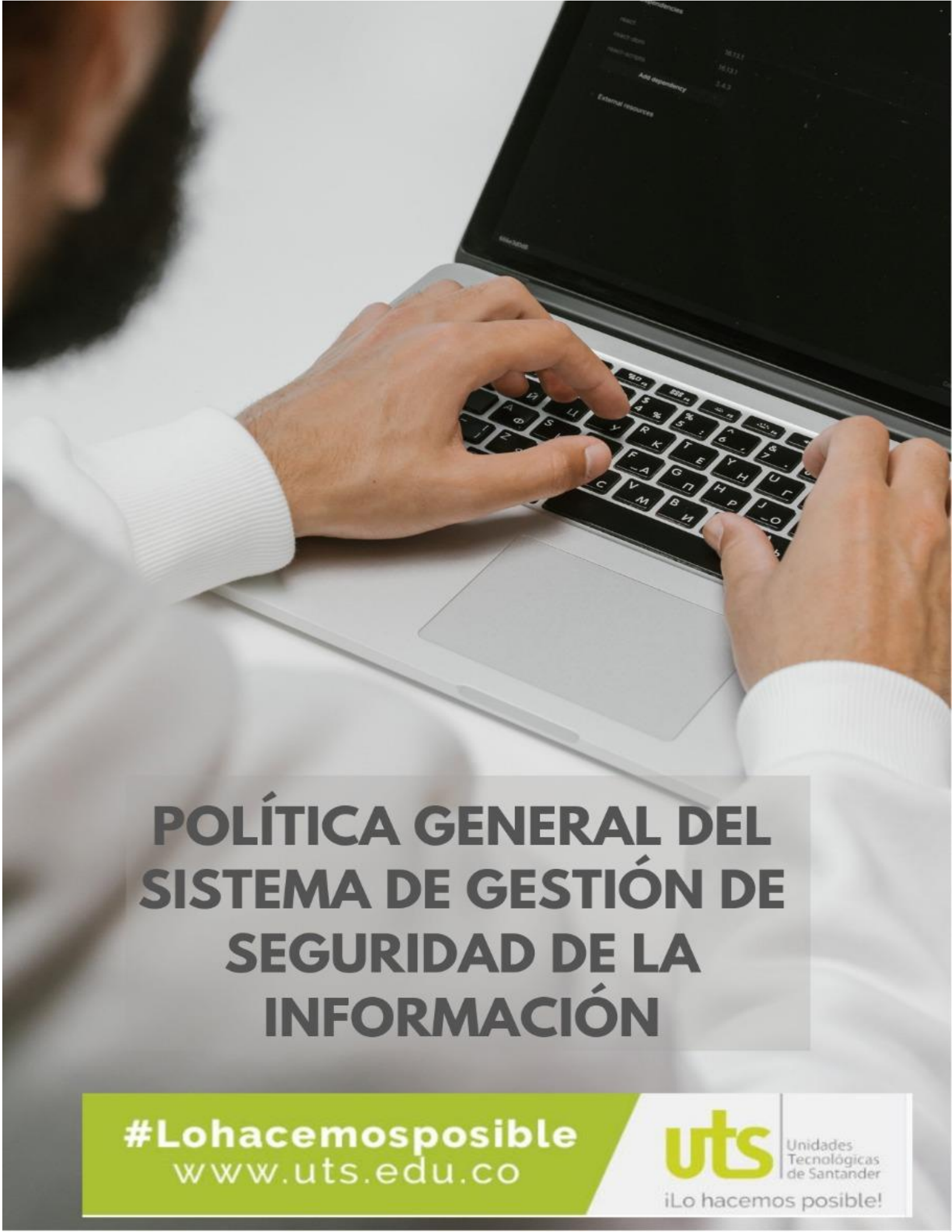

POLÍTICA GENERAL DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

TABLA DE CONTENIDO

1 OBJETIVO

Establecer los lineamientos que permitan gestionar, proteger, asegurar y salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información de las Unidades Tecnológicas de Santander, evitando su posible pérdida mediante exposición a amenazas latentes en el entorno, teniendo en cuenta los procesos, la operación, los objetivos de negocio y los requisitos legales vigentes en la institución, tomando como guía el Modelo de Seguridad y Privacidad de la Información (MSPI) del Ministerio de las Tecnologías de la Información y la Comunicación.

2 OBJETIVOS ESPECIFICOS

- Disminuir riesgos y detectar posibles problemas y amenazas de seguridad.
- Establecer las condiciones de seguridad.
- Garantizar el uso adecuado de recursos y aplicaciones del sistema.
- Cumplir con los lineamientos estipulados en la normatividad legal vigente.
- Fomentar la cultura en el manejo, control y seguridad de la información.

3 ALCANCE

La Política General de Seguridad y Privacidad de la Información es aplicable a todos los activos de información en operación de las Unidades Tecnológicas de Santander, al igual que a toda la comunidad académica que desempeñe alguna labor dentro de la institución.

4 DEFINICIONES

Confidencialidad: propiedad de que la información no esté disponible o revelada a personas no autorizadas, entidades o procesos. [ISO/IEC 27000: 2016].

Disponibilidad: propiedad de ser accesible y utilizable a la demanda por una entidad autorizada. [ISO/IEC 27000: 2016].

Integridad: propiedad de exactitud y completitud. [ISO/IEC 27000:2016].

Política: intenciones y direcciones de una organización como se expresan formalmente por la Alta Dirección. [ISO/IEC 27000: 2016].

Activo de Información: Conocimientos o datos que tienen valor para la Institución.

Información: Todo aquel conjunto de datos organizados en poder de la institución y que son de valor, independientemente de la forma en que se guarde o transmita (escrita, en imágenes, oral, impresa en papel, almacenada electrónicamente, proyectada, enviada por correo, fax o e-mail, transmitida en conversaciones, etc.), de su origen (de la propia organización o de fuentes externas) o de la fecha de elaboración.

Seguridad de la Información: Es la preservación de la Confidencialidad, Integridad y Disponibilidad de la información Institucional y. Preservación de la confidencialidad, integridad y disponibilidad de la información para propender por la autenticidad, trazabilidad, no repudio y fiabilidad de la misma.

Riesgo de Seguridad de la Información: Posibilidad que una amenaza dada explote vulnerabilidades de un activo o de un grupo de activos y por lo tanto cause daño a la Institución.

Terceros: Todas aquellas personas naturales o jurídicas, que no son funcionarios de la institución, pero que por las actividades que realizan en la institución, deban tener acceso a recursos de la plataforma tecnológica y activo de información.

Ataque Cibernético: Intento de penetración aprovechando una brecha de seguridad a un sistema informático por parte de un usuario no deseado ni autorizado a accederlo, por lo general con intenciones insanas y perjudiciales.

Brecha de Seguridad: Deficiencia de algún recurso informático o telemático que pone en riesgo los servicios de información o expone la información en sí misma, sea o no protegida por reserva legal.

Criptografía: Es el arte o ciencia de cifrar y descifrar información utilizando técnicas matemáticas que hagan posible el intercambio de mensajes de manera que sólo puedan ser leídos por las personas a quienes van dirigidos.

Cifrar: Quiere decir transformar un mensaje en un documento no legible, y el proceso contrario se llama “descodificar" o “descifrar". Los sistemas de ciframiento se llaman “sistemas criptográficos".

Certificado Digital: Un bloque de caracteres que acompaña a un documento y que certifica quién es su autor (autenticación) y que no haya existido ninguna manipulación de los datos (integridad). Para firmar, el firmante emisor utiliza una clave secreta que le vincula al documento. La validez de la firma podrá ser comprobada por cualquier persona que disponga de la clave pública del autor.

No Repudio: Este mecanismo genera registros especiales con alcances de "prueba judicial" acerca de que el contenido del mensaje de datos es la manifestación de la voluntad del firmante y que se atiene a las consecuencias de su decisión.

Sistema Operativo: Es un software de sistema que permite la comunicación entre el equipo de cómputo y el usuario, mediante la interpretación de comando dados por periféricos de entrada (teclado, Mouse, etc.).

Sistema de Gestión: Marco de políticas, procedimientos, guías y recursos asociados para lograr los objetivos de la Institución.

Procedimiento: Forma especificada para llevar a cabo una actividad o un proceso

Registro: Documento que presenta resultados obtenidos o proporciona evidencias de actividades desempeñadas

Información Pública: Información que por sus características puede o debe estar a disposición de cualquier persona natural o jurídica en el Estado Colombiano, ha sido

declarada de conocimiento público de acuerdo con alguna norma jurídica o por parte de la persona o grupo de personas con autoridad para hacerlo.

Información Pública Clasificada: Toda información que pertenece al ámbito propio, particular y privado o semiprivado de la institución 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 de 2014.

Información Pública Reservada: Toda información que estando en poder o custodia de la institución, 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 19 de la ley 1712 de 2014.

