el correo electrónico institucional proporcionados por la entidad.

7.3. ESCRITORIO LIMPIO Y PANTALLA LIMPIA

7.3.1. Objetivo

Establecer lineamientos para el manejo de información por parte de los usuarios en sus escritorios físicos y para el manejo seguro de medios de almacenamiento en el Departamento de Santander

7.3.2. Alcance

Esta política es aplicable a todos los usuarios que, mediante la utilización de documentación impresa y medios de almacenamiento que contengan información del Departamento de Santander, utilicen dicha información en el ejercicio de sus funciones específicas o por obligaciones contractuales.

7.3.3. Descripción

- En búsqueda de mitigar el riesgo de acceso no autorizado, pérdida y daño de la información durante el horario laboral, se establece que no deben ubicarse sin supervisión medios de almacenamiento (CDs, DVDs, cintas, memorias USB) ni documentos físicos

sobre el escritorio o puesto de trabajo cuando no estén en uso. Estos deberán quedar bajo llave en gabinetes o archivadores seguros.

- Todos los equipos de cómputo, impresoras y escáneres de la entidad deberán apagarse o ponerse en estado de suspensión cuando no estén en uso. Además, se deberán retirar los documentos de las impresoras y no dejarlos sin protección.
- Bloquear o suspender el equipo (instrucción: + L). Utilizar protector de pantalla protegido con contraseña para que el bloqueo sea automático después de unos minutos de inactividad (entre tres y cinco minutos es razonable).
- Para todos los usuarios de las aplicaciones y sistemas de información de la Entidad, es obligatorio que las sesiones sean cerradas al finalizar las actividades y no se deben dejar abiertas o desatendidas.
- Salir de todas las aplicaciones y apagar los equipos de cómputo y otros equipos de hardware al finalizar las actividades diarias.
- Destruir el papel que contenga información con alto nivel de sensibilidad antes de reciclar y evitar reutilizar documentos impresos de este carácter.
- Crear e implementar el bloqueo automático de las sesiones de los usuarios en los equipos de cómputo después del tiempo de inactividad establecido.

7.4. PARA LA SEGURIDAD LIGADA A LOS RECURSOS HUMANOS

7.4.1. Objetivo

Establecer lineamientos para tener en cuenta durante todo el ciclo de gestión estratégica del talento humano y definir las responsabilidades de los usuarios en la protección de los activos de información en el Departamento de Santander.

7.4.2. Alcance

Esta política es aplicable a todos los usuarios que tengan relación laboral con el Departamento de Santander, incluyendo servidores públicos, contratistas, practicantes y partes externas que, dentro de sus funciones legales y contractuales, tengan acceso a las instalaciones, la información y los servicios tecnológicos propiedad de la entidad.

7.4.3. Descripción

A continuación, los lineamientos para la Seguridad Digital y Privacidad de la Información en la gestión del talento humano, se debe:

- Realizar la verificación de antecedentes disciplinarios, policiales y fiscales, así como validar la veracidad de la información proporcionada por los funcionarios en sus hojas de vida.
- Validar y documentar la experiencia laboral y académica de los aspirantes y candidatos a cargos públicos dentro de la Entidad.
- Garantizar que todos los funcionarios públicos firmen un acuerdo de confidencialidad al momento de su vinculación, que especifique sus responsabilidades con respecto a la Seguridad Digital y Privacidad de la Información. Este acuerdo debe incluir la aceptación y

cumplimiento obligatorio de las políticas establecidas, especialmente para aquellos que manejen información sensible o tengan acceso a sistemas tecnológicos.

- Informar a todo el personal sobre las políticas vigentes, señalando que el incumplimiento o violación será considerado una falta grave y remitido a la Oficina de Control Disciplinario del Departamento de Santander para iniciar las investigaciones y aplicar las sanciones correspondientes según las normativas estatales.
- Obtener el consentimiento explícito de los funcionarios públicos para el tratamiento de sus datos personales de acuerdo con la Ley 1581 de 2012 y la política de tratamiento de datos personales adoptada por la Entidad. Esto incluye informar claramente sobre la recolección, uso y derechos que tienen como titulares de los datos, como el derecho a actualizar o rectificar la información.
- Realizar formaciones continuas y capacitaciones en Seguridad Digital y Privacidad de la Información para los funcionarios de carrera administrativa, formalizándolas a través del Plan Institucional de Capacitaciones (PIC) de la Entidad.
- Comunicar de manera oficial cualquier actualización sobre responsabilidades en Seguridad Digital y Privacidad de la Información cuando haya cambios de cargo o reasignaciones contractuales.
- Asignar recursos económicos y humanos específicos para fortalecer la Seguridad Digital y Privacidad de la Información en la Entidad, buscando siempre cumplir con los estándares y normas nacionales e internacionales.

