Republica de Colombia

Gobernación de Santander

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

TABLA DE CONTENIDO

1. INTRODUCCIÓN 3
2. OBJETIVO 3
3. ALCANCE Y APLICABILIDAD 3
4. DEFINICIONES 3
5. COMPROMISO DE LA ALTA DIRECCIÓN 8
6. CUMPLIMIENTO DE LAS POLÍTICAS 8
7. POLÍTICAS ESPECÍFICAS DE SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN 9

7.1. PARA LOS ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DIGITAL Y PRIVACIDAD DE LA INFORMACIÓN 9
7.2. PARA EL USO DE DISPOSITIVOS MÓVILES Y EL TRABAJO EN CASA 10
7.3. PARA LA SEGURIDAD LIGADA A LOS RECURSOS HUMANOS 12
7.4. PARA LA GESTIÓN DE ACTIVOS 14
7.5. PARA EL CONTROL DE ACCESO 16
7.6. PARA EL USO DE CIFRADO 18
7.7. PARA LA SEGURIDAD FÍSICA Y AMBIENTAL 18
7.8. PARA LA SEGURIDAD OPERATIVA 20
7.9. PARA LA SEGURIDAD DE LAS COMUNICACIONES 23
7.10. PARA LA ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN 25
7.11. PARA LAS RELACIONES CON PROVEEDORES 26
7.12. PARA LA GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN 28
7.13. PARA LOS ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO 29
7.14. CUMPLIMIENTO 30

1. INTRODUCCIÓN

En la actualidad, la información es uno de los activos más importantes de cualquier entidad y a medida que las tecnologías de la información apoyen cada vez más sus procesos se hace importante contar con lineamientos claros que permitan el control y la protección de sus activos de información, puntualmente, ante la pérdida de confidencialidad, integridad y disponibilidad.

El presente documento, proporciona una visión de alto nivel de los requisitos de Seguridad Digital y Privacidad de la Información que se deben cumplir en la Gobernación de Santander.

2. OBJETIVO

Establecer el Manual de Políticas de Seguridad Digital y Privacidad de la Información para la Gobernación de Santander, con el fin de preservar la confidencialidad, integridad y disponibilidad de la información y sus activos asociados, fortaleciendo los procesos de la entidad en un entorno de confianza digital, según los lineamientos establecidos por el MinTIC a través del Modelo de Seguridad y Privacidad de la Información - MSPI.

3. ALCANCE Y APLICABILIDAD

El presente Manual de Políticas de Seguridad Digital y Privacidad de la Información cubre los aspectos de privacidad, acceso, autenticación, mantenimiento y divulgación relacionados con cualquier activo de información, dichas políticas, son de obligatorio cumplimiento y aplicación para todo el personal, proveedores, contratistas y aplicaciones tecnológicas en la Gobernación de Santander.

4. DEFINICIONES

Activo de información: Es la información que por su importancia para las actividades de la Gobernación de Santander, es reconocida como un bien que tiene un valor significativo para la Entidad; en el contexto de la norma ISO/IEC 27001 se entiende como: “Conocimientos, datos o información que una organización o entidad valora y por lo tanto debe proteger”, los activos de información pueden existir de forma física (archivos impresos, libros, personas, Cd’s, etc.) o lógica (Aplicativos, bases de datos, archivos en Word, Excel PDF, fotografías, videos, etc.).

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 de la Gobernación 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 organización, por ejemplo, un incendio, una inundación, deficiencia en el suministro de energía o Usuarios malintencionados.

Centros de procesamiento de datos: Es la instalación que se encarga del procesamiento de datos e información de manera sistematizada. El procesamiento se lleva a cabo con la utilización de computadoras (Hardware) y programas (Software) necesarios para cumplir con dicha tarea, en la Gobernación de Santander está a cargo de la Dirección de Sistemas de Información y es llamado DataCenter.

Ciclo de vida de un activo: Son todas las actividades que se ejecutan sobre un activo de información, desde su creación incluye su buen uso y disposición final.

Cifrado: Proceso que convierte el texto plano en texto ilegible a través del uso de algoritmos matemáticos, es utilizado principalmente para proteger la confidencialidad de la información con alto nivel de criticidad para la entidad.

ColCERT: Grupo de respuesta a emergencias cibernéticas de Colombia, tiene como responsabilidad central la coordinación de la ciberseguridad y ciberdefensa nacional, está enmarcada dentro del Proceso Misional de Gestión de la Seguridad y Defensa del Ministerio de Defensa Nacional. Su propósito principal es la coordinación de las acciones necesarias para la protección de la infraestructura crítica del Estado colombiano frente a emergencias de ciberseguridad que atenten o comprometan la seguridad y defensa nacional.

Comité Institucional de Gestión y Desempeño: Comité creado a partir del Decreto 494 de 2018, es el órgano rector, articulador y ejecutor, a nivel institucional, de las acciones y estrategias para la correcta implementación, operación, desarrollo, evaluación y seguimiento del modelo integrado de planeación y gestión MIPG.

Confidencialidad: Propiedad que determina que la información sólo esté disponible y sea revelada a individuos, entidades o procesos autorizados; en seguridad digital, proteger la confidencialidad de la información hace referencia a evitar que la información sea accedida por personas no autorizadas.

Contraseña: Es una forma de autenticación privada, compuesta por un conjunto de números, letras y caracteres, que permiten al Usuario tener acceso a un computador, a un archivo y/o a un programa.

CSIRT: Centro de respuesta para incidentes de seguridad en tecnologías de la información, brinda acompañamiento y apoyo a las entidades del estado, a través de su portafolio de servicios, con el fin de mejorar los procesos de seguridad de la infraestructura tecnológica, la gestión de los incidentes cibernéticos y generación de conciencia en seguridad digital.

Custodio del activo de información: Es la parte encargada de administrar y hacer efectivos los controles de seguridad que el dueño o propietario del activo de la información haya definido, por ejemplo, realizar las copias de respaldo o Backup, la asignación privilegios de acceso, modificación y borrado, la identificación de posibles incidentes relacionados con el activo, etc.

Disponibilidad: Propiedad de que la información sea accesible y utilizable por Usuarios autorizados, cuando esta así lo requiera; en seguridad digital, proteger la disponibilidad de la información hace referencia a tener garantía que la información pueda ser accedida por Usuarios autorizados cuando estos lo requieran.

Dispositivo móvil: Es un dispositivo electrónico de fácil movilidad que puede almacenar y procesar información, generalmente comparten funciones comunes con los dispositivos de uso fijo, por ejemplo, trabajo en red, acceso a internet, correo electrónico y manejo de archivos, para el presente documento, dispositivo móvil se entiende por: equipo computador portátil, equipo móvil celular, tabletas, etc.