5 REFERENCIA NORMATIVA

Norma	Descripción
Decreto 1151 de 2008	Lineamientos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamenta parcialmente la Ley 962 de 2005, y se dictan otras disposiciones
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones
Ley 1581 de 2012	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley 1712 de 2014	Por medio de la cual se crea la ley de transparencia y del derecho de acceso a la información pública nacional y se dictan otras disposiciones.
Ley 1753 de 2015	Por la cual se expide el Plan Nacional de Desarrollo 2014-2018 "TODOS POR UN NUEVO PAÍS" "Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Ley 962 de 2005	El artículo 14 lo siguiente “Cuando las entidades de la Administración Pública requieran comprobar la existencia de alguna circunstancia necesaria para la solución de un procedimiento o petición de los particulares, que obre en otra entidad pública, procederán a solicitar a la entidad el envío de dicha información. En tal caso, la carga de la prueba no corresponderá al usuario. Será permitido el intercambio de información entre distintas entidades oficiales, en aplicación del principio de colaboración. El envío de la información por fax o por cualquier otro medio de transmisión electrónica, proveniente de una entidad pública, prestará mérito suficiente y servirá de prueba en la actuación de que se trate, siempre y cuando se encuentre debidamente certificado digitalmente por la entidad que lo expide y haya sido solicitado por el funcionario superior de aquel a quien se atribuya el trámite”.

Norma	Descripción
Decreto 1413 de 2017	En el Capítulo 2 Características de los Servicios Ciudadanos Digitales, Sección 1 Generalidades de los Servicios Ciudadanos Digitales
Decreto 2150 de 1995	Por el cual se suprimen y reforman regulaciones, procedimientos o trámites innecesarios existentes en la Administración Pública
Decreto 4485 de 2009	Por medio de la cual se adopta la actualización de la Norma Técnica de Calidad en la Gestión Pública.
Decreto 235 de 2010	Por el cual se regula el intercambio de información entre entidades para el cumplimiento de funciones públicas.
Decreto 2364 de 2012	Por medio del cual se reglamenta el artículo 7 de la Ley 527 de 1999, sobre la firma electrónica y se dictan otras disposiciones.
Decreto 2693 de 2012	Por el cual se establecen los lineamentos generales de la Estrategia de Gobierno en Línea de la República de Colombia, se reglamentan parcialmente las Leyes 1341 de 2009, 1450 de 2011, y se dictan otras disposiciones.
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012" o Ley de Datos Personales.
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones
Decreto 2433 de 2015	Por el cual se reglamenta el registro de TIC y se subroga el título 1 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 1078 de 2015	Por medio del cual se expide el Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de 2014 y se dictan otras disposiciones
Decreto 415 de 2016	Por el cual se adiciona el Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las Comunicaciones.
Decreto 728 2016	Actualiza el Decreto 1078 de 2015 con la implementación de zonas de acceso público a Internet inalámbrico
Decreto 728 de 2017	Por el cual se adiciona el capítulo 2 al título 9 de la parte 2 del libro 2 del Decreto Único Reglamentario del sector TIC, Decreto 1078 de 2015, para fortalecer el modelo de Gobierno Digital en las entidades del orden nacional del Estado colombiano, a través de la implementación de zonas de acceso público a Internet inalámbrico.
Decreto 1499 de 2017	Por medio del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015.

Norma	Descripción
Decreto 612 de 2018	Por el cual se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.
Decreto 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones.
Decreto 2106 del 2109	Por el cual se dictan normas para simplificar, suprimir y reformar trámites, procesos y procedimientos innecesarios existentes en la administración pública Cap. II Transformación Digital Para Una Gestión Publica Efectiva
Decreto 620 de 2020	Estableciendo los lineamientos generales en el uso y operación de los servicios ciudadanos digitales"
Resolución 2710 de 2017	Por la cual se establecen los lineamientos para la adopción del protocolo IPv6.
Resolución 3564 de 2015	Por la cual se reglamentan aspectos relacionados con la Ley de Transparencia y Acceso a la Información Pública.
Resolución 3564 2015	Reglamenta algunos artículos y parágrafos del Decreto número 1081 de 2015 (Lineamientos para publicación de la Información para discapacitados)
Norma Técnica Colombiana NTC 5854 de 2012	Accesibilidad a páginas web El objeto de la Norma Técnica Colombiana (NTC) 5854 es establecer los requisitos de accesibilidad que son aplicables a las páginas web, que se presentan agrupados en tres niveles de conformidad: A, AA, y AAA.
CONPES 3292 de 2004	Señala la necesidad de eliminar, racionalizar y estandarizar trámites a partir de asociaciones comunes sectoriales e intersectoriales (cadenas de trámites), enfatizando en el flujo de información entre los eslabones que componen la cadena de procesos administrativos y soportados en desarrollos tecnológicos que permitan mayor eficiencia y transparencia en la prestación de servicios a los ciudadanos.
CONPES 3920 de Big Data, del 17 de abril de 2018	La presente política tiene por objetivo aumentar el aprovechamiento de datos, mediante el desarrollo de las condiciones para que sean gestionados como activos para generar valor social y económico. En lo que se refiere a las actividades de las entidades públicas, esta generación de valor es entendida como la provisión de bienes públicos para brindar respuestas efectivas y útiles frente a las necesidades sociales.
CONPES 3854 Política Nacional de Seguridad Digital de Colombia, del 11 de abril de 2016	El crecimiento en el uso masivo de las Tecnologías de la Información y las Comunicaciones (TIC) en Colombia, reflejado en la masificación de las redes de telecomunicaciones como base para cualquier actividad socioeconómica y el incremento en la oferta de servicios disponibles en línea, evidencian un aumento significativo en la participación digital de los ciudadanos. Lo que a su vez se traduce en una economía digital con cada vez más participantes en el país. Desafortunadamente, el incremento en la

Norma	Descripción
	participación digital de los ciudadanos trae consigo nuevas y más sofisticadas formas para atentar contra su seguridad y la del Estado. Situación que debe ser atendida, tanto brindando protección en el ciberespacio para atender estas amenazas, como reduciendo la probabilidad de que estas sean efectivas, fortaleciendo las capacidades de los posibles afectados para identificar y gestionar este riesgo
CONPES 3975	Define la Política Nacional de Transformación Digital e Inteligencia Artificial, estableció una acción a cargo de la Dirección de Gobierno Digital para desarrollar los lineamientos para que las entidades públicas del orden nacional elaboren sus planes de transformación digital con el fin de que puedan enfocar sus esfuerzos en este tema.
Circular 02 de 2019	Con el propósito de avanzar en la transformación digital del Estado e impactar positivamente la calidad de vida de los ciudadanos generando valor público en cada una de las interacciones digitales entre ciudadano y Estado y mejorar la provisión de servicios digitales de confianza y calidad.
Directiva 02 2019	Moderniza el sector de las TIC, se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones

6 POLÍTICA GENERAL

La directiva de LAS UNIDADES TECNOLÓGICAS DE SANTANDER, entendiendo la importancia de una adecuada gestión de la información, se ha comprometido con la implementación de un sistema de gestión de seguridad de la información buscando establecer un marco de confianza en el ejercicio de sus deberes con el Estado, la Comunidad académica y los ciudadanos, todo enmarcado en el estricto cumplimiento de las leyes y en concordancia con la misión y visión de la Institución.

LAS UNIDADES TECNOLÓGICAS DE SANTANDER identificará y comprenderá los requisitos de las partes interesadas en el Sistema de Gestión de Seguridad de la Información, tanto internas como externas, que puedan afectar la capacidad del sistema para alcanzar los resultados previstos, o aquellas que puedan influir en la dirección estratégica de la organización.

Para LAS UNIDADES TECNOLÓGICAS DE SANTANDER, la protección de la información busca la disminución del impacto generado sobre sus activos, por los riesgos identificados de manera sistemática con objeto de mantener un nivel de exposición que permita responder por la integridad, confidencialidad y la disponibilidad de la misma, acorde con las necesidades de los diferentes grupos de interés identificados.

De acuerdo con lo anterior, esta política aplica a la Institución según como se defina en el alcance, sus funcionarios, terceros, estudiantes, docentes y la comunidad académica en general, teniendo en cuenta que los principios sobre los que se basa el desarrollo de las acciones o toma de decisiones alrededor del SGSI[1] estarán determinadas por las siguientes premisas:

[1] Sistema de Gestión de Seguridad de la Información (SGSI)

- Minimizar el riesgo en las funciones más importantes de la Institución.
- Cumplir con los principios de seguridad de la información.
- Cumplir con los principios de la función administrativa.
- Mantener la confianza de su comunidad académica, funcionarios, terceros y la ciudadanía en general.
- Proteger los activos tecnológicos.
- Establecer las políticas, procedimientos e instructivos en materia de seguridad de la información.
- Fortalecer la cultura de seguridad de la información en los funcionarios, terceros, y la comunidad académica en general.
- Garantizar la continuidad del servicio frente a incidentes.

LAS UNIDADES TECNOLÓGICAS DE SANTANDER ha decidido definir, implementar, operar y mejorar de forma continua un Sistema de Gestión de Seguridad de la Información, soportado en lineamientos claros alineados a las necesidades del servicio, y a los requerimientos regulatorios.

A continuación, se establecen 12 principios de seguridad que soportan el SGSI de LAS UNIDADES TECNOLÓGICAS DE SANTANDER:

- Las responsabilidades frente a la seguridad de la información serán definidas, compartidas, publicadas y aceptadas por cada uno de los funcionarios, proveedores, terceros y la comunidad académica en general.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER protegerá la información generada, procesada o resguardada por los procesos de negocio, su infraestructura tecnológica y activos del riesgo que se genera de los accesos otorgados a terceros (ej.: proveedores, contratistas), o como resultado de un servicio interno en outsourcing.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER protegerá la información creada, procesada, transmitida o resguardada por sus procesos institucionales, con el fin de minimizar impactos financieros, operativos o legales debido a un uso incorrecto de esta. Para ello es fundamental la aplicación de controles de acuerdo con la clasificación de la información de su propiedad o en custodia.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER protegerá su información de las amenazas originadas por parte del personal.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER protegerá las instalaciones de procesamiento y la infraestructura tecnológica que soporta sus procesos críticos.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER controlará la operación de sus procesos de negocio garantizando la seguridad de los recursos tecnológicos y las redes de datos.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER implementará control de acceso a la información, sistemas y recursos de red.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER garantizará que la seguridad sea parte integral del ciclo de vida de los sistemas de información.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER garantizará a través de una adecuada gestión de los eventos de seguridad y las debilidades asociadas con los sistemas de información una mejora efectiva de su modelo de seguridad.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER garantizará la disponibilidad de sus procesos de negocio y la continuidad de su operación basada en el impacto que pueden generar los eventos.