7.5. PARA LA GESTIÓN DE ACTIVOS

7.5.1. Objetivo

Definir los lineamientos para la gestión, y protección de los activos de información del departamento de Santander, con el fin de determinar los activos que posee la Entidad, cómo deben ser utilizados, las responsabilidades que tienen los Usuarios sobre los mismos y, el nivel de clasificación de la información que a cada uno de ellos debe tener.

7.5.2. Alcance

La gestión de activos de información aplica a todos los procesos estratégicos, misionales, de control y seguimiento, así como de apoyo en el Departamento de Santander. Este proceso comienza con la identificación de los activos de información y la asignación de su propiedad, seguido de su clasificación y la gestión que los usuarios deben realizar para su protección, basada en su nivel de riesgos.

7.5.3. Descripción

Toda la información, archivos físicos, sistemas, servicios, y los equipos (ej. estaciones de trabajo, portátiles, impresoras, redes, Internet, correo electrónico, herramientas de acceso remoto, aplicaciones, teléfonos, entre otros) son activos de información propiedad del Departamento de Santander, y se proporcionan a los usuarios para el desarrollo de sus funciones en la Entidad.

A continuación, los criterios establecidos para la gestión de activos de información en el Departamento de Santander, se debe:

- Realizar y mantener actualizado un inventario de activos de información de toda la Entidad.
- Asignar un propietario o dueño del activo de información, que se encargará de gestionarlo adecuadamente durante su ciclo de vida. Este deberá asegurar que los activos estén inventariados, clasificados y protegidos de manera apropiada. Deberá también garantizar que se apliquen restricciones y clasificaciones de acceso según la criticidad del activo, y asegurar el manejo adecuado del activo cuando sea eliminado o destruido.
- Garantizar que se devuelvan todos los activos del Departamento de Santander que estén bajo responsabilidad de los Usuarios al finalizar su empleo, contrato o asignación de labores.
- Clasificar la información de acuerdo con los niveles definidos en la ley 1712 de 2014. Los niveles de clasificación para el Departamento de Santander son los siguientes: Información pública (bajo), Información pública clasificada (medio) e Información pública reservada (alto).
- Promover el almacenamiento seguro de información digital, usando para esto los medios institucionales como el SharePoint, OneDrive, carpetas compartidas, etc.
- Evitar cuando sea posible el almacenamiento en medios removibles para el intercambio de la información, como, por ejemplo, USB, Discos Duros.
- Realizar la disposición segura de los medios electrónicos cuando ya no sean necesarios, garantizando un mínimo riesgo de fuga de información.
- Realizar borrado seguro a los dispositivos utilizados para el almacenamiento de copias de respaldo que contienen Información pública clasificada o Información pública reservada y que deban darse de baja.
- Destruir controladamente los dispositivos dañados o inservibles que contengan información sensible, como información pública clasificada o información pública reservada.
- Proteger los medios tangibles como papel, archivos, carpetas o presentaciones cuando se utilicen para trasportar información, esta deberá ser protegida según su nivel de clasificación, restringiendo el acceso a la misma de personas no autorizadas.

7.6. PARA EL CONTROL DE ACCESO

7.6.1. Objetivo

Establecer elementos que aseguren un acceso controlado a la información y definir los privilegios necesarios para el acceso a los servicios tecnológicos del Departamento de Santander, con el fin de evitar el uso o acceso no autorizado, adulteración, pérdida o fuga de información.

7.6.2. Alcance

La presente política y las directrices definidas son aplicables para todos los Usuarios que en el marco de sus funciones deban acceder a los sistemas de información, bases de datos, sistemas operativos y en general a todos los activos de información de la Departamento de Santander.