Dispositivos de almacenamiento externo: Dispositivos utilizados para el almacenamiento externo de volúmenes de información, tales como, memorias USB, Discos Duros extraíbles, Cd, DVD, etc.

Dueño o propietario del activo de información: Se entiende como dueño o propietario de un activo de información al responsable por la gestión del mismo, es decir, quien debe asegurar que el activo de información está protegido adecuadamente y conocer su valor, sensibilidad y relevancia para la Entidad; esta responsabilidad es delegada a los cargos con roles directivos de la Gobernación de Santander.

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: La firma digital hace referencia, en la transmisión de mensajes telemáticos y en la gestión de documentos electrónicos, a un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento.

Incidente de seguridad digital y privacidad de la información: Uno o más eventos de seguridad digital que comprometen las diferentes operaciones en la Entidad y la seguridad digital que se maneja; a diferencia del evento un incidente si logra afectar negativamente la Entidad e incluso la seguridad de su información.

Información pública clasificada: Es aquella información que estando 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 por lo que su acceso podrá ser negado o exceptuado, siempre que se trate de las circunstancias legítimas y necesarias y los derechos particulares o privados consagrados en el artículo 18 de la ley 1712 del 2014; para efectos de la Gobernación de Santander, se entiende como Información pública clasificada a la información que se genera y procesa en el día a día y que puede ser compartida libremente con otros procesos al interior de la Entidad.

Información pública reservada: Es aquella información "que estando en poder o custodia de un sujeto obligado en su calidad de tal, es exceptuada, de acceso a la ciudadanía por daño a intereses públicos y bajo cumplimiento de la totalidad de los requisitos consagrados en el artículo de la ley 1712 del 2014; para efectos de la Gobernación de Santander, se entiende como Información Pública Reservada a la información que por su nivel de confidencialidad únicamente debe 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 al interior de la Entidad ni a la ciudadanía.

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

Integridad: Propiedad de salvaguardar la exactitud y estado completo de los activos; en seguridad digital, proteger la integridad de la información hace referencia a garantizar que solo sea modificada por Usuarios autorizados cuando estos lo requieran.

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 (algoritmos) que se generan de forma automática y se guardan en un directorio especial durante la instalación; buscan asociar la identidad de una persona o de un equipo informático a un documento o un privilegio.

Malware: Código malicioso o cualquier tipo de programa desarrollado para causar daños o introducirse de forma no autorizada en algún sistema o servicio de información.

No Repudio: Atributo utilizado para demostrar o probar la participación de un emisor cuando se transmiten mensaje de datos; a través de esto, se busca tener certeza del emisor de un mensaje, sin que este último pueda ejercer rechazo o negación de dicho envío.

Política: Son instrucciones mandatarias que regulan la forma en que una organización previene, protege y maneja los riesgos de diferentes daños.

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

Responsable del Usuario: es aquel rol que los funcionarios tienen como responsable, en la Gobernación de Santander son: Gobernador, Secretarios o Secretarias de Despacho, Jefe(s) de Oficina o Dependencia, para los contratistas, se tiene como responsable al Gobernador, Secretarios o Secretarias de Despacho, Jefe(s) de Oficina o Dependencia o al Supervisor de Contrato.

Servicios de almacenamiento en la nube: Servicios en el cual los datos son almacenados, administrados, y respaldados de forma remota, típicamente en servidores que están en la nube y que son administrados por un proveedor del servicio, por ejemplo, OneDrive.

Servidores públicos: Persona con una vinculación laboral al estado, que ejerce funciones públicas que están al servicio del estado y de la comunidad.

Servidor: Computadora que comparte recursos con otras computadoras, conectadas con ella a través de una red, su función principal es proveer servicios tecnológicos a los Usuarios.

Sistema Operativo: Programa o conjunto de programas que permiten administrar los recursos de hardware y software de una computadora, servidor o dispositivo móvil, es el programa que hace funcionar al hardware.

Sistemas y servicios de información: Son elementos relacionados con las tecnologías de la información y las comunicaciones, estos pueden ser físicos (por ejemplo, servidores, red, discos duros, teléfonos, impresoras, computadores) y lógicos (por ejemplo, aplicaciones, bases de datos, sistemas operativos).

Terceros: Se entiende por tercero a toda persona, jurídica o natural ajena a la Gobernación de Santander, como proveedores, contratistas o consultores, que provean servicios o productos a la Entidad.

Trabajo en casa: Modalidad de trabajo ocasional distinta al teletrabajo o el trabajo remoto; está definido como la habilitación al servidor público o trabajador del sector privado para desempeñar transitoriamente sus funciones o actividades laborales por fuera del sitio donde habitualmente las realiza.

Usuarios: Se entiende por Usuarios, a cualquier persona, entidad, cargo, proceso, sistema automatizado o grupo de trabajo que acceda a los activos de información de la Gobernación de Santander, para generar, obtener, transformar, conservar o utilizar información de la Entidad en papel o en medio digital, esto incluye: funcionarios de carrera administrativa y de

libre nombramiento, temporales, practicantes, contratistas, recurso humano de empresas proveedoras de servicio y aplicaciones que consuman servicios o información de la entidad

Virus: Software malicioso que tiene por objeto alterar el normal funcionamiento de una computadora, reemplazando así 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

La Alta dirección en la Gobernación de Santander está representada a través del Comité Institucional de Gestión y Desempeño quien es el responsable de orientar la implementación y operación del Modelo Integrado de Planeación y Gestión – MIPG; dicho comité es quien aprueba las Políticas de Seguridad Digital y Privacidad de la Información como muestra de su compromiso y apoyo en el diseño e implementación de prácticas eficientes que garanticen la seguridad digital y la privacidad de la información de la Entidad.

La Alta Dirección de la Gobernación 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 a las Políticas de Seguridad Digital y Privacidad de la Información es gestionado a través de procedimientos administrativos que repercuten en procesos disciplinarios, judiciales y procesos administrativos según las circunstancias de modo, tiempo, lugar y gravedad de la falta.

Por lo anterior, todas las violaciones probadas a la presente política por parte de funcionarios públicos serán remitidas a la Oficina de Control Disciplinario de la Gobernación de Santander.

Para el caso de personal contratista y las empresas proveedoras se aplicarán las investigaciones y/o sanciones correspondientes de acuerdo a las cláusulas establecidas en el objeto contractual.