- LAS UNIDADES TECNOLÓGICAS DE SANTANDER garantizará el cumplimiento de las obligaciones legales, regulatorias y contractuales establecidas.

7 POLÍTICAS ESPECÍFICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

7.1 ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

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

7.1.1 ROLES Y RESPONSABILIDADES PARA LA SEGURIDAD DE LA INFORMACIÓN

Las Unidades Tecnológicas de Santander asigna las funciones relacionadas con la seguridad de la información al comité institucional de gestión y desempeño, el cual deberá asegurar que exista una dirección y apoyo para la administración y desarrollo de las iniciativas sobre seguridad de la información. Se deberán asignar las funciones de seguridad de la información en el instrumento destinado para tal fin

Para asegurar la aplicación de la Política General del Sistema de Gestión de Seguridad de la Información se hace necesario definir los roles con sus respectivas responsabilidades.

7.1.1.1 Comité Institucional de Gestión y Desempeño

- Aprobar la política de seguridad y privacidad
- Asignar los recursos para el establecimiento, implementación, mantenimiento y mejora continua del Sistema de Gestión de Seguridad de la Información atendiendo a las necesidades institucionales.
- Revisar y validar las políticas generales, complementarias, procedimientos y protocolos en materia de seguridad y privacidad.
- Coordinar la implementación de las políticas generales, complementarias, procedimientos y protocolos en materia de seguridad y privacidad.
- Evaluar y coordinar la implementación de controles específicos de seguridad y privacidad de la información para los sistemas o servicios de las Unidades Tecnológicas de Santander, sean preexistente o nuevos.

- Revisar y validar los informes o reportes de actividades en el marco de la Seguridad y Privacidad de la Información.

7.1.1.2 Proceso Gestión Jurídica

- Asegurar que lo establecido en las políticas generales, complementarias, procedimientos y protocolos den cumplimiento a la normatividad relacionada a la seguridad y privacidad de la información.

7.1.1.3 Proceso de Comunicación Institucional

- Garantizar que las políticas generales, principios, políticas complementarias, procedimientos y protocolos de seguridad y privacidad de la información se comuniquen y apropien adecuadamente.
- Garantizar que la seguridad y privacidad de la información sean parte de la cultura organizacional.

7.1.1.4 Proceso Soporte al Sistema Integrado de Gestión.

- Evaluar de manera independiente el cumplimiento de las políticas generales, principios, políticas complementarias, procedimientos y protocolos de seguridad y privacidad de la información.

7.1.1.5 Responsables de los Procesos

- Participar activamente en la definición de las políticas, procedimientos y protocolos en materia de seguridad y privacidad de la información, de su competencia.
- Implementar las políticas, procedimientos y protocolos en materia de seguridad y privacidad de la información.
- Asegurar que el personal a cargo y sus partes interesadas cumplan con las políticas, procedimientos y protocolos en materia de seguridad y privacidad de la información.
- Generar retroalimentación sobre la efectividad de las políticas, procedimientos y protocolos en materia de seguridad y privacidad de la información.

7.1.1.6 Oficial de Seguridad de la Información.

- Liderar y coordinar la implementación de las políticas de seguridad de la información, con la participación activa de las dependencias de la Institución.
- Evaluar y coordinar la implementación de controles específicos de seguridad de la información para nuevos sistemas de información o servicios informáticos.
- Monitorear cambios significativos en los riesgos que afectan a los recursos de información frente a las amenazas más importantes.
- Identificar las necesidades y recursos necesarios (tecnológicos, humanos, de
- capacitación, financieros, etc.) para el mantenimiento de la infraestructura de
- seguridad de la información.
- Identificar las necesidades de formación (capacitación y entrenamiento) del
- grupo de recursos informáticos y establecer un plan de capacitación para formar y

entrenar a sus integrantes.

- Actuar como un asesor en seguridad de la información para la Institución.
- Hacer seguimiento al comportamiento de los indicadores de gestión de la seguridad de la información que adopte el Comité de Seguridad de la Información
- Hacer la evaluación del desempeño del SGSI.
- Realizar la revisión y supervisión del SGSI.
- Establecer un programa periódico (por lo menos una vez al año) de revisión
- de vulnerabilidades de la plataforma tecnológica de la Institución y coordinar los respectivos aseguramientos conforme los resultados de las mencionadas
- pruebas.
- Reportar al Comité Institucional de Gestión y Desempeño el estado de la investigación y monitoreo de los incidentes de seguridad de la información, la revisión y supervisión del SGSI.
- Presentar al Comité Institucional de Gestión y Desempeño la Información iniciativas e informes periódicos del estado de seguridad de la información de la Institución.
- Identificar los organismos externos que ejerzan autoridad en lo relacionado con los aspectos de seguridad de la información e identificar los mecanismos de contacto respectivos
- Identificar comunidades y grupos de interés relacionados con Seguridad de la Información que le permitan mantenerse actualizado y en contacto con expertos en los temas de seguridad.

7.1.2 POLÍTICA – CONTACTO CON LAS AUTORIDADES

El Oficial de Seguridad de la Información, será el encargado de coordinar los conocimientos disponibles en las Unidades Tecnológicas de Santander, a fin de brindar ayuda en la toma de decisiones en materia de seguridad, éste podrá obtener asesoramiento de otros Organismos.

Se debe mantener contacto permanente con las instituciones de educación superior, los grupos de investigación, entidades del gobierno, proveedores de tecnología que trabajan en pro de mantener actualizado a las personas que se desarrollan dentro del ámbito de la tecnología, para de esta manera mantenerse al tanto en amenazas, incidentes y soluciones, para lo cual se definió guía de contacto con autoridades en materia de seguridad y privacidad de la información.

7.1.3 POLÍTICA – CONTACTO CON LOS GRUPOS DE INTERESES ESPECIALES

El Oficial de Seguridad de la Información, será el encargado de coordinar los conocimientos disponibles en las Unidades Tecnológicas de Santander, quien debe adelantar las gestiones para pertenecer a grupos de intereses especiales en seguridad de la información, a través de los cuales se tenga acceso a los foros, actualizaciones o novedades en temas de seguridad de la información, para lo cual se definió guía de contacto con autoridades en materia de seguridad y privacidad de la información.

7.1.4 POLÍTICA DE SEGURIDAD EN PROYECTOS

Teniendo en cuenta la metodología de gestión de proyecto de la Institución, los líderes deben incluir dentro de la etapa de planeación del proyecto las actividades necesarias para identificar cualquier impacto que afecte la seguridad de la información de los activos entre otros:

- Disposición de los activos de información susceptibles al uso de los usuarios del proyecto.
- La creación o disposición final de activos de la información.
- Cambio en los niveles de riesgos asociados a los activos de la información actuales.
- Impacto en los controles de los activos de la información actuales.

Definir los responsables dentro del equipo del proyecto frente a las actividades de seguridad de la información. Los objetivos y políticas de seguridad de la información son aplicables y deben ser conocidos y tenidos en cuenta por parte de todos los proyectos de la Institución.

Gestionar el acompañamiento de los responsables de la seguridad de la información para la validación y aprobación de cualquier cambio o impacto que modifique el nivel de riesgo a los procesos o activos de información relevantes al proyecto y controles asociados.

7.2 POLÍTICA DE USO DE DISPOSITIVOS MÓVILES

Las Unidades Tecnológicas de Santander implementará las directrices necesarias para la autorización de acceso a los recursos y activos de información a través de los dispositivos de tecnología móviles (computadores portátiles, smartphones, tabletas, o cualquier equipo de dispositivos electrónicos con capacidad de acceso a las redes inalámbricas), conforme a los riesgos asociados. Así mismo, establecerá mecanismos de control de seguridad de la información de estricto cumplimiento por parte de los funcionarios, contratistas y demás comunidad académica para el acceso a la información, tecnologías de la información y comunicaciones o servicios y recursos de la Institución desde dichos dispositivos.

El uso de servicios tecnológicos de la Institución desde dispositivos móviles será administrado por el Grupo de Recursos Informáticos, que tendrá la potestad de realizar la desactivación, borrado y retiro de los accesos a los servicios tecnológicos, cuando el dispositivo móvil haya sido extraviado o robado al funcionario o contratista responsable o cuando se incumplan las políticas de seguridad y privacidad.

Se deberán proteger física y lógicamente los dispositivos móviles propiedad de la Institución para evitar el hurto, acceso o la divulgación no autorizada de la información, por parte de los funcionarios, contratistas y terceros a los que se les asigne el dispositivo móvil.

En caso de extravío o hurto de un dispositivo móvil asignado por la Institución, el funcionario, contratista o tercero será el responsable de informar de manera inmediata a las UTS, con el propósito de establecer las medidas de seguridad adecuadas para la protección de la información contenida o acceso a los sistemas de información desde el dispositivo.