7.6.3. Descripción

A continuación, se presentan los criterios establecidos para el control de acceso en el Departamento de Santander, que se deben cumplir:

- Proteger y gestionar el ciclo de vida del acceso de los usuarios a los sistemas y servicios de información, verificando desde la autorización inicial hasta la baja definitiva por desvinculación laboral, cambio de cargo o reasignación de funciones.
- Establecer el control de acceso a los activos de información basado en el principio del mínimo privilegio, asignando únicamente los permisos suficientes y necesarios para el desempeño de las funciones.
- Definir e implementar controles robustos de autenticación para el acceso a los sistemas y servicios de información, incluyendo técnicas como reglas de complejidad de contraseñas, autenticación multifactor, longitud mínima de contraseña y uso de datos biométricos, especialmente para los activos de información con alto nivel de criticidad.
- Establecer y documentar procedimientos que garanticen la entrega segura y controlada de credenciales de acceso, preservando su confidencialidad.
- Ejecutar tareas permanentes de monitoreo de las redes para detectar posibles accesos no autorizados o comportamientos inusuales en el tráfico de red.
- Establecer y ejecutar procesos de revisión de todos los sistemas y servicios de información por parte de los propietarios de los activos, en conjunto con el custodio de los mismos, para identificar e inhabilitar usuarios redundantes, innecesarios o inactivos.
- Definir e implementar un registro documental de todas las solicitudes y autorizaciones de acceso otorgadas en los sistemas y servicios de información, que sirva como soporte para futuros requerimientos de los entes de control o revisiones de incidentes.
- Garantizar que las credenciales de acceso definidas por defecto por los fabricantes de dispositivos, equipos tecnológicos, sistemas y servicios de información sean cambiadas antes de su paso a producción.
- Comunicar explícitamente a todos los usuarios que las contraseñas de acceso a los sistemas de información y servicios tecnológicos son personales e intransferibles, y que toda acción ejecutada será responsabilidad del usuario a quien se le haya asignado.
- Establecer una relación única entre los usuarios y sus identificadores asignados, para que no puedan reasignarse ni reutilizarlos.
- Implementar un mecanismo para el cambio de contraseña de acceso a los diferentes sistemas y servicios tecnológicos, que contemple la ejecución del cambio cada 3 meses o menos, según la criticidad de la información a la que se accede.
- Establecer auditoría periódica para cuentas privilegiadas que permita identificar, deshabilitar y/o eliminar cuentas de usuarios con privilegios redundantes, en desuso o con reducción de privilegios.
- Renovar las contraseñas de los diferentes sistemas y servicios tecnológicos en un periodo máximo de 90 días
- Gestionar la solicitud de creación o modificación de acceso a los sistemas y servicios tecnológicos a través del procedimiento establecido, el cual debe estar siempre autorizado por el responsable del usuario.

7.7. PARA EL USO DE CIFRADO

7.7.1. Objetivo

Garantizar el uso adecuado y eficaz de los controles criptográficos para proteger la confidencialidad, autenticidad, integridad y el no repudio de la información pública y reservada, tanto en almacenamiento como en tránsito.

7.7.2. Alcance

Toda la información digital que, según su clasificación, requiera protegerse, para mantener la confidencialidad, autenticidad e integridad y donde se puedan aplicar controles criptográficos.

7.7.3. Descripción

A continuación, los lineamientos establecidos para la protección de información a través del cifrado, se debe:

- Promover el uso apropiado y eficaz de la criptografía para asegurar la confidencialidad, autenticidad e integridad de la información.
- Implementar controles criptográficos basados en el riesgo del activo de información a proteger, de acuerdo con su nivel de sensibilidad, exposición y la posibilidad de aplicación.
- Gestionar y generar llaves criptográficas mediante mecanismos tecnológicos diseñados para tal fin.
- Utilizar controles criptográficos para proteger las claves utilizadas por los usuarios en sistemas, datos y servicios, así como para la transmisión y almacenamiento de información clasificada como pública reservada.
- Utilizar firmas digitales a través de una entidad certificadora acreditada para garantizar el no repudio del firmante.
- Promover el uso adecuado y eficaz de la criptografía para asegurar la confidencialidad, autenticidad e integridad de la información.

7.8. PARA LA SEGURIDAD FÍSICA Y AMBIENTAL

7.8.1. Objetivo

Establecer lineamientos para prevenir el acceso físico no autorizado a todas las instalaciones del Departamento de Santander mediante la implementación de mecanismos y controles de seguridad física y ambiental. Incluir los centros de procesamiento de datos y todas las áreas que alojen activos de información destinados al almacenamiento y

procesamiento de información sensible. Aplicar controles específicos para evitar robos, daños o accesos no autorizados.