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

A continuación, se detallan cada una de las políticas específicas de Seguridad Digital y Privacidad de la Información que rigen para la Gobernación de Santander, deberán ser cumplidas por todos los Usuarios:

7.1. Para los aspectos organizativos de la Seguridad Digital y Privacidad de la Información

7.1.1. Objetivo

Definir las funciones y responsabilidades para la protección de los activos de información de la Gobernación 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 la Gobernación 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:

La alta dirección en la Gobernación de Santander está representada en el Comité Institucional de Gestión y Desempeño, entre sus responsabilidades están:

- Aprobar las modificaciones o las nuevas Políticas 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.
- Definir y establecer los roles y responsabilidades relacionados con la Seguridad Digital y Privacidad de la Información en niveles directivo y operativo.
- Aprobar el uso de metodologías y procesos específicos para la seguridad de la Información.
- Promover activamente una cultura de Seguridad Digital y Privacidad de la Información en la Entidad.
- Asignar los recursos, la infraestructura física y el personal necesario para 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 divulgar las políticas, normas, procedimientos y estándares referentes a la Seguridad Digital y Privacidad de la Información.
- Mantener en estricta confidencialidad la información a la que se tenga acceso y no compartirla ni modificarla sin autorización.
- Acceder exclusivamente a la información a la que tienen permisos y que es necesaria para cumplir sus funciones
- Reportar cualquier incidente o evento de seguridad que se presente durante el ejercicio de sus funciones.
- Participar en sesiones de capacitación en Seguridad Digital y Privacidad de la información realizadas en la Entidad.
- Aplicar los controles que sean establecidos para la Gestión de Riesgos de Seguridad Digital.

De la Secretaría de las TIC:

- Establecer, implementar, mantener y mejorar continuamente todas las acciones referidas a la gestión de Seguridad Digital y Privacidad de la Información de la Gobernación de Santander.
- Mantener la vigencia de las políticas de acuerdo con las necesidades y requerimientos de la Entidad.
- Asesorar y supervisar la adecuada gestión de riesgos y controles de seguridad digital.
- Asegurar que exista una dirección y apoyo de la alta dirección sobre los principios y las metas para soportar la administración y desarrollo de iniciativas sobre la gestión de la seguridad de los activos de la información.
- Validar las políticas de Seguridad Digital y Privacidad de la Información y procedimientos para el uso adecuado y administración de los recursos informáticos asignados a los funcionarios de la entidad, asegurando que la información se encuentre protegida.
- Asesorar, orientar y capacitar a los Usuarios de los procesos en buenas prácticas de Seguridad Digital y Privacidad de la Información.
- Mantener contacto con las autoridades y grupos de interés especial (por ejemplo, colCERT, Csirt) para el reporte de 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 de la Gobernación de Santander almacenada o accesible desde dispositivos móviles, evitando la infección o distribución de Malware a través de su utilización; a través de medidas que garanticen la seguridad, integridad y confidencialidad de la información tratada por medios remotos a los diferentes recursos informáticos e infraestructura tecnológica de la Entidad.

7.2.2. Alcance

La presente política es aplicable a todos los Usuarios que a través de la utilización de dispositivos móviles accedan a información de la Gobernación de Santander y que por motivo estricto de las funciones del cargo o de las obligaciones contractuales deban acceder por medios remotos a los recursos informáticos e infraestructura tecnológica de la Entidad.

7.2.3. Descripción

A continuación, se presentan los lineamientos indicados para el uso de dispositivos móviles de propiedad de la Gobernación de Santander, se debe:

- Registrar e inventariar todos los dispositivos móviles de forma centralizada.
- Asignar un responsable (funcionario, contratista, o líder de proceso) encargado de garantizar la protección física y lógica del mismo, así como su entrega o devolución a la Entidad.
- Reportar cualquier novedad que suceda con los dispositivos móviles inmediatamente a la secretaría administrativa.
- Contar con bloqueo mediante contraseña u otro medio robusto de autenticación.
- Contar con aplicaciones de antivirus instalada.
- Contar con Sistema Operativo obtenido por canales oficiales o instalados de fábrica.
- Contar con procedimientos documentado que permitan su reutilización o baja de manera segura, estos procedimientos deben garantizar la eliminación completa y segura de la información previa y sensible allí almacenada.
- Evitar el almacenamiento de información de carácter personal sensible en los términos especificados por la Ley 1581 de 2012 de protección de datos personales.
- Permitir a la Secretaría de las TIC realizar revisión del cumplimiento de la presente política directamente en los dispositivos móviles que son propiedad de la Entidad.

A continuación, se presenta los criterios relacionados al uso de dispositivos móviles de propiedad personal o de proveedores que acceden a la información o utilizan los recursos tecnológicos de la Gobernación de Santander, se debe:

- Contar con aplicaciones de antivirus instaladas.
- Contar con bloqueo mediante contraseña u otro medio robusto de autenticación.
- Evitar almacenar información de la Gobernación de Santander en los dispositivos móviles de propiedad personal o de los proveedores.
- Realizar el cumplimiento estricto a la totalidad de numerales definidos en el presente documento para los dispositivos móviles de propiedad personal o de proveedores que acceden a la información de la Gobernación de Santander.

Para el trabajo en casa, se debe tener en cuenta los criterios establecidos en la Gobernación de Santander:

- Establecer y garantizar un ambiente seguro y controlado para el acceso remoto a los activos de información y a la red interna de la Entidad.

- Definir e implementar procedimientos de auditoría técnica sobre los accesos habilitados, los cuales deben ser revisados periódicamente o cuando las circunstancias lo ameriten.
- Definir el procedimiento para la solicitud de acceso remoto y segregación de privilegios al interior de los recursos informáticos y la infraestructura tecnológica de la Gobernación de Santander.
- Establecer y limitar el acceso autorizado a la red interna de la Gobernación de Santander de acuerdo a los criterios establecidos en el procedimiento de solicitud de acceso.

A continuación, los criterios establecidos para los Usuarios durante el trabajo en casa, se debe:

- Solicitar el acceso remoto a cualquier recurso de la Gobernación de Santander a través del diligenciamiento del formato establecido, dicha solicitud debe ser aprobada por el responsable del Usuario.
- Garantizar que la información accedida y gestionada de manera remota sea usada en el estricto cumplimiento de las funciones del cargo o de las obligaciones contractuales.
- Contar con los recursos mínimos de seguridad para La red de internet desde donde se realice la conexión remota, como mínimo, una contraseña robusta de autenticación a la red, evitando las redes públicas.
- Contar con antivirus actualizado en todos los dispositivos que sean utilizados para la realización del trabajo remoto.
- Realizar el bloqueo de pantalla cada vez que por algún motivo el Usuario deba ausentarse de su puesto de trabajo.
- Resguardar y almacenar la información propiedad de la Gobernación de Santander en los recursos tecnológicos provistos por la Entidad, evitando en todo lo posible la utilización de dispositivos de almacenamiento externo o servicios gratuitos de almacenamiento en la nube.
- Compartir y almacenar la información de la Gobernación de Santander únicamente a través de los servicios de almacenamiento en la nube y/o el correo electrónico institucional provistos por la entidad.