Es responsabilidad de los usuarios velar por la confidencialidad de la información a la cual se accede desde los dispositivos móviles, por lo tanto, de acuerdo con los niveles de clasificación de la información, deberá si es necesario realizar el cifrado de la información, así como la ejecución de copias de respaldo.

Al momento de reintegrar un dispositivo móvil y/o activo de información al cual se le haya dado uso por fuera de las instalaciones físicas de la Institución, el grupo de recursos informáticos adelantará las acciones de seguridad necesarias como análisis completo de antivirus, actualizaciones de sistema operativo y demás que aplique, de manera que permite garantizar que es seguro conectarlo a la red local.

Es responsabilidad del funcionario, contratista o tercero al cual se le haya asignado un dispositivo móvil, realizar la copia de seguridad de la información que dentro del desarrollo de su función institucional se genere, este mismo indicará la periodicidad de acuerdo a la importancia y relevancia de la información gestionada.

7.3 POLÍTICA DE ACCESO REMOTO

Las UTS autorizará el acceso remoto, conforme a las necesidades y funciones del solicitante. En todo caso, es responsabilidad de los colaboradores que accedan remotamente a los activos de información institucionales disponibles en la red local, garantizar el cumplimiento de las políticas de seguridad y privacidad de la información de Las UTS y frente al respectivo análisis del riesgo.

Las UTS dispondrá de los recursos tecnológicos y organizacionales para el acceso remoto a activos de información institucionales disponibles en la red local, que permita cumplir con los intereses y necesidades de la institución, considerando los riesgos y su respectiva gestión.

Al momento de habilitar y configurar el acceso remoto a los servicios tecnológicos, el grupo de recursos informáticos, establecerá mecanismos de cifrado y no repudio en sus comunicaciones, de manera que ofrezcan una mayor protección a los activos de información.

Las UTS preverá mecanismos de seguridad física y lógica para el acceso remoto a los activos de información institucionales disponibles en la red local, con el fin de conservar las características de integridad, disponibilidad y confidencialidad de la información.

Para el desarrollo de las actividades de acceso remoto se deberá realizar un análisis de riesgos, a partir del cual se adopten los mecanismos de control para la protección de los activos de información accedidos durante las actividades, en donde sólo se podrán conectar remotamente los usuarios autorizados.

El grupo de Recursos informáticos seleccionará la herramienta y tecnología para facilitar el acceso remoto, teniendo en cuenta criterios de seguridad que para el momento se definan.

En caso de pérdida o hurto de un equipo en el cual se lleven actividades de acceso remoto o perdida de confidencialidad, será responsabilidad del funcionario, contratista o tercero informar de forma inmediata a las UTS el evento, con el fin de establecer las medidas de seguridad adecuadas para la protección de la información contenida.

Referente a los componentes de tecnología, el jefe directo del área deberá notificar y justificar la necesidad de trabajo de acceso remoto, indicando el nombre del usuario y los servicios que requiere en los formatos que para el caso se definan.

El Grupo de Recursos Informáticos, previa solicitud del jefe de área, otorgará o denegará el acceso remoto a servicios tecnológicos disponibles en la red local.

El Grupo de Recursos Informáticos será la responsable de implementar los controles de seguridad necesarios para llevar a cabo las actividades de acceso remoto.

Los funcionarios, contratistas y terceros que se encuentren autorizados para el desarrollo de actividades de acceso remoto, deberán cumplir con las responsabilidades aplicables en la red local, así mismo reportar cualquier situación que pueda afectar el desarrollo de las actividades o ponga en peligro los servicios tecnológicos de las UTS.

El Grupo de Recursos Informáticos, en coordinación con el Oficial de Seguridad, determinará los canales de comunicación y métodos de autenticación apropiados para controlar el acceso de usuarios remotos a los servicios tecnológicos de Las UTS.

El Grupo de Recursos Informáticos, en coordinación con el Oficial de Seguridad, generarán protocolos que den respuesta a situaciones de alerta como una avería del ordenador causada por un virus, una configuración incorrecta o un fallo de hardware. Estableciendo controles de seguridad tales como copias de respaldo o equipos o dispositivos de reserva en caso de daño o pérdida de los equipos.

7.4 GESTIÓN DE RECURSO HUMANO

Previa a la vinculación al empleo para el caso de los funcionarios o la formalización del contrato para el caso de los contratistas, el grupo de Talento Humano debe verificar el cumplimiento delos requisitos necesarios para el perfil.

Al iniciar un proceso de contratación o vinculación, el grupo de Talento Humano realiza las verificaciones necesarias para confirmar la veracidad de la información suministrada por el personal candidato a ocupar un cargo vacante, antes de su vinculación definitiva.

Se deberán establecer mecanismos para establecer un Acuerdo de no divulgación o Cláusula de Confidencialidad, así como la aceptación y cumplimiento de Políticas de Seguridad de la Información teniendo en cuenta los lineamientos del procedimiento de gestión de seguridad del talento humano que permitan garantizar la seguridad de los datos personales en las operaciones.

Al momento de la vinculación, se deberá realizar la inducción a los empleados y contratistas en la Políticas en Seguridad de la Información y política de protección de datos personales.

Se deberá informar a los funcionarios, contratistas y partes interesadas las directrices sobre la seguridad de la información.

Se deberá motivar a funcionarios y contratistas e interesados a cumplir las políticasde seguridad de la información de la Institución.

En cumplimiento al compromiso del Sistema de Gestión de Seguridad de la Información deberá establecer Planes de Sensibilización de Seguridad de la Información, alineado con las políticas y procedimientos pertinentes, con el fin de generar una cultura de seguridad de la información.

Cuando ocurra un incidente de seguridad de la información y producto de ello se determine un grado de culpabilidad o responsabilidad por parte de los servidores públicos o contratistas, la institución tomará las acciones pertinentes y remitirá a las entidades competentes para su investigación.

Los cambios de funciones o retiro de los servidores públicos deben estar guiados por procesos donde se asegure la entrega de activos, el retiro de los accesos físicos y lógicos, la no eliminación y copiado de información no autorizada por el jefe directo o el grupo de recursos informáticos, así como la posterior entrega de estos (activos) de acuerdo con su nuevo rol.

El proceso de gestión de talento humano o quien corresponda para el caso de los contratistas notificará formalmente al Grupo de Recursos Informáticos a través de los canales establecidos, los retiros del personal y las novedades administrativas, para el bloqueo o eliminación de datos de acceso y cuentas de correo.

Las UTS establece controles para asegurar que los servidores públicos se les aplique los controles de seguridad de la información definidos en el proceso de ingreso y se les presente las responsabilidades en seguridad de la información durante el proceso de inducción.

Las UTS diseña define y ejecuta de manera permanente un programa desensibilización en seguridad de la información.

Las UTS establece los controles para proteger los intereses de la institución como parte del proceso de cambio de cargo, perfil o en la terminación laboral.

7.5 GESTIÓN DE LOS ACTIVOS

Las UTS tiene la custodia sobre todo dato, información y mensaje generado, procesado y contenido en la plataforma tecnológica, así como también de todo aquello transmitido a través de su red de datos o cualquier otro medio de comunicación físico o electrónico y se reserva el derecho de conceder el acceso a la información.

Los funcionarios, contratistas y comunidad académica de las UTS que se les haya asignado dispositivos móviles y/o activo de información de propiedad de la institución, no podrán instalar software sin previa autorización y coordinación por la Oficina de las TICS, así mismo, no se deberá realizar conexiones externas a redes públicas que no cuenten con protecciones de seguridad equivalentes a las definidas por el SGSI.

Los funcionarios, contratistas y comunidad académica de las UTS que se les haya asignado dispositivos móviles y/o activo de información de propiedad de la institución no podrán conectarse a las redes públicas desde los dispositivos móviles de la Institución, sin haberse configurado medidas de seguridad que afecten la disponibilidad, integridad y confidencialidad de la información allí contenida entre las que se cuentan por lo menos un antivirus instalado

Identificar y mantener un inventario de los activos de información asociados a cada proceso de la Institución. Cada activo debe ser claramente identificado, también su propietario y clasificación asociada a cada activo de información.

Antes de extraer el dispositivo móvil de la institución, el funcionario, contratista o tercero a cargo del mismo, deberá diligenciar el formato salida de activos, y debe ir con el visto bueno del Coordinador de Recursos Físicos.

Cada activo de información de la Institución debe tener asociado un responsable que debe velar por su seguridad. Los responsables identificados deben garantizar que sus activos de información reciban un apropiado nivel de protección basados en su valor de confidencialidad, integridad, disponibilidad, riesgos identificados y/o requerimientos legales de retención incluso si estos están por fuera de la institución, en donde nunca se debe perder de la vista del responsable.

El responsable debe reportar las fallas o deterioros de los activos asignados, al grupo de recursos informáticos, quienes adelantarán las acciones necesarias para su reparación.

La Institución debe realizar la clasificación y control de activos con el objetivo de garantizar que los mismos reciban un apropiado nivel de protección, clasificar la información para señalar su sensibilidad y criticidad y definir los niveles de protección y medidas de tratamiento, evaluando los tres dominios de la información en las cuales se basa la Seguridad de la Información: confidencialidad, integridad y disponibilidad

Se debe promover el buen uso de los activos de Información, conservando el derecho a la intimidad, la privacidad, el habeas data si aplica, y la protección de los datos de sus propietarios o custodios.