7.8.2. Alcance

Los lineamientos establecidos en la política aplican para los funcionarios, contratistas, proveedores y visitantes que ingresen a las instalaciones físicas del Departamento de Santander y sus sedes alternas, y a todas las áreas seguras donde se custodie y procese información sensible y a las dependencias donde haya activos de información catalogados con alto nivel de criticidad.

7.8.3. Descripción

A continuación, los criterios establecidos para la prevención y control en el acceso físico, en el Departamento de Santander, se debe:

- Delimitar las áreas y perímetros de seguridad con controles adecuados basados en los resultados del proceso de gestión de riesgos implementado en la entidad.
- Garantizar que las edificaciones o áreas dentro del perímetro de seguridad, que contengan activos de información para almacenamiento o procesamiento, cuenten con estructuras sólidas, asegurando que las puertas y ventanas tengan mecanismos de protección contra accesos no autorizados.
- Asegurar que el centro de procesamiento de datos y los centros de cableado cuenten con sistemas de control de acceso adecuados, tales como tarjetas de proximidad, autenticación biométrica, monitorización por circuito cerrado de televisión, cerraduras de seguridad y/o alarmas de detección de intrusos.
- Garantizar que el acceso físico al centro de procesamiento de datos sea exclusivo para el personal autorizado.
- Garantizar que el ingreso a áreas seguras por parte de visitantes, personal de soporte técnico o terceros esté previamente aprobado por la Dirección de Sistemas de Información. Asegurar el acompañamiento permanente del personal que autorizó el ingreso, quien será responsable de los visitantes durante su permanencia en las instalaciones.
- Implementar un mecanismo de registro, mediante una bitácora o sistema de información, para el personal que ingrese a áreas seguras, proporcionando información relevante para futuras auditorías.
- Garantizar condiciones físicas y medioambientales adecuadas dentro de las áreas seguras mediante sistemas de control de temperatura y humedad, detección de incendios y unidades de suministro ininterrumpido de energía.
- Garantizar que las áreas seguras sin personal permanente cuenten con un bloqueo físico como cerraduras y sean inspeccionadas continuamente por el personal de vigilancia.
- Disponer de elementos de señalización para todos los equipos y dispositivos dentro de las áreas seguras, así como luces y salidas de emergencia.

- Garantizar que todos los equipos destinados al procesamiento de información sensible se encuentren en un ambiente protegido para minimizar riesgos de fuga, pérdida o modificación no autorizada de la información.
- Asegurar que los equipos tecnológicos de las diferentes áreas y dependencias estén conectados a una red eléctrica regulada. En caso de no contar con una red eléctrica adecuada, disponer de un regulador externo y un respaldo para el suministro eléctrico.
- Garantizar que los equipos destinados al procesamiento de información sensible estén aislados y cuenten con mecanismos de protección para reducir el riesgo de fuga, pérdida o robo de información.
- Asegurar que los equipos desatendidos cuenten con bloqueo de pantalla u otro mecanismo para prevenir el acceso no autorizado a la información almacenada.

7.9. PARA LA SEGURIDAD OPERATIVA

7.9.1. Objetivo

Garantizar que las operaciones en todas las instalaciones de procesamiento de información del Departamento de Santander se controlen y protejan de acuerdo con su nivel de riesgo y exposición.

7.9.2. Alcance

Aplica a todos los procesos operacionales realizados sobre la infraestructura tecnológica local y en la nube que soporte el procesamiento de información y a los sistemas y servicios de información del Departamento de Santander.

7.9.3. Descripción

A continuación, criterios establecidos para la seguridad operativa sobre la infraestructura tecnológica, se debe:

- Implementar la realización de copias de respaldo seguras de la información en los sistemas y servicios de información.
- Realizar el reinicio y la recuperación del sistema de manera controlada en caso de fallas
- Hacer seguimiento al uso de los recursos en los sistemas y servicios de información, para identificar oportunamente posibles anomalías que afecten su desempeño.
- Implementar mecanismos que permitan segregar las funciones de administración, monitoreo y operación de los sistemas y servicios de información.
- Implementar como mínimo 3 ambientes (desarrollo, prueba y producción) para los sistemas y servicios de información de la entidad, con el fin, de evitar cambios no autorizados en ambientes de producción
- Ejecutar controladamente las actualizaciones automáticas sobre la infraestructura donde se encuentran los Sistemas y servicios de información, estas por defecto deben estar deshabilitadas
- Contar con aplicaciones licenciadas y actualizadas para la detección de códigos maliciosos y virus informáticos para todas las máquinas donde se ejecutan los sistemas y servicios de información.