7.3. Para la Seguridad ligada a los recursos humanos

7.3.1. Objetivo

Brindar lineamientos a 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 la Gobernación de Santander.

7.3.2. Alcance

La presente política es aplicable para todo los Usuarios que tengan relación laboral con la Gobernación de Santander, servidores públicos, contratistas, practicantes y partes externas que dentro de sus funciones legales y contractuales tengan acceso a las instalaciones, a la información y a los servicios tecnológicos de propiedad de la entidad.

7.3.3. Descripción

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

- Establecer un procedimiento documentado y consistente para la verificación de antecedentes disciplinarios, policiales y fiscales, así como la veracidad de la información relacionada en su hoja de vida.
- Realizar la validación y constancia de la experiencia laboral y académica para los aspirantes y candidatos a ocupar un cargo público dentro de la Entidad.
- Garantizar la firma de un acuerdo de confidencialidad por parte de todos los funcionarios públicos y contratistas al momento de su vinculación formal, dicho acuerdo debe establecer como mínimo sus responsabilidades puntuales con respecto a la Seguridad Digital y Privacidad de la Información, así como la aceptación y cumplimiento obligatorio de las presentes políticas.
- Informar a todo el personal vinculado a la Entidad que el incumplimiento y/o violación de cualquiera de las presentes políticas, será considerada como una falta grave y remitirlas a la Oficina de Control Disciplinario de la Gobernación de Santander, con el fin de se inicie las investigaciones y sanciones correspondientes establecidas por las normas y leyes que reglamenten los procesos disciplinarios para los funcionarios del estado.
- Informar a las empresas contratistas que cualquier incumplimiento y/o violación de la presente política por parte de su personal conllevará las investigaciones y/o sanciones correspondientes de acuerdo a las cláusulas establecidas en el objeto contractual.
- Establecer un mecanismo por el cual los funcionarios públicos y/o contratistas una vez sean vinculados aprueben el tratamiento de sus datos personales de acuerdo lo estipulado en la Ley 1581 de 2012 y en la política de tratamiento de datos personales adoptada por la Entidad.
- Informar de forma explícita al titular de los datos personales el tratamiento al cual serán sometidos y la finalidad de los mismos, así como el derecho a actualizar o rectificar la información recopilada.
- Definir e implementar un procedimiento para la realización de procesos continuos de formación y capacitación en Seguridad Digital y Privacidad de la Información para los funcionarios de carrera administrativa de la entidad y formalizarlos a través de su Plan Institucional de Capacitaciones (PIC).
- Definir e implementar un procedimiento para la realización de procesos continuos de formación y capacitación en Seguridad Digital y Privacidad de la Información para los contratistas y personal humano de los proveedores que presten servicios y tengan acceso a los activos de información de la Gobernación de Santander.
- Comunicar a los funcionarios, contratistas y practicantes los resultados que espera obtener de sus funciones en relación con Seguridad Digital y Privacidad de la Información.
- Comunicar de manera formal y documentada cualquier actualización con respecto a las responsabilidades en Seguridad Digital y Privacidad de la Información en los términos y condiciones por consecuencia de cambio de cargo o reasignación de funciones contractuales para funcionarios, contratistas o practicantes.
- Identificar y definir responsabilidades especificas relacionadas con los riesgos y la Seguridad Digital y Privacidad de la Información en relación con la naturaleza de los roles.

- Definir una estrategia de Información, Educación y Comunicación (IEC) con el fin de garantizar que los Usuarios reciban entrenamiento adecuado en las políticas y procedimientos institucionales ligados con la Seguridad Digital y Privacidad de la Información.
- Definir e implementar un canal de denuncia anónimo para los Usuarios ante posibles fallas o violaciones deliberadas a las normas y políticas institucionales de Seguridad Digital y Privacidad de la Información y tratamiento de datos personales.
- Firmar acuerdos de confidencialidad y de no divulgación que obliguen a los Usuarios que dentro de sus funciones tengan acceso a los sistemas y servicios tecnológicos que procesen y/o almacenen información pública reservada o datos sensibles.
- Establecer como propiedad de la Gobernación de Santander toda la información, documentación y archivos que se generen durante el ejercicio de cumplimiento de los objetos contractuales, esto es aplicable para los Usuarios que tengan acceso a la misma.
- Establecer criterios de verificación de los perfiles de los candidatos en relación a su idoneidad y confiabilidad cuando vayan a desempeñar actividades y tareas sensibles para el cumplimiento de los objetivos de la Entidad en materia de Seguridad Digital y Privacidad de la Información.
- Destinar recursos económicos y humanos específicos para fortalecer la Seguridad Digital y Privacidad de la Información en la Entidad y avanzar en el cumplimiento de los estándares y normas nacionales e internacionales.
- Definir periodos de vigencia relacionados con los deberes y responsabilidades que permanecen validos después de la desvinculación.

7.4. Para la gestión de activos

7.4.1. Objetivo

Definir los lineamientos para la gestión, y protección de los activos de información de la Gobernación 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.

7.4.2. Alcance

La gestión de activos de información aplica para todos los procesos estratégicos, misionales, de control y seguimiento, y de apoyo en la Gobernación de Santander; inicia con la identificación de los activos de información y la asignación de su propiedad, continuando con su clasificación y la gestión que deben dar los Usuarios para la protección de los mismos.

7.4.3. 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 de la Gobernación 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 la Gobernación de Santander, se debe:

- Realizar y mantener actualizado el inventario de activos de información.
- Asignar un propietario o dueño del activo de información, este último es el responsable sobre la gestión del mismo y dentro de su ciclo de vida debe:
  - ✓ Asegurar que los activos están inventariados.
  - ✓ Asegurar que los activos están clasificados y protegidos apropiadamente.
  - ✓ Definir y revisar periódicamente las restricciones y clasificaciones de acceso a activos importantes.
  - ✓ Asegurar el manejo apropiado del activo cuando es eliminado o destruido.
- Asignar la responsabilidad del uso adecuado que se realice con los activos de información a los Usuarios que los tengan bajo su cargo.
- Devolver todos los activos de la Gobernación de Santander que se encuentren a cargo de los Usuarios, al terminar su empleo, contrato o asignación de labores.
- Clasificar la información de acuerdo a los niveles definidos en la ley 1712 de 2014, los niveles de clasificación de la información en la Gobernación de Santander son: Información pública (bajo), Información pública clasificada (medio) e Información pública reservada (alto).
- Clasificar toda la información en función de su nivel de confidencialidad.
- Definir y documentar un procedimiento para la clasificación de la información, este documento debe estar ajustado a los lineamientos de la presente política; este, debe ser socializado en toda la Entidad y debe contener el esquema a utilizar para el etiquetado de la información.
- Promover el almacenamiento seguro de información digital, usando para esto los medios institucionales como el SharePoint, OneDrive, carpetas compartidas, etc. Evitando cuando sea posible el almacenamiento en medios removibles para el intercambio de la información, como, por ejemplo, USB, Discos Duros, servicio de transferencia o almacenamiento inseguro de archivos informáticos por Internet.
- Evitar almacenar la información que haya sido clasificada como Información pública clasificada o Información pública reservada en cualquier medio removible, en caso de requerirse, la información debe contar con mecanismos de cifrado fuertes de protección y respaldo en algún medio institucional de almacenamiento, como son el SharePoint, OneDrive, carpetas compartidas, etc.
- Garantizar la definición, documentación e implementación de un procedimiento orientado a la disposición de los medios electrónicos cuando ya no son requeridos, garantizando el mínimo riesgo de fuga de información.
- Disponer en forma segura los medios que contienen información clasificada como Información pública clasificada o Información pública reservada, ya sea mediante incineración, destrucción o el borrado de datos antes de ser reutilizados o dados de baja.
- 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.