Los servidores públicos y contratistas son los responsables del tratamiento de la información que se encuentra en los equipos de cómputo, dispositivos, nube y documentación física para llevar a cabo sus funciones y deben abstenerse de realizar en ellos tratamiento de información no institucional.

Los dispositivos de almacenamiento o equipos de cómputo, el servicio de acceso a servicios de red locales y externas a las UTS, las aplicaciones, sistemas de información, correo electrónico y usuarios de red son propiedad de la institución y deben ser usados únicamente para el cumplimiento de actividades laborales o contractuales en el desarrollo de la gestión académica misional.

Para los dispositivos móviles, activos de información y medios extraíbles (cintas, discos flash, discos duros, discos compactos, DVDs y medios impresos) propiedad de la Institución que se dejen de utilizar ya sea porque se le dio de baja o entregó en donación

deben pasar por un proceso que haga irrecuperable la información allí almacenada, teniendo en cuenta las TRD si aplica, el proceso debe ser coordinado y autorizado por el grupo de recursos informáticos.

7.5.1 USO ADECUADO DEL SOFTWARE

El software licenciado de las UTS debe ser usado únicamente en los equipos institucionales, toda copia, comercialización y/o sesiones no autorizadas, bien sea para uso propio o para proporcionarlo a personal externo a la institución no está permitido. Salvo previa autorización del grupo de recursos informáticos

La coordinación y ejecución de mantenimiento de programas o aplicaciones instaladas en las estaciones de trabajo es del grupo de recursos informáticos.

Los servidores públicos y contratistas no deben efectuar ninguna de las siguientes actividades:

- Copiar software licenciado de la institución para utilizar en sus computadores personales o en cualquier tipo de dispositivo diferente a los autorizados por la institución, cualquiera sea su ubicación, salvo autorización del grupo de recursos informáticos.
- Introducir programas maliciosos en las redes o a los servidores (ejemplo: virus informáticos, gusanos, troyanos, spyware, adware, puertas traseras, spam, ataques DDOS, keyloggers o cualquier otro tipo de malware).

7.5.2 USO ADECUADO DE LOS RECURSOS TECNOLÓGICOS

Los usuarios no deben realizar cambios en las estaciones de trabajo relacionados con la configuración del equipo, tales como conexiones de red, usuarios locales de la máquina, fondo de pantalla y protector de pantalla institucional.

Todos los escritorios físicos y virtuales de los servidores públicos o contratistas de la Institución se deben mantener despejados y libres de información pública reservada o pública clasificada en ausencia de este.

Se debe velar por evitar accesos no autorizados, pérdida o daño de la información clasificada, almacenándola de forma segura, realizando el bloqueo del equipo de cómputo en el momento en que será requerido.

La navegación a internet en los servidores de la infraestructura será restringida, en donde sólo se habilitará el acceso para servicios esenciales y de actualización necesaria para la correcta operación de los servicios tecnológicos.

Está prohibida la instalación de Add-ons en los navegadores Web, salvo aquellas autorizadas e instaladas por el grupo de recursos informáticos.

7.5.3 USO ADECUADO DEL CORREO ELECTRÓNICO

Los correos creados para estudiantes y temporales, tienen la siguiente sintaxis: nombre_de_usuario@uts.edu.co. Para el nombre de usuario se toma el usuario del sistema académico Academusoft.

Los correos de office 365 son un recurso tecnológico a disposición de la Comunidad Académica para la gestión administrativa, académica de formación, investigación y extensión.

Los servicios de office 365 deben ser utilizados solamente para propósitos institucionales y evitarse su uso para tratar asuntos personales.

El uso del correo electrónico de Office 365 es obligatorio para el envío y recepción de comunicaciones a nivel Institucional, para la realización de trámites internos que requieran del uso de este medio y para interacción con los Sistemas de Información Institucionales.

La institución se reserva el derecho de deshabilitar, modificar o eliminar los correos institucionales, en las cuales se evidencie un uso inadecuado o que incurran en el incumplimiento de las políticas y condiciones plasmadas en el presente documento.

La institución se reserva el derecho de suspender o cancelar el uso del correo de Office 365 asignada al usuario, en cualquier momento, sin necesidad de aviso previo.

La institución se reserva el derecho de acceder al correo de Office 365 asignada al usuario, en caso de que sea necesario.

La información enviada a través de los servicios de los correos institucionales, está regida por la Política de Protección de Datos Personales de las UTS, las condiciones de uso y Política de Privacidad de Microsoft (https://privacy.microsoft.com/es-ES/privacy), por la Ley de Protección de Datos Personales de la República de Colombia (Ley 1581 de 2012) y demás normativas relacionadas.

Por medio del Correo electrónico o cualquiera de los servicios de Office 365 no está permitido publicar, compartir, enviar o retransmitir mensajes que puedan constituir acoso, considerado difamatorio, explícitamente sexual o que pueda ofender a alguien con base en su raza, género, nacionalidad, orientación sexual, religión, política o discapacidad, como tampoco abrir correos que provengan de destinatarios desconocidos o que tengan asuntos o archivos adjuntos sospechosos.

El servicio ofrecido a través de Office 365 cuenta con diferentes medidas de seguridad que deben ser tenidas en cuenta y configuradas por los usuarios (correo alterno de recuperación, doble factor de autenticación y registro de número telefónico celular). Éstos métodos permitirán al usuario enterarse inmediatamente, si se presenta actividad inusual en el correo. Si llega a presentarse tal situación, cambie inmediatamente la contraseña y reporte la eventualidad al Grupo de Recursos Informáticos.

La información contenida en el correo electrónico institucional o en cualquiera de los servicios de Office 365 asignado por la institución para el cumplimiento de sus responsabilidades académicas, administrativas y de investigación, son de propiedad de la institución y podrán ser revisadas en el momento en que ella lo determine.

Los mensajes de correo electrónico revisten la misma fuerza probatoria que tienen los documentos físicos, según lo establecido por artículo 10 de la ley 527 de 1999, el cual indica que los mensajes de datos serán admisibles como medios de prueba y su fuerza probatoria es la otorgada en las disposiciones del Código de Procedimiento Civil, hoy Código General del Proceso.

Se prohíbe copiar o reenviar correos electrónicos que se encuentren clasificados como CONFIDENCIALES, CON RESERVA o PRIVADOS en el asunto del mensaje, sin tener la autorización del remitente.

Se prohíbe descargar, compartir o imprimir documentos digitales almacenados en Office 365 que se encuentren clasificados como CONFIDENCIALES, CON RESERVA o PRIVADOS, sin tener la autorización del remitente.

Después de 24 meses sin realizar Matrícula Académica, el estudiante será considerado inactivo y la institución puede disponer de la licencia del correo de Office 365 para ser asignada a otro estudiante.

Los correos pertenecientes a dependencias y/o eventos, solo deben ser utilizadas por la persona a quien designe el jefe de la dependencia responsable de dicha cuenta.

Los correos creados para el apoyo a las actividades de contratistas administrativos, no estará relacionado con el nombre del contratista sino con el nombre de la dependencia o proceso que apoya el contratista. Por ejemplo: contratista.soporte@correo.uts.edu.co

El titular del correo debe realizar copias de respaldo de la información almacenada en su cuenta de correo electrónico. Más información en https://www.veeam.com/blog/es/how-backup-office-365-email.html

La Dirección Administrativa de Talento Humano o coordinación de la institución deberá notificar la finalización de contrato (prestación de servicios, docente hora cátedra, funcionario nombrado,) o el cierre del proyecto o evento, al grupo de recursos informáticos, dentro de los quince (15) días hábiles posteriores a la finalización del evento.

Creación de correo institucionales.

- Estudiantes.

  La creación y notificación de correos de Office 365 institucional para estudiantes nuevos, se llevará a cabo según el calendario académico del grupo de Admisiones, Registro y Control Académico.

  Dentro del tiempo establecido para la inscripción de nuevos estudiantes, el grupo de recursos informáticos generará de manera periódica la creación mediante masivo de los nuevos estudiantes la cuenta de office 365. El grupo de recursos informáticos tendrá un tiempo aproximado de cinco (05) días hábiles para realizar la creación de los correos y notificar a los estudiantes a los correos personales registrados en Academusoft.

- Funcionarios y docentes.

  La creación y notificación de correos de Office 365 institucional para funcionarios y docentes nuevos, se llevará a cabo en la medida que se vayan realizando los nombramientos.

  La dirección Administrativa de Talento Humano envía la solicitud para creación de nuevos correos institucionales. El grupo de Recursos informáticos tendrá un tiempo aproximado de cinco (05) días hábiles para realizar la creación las cuentas y notificar

  Una vez creado el correo, los datos de acceso serán enviados a la dirección Administrativa de Talento Humano para su posterior notificación.

- Dependencias, eventos y contratistas.

  Los correos temporales o para dependencias, deben ser solicitadas por el coordinador o el jefe de la dependencia, diligenciando el formato de Solicitud de Cuenta de Correo Temporal, el cual se puede descargar del sitio web https://www.dropbox.com/sh/op8bmnpioxnutkq/AABbdxnf6f3dN6eTAj-bSuxoa?dl=0 el responsable del correo debe diligenciar el formato de solicitud completamente y con información veraz.

  El formulario diligenciado debe ser enviado al correo electrónico recursosinformaticos@correo.uts.edu.co o entregado en el grupo de recursos informáticos quién enviará notificación de la creación del correo y las credenciales de acceso al Responsable del correo.

  Cada miembro de la comunidad académica tiene derecho a solo un correo electrónico institucional, para uso exclusivo del titular, independientemente de la cantidad de vinculaciones que tenga con la institución.