- Verificar la correcta ejecución de los procesos de copias de respaldo, como mínimo una vez cada 6 meses.
- Realizar tareas de restauración aleatorias de la información con el fin de validar su calidad.
- Realizar copias de respaldo de la información que tenga valor, alto nivel de confidencialidad o que sea crítica. Esta es responsabilidad de los usuarios que la tengan a su cargo.
- Reportar los incidentes que resulten del uso inadecuado de dispositivos de almacenamiento externo (por ej, dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, Discos Duros extraíbles, celulares, etc.).
- Activar, conservar y revisar todos los registros de eventos (log de auditoria) en los sistemas y servicios de información.
- Garantizar que los registros de eventos de los sistemas y servicios de información contengan la información suficiente para permitir la trazabilidad de las acciones realizadas. Los registros deben incluir, como mínimo: la identificación única del usuario en el evento, la actividad ejecutada, la fecha y hora de entrada y salida del usuario, cambios en la configuración del sistema, archivos accedidos y el tipo de acceso.
- Proteger todos los registros de eventos en los sistemas y servicios de información contra alteración y acceso no autorizado.
- Sincronizar todos los relojes de los de los sistemas de procesamiento de información con la hora legal del Instituto Nacional de Metrología de Colombia http://horalegal.inm.gov.co
- Controlar el acceso y uso de los programas fuente, el acceso a los archivos de los sistemas y/o a las aplicaciones que operan en dichos servicios y la programación de las actualizaciones necesarias.
- Evitar el uso de versiones de software no soportados por los fabricantes en los sistemas de producción.
- Realizar análisis de vulnerabilidades técnicas para todos los sistemas y servicios de información, la periodicidad de estos análisis debe estar ajustada a su criticidad para la entidad, para todos, esta periodicidad debe ser como mínimo 1 vez al año.
- Identificar los riesgos asociados resultantes de los análisis de vulnerabilidades y aplicar los controles de seguridad que los mitiguen.
- Bloquear la instalación de programas por parte de usuarios comunes.

7.10. PARA LA SEGURIDAD DE LAS COMUNICACIONES

7.10.1. Objetivo

Proteger de manera adecuada y oportuna la información y las comunicaciones, tanto en la red interna como en el intercambio con partes externas.

7.10.2. Alcance

Aplicable a todas las conexiones de red, así como a todos los sistemas y servicios de información que conforman la infraestructura de red en el Departamento de Santander.

7.10.3. Descripción

A continuación, se presentan los criterios establecidos para la seguridad en las comunicaciones, se debe:

- Definir controles y mecanismos de protección adecuados que garanticen la seguridad y privacidad en la infraestructura de red y que abarque todas las capas, tales como aplicaciones, infraestructura y servicios de red.
- Realizar monitoreo de las conexiones de red que permitan registrar todas las actividades, manteniendo estos registros protegidos y accesibles para futuras auditorías.
- Garantizar que todo acceso remoto a la red interna del Departamento de Santander se realice a través de una conexión VPN segura y sea controlado mediante permisos de acceso para usuarios autorizados.
- Asegurar que los niveles de revisión del software actual en los equipos de red y entornos de servidor cumplan con la configuración de seguridad necesaria para proteger la integridad y confidencialidad de la información que circula por la red interna.
- Implementar configuraciones mediante políticas de segmentación adecuadas, utilizando cortafuegos, VLAN y todos los parámetros necesarios para asegurar un entorno seguro y controlado para la red de datos interna del Departamento de Santander.
- Definir una segmentación adecuada para la red inalámbrica con el objetivo de separar los recursos de red asignados a dispositivos destinados a labores institucionales de los asignados a dispositivos de visitantes y personal externo.
- Establecer mecanismos de control sobre los recursos de la red interna e inalámbrica, limitando la conexión de ancho de banda, el acceso a páginas no autorizadas y la descarga de archivos.
- Controlar el acceso de los usuarios a la red inalámbrica mediante mecanismos de autenticación y siguiendo los criterios establecidos en la política de control de acceso del presente manual.
- Verificar periódicamente la efectividad de los controles implementados, utilizando técnicas y mecanismos de evaluación como análisis de vulnerabilidades y pruebas de intrusión, para determinar el nivel de seguridad de los componentes de la infraestructura de red.
- Garantizar una conexión a internet segura en las diferentes dependencias del Departamento de Santander, para apoyar las labores de los funcionarios y contratistas en el cumplimiento de sus funciones.
- Asegurar que todos los servicios de red prestados por el Departamento de Santander o contratados externamente cuenten con controles de seguridad y requisitos de gestión, y que estos se incorporen en los acuerdos de niveles de servicio.
- Definir e implementar procedimientos y controles de seguridad para el intercambio seguro y controlado de información.
- Proporcionar mecanismos dentro de los servicios tecnológicos del Departamento de Santander que garanticen un proceso adecuado de transferencia de información, como el correo electrónico institucional, el protocolo seguro de transferencia de archivos (SFTP) y servicios en la nube.
- Implementar esquemas de seguridad para el intercambio de información con partes externas, asegurando la integridad y confidencialidad de los datos que sean transmitidos.
- Definir controles de autenticación y autorización para la implementación de servicios web donde el Departamento de Santander provea o consuma datos.