- Identificar claramente los medios físicos que requieran ser transportados, en caso que contengan información clasificada como Información pública reservada, esta deberá encontrarse cifrada, y para este caso, no debe estar etiquetada.
- 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.

7.5. Para el control de acceso

7.5.1. Objetivo

Establecer elementos que permitan asegurar un acceso controlado a la información y establecer privilegios necesarios para el acceso a los servicios tecnológicos de la Gobernación de Santander, con el fin de evitar el uso o acceso no autorizado, adulteración, pérdida o fuga de información.

7.5.2. 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 Gobernación de Santander.

7.5.3. Descripción

A continuación, los criterios establecidos para el control de acceso, en la Gobernación de Santander se debe:

- Definir un procedimiento para proteger y gestionar el ciclo de vida del acceso de los Usuarios a los sistemas y servicios de información, el cual debe ser verificado desde la autorización hasta la baja definitiva por desvinculación laboral, cambio de cargo o reasignación de funciones.
- Establecer el control de acceso a los activos de información en el principio del mínimo privilegio otorgado, con el fin de asignar los permisos suficientes y necesarios únicamente para el desempeño de sus funciones.
- Garantizar que todos los accesos que han sido autorizados a los sistemas y servicios de información se encuentren alineados con la presente política y contar con el análisis en los privilegios otorgados y la segregación de funciones.
- Definir e implementar controles robustos de autenticación para el acceso a los sistemas y servicios de información, que incluyan técnicas como reglas de complejidad de las contraseñas, múltiple factor de autenticación, longitud mínima de la contraseña y datos biométricos, especialmente para los activos de información categorizados con un nivel de criticidad alto.
- Establecer y documentar procedimientos que garanticen la entrega de credenciales de acceso de forma segura y controlada preservando la confidencialidad de las mismas.

- Implementar mecanismos que permitan almacenar las contraseñas de acceso de forma segura, empleando técnicas de cifrado robustas para los diferentes sistemas y aplicaciones desarrollados de manera interna o externa.
- Controlar el acceso de los desarrolladores internos y externos a los servidores de aplicaciones en ambientes de producción o en ambiente de pruebas.
- Ejecutar tareas permanentes de monitoreo sobre las redes para detectar posibles accesos no autorizados o comportamientos inusuales en el tráfico de red.
- Establecer y ejecutar procesos de revisión a todos los sistemas y servicios de información por parte de los propietarios de los activos en conjunto con el custodio de los mismos, con el fin de identificar e inhabilitar Usuarios redundantes, innecesarios o inactivos.
- Definir e implementar un registro documental de todas las solicitudes y autorizaciones de acceso otorgadas en todos los sistemas y servicios de información que puedan servir de soporte para futuros requerimientos de los entes de control o revisiones de incidentes que se presenten.
- Garantizar que las credenciales de acceso que han sido definidas por defecto por parte de los fabricantes de dispositivos y equipos tecnológicos o sistemas y servicios de información sean cambiadas al momento de su paso a producción.
- Comunicar de manera explícita a todos los Usuarios que las contraseñas de acceso a los sistemas de información y servicios tecnológicos son personales e intransferibles y toda actuación ejecutada será responsabilidad de cada Usuario que en el marco de sus funciones se le haya asignado.
- Establecer una relación única entre los Usuarios y sus identificadores asignados, por lo que los identificadores no podrán ser reasignados o reutilizados.
- Implementar un mecanismo para el cambio de contraseña de acceso de los diferentes sistemas y servicios tecnológicos, este último debe contemplar como mínimo la ejecución del cambio cada 3 meses o menos dependiendo de la criticidad de la información a la que accede.
- Implementar un mecanismo para el cambio obligatorio de contraseña para todos los sistemas y servicios de información cuando se efectúe el primer inicio de sesión.
- Evitar registrar en archivos físicos o digitales las contraseñas y que puedan quedar expuestos o al alcance de personal no autorizado.
- Establecer un procedimiento de auditoria periódica para cuentas privilegiadas que permita identificar, deshabilitar y/o eliminar cuentas de Usuarios con privilegios redundantes, en desuso o reducción de privilegios.
- Asignar un identificador (ID) de Usuario diferente para los Usuarios con acceso privilegiado.
- Asignar los derechos de acceso a cuentas privilegiadas a cada Usuario con base a la necesidad de uso, teniendo en cuenta las funciones del cargo y de acuerdo a la presente política de control de acceso.
- Establecer un proceso de autorización y registro de Usuarios con nivel de acceso privilegiado, que incluya el compromiso por parte de este de mantener la confidencialidad y su buen uso.
- Renovar las contraseñas de los diferentes sistemas y servicios tecnológicos en un periodo de vigencia máximo de 90 días.
- Documentar y comunicar el procedimiento para la asignación de Usuarios con acceso privilegiado.

- Gestionar por parte de los Usuarios la solicitud de creación o modificación de acceso a los diferentes sistemas y servicios tecnológicos a través del procedimiento establecido para tal fin, el cual debe ser autorizado por el responsable del Usuario.

7.6. Para el uso de Cifrado

7.6.1. 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 reservada, tanto la información que sea almacenada como en tránsito.

7.6.2. Alcance

Toda la información digital que en función de su clasificación requiera ser protegida, para mantener la confidencialidad, autenticidad e integridad y en donde técnicamente sea posible la aplicación de controles criptográficos.