  Para empleados con vinculación temporal (contratistas, docentes hora cátedra, etc.) se creará un correo electrónico institucional, cuya vigencia estará regida por el tiempo de duración del contrato con la institución.

Cancelación de Correo Institucional.

La institución procederá a la cancelación de los correos en los siguientes casos:

- Estudiantes.

  Cuando se pierda la condición de estudiante de acuerdo a las diferentes condiciones definidas en el reglamento estudiantil.

  Ante la evidencia de incumplimiento de las políticas definidas en este documento.

  Por inactividad de acuerdo a los tiempos establecidos en la presente política.

- Servidores públicos y docentes.

Finalización de vinculación con la institución para funcionarios, docentes y contratistas.

Ante la evidencia de incumplimiento de las políticas definidas en este documento

- Dependencias, eventos y contratistas.

  Se eliminarán los correos 60 días después de la finalización del contrato o el evento, previa notificación al Responsable del correo.

7.5.4 CLASIFICACIÓN DE LA INFORMACIÓN

Los niveles de clasificación de la información de las UTS permiten identificar las características de protección, manejo y tratamiento de la información, se establecen los siguientes niveles de clasificación: información pública, información pública reservada e información pública clasificada.

Todos los Colaboradores y terceros cuando sea el caso, deben mantener organizado el archivo de gestión, siguiendo los lineamientos establecidos por el Proceso de Gestión Documental.

Los Jefes de Oficina, Coordinadores de Grupo deben establecer mecanismos de control de documentos, con el fin de garantizar y mantener la disponibilidad, integridad y confidencialidad de la información.

Todos los Colaboradores y Terceros cuando sea el caso de las UTS son responsables de la organización, conservación, uso y manejo de los documentos en los medios que son dispuestos por la institución.

Los líderes de proceso son los responsables de identificar, actualizar e informar al oficial o líder de seguridad o quién haga sus veces en la institución, sobre nuevos activos de información en el proceso o comunicar cambios (estado, responsable, valoración, etc.) que se presenten en los actuales.

Todos los servidores públicos serán responsables de proteger la información a la cual accedan o procesen, para evitar su pérdida, alteración, destrucción o uso indebido.

Los servidores públicos y contratistas deben hacer el respectivo proceso de devolución de los activos de información asignados a su cargo una vez finalice la relación contractual con la institución.

Cada usuario en la institución es responsable de dar uso adecuado y en ningún momento el activo puede ser usado para realizar prácticas ilícitas o mal intencionadas que atenten contra terceros.

Los usuarios deben cerrar la sesión activa en el equipo de cómputo al dejar el puesto de trabajo o bloquearla mediante la combinación de las teclas Windows + L para un bloqueo manual, el bloqueo se debe realizar incluso para periodos de ausencia cortos.

El usuario debe realizar constantemente la depuración de su correo electrónico, tanto a los correos enviados como los recibidos.

Los líderes de proceso deben realizar la clasificación y calificación en términos de seguridad de los activos de información a su cargo con la ayuda del grupo de recursos informáticos.

Se deberá realizar el proceso de etiquetado a los activos de información tipo información, de acuerdo con la clasificación de la información asignada por cada propietario del activo.

7.5.5 GESTIÓN DE MEDIOS REMOVIBLES

Al momento de conectar un dispositivo de almacenamiento externo, al responsable que se le haya asignado un dispositivo móvil a activo informático compatible de propiedad de las UTS, debe realizar un proceso de escaneo con el antivirus instalado, para evitar una infección por virus cibernético que pueda afectar la seguridad de la información del dispositivo.

Se encuentra restringida la conexión no autorizada a la infraestructura tecnológica de las UTS, de cualquier elemento de almacenamiento como dispositivos personales USB, discos duros externos, CDs, DVDs, cámaras fotográficas, cámaras de video, teléfonos celulares, módems, entre otros dispositivos no institucionales.

Los medios de almacenamiento removibles como cintas, discos duros removibles, CDs, DVDs, medios impresos y dispositivos USB, entre otros, que contengan información institucional, deben ser controlados y físicamente protegidos.

Los dispositivos removibles, así como toda información CONFIDENCIAL de la institución, independientemente del medio en que se encuentre, deben permanecer bajo seguridad durante horario no hábil o en horarios en los cuales los funcionarios, contratistas o terceros responsables no se encuentre en su sitio de trabajo.

La Institución definirá los medios removibles de almacenamiento que podrán ser utilizados por las personas autorizadas el grupo de recursos informáticos, en la plataforma tecnológica si es requerido para el cumplimiento de sus funciones.

Cada medio removible de almacenamiento deberá estar identificado de acuerdo con el tipo de información que almacene.

Para los procesos de baja, reutilización o garantías de los dispositivos que contengan medios de almacenamiento, se debe cumplir según sea el caso con la destrucción física del mismo o borrado seguro vigilado y autorizado por el grupo de recursos informáticos.

El tránsito o préstamo de medios removibles deberá ser autorizado por el propietario del activo de información.

La información crítica de la institución no deberá ser almacenada ni transportada en medios removibles.

7.6 POLÍTICA DE CONTROL DE ACCESO

Las UTS, como se ha mencionado, vela por preservar la confidencialidad,integridad y disponibilidad de los activos de información que son accedidos o se encuentrana cargo de los funcionarios o contratistas debido a su cargo y/o responsabilidades. Por tal motivo, ha establecido controles que permitan regular el acceso a las redes, datos e información, así como la implementación de perímetros de seguridad para la protección de las instalaciones, especialmente, aquellas clasificadas como áreas seguras, como los centros de procesamiento de información, áreas de almacenamiento de información física, cuartos de suministro de energía eléctrica, aire acondicionado, entre otras.

El Data Center cuenta con un sistema de control de acceso biométrico (huella dactilar), tarjeta de proximidad y chapa de seguridad. Además, cuenta con una cámara que graba toda actividad al interior del Data Center, sólo personal autorizado por el coordinador del grupo de recursos informáticos ingresa al Data Center.

Todas las puertas que utilicen sistema de control de acceso deberán permanecer cerradas, y es responsabilidad de todos los funcionarios y contratistas evitar que las puertas se dejen abiertas. Las personas que tengan acceso al Datacenter serán definidas única y exclusivamente por el grupo de recursos informáticos.

Los sistemas de información, dispositivos de procesamiento y comunicaciones definidos y autorizados por el grupo de recursos tecnológicos contarán con mecanismos de identificación de usuarios y procedimientos para el control de acceso a los mismos.

Todas las conexiones remotas deberán ser autenticadas y seguras antes de conceder el acceso y el tráfico de datos deberá estar cifrado.

Todas las conexiones habilitadas de acceso remoto, deberán contar con restricción de fecha y hora, teniendo en cuenta las funciones a desarrollar por el funcionario, contratista o tercero autorizado por el grupo de recursos informáticos.

Todos los usuarios tendrán un usuario personal e intransferible, que permitirá los acceso y uso de la información. Todas las acciones realizadas con el usuario asignado serán responsabilidad del funcionario, contratista o tercero a quien se le asignó el usuario.

Al momento de crear una cuenta de acceso a cualquiera de los sistemas de información y dispositivos de red, para contratista o tercero debe tener una fecha de vencimiento especificada, la cual en ningún caso debe superar la fecha de sus obligaciones contractuales.

En los casos en los que el otorgamiento de acceso se lleve a cabo por medio de una asignación de contraseña, se debe consultar la Política de Contraseñas, del presente documento.

Las asignaciones de privilegios en las aplicaciones para las diferentes cuentas de usuario estarán determinadas por el grupo de recursos informáticos, deben revisarse a intervalos regulares y modificar o reasignar estos cuando se presenten cambios en el perfil del

usuario, ya sea por promociones, ascensos, traslados, cambios de cargo o terminación de la relación laboral.

Los propietarios de los activos de información periódicamente propenderán por la verificación de los niveles de acceso (o también llamados niveles de privilegios) asignados a los usuarios, para garantizar que sean apropiados de acuerdo con el propósito institucional y se conserve la separación de funciones.

A la red Wifi de SOYUTEISTA, se permite el acceso sin restricción, de conexión y está habilitada para que cualquier dispositivo con la capacidad tecnológica pueda navegar y establecer comunicación. El acceso solo estará permitido.

A la red Wifi de UTSCONCORAZON, el acceso está restringido a personal autorizado por el grupo de recursos informáticos, quienes, con la información suministrada por el Área de Talento Humano, brindará o denegará el acceso a los funcionarios, contratistas y terceros a la información o sistemas de información que son accedidos a través de dispositivos móviles.

Las UTS establecerá controles para restringir accesos a áreas seguras, entre otros, deberá registrar los sistemas, datos de identificación de la persona que accede a la información, el motivo de ingreso, el tiempo empleado para el desarrollo de la actividad y, asimismo, cuidará que un responsable del activo de información acompañe a la persona durante su instancia en el área.

Todos los formularios de los sistemas de información que para su acceso requieran credenciales, deberán incorporan herramientas que no permitan el autocompletado.

El otorgamiento de un determinado nivel de acceso a un usuario o aplicativo en un sistema de información debe ser autorizado previamente por el líder del proceso, grupo de talento humano o el dueño de la información del sistema de información, siempre partiendo del concepto de que se debe autorizar el mínimo nivel de privilegios necesarios para la realización de las funciones del usuario o el funcionamiento del aplicativo.

Se debe verificar y retirar las cuentas redundantes de usuarios.