- Implementar técnicas de enmascaramiento y cifrado para el intercambio de información sensible, con el fin de aumentar los niveles de seguridad y proteger los datos.

7.11. PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN

7.11.1. Objetivo

Asegurar la integración de la Seguridad Digital y la Privacidad de la Información como parte esencial de los sistemas de información durante todo el ciclo de vida del desarrollo de software.

7.11.2. Alcance

Aplica a todos los desarrollos, adquisiciones y mantenimientos de aplicaciones internos y externos que realice cualquier dependencia del Departamento de Santander.

7.11.3. Descripción

A continuación, los criterios establecidos para la adquisición, desarrollo y mantenimiento de los sistemas de información en el Departamento de Santander, se debe:

- Contemplar desde las fases iniciales de los proyectos de sistemas de información todos los lineamientos de Seguridad Digital y Privacidad de la Información como parte integral de los sistemas de información.
- Proteger contra actividades fraudulentas, divulgación y modificación no autorizadas toda la información en las aplicaciones que sea transferida sobre redes de dominio de acceso público.
- Evaluar y valorar el riesgo de los sistemas de información que se encuentren expuestos públicamente o en el ciberespacio y que estén sometidos a amenazas relacionadas con la red pública.
- Proteger toda la información transmitida a través de la utilización de servicios web entre aplicaciones evitando que se transmita de manera incompleta, errada o sea alterada o duplicada de forma no autorizada.
- Implementar y garantizar el cumplimiento de la lista de chequeo de Seguridad Digital y Privacidad de la Información a todas las mejoras o desarrollos internos o externos realizados para el Departamento de Santander, así como la ejecución de pruebas de aceptación y seguridad al software.
- Aplicar a los ambientes utilizados para desarrollo y pruebas de los sistemas de información las características mínimas de aseguramiento que se tendrán en el ambiente productivo.
- Documentar los cambios que se realicen sobre los sistemas de información con el fin de asegurar la integridad del sistema, las aplicaciones y los productos. Desde las primeras etapas de diseño, contar con un proceso formal de documentación, especificación, pruebas, y control de calidad.
- Realizar las pruebas y actualizaciones a los sistemas y proyectos de desarrollo de sistemas de información en ambientes separados al de producción.

- Contar con acuerdos de licenciamiento para todos los sistemas de información adquiridos o desarrollados por terceros. Especificar como mínimo las condiciones de uso del software y los derechos de propiedad intelectual.
- Aplicar los principios de desarrollo seguro a todos los desarrollos contratados externamente.
- Garantizar el derecho del Departamento de Santander a realizar auditorías a los terceros durante cualquier etapa del desarrollo del contrato.
- Garantizar que haya cumplimiento de los niveles de soporte requeridos por el Departamento de Santander cuando se contrata un desarrollo externo.
- Garantizar que se realice la entrega de manual(es) técnico(s), que describan la estructura interna del sistema, así como el diccionario de datos, librerías y archivos que lo conforman; y manual(es) funcional(es), que describan las funcionalidades de cada una de las opciones del menú de la aplicación.
- Contar con la ejecución de pruebas funcionales que incluyan la evaluación de los requisitos de seguridad de la información y la protección contra vulnerabilidades técnicas conocidas para todos los desarrollos internos y externos.
- Ejecutar pruebas de aceptación del software para todos los desarrollos internos o externos. Orientar dichas pruebas a validar el cumplimiento de los requisitos funcionales y de Seguridad Digital.
- Corregir todos los defectos relacionados con Seguridad Digital conocidos o encontrados durante las pruebas realizadas antes del paso a producción.
- Evitar el uso de datos reales con información personal o cualquier otra clasificada como información pública restringida para realizar pruebas. Si es necesario su uso, proteger todos los detalles y contenidos sensibles eliminándolos o modificándolos.