7.6.3. 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, la autenticidad y la integridad de la información.
- Implementar controles criptográficos basados en el riesgo del activo de información a proteger, acorde a su nivel de sensibilidad y exposición; y la posibilidad de su aplicación.
- Gestionar y generar llaves criptográficas a través de mecanismos tecnológicos dispuestos para tal fin.
- Utilizar controles criptográficos cuando se presenten los siguientes casos:
    - ✓ Para la protección de las claves que utilizan los Usuarios para los sistemas, datos y servicios.
    - ✓ Para la transmisión y almacenamiento de información clasificada como Información pública reservada.
- Realizar el uso de firma digitales a través de una entidad certificadora acreditada, dicha utilización debe garantizar el No repudio del firmante.
- Promover el uso apropiado y eficaz de la criptografía para asegurar la confidencialidad, la autenticidad y la integridad de la información.

7.7. Para la seguridad física y ambiental

7.7.1. Objetivo

Brindar lineamientos para prevenir el acceso físico no autorizado a todas las instalaciones de la Gobernación de Santander a través de la implementación de mecanismos y controles de seguridad física y ambiental, que incluya los centros de procesamiento de datos y a todas las

áreas donde se encuentren activos de información destinados al almacenamiento y procesamiento de información sensible, empleando controles específicos de seguridad para evitar robo, daño o accesos no autorizados.

7.7.2. Alcance

Los lineamientos establecidos en la presente política aplican para todos los funcionarios, contratistas, proveedores y visitantes que ingresen a las instalaciones físicas de la Gobernación de Santander y sus sedes alternas, así mismo a todas las áreas seguras definidas donde se custodie y procese información sensible y a las dependencias donde se encuentren activos de información catalogados con un nivel de criticidad alto.

7.7.3. Descripción

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

- Delimitar las áreas y perímetros de seguridad con sus respectivos controles con base en los resultados obtenidos durante el proceso de gestión de riesgos implementado en la entidad.
- Garantizar que las edificaciones o áreas que se encuentren dentro del perímetro de seguridad y que contengan activos de información que sean utilizados para el almacenamiento o procesamiento de información cuenten con estructuras sólidas, así mismo las puertas y ventanas deben contar con 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 como tarjetas de proximidad, autenticación biométrica, monitorización a través de circuito cerrado de televisión, cerraduras de seguridad y/o alarma de detección de intrusos.
- Garantizar que el acceso físico al centro de procesamiento de datos sea exclusivamente para el personal autorizado.
- Definir un procedimiento para la autorización de ingreso a áreas seguras por parte de visitantes, personal de soporte técnico o de terceros, el cual debe ser previamente autorizado por la Dirección de Sistemas de Información y garantizar un acompañamiento permanente por parte del personal que autorizó su ingreso el cual se hará responsable del personal ajeno al área segura durante el tiempo que permanezca en las instalaciones.
- Implementar un mecanismo de registro por medio de una bitácora o sistema de información para el personal que ingrese a áreas seguras y que pueda proporcionar información relevante para futuras auditorías.
- Establecer y documentar un procedimiento para el control de ingreso físico al personal con acceso permanente a las áreas seguras en el marco de las funciones del cargo desempeñado.
- Garantizar dentro de las áreas seguras las condiciones físicas y medioambientales adecuadas por medio de sistemas de control de temperatura y humedad, sistemas de detección de incendios y unidades de suministro ininterrumpido de energía.
- Garantizar que las áreas seguras se encuentren alejadas de espacios que cuenten con material inflamable o que presenten riesgo de incendios o inundaciones.

- Restringir el acceso a las áreas seguras de dispositivos electrónicos como celulares inteligentes, cámaras fotográficas o de video y cualquier otro dispositivo que permita capturar información reservada, excepto que haya sido previamente autorizado por la Dirección de Sistemas.
- Garantizar que las áreas seguras que no dispongan de personal permanente cuenten con un bloqueo físico como cerraduras y sean inspeccionadas permanentemente por el personal de vigilancia.
- Restringir el consumo de todo tipo de alimento o bebidas dentro de las instalaciones de las áreas seguras.
- Realizar auditorías periódicas con el fin de evaluar la efectividad de los controles físicos y ambientales implementados.
- Disponer dentro de las instalaciones de las áreas seguras de elementos de señalización para todos los equipos y dispositivos, así mismo con luces y salidas de emergencia.
- Garantizar que todos los equipos que estén destinados para el procesamiento de información sensible se encuentren en un ambiente protegido con el fin de minimizar los riesgos de fuga, pérdida o modificación no autorizada de la información.
- Garantizar las condiciones de seguridad física y ambiental adecuadas, tales como ventilación, iluminación, humedad y temperatura para todas las oficinas o áreas destinadas al almacenamiento de activos donde repose información sensible o relevante para el cumplimiento de las funciones y actividades estratégicas de las diferentes dependencias de la Gobernación de Santander.
- Definir e implementar controles de seguridad específicos para garantizar la protección de los activos de información frente a posibles amenazas accidentales, ambientales o deliberadas.
- Asegurar que los equipos tecnológicos de las diferentes áreas y dependencias se encuentren conectados a la red eléctrica regulada, en el escenario donde no se cuente con una red eléctrica dentro del área se debe disponer de un regulador externo y contar con un respaldo en caso de falla del suministro eléctrico.
- Definir un mecanismo de protección para el cableado estructurado dentro de las instalaciones de la Gobernación de Santander contra daño o manipulación no autorizada, aplicando las normas y estándares nacionales e internacionales en la materia con el propósito de brindar disponibilidad permanente en los diferentes servicios de red.
- Garantizar que los equipos destinados al procesamiento de información sensible se encuentren 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 que prevenga el acceso no autorizado a la información allí almacenada.

7.8. Para la seguridad operativa

7.8.1. Objetivo

Asegurar que las operaciones que se realicen en todas las instalaciones de procesamiento de información de la Gobernación de Santander se controlen y protejan de acuerdo a su nivel de riesgo y exposición.

7.8.2. 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 de la Gobernación de Santander.