Antes de instalar en la plataforma tecnológica de las UTS dispositivos de red y activos de información, se le debe cambiar usuario y clave por defecto al igual que a los sistemas de información y base de datos.

7.6.1 CONTRASEÑAS SEGURAS

Las contraseñas de usuario son de carácter confidencial, personal e intransferible.

Por defecto debe existir una obligatoriedad para el cambio inmediato en el primer uso de contraseñas de usuario en las nuevas cuentas de la institución, o en proceso de restablecimiento de contraseñas.

Las Unidades Tecnológicas de Santander, establecerá mecanismos que permitan que los usuarios de los diferentes sistemas de información de la plataforma tecnológica cambien contraseña de acceso a los mismos.

Los mensajes de error generado por los sistemas de información, no deben revelar información sensible como: tecnología usada, excepciones o parámetros que dispararon el error específico, entre otros. El mensaje de error debe ser genérico.

Después de seis intentos fallidos de inicio de sesión por error de contraseña, el sistema de información o plataforma tecnológica bloqueará al usuario, para lo cual sólo el grupo de recursos informáticos habilitará nuevamente el acceso.

Se debe habilitar el registro de auditoría de identificación de ingresos fallidos y exitosos a los diferentes sistemas de información y plataforma tecnológica.

No se deben mostrar contraseñas en pantalla en el momento del ingreso, se debenutilizar caracteres de ofuscación.

Las contraseñas se deben distribuir de forma segura, nunca mediante sistemas de transporte no cifrado (texto claro).

Las solicitudes de cambio de contraseña deben ser realizadas personalmente por el propietario de la cuenta, mediante los canales habilitados para tal fin, el grupo de recursos informáticos verificará que el peticionario sea el dueño de la cuenta solicitada.

Los usuarios no deben mantener registros de las contraseñas (hojas de papel, archivos de software, etc.), a menos de que sea un método de almacenamiento seguro para tal fin, que no represente riesgo ni exponga las contraseñas almacenadas.

Los usuarios deben cambiar la contraseña siempre que haya indicio de puesta en peligro del sistema o a intervalos regulares, evitando la reutilización decontraseñas antiguas.

Los usuarios deben evitar usar la misma contraseña para diferentes sistemas de la plataforma tecnológica.

Los usuarios deben seleccionar contraseñas con un mínimo de 8 caracteres conlas siguientes características:

a. Que contenga mayúsculas.
b. Que contenga minúsculas.
c. Que contenga números.
d. Que contenga caracteres especiales (#$%@/).
e. Que no tengan relación con el nombre propio, familiares, cargo de trabajo,etc.
f. No se deben usar secuencias de números ni caracteres, por ejemplo “1234”, “abcd” o “7777”.

No se deben compartir las contraseñas con ningún usuario ni personal de soporte.

No se deben usar las mismas contraseñas para propósitos institucionales y para propósitos personales.

Los sistemas de la plataforma tecnológica deben obligar al cambio de contraseña mínimo cada 90 días, la cual debe cumplir con todos los requerimientos de la presente política.

Se debe permitir a los usuarios la selección y el cambio de sus contraseñas, en elmomento que se requiera.

La directiva de contraseñas implementada no deberá permitir que los usuariosreutilicen alguna de las cinco (5) contraseñas previas utilizadas por los mismos.

El usuario debe notificar oportunamente cualquier incidente de seguridad relacionado con sus contraseñas: pérdida, robo o indicio de pérdida de confidencialidad.

Las contraseñas de acceso a los sistemas de información, datos y servicios de la organización deben ser protegidas por medio de técnicas de cifrado.

7.6.2 CONTROL DE ACCESO A CÓDIGO FUENTE DE PROGRAMA

El control de acceso al código fuente de los programas y/o aplicaciones, debe ser restringido solo al personal autorizado.

Es responsabilidad de los administradores de sistemas de información, otorgar los accesos necesarios a los códigos fuente de cada uno de los proyectos.

El grupo de recursos informáticos deberá tener acceso restringido a librerías de las fuentes de los programas.

Se deberá mantener y copiar las librerías de fuentes de programa a través de procedimientos estrictos de control de cambios.

7.7 POLÍTICAS SOBRE USO DE CONTROLES CRIPTOGRÁFICOS

El grupo de recursos informáticos, con el apoyo del Oficial de Seguridad de la Información, serán los encargados de definir los mecanismos de cifrado de información más apropiados frente alas necesidades de las UTS en relación a los sistemas de información, bases de datos, controles de acceso entre otros, con base en el análisis de riesgos y considerando los criterios de confidencialidad, integridad, autenticidad y no repudio en las comunicaciones o en el tratamiento de la información. El uso de herramientas de cifrado será autorizado conforme a los roles o responsabilidades de los funcionarios y contratistas de las UTS.

Para establecer el sistema de cifrado, los responsables tendrán en cuenta la normatividad colombiana vigente frente a la protección de los datos, estándares aplicables y la tecnología existente, primando las necesidades institucionales. Así mismo, serán los encargados de realizar la respectiva creación, activación, distribución y revocación de las llaves criptográficas a los usuarios autorizados y velarán porque la llavese encuentre activa en el período de tiempo previsto.

Toda trasmisión por redes públicas, inclusive los accesos remotos, se deben configurar para que la comunicación de la información no viaje en texto claro, se deben habilitar herramientas de encriptación de la misma.

La información que de acuerdo a la normatividad sea catalogada como de carácter sensible se debe cifrar para evitar afectar la integridad, disponibilidad y confidencialidad de la misma.

Garantizar conexiones seguras a través de uso de certificados, SSL (HTTPS para la confianza de usuarios) y cifrado en la estructura de las peticiones para portales transaccionales con protocolos TLS 1.1 o superior y algoritmos de cifrado SHA2, para evitar la manipulación de parámetros en las peticiones.

La solicitud de acceso o actualización al sistema o llaves de cifrado se debe efectuar de manera formal de acuerdo con los procedimientos establecidos para tal fin, en la medida en que las actividades laborales así lo demanden. Aquellas personas autorizadas deberán velar por la conservación de la disponibilidad, integridad y confidencialidad de las llaves, así como de la información a la cual se le haya aplicado algún proceso de cifrado. De igual modo, la información cifrada o descifrada deberá ser tratada conforme a su nivel de clasificación y su eliminación deberá realizarse a través de borrado seguro.

Los responsables del sistema de cifrado y de las llaves criptográficas serán los encargados de establecer los controles para asegurar el sistema y las llaves, así como gestionar el acceso sólo a los funcionarios, contratistas y terceros autorizados.

Las UTS deberá establecer mecanismos de control y gestión para la creación, activación, distribución, recuperación y revocación de las llaves criptográficas.

Las actividades relacionadas con la administración y eliminación de las llaves criptográficas deberán ser registradas por la persona encargada. Las llaves serán deshabilitadas cuando estas tengan riesgo de divulgación o cuando los funcionarios, contratistas y terceros autorizados culminen la relación laboral o contractual con las UTS.

Los funcionarios, contratistas y terceros tendrán la responsabilidad de reportar, mediante los canales autorizados, las fallas reales o potenciales y los posibles riesgos del sistema de cifrado.

7.7.1 GESTIÓN DE CLAVES CRIPTOGRÁFICAS

En caso de que aplique, el grupo de recursos informáticos será la encargada de dar los lineamientos asociadas a los algoritmos de cifrado a utilizar.

La contraseña de cifrado deberá cumplir con la Política de sistema de gestión de contraseña.

7.8 SEGURIDAD FÍSICA Y DEL ENTORNO

En donde sea aplicable la Institución deberá construir barreras físicas para impedir el acceso físico no autorizado.

Se deberán implementar medidas de protección con vigilancia que permitan controlar el acceso a las instalaciones de la Institución.

Las instalaciones de procesamiento de información de la Institución deberán estar debidamente separadas físicamente.

Las instalaciones de las UTS deben estar dotadas de un circuito cerrado de TV con el fin de monitorear y registrar las actividades de funcionarios, contratistas, visitantes y comunidad académica en general.

Los sitios de trabajo de los funcionarios, contratistas o terceros de las UTS, deben con controles de acceso mínimos y se deben localizar en lugares donde no queden expuestos al acceso de personas externas o no autorizadas.

7.8.1 SEGURIDAD CENTRO DE DATOS

El Datacenter debe estar ubicado en un lugar alejado de áreas que contengan líquidos inflamables o presenten alto riesgo de incendio. No puede estar ubicado cerca de un sótano o en un último piso.

Los gabinetes y puertas de los equipos que se encuentran en el Datacenter deben permanecer cerrados, siempre y cuando se garanticen los niveles de temperatura y humedad requeridos por la infraestructura de cómputo allí instalada.

No se debe enchufar, ni desenchufar ningún cable eléctrico, de datos o voz sin autorización y supervisión de algún responsable del Datacenter.

Los niveles de temperatura y humedad relativa en el Datacenter deben ser mantenidos dentro de los límites requeridos por la infraestructura de cómputo que en éste se resguardan.

Las credenciales de autenticación que vienen por defecto en los sistemas o software (dispositivos de red, sistemas operativos, cámaras, DVR), deben ser cambiados antes de ponerlos en un ambiente de producción.

El grupo de recursos informáticos debe realizar el control de la programación de los mantenimientos preventivos y pruebas de funcionalidad del sistema de UPS, Switch y servidores. Los mantenimientos deberán realizarse al menos dos veces por año.