7.12. PARA LAS RELACIONES CON PROVEEDORES

7.12.1. Objetivo

Asegurar y mantener los niveles adecuados de seguridad de la información de los sistemas y servicios de información accedidos, administrados o procesados por proveedores y usuarios externos.

7.12.2. Alcance

Aplicable a todos los contratistas, proveedores y partes externas que dentro de sus funciones legales y contractuales tengan acceso a los sistemas y servicios de información del Departamento de Santander.

7.12.3. Descripción

A continuación, los criterios establecidos a tener en cuenta para la Seguridad Digital y Privacidad de la Información en el relacionamiento con los proveedores, se debe:

- Establecer de manera explícita en los acuerdos con los proveedores que la propiedad de la información es del Departamento de Santander, incluyendo los activos que la entidad disponga para la ejecución de los compromisos contractuales.

- Establecer y aplicar acuerdos de confidencialidad para el uso y tratamiento de información sensible y de propiedad del Departamento de Santander en la relación con proveedores y usuarios externos.
- Garantizar el estricto cumplimiento del presente manual de políticas por parte de los proveedores y usuarios externos que, dentro de sus obligaciones contractuales, tengan acceso a la información y a los servicios tecnológicos de la entidad.
- Considerar como falta grave el incumplimiento de la presente política, lo cual conllevará a investigaciones y sanciones que apliquen ante los entes judiciales y de control correspondientes.
- Verificar el cumplimiento de los criterios establecidos en la política de tratamiento de datos personales adoptada por la entidad cuando los proveedores o usuarios externos almacenen o recopilen información que contenga datos personales y en su calidad de responsables o encargados del tratamiento.
- Definir, aplicar, evaluar y monitorear los acuerdos de nivel de servicio para asegurar que los servicios tecnológicos soportados por proveedores y partes externas se entreguen según lo contratado y dentro de los objetivos establecidos.
- Garantizar que los acuerdos con proveedores incorporen requisitos para la gestión y tratamiento de riesgos de seguridad de la información asociados a los activos a los que tengan acceso.
- Establecer requisitos legales y normativos como el cumplimiento de certificaciones en normas y estándares nacionales e internacionales en la gestión de seguridad de la información para la relación contractual con proveedores de tecnología.
- Documentar de manera explícita y en un anexo específico dentro del contrato laboral los requisitos de seguridad de la información acordados con el proveedor de servicios.
- Asegurar que todos los proveedores que subcontraten partes del servicio de tecnología exijan el cumplimiento de los requisitos de seguridad establecidos por el Departamento de Santander para toda la cadena de suministro.
- Verificar que cada proveedor designe un encargado de Seguridad Digital y Privacidad de la Información que actúe como interlocutor permanente y responsable para el cumplimiento de los requisitos de seguridad acordados entre ambas partes.
- Definir un protocolo de ingreso físico a las áreas seguras del Departamento de Santander por parte de proveedores y partes externas, teniendo en cuenta los lineamientos establecidos en la política de Seguridad Física y Ambiental del presente manual.
- Verificar que los proveedores de tecnología cuenten con esquemas de monitoreo predictivos y preventivos sobre los activos de información suministrados y que soportan los servicios tecnológicos del Departamento de Santander.

7.13. PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN

7.13.1. Objetivo

Brindar los lineamientos mínimos para la adecuada gestión de incidentes de seguridad de la información en el Departamento de Santander.

7.13.2. Alcance

Todos los procesos estratégicos, misionales, de apoyo y de control y seguimiento en el Departamento de Santander que deban atender incidentes de seguridad y privacidad de la información.

7.13.3. Descripción

Criterios establecidos para la gestión de incidentes de seguridad de la información, se debe:

- Definir, documentar y ejecutar un procedimiento para la gestión de incidentes de seguridad de la información, orientado a asegurar una respuesta rápida, eficaz y ordenada.
- Garantizar que el procedimiento para gestionar incidentes de seguridad digital y privacidad de la información incluya: responsables, paso a paso, planificación y preparación de respuestas, seguimiento, detección, análisis y reporte de eventos, manejo de evidencia forense, valoración y toma de decisiones, punto de contacto y formatos para el reporte de eventos.
- Reportar cualquier situación sospechosa o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información.
- Reportar las vulnerabilidades de Seguridad Digital y Privacidad de la Información que se presenten o identifiquen en los sistemas y servicios de información del Departamento de Santander.