7.8.3. Descripción

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

- Definir, documentar e implementar procedimientos para:
  - ✓ La instalación y configuración de sistemas y servicios de información
  - ✓ La realización de copias de respaldo de la información en los sistemas y servicios de información
  - ✓ El manejo de errores más comunes en los sistemas y servicios de información
  - ✓ El reinicio y recuperación del sistema para uso en el caso de fallas
- Aplicar a los cambios realizados sobre los sistemas y servicios de información:
  - ✓ La identificación y registro de cada uno de los cambios realizados
  - ✓ Las pruebas a todos los cambios antes de su ejecución
  - ✓ La Valoración de los impactos potenciales que pueden tener los cambios en seguridad de la información
  - ✓ El detalle de todos los cambios a todas las personas interesadas y afectadas por el mismo
- 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, para lo anterior, se debe considerar:
  - ✓ La definición y documentación de las reglas para la transferencia de aplicaciones desde un ambiente a otro, por ejemplo, del ambiente de desarrollo al de producción.
  - ✓ Que cada uno de los ambientes funcione en diferentes máquinas y con distintas instancias o bases de datos.
  - ✓ Todos los cambios que se realicen en las aplicaciones deben ser probados en un ambiente distinto al de producción.
  - ✓ Las pruebas deben realizarse en un ambiente distinto al de producción, únicamente en circunstancias excepcionales, se permitirá la ejecución en dicho ambiente.
  - ✓ Las aplicaciones deben tener mensajes o avisos de identificación del ambiente en el que se están ejecutando.
  - ✓ La información en los ambientes de pruebas y desarrollo debe ser distinta a la información que reposa y es utilizada en el ambiente 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.
- Aprobar, revisar y controlar todas las instalaciones que se realicen para apoyar los procesos operacionales realizados sobre la infraestructura tecnológica que soporta el procesamiento de información en la Gobernación de Santander.
- Aprobar todas las restauraciones realizadas a las copias de respaldo que se ejecuten en ambientes de producción, esta aprobación debe ser realizada por el propietario de la información y debe ser solicitada formalmente por el área encargada de su custodia.
- Definir, documentar e implementar los requisitos de retención y de protección de las copias de respaldo de la 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, los resultados deben ser documentados.
- Realizar la copia de respaldo de la información que tenga valor, alto nivel de confidencialidad o que sea crítica, esto 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.
- Incluir en todos los registros de eventos de los sistemas y servicios de información:
    - ✓ La identificación única de Usuario en el evento
    - ✓ La actividad ejecutada
    - ✓ Fecha y hora de la entrada y salida de Usuario
    - ✓ Identidad del dispositivo usado por el Usuario
    - ✓ Registro de los intentos de acceso al sistema, tanto los exitosos como los rechazados
    - ✓ Cambios en la configuración del sistema
    - ✓ Uso de privilegios
    - ✓ Archivos a los que se tuvo acceso, y el tipo de acceso;
    - ✓ Dirección de red
    - ✓ Activación y desactivación de los sistemas de protección, como los antivirus
    - ✓ Registros de las transacciones ejecutadas por los Usuarios en las aplicaciones
- Proteger todos los registros de eventos en los sistemas y servicios de información contra alteración y acceso no autorizado.
- Registrar y proteger contra alteración por parte de Usuarios con altos privilegios las actividades realizadas por los administradores y operadores de los sistemas y servicios de información.
- 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, así como a la programación de las actualizaciones necesarias a realizar.
- Evitar el uso de versiones de software no soportados por los fabricantes en los sistemas de producción.
- Definir, documentar e implementar procedimientos para la instalación de software en sistemas operativos, este procedimiento debe considerar:
  - ✓ El proceso de actualización del software, parches de seguridad, librerías y sus aprobaciones.
  - ✓ El proceso de retroceso (RollBack) planificado para la implementación de las instalaciones y los cambios.
  - ✓ El registro de auditoria de todas las actualizaciones de las librerías de los sistemas y servicios de información.
- 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.
- Definir, documentar e implementar procedimientos para la instalación de software por parte de los Usuarios, partiendo del principio de menor privilegio, identificando los tipos de instalaciones de software que se pueden instalar y que tipo de instalaciones están prohibidas.

7.9. Para la seguridad de las comunicaciones

7.9.1. Objetivo

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

7.9.2. Alcance

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

7.9.3. Descripción

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

- Establecer, documentar e implementar un procedimiento para la gestión de los equipos de redes.
- 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.

- Diseñar e implementar mecanismos de monitorización sobre las conexiones de red que permitan registrar todas las actividades, manteniendo estos registros protegidos y disponibles para futuras auditorías.
- Garantizar que todo acceso remoto a la red interna de la Gobernación de Santander se realice a través de una conexión VPN segura y sea controlado a través de permisos de acceso a Usuarios autorizados.
- Asegurar que los niveles de revisión del software actual de los equipos de red y los entornos de servidor cumplan con la configuración de seguridad necesaria para garantizar la integridad y confidencialidad de la información que circula a través de la red interna.
- Implementar configuraciones a través de políticas de segmentación adecuadas utilizando cortafuegos, VLAN y todos los parámetros necesarios para garantizar un ambiente seguro y controlado para la red de datos interna de la Gobernación de Santander.
- Definir una segmentación adecuada para la red inalámbrica con el fin de separar los recursos de red asignados para la conexión de dispositivos destinados a labores institucionales de la conexión asignada para dispositivos de visitantes y personal externo a la entidad.
- Establecer mecanismos de control a los recursos tanto de la red interna como inalámbrica, limitando la conexión de ancho de banda, acceso a páginas no autorizadas y descarga controlada de archivos.
- Controlar el acceso de los Usuarios a la red inalámbrica por medio de mecanismos de autenticación y teniendo en cuenta los criterios establecidos en la política de control de acceso del presente manual.
- Verificar de forma periódica la efectividad de los controles implementados, utilizando diferentes técnicas y mecanismos de evaluación tales como análisis de vulnerabilidades y test de intrusión con el objetivo de determinar el nivel de seguridad de los distintos componentes que conforman la infraestructura de red.
- Garantizar una conexión a internet segura dentro de las diferentes dependencias de la Gobernación de Santander con el fin de apoyar las labores de los funcionarios y contratistas y el cumplimiento de sus funciones.
- Asegurar que todos los servicios de red prestados por la Gobernación de Santander o contratados de manera externa deben contar con controles de seguridad y requisitos de gestión y deben ser incorporados en los acuerdos de niveles de servicio.
- Definir e implementar procedimientos y controles de seguridad para el intercambio seguro y controlado de información.
- Proporcionar dentro de los servicios tecnológicos de la Gobernación de Santander mecanismos que garanticen un adecuado proceso de transferencia de información, tales como el correo electrónico institucional, protocolo seguro de transferencia de archivos (SFTP) y servicios en la nube.
- Implementar esquemas de seguridad para el intercambio de información con partes externas, estableciendo protocolos y estándares que garanticen la integridad y confidencialidad de los datos transmitidos.
- Definir controles de autenticación y autorización para la implementación de servicios web donde la Gobernación de Santander provea o consuma datos.
- Implementar técnicas de enmascaramiento y cifrado para el intercambio de información considerada como sensible, con el fin de aumentar los niveles de seguridad y garantizar la protección de los datos transmitidos.

- Garantizar la seguridad de la información cuando se realice intercambio o transferencia de la misma con partes y entidades externas.

7.10. Para la adquisición, desarrollo y mantenimiento de los sistemas de información

7.10.1. Objetivo

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

7.10.2. Alcance

Aplica a todos los desarrollos, adquisiciones y mantenimientos de aplicaciones internos y externos realizados para la Gobernación de Santander.