La asignación de espacio, ubicación, movimiento y demás requerimientos físicos para la infraestructura de cómputo instalada en el Datacenter debe ser autorizada por el coordinador del grupo de recursos informáticos.

Debe existir un sistema de detección y prevención de incendios en el Datacenter, que minimice el impacto que puede generar la ocurrencia de un evento o situación de incendio en el lugar.

7.8.2 ACCESO FÍSICO AL CENTRO DE DATOS

Las puertas de acceso al Datacenter deben permanecer cerradas y aseguradas, siempre y cuando se garanticen los niveles de temperatura y humedad requeridos por la infraestructura de cómputo allí instalada.

Únicamente se permite el ingreso de manera regular al Datacenter al personal autorizado por el coordinador del grupo de recursos informáticos.

De ser necesario el ingreso de algún visitante al Datacenter, podrá realizarse siempre y cuando sea para actividades que no afecten o modifiquen el correcto funcionamiento de la infraestructura instalada. Durante la visita deberá estar siempre acompañado y bajo la supervisión del responsable del Datacenter o autorizado por el coordinador del grupo de recursos informáticos.

Los registros de ingreso al Datacenter deben ser auditados con frecuencia para identificar accesos no autorizados y confirmar que los controles de acceso definidos son efectivos.

7.8.3 PROTECCIÓN CONTRA AMENAZAS AMBIENTALES ARCHIVO

Se debe asegurar que en las instalaciones de la institución se cuente con un equipamiento apropiado de seguridad: sistemas de extinción de incendios; salidas de emergencia, cableado, etc.

El consumo de cigarrillo, o de sustancias que pueden afectar la integridad y correcto funcionamiento de los activos de información está restringido en las áreas internas.

7.8.4 EQUIPOS DE CÓMPUTO

En horario laboral, cuando el usuario no esté haciendo uso del equipo de cómputo, el mismo deberá estar bloqueado, en horario no laboral deberá permanecer apagado siempre y cuando no se esté procesando información.

Los equipos de cómputo deben ser usados apropiadamente, velando por el buen estado de cada uno de sus componentes.

Para el uso de los equipos de cómputo debe existir un responsable de estos.

La plataforma tecnológica (Hardware, software y comunicaciones) debe contar con las medidas de protección física y eléctrica, con el fin de evitar daños, fraudes, interceptación de la información o accesos no autorizados.

Los equipos dispuestos para las tareas de impresión solamente deberán utilizados para imprimir documentos institucionales.

Todas las actividades de mantenimiento y reparación de los equipos de impresión deberán ser realizadas únicamente por el grupo de recursos informáticos o personal autorizado por este.

Los usuarios no deberán realizar acciones que afecten el normal funcionamiento de los equipos de impresión.

Equipos como impresoras, fotocopiadoras deben estar en áreas definidas como seguras, esto aplica también para equipos de comunicaciones como Switch, enrutadores, firewalls entre otros.

No dejar documentos impresos abandonados con información que contengan datos personales sensibles en las impresoras o en lugares sin acceso restringido.

7.8.5 SUMINISTRO ELÉCTRICO

Todos los equipos de cómputo estarán conectados a la red de energía regulada, con respaldo de UPS para evitar deterioros por posibles fallas eléctricas.

Las impresoras y fotocopiadoras estarán conectados a energía regulada sin respaldo de UPS, para evitar deterioros por posibles fallas eléctricas

Se deberá disponer de un Sistema de Energía interrumpible como UPS, para asegurar el Apagado Regulado y Sistemático de los Equipos de TI de la Institución, asegurando la continuidad de las operaciones mientras se restablece las fallas de suministro de energía eléctrica.

Se deberá contar un sistema de respaldo eléctrico (planta eléctrica) que garantice la continuidad del fluido eléctrico cuando el servicio del proveedor no esté disponible.

7.8.6 CABLEADO ESTRUCTURADO

Deben existir planos de ubicación física y de conectividad de los equipos de cómputo.

Los canales de energía eléctrica deberán estar separadas de la estructura cableada de comunicaciones.

Se deberá realizar el proceso de certificación del cableado, garantizando la calidad de sus componentes y su instalación.

7.8.7 POLÍTICA DE MANTENIMIENTO DE EQUIPOS DE TI

CONTRATISTAS

Tomar las medidas necesarias para proteger la información alojada en los activos, suscribiendo las cláusulas de protección de datos personales para encargados del tratamiento.

Tomar en los casos que aplique respaldos de la información, sistemas operativos y demás con medidas de protección de datos personales de manera que no se vea afectada la continuidad del servicio.

Asignar el personal adecuado para que realice los trabajos de acuerdo a la programación de mantenimiento preventivo y a las solicitudes realizadas por las dependencias

Informar a la coordinación del grupo de recursos informáticos cualquier inconveniente presentado durante la ejecución de los trabajos o sugerencias, observaciones o propuestas de mejora que tenga al respecto.

Ejecutar óptima y oportunamente los servicios de mantenimiento asignados

GENERALES

Elaborar el plan de mantenimientos de la plataforma tecnológica y socializarlos con los interesados.

Deberá llevarse registro de los mantenimientos preventivos y correctivos de los equipos informáticos, mediante los formatos establecidos, señalando fecha, información del equipo, responsable del mantenimiento, entre otros campos.

Para los mantenimientos preventivos físicos:

a. Informar previamente la fecha de ejecución del mantenimiento, a las dependencias responsables de los correspondientes activos.
b. Evitar destapar físicamente equipos con garantía vigente.
c. Verificar y registrar el funcionamiento del equipo, antes de realizar el mantenimiento.
d. Verificar que las especificaciones del equipo coincidan con las del inventario.
e. El equipo debe ser destapado y limpiado con compresora de aire, así mismo deberán limpiarse los contactos de los componentes electrónicos.
f. Después de realizado el mantenimiento, verificar el funcionamiento del equipo de cómputo.

Para los mantenimientos correctivos:

a. Previo al mantenimiento correctivo, se debe verificar junto con el responsable, los inconvenientes que presenta el equipo.
b. Identificar y verificar las partes afectadas, si hay existencias cambiarlas, de lo contrario se debe hacer una solicitud de repuesto.
c. Instalar el repuesto y realizar las pruebas necesarias
d. El equipo debe ser entregado al responsable, verificando previamente su funcionamiento.

Para los mantenimientos lógicos (cuando se detecten fallas en el software):

a. Generar una copia de seguridad de la información, bases de datos, sistema operativo y licencias de software, según se establezca en el procedimiento de Gestión de Copias de Respaldo.
b. Al terminar debe verificarse el funcionamiento correcto del sistema operativo del equipo.
c. Solo se deben restaurar la información cuando el mantenimiento sea satisfactorio.

7.8.8 POLÍTICA DE ESCRITORIO DESPEJADO Y PANTALLA LIMPIA OBJETIVO

Para lograr un adecuado aseguramiento de la información, los funcionarios, contratistas y terceros las UTS deberán adoptar buenas prácticas para el manejo y administración de la información física y electrónica que se encuentra a su cargo, conforme a su clasificación, con el fin de evitar que personas no autorizadas accedan a dicha información. Para ello, los funcionarios, contratistas y terceros deberán tener presente:

- Almacenar de forma segura documentos y elementos de almacenamiento externos (CD, DVD, USB, etc.) conforme los niveles de clasificación de la información, para evitar accesos no autorizados, pérdida o daño de la información en la jornada laboral o fuera de ella.
- Durante los lapsos en los que se deja desatendidas las estaciones de trabajo, se tendrá cuidado con bloquear la sesión del equipo para evitar que terceros no autorizados accedan a la información contenida en el computador. Así mismo, se generarán los controles adecuados con la información que reposa sobre el lugar de trabajo.
- Al imprimir información reservada o pública clasificada, los documentos deberán ser retirados de forma inmediata para evitar divulgación no autorizada de la información.
- Los archivos que contengan información sensible o confidencial deberán ser almacenados en rutas que impidan el fácil acceso por terceros, evitando, por ejemplo, guardarlos en el área de escritorio de la pantalla del computador.
- Los funcionarios y contratistas deberán asegurar que sus escritorios se encuentren libres de los documentos que son utilizados durante el desarrollo de sus funciones al terminar la jornada laboral y que estos sean almacenados bajo las protecciones de seguridad adecuadas.

El grupo de recursos informáticos, con el apoyo del Oficial de Seguridad, será la encargada de establecer controles de bloqueo sobre las sesiones de los usuarios para que el equipo se bloquee enun lapso determinado.

Los funcionarios, contratistas y terceros que tengan dentro de sus funciones la atención al público, deberán almacenar los documentos y dispositivos de almacenamiento bajo llave y ubicar el equipo de cómputo de tal forma que se evite el acceso o revisión de la información por parte de los visitantes no autorizados.

En las áreas donde se encuentren activos informáticos, se debe cumplir como mínimo con los siguientes lineamientos no se deben consumir alimentos ni bebidas.

7.9 POLÍTICA DE RESPALDO DE INFORMACIÓN

La información requerida para el cumplimiento de las actividades misionales y los objetivos estratégicos las UTS deberá ser respaldada conforme a los lineamientos legales, técnicos, requisitos de las tablas de retención documental, la gestión de riesgos, así como a los niveles de clasificación de la información. Los tiempos de preservación de las copias de respaldo serán definidos teniendo en cuenta los requerimientos anteriormente expuestos, así como también la tecnología requerida para la restauración de la información contenida.

Cuando se presente un cambio de equipo o desvinculación informada previamente