7.14. PARA LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

7.14.1. Objetivo

Establecer lineamientos para la continuidad de la seguridad de la información ante posibles incidentes, interrupciones o desastres con el propósito de minimizar los daños y facilitar el restablecimiento de las operaciones.

7.14.2. Alcance

Esta política es aplicable a todos los procesos institucionales y a los sistemas y servicios de información del Departamento de Santander.

7.14.3. Descripción

A continuación, se presentan los criterios establecidos para la continuidad de la seguridad de la información dentro de la gestión de la continuidad del negocio, se debe:

- Contar con una estructura que permita preparar, mitigar y responder ante un evento perturbador o adverso. Esta estructura debe estar compuesta por personal con el más alto nivel de autoridad, experiencia y competencia para la recuperación operativa.
- Definir y documentar por cada sistema y servicio planes de continuidad, procedimientos de respuesta y recuperación, especificando cómo se gestionará un evento adverso y se mantendrá la seguridad de la información en un nivel aceptable.

- Definir y documentar los controles mínimos de seguridad de la información que deben mantenerse en caso de presentarse una situación adversa, incluyendo los controles compensatorios.
- Verificar cada 6 meses la efectividad de los controles de continuidad de la seguridad de la información establecidos e implementados, para asegurar que son válidos y eficaces durante situaciones adversas.
- Capacitar y difundir las estrategias para la continuidad de la seguridad de la información a todas las partes interesadas.

7.15. CUMPLIMIENTO

7.15.1. Objetivo

Cumplir con las obligaciones legales, normativas o contractuales relacionadas con la seguridad de la información, la protección de los derechos de autor, la privacidad y la protección de los datos personales.

7.15.2. Alcance

Todos los procesos estratégicos, misionales, de control y seguimiento, y de apoyo, del Departamento de Santander que tenga a su cargo obligaciones legales, estatutarias, de reglamentación o contractuales relacionadas con seguridad de la información, y de cualquier requisito de seguridad.

7.15.3. Descripción

El Departamento de Santander se compromete con el cumplimiento normativo en Seguridad Digital y Privacidad de la Información para las entidades públicas en Colombia, normativas entre las que se incluyen, pero no se limitan a:

- CONPES 3854 de 2016 - Política Nacional de seguridad digital
- CONPES 3995 de 2020 - Política Nacional De Confianza Y Seguridad Digital
- Decreto Nacional 1008 de 2018 - Política Gobierno Digital
- Decreto Nacional 1078 de 2015 - Decreto único reglamentario del sector de tecnologías de información y las comunicaciones.
- Decreto 1413 de 2017 - Lineamientos generales en el uso y operación de los servicios ciudadanos digitales
- Decreto 612 de 2018 - Directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
- Decreto Departamental 494 de 2018 - Por el cual se adopta el modelo integrado de planeación y gestión - MIPG y se organiza el funcionamiento del comité institucional de gestión y desempeño del Departamento de Santander.
- Directiva presidencial 02 de 2019
- Decreto Nacional 620 de 2020 - lineamientos generales en el uso y operación de los servicios ciudadanos digitales

- Resolución número 00500 de marzo 10 de 2021 - Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital
- Ley 1581 de 2012 - disposiciones generales para la protección de datos personales.
- Ley 1712 de 2014 - Transparencia en el acceso a la información pública
- Norma ISO 27001
- Modelo de Seguridad y Privacidad de la información - MINTIC
- El Departamento de Santander garantiza el cumplimiento de los requisitos legislativos, de reglamentación y contractuales relacionados con los derechos de propiedad intelectual y el uso de productos de software legal.

CONTROL DE CAMBIOS				
VERSIÓN	**FECHA**	**DESCRIPCIÓN DEL CAMBIO**	**REVISÓ**	**APROBÓ**
1	22/03/2023	Creación del manual de políticas de Seguridad y Privacidad de la Informacion	Cristhian Becerra Hernández Director de Gobierno Digital	Comité Institucional de Gestión y Desempeño 2022
2	13/09/2024	Actualización del manual de políticas de Seguridad y Privacidad de la Información: se agrega la política de escritorio y pantalla limpia por requerimiento de la Registraduría Nacional.	Sandra Liliana Bautista Escobar Directora de Gobierno Digital	Comité Institucional de Gestión y Desempeño 2024