7.10.3. Descripción

A continuación, los criterios establecidos para la adquisición, desarrollo y mantenimiento de los sistemas de información en la Gobernación 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 la Gobernación 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, se debe 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.
- Definir, documentar y ejecutar procedimientos de construcción de sistemas de información seguros y/o desarrollo seguro; La seguridad se debe incluir en el diseño de todas las capas

de arquitectura (negocio, datos, aplicaciones y tecnología) equilibrando la necesidad de seguridad de información con la necesidad de accesibilidad y rendimiento.

- Aplicar los mismos controles implementados en el ambiente de producción al ambiente de desarrollo, tales como, control de acceso, copias de respaldo, registro de eventos.
- Contar con acuerdos de licenciamiento para todos los sistemas de información adquiridos o desarrollados por terceros, como mínimo se debe especificar 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 de la Gobernación de Santander a realizar auditorías a los terceros durante cualquier etapa del desarrollo del contrato.
- Acordar el cumplimiento de los niveles de soporte requeridos por la Gobernación de Santander cuando se contrata un desarrollo externo. Adicionalmente, se debe acordar la entrega de manual(es) técnico(s), que describa(n) la estructura interna del sistema, así como el diccionario de datos, librerías y archivos que lo conforman; y manual(es) funcional(es), que describa(n) 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 como externos.
- Ejecutar pruebas de aceptación del software para todos los desarrollos internos o externos, dichas pruebas deben estar orientadas 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 la utilización de datos reales que contengan información de datos personales o cualquier otra que haya sido clasificada como información pública restringida para la realización de pruebas, en caso de ser necesaria su utilización, todos los detalles y contenido sensibles se deberán proteger eliminándolos o modificándolos.

7.11. Para las relaciones con proveedores

7.11.1. Objetivo

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

7.11.2. 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 de la Gobernación de Santander.

7.11.3. 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, en la Gobernación de Santander se debe:

- Establecer de manera explícita en los acuerdos con los proveedores que la propiedad de la información es de la Gobernación 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 de la Gobernación 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 y conllevará a investigaciones y sanciones que apliquen ante los entes judiciales y de control correspondientes.
- Definir lineamientos regulatorios sobre el uso, tratamiento y privacidad de la información y propiedad intelectual de la entidad cuando se genere un proceso contractual entre la Gobernación de Santander y un proveedor o Usuario externo.
- Verificar el cumplimiento de los criterios establecidos en la política de tratamiento de datos personales adoptado por la Entidad cuando los proveedores o Usuarios externos almacene o recopile información que contenga datos personales y en su calidad de responsable o encargado del tratamiento.
- Definir e implementar un procedimiento de autorización y control de acceso a los servicios tecnológicos y activos de información de la Gobernación de Santander por parte de proveedores y Usuarios externos de acuerdo a las funciones establecidas en la obligación contractual.
- Definir e implementar un procedimiento de control de cambios sobre los servicios tecnológicos soportados por proveedores externos con el fin de garantizar la continuidad del negocio, basado en los principios de confidencialidad, integridad y disponibilidad de la información.
- Definir, aplicar, evaluar y monitorear los acuerdos de nivel de servicio con el fin de asegurar que los servicios tecnológicos soportados por proveedores y partes externas sean entregados de acuerdo a 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 que tengan acceso los proveedores.
- Establecer requisitos legales y normativos como el cumplimiento o 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 en 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 la Gobernación de Santander para toda la cadena de suministro.
- Verificar que cada proveedor designe un encargado de Seguridad Digital y Privacidad de la Información que actué 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 de la Gobernación 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.
- Definir e implementar un procedimiento periódico de auditoría sobre los servicios tecnológicos soportados por los diferentes proveedores y partes externas que permita validar la adecuada gestión de los incidentes de seguridad.
- 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 de la Gobernación de Santander.
- Definir un mecanismo para revocar los permisos de acceso asignados tanto a instalaciones como a los activos de información finalizados el objeto contractual con cualquier proveedor y Usuario externo.

7.12. Para la gestión de incidentes en la seguridad de la información

7.12.1. Objetivo

Brindar los lineamientos mínimos para la adecuada gestión de incidentes de seguridad de la información en la Gobernación de Santander

7.12.2. Alcance

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

7.12.3. Descripción

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

- Definir, documentar y ejecutar un procedimiento para la gestión de incidentes de seguridad de la información, que este orientado a asegurar una respuesta rápida, eficaz y ordenada de los mismos.
- Garantizar a través del procedimiento para la gestión de incidentes de seguridad digital y privacidad de la información los siguiente:
    - ✓ El detalle de los responsables de la gestión de incidentes de seguridad digital y privacidad de la información.
    - ✓ El paso a paso que se va a seguir en el caso de un evento de seguridad digital y privacidad de la información

- ✓ La Planificación y preparación de respuesta a incidentes de seguridad digital y privacidad de la información
- ✓ Seguimiento, detección, análisis y reporte de eventos e incidentes de seguridad digital y privacidad de la información.
- ✓ Manejo de evidencia forense.
- ✓ Valoración y toma de decisiones sobre eventos de seguridad digital y privacidad de la información y la valoración de debilidades.
- ✓ Punto de contacto para la detección y reporte de incidentes de Seguridad Digital y Privacidad de la Información
- ✓ Los Formatos para el reporte de eventos de seguridad digital y privacidad de la información

- Reportar cualquier situación sospechosa, o incidente de seguridad que comprometa la confidencialidad, integridad y disponibilidad de la información y conocer el procedimiento establecido para tal fin.
- Reportar las vulnerabilidades de Seguridad Digital y Privacidad de la Información que se presenten o identifiquen en los sistemas y servicios de información.

7.13. Para los aspectos de seguridad de la información en la gestión de la continuidad del negocio

7.13.1. 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.

7.13.2. Alcance

La presente política es aplicable a todos los procesos institucionales, así como a todos los sistemas y servicios de información de la Gobernación de Santander.

7.13.3. 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, en la Gobernación de Santander 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 más alto nivel de autoridad, experiencia y competencia para la recuperación operativa.
- Definir y documentar planes de continuidad, procedimientos de respuesta y recuperación, donde se especifique como la Gobernación de Santander gestionará un evento adverso y mantendrá su 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, con el fin de 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

7.14. Cumplimiento

7.14.1. Objetivo

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

7.14.2. Alcance

Todos los procesos estratégicos, misionales, de control y seguimiento, y de apoyo, de la Gobernación 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.

7.14.3. Descripción

- La Gobernación 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:
  - ✓ 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 de la Gobernación 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

▪ La Gobernación 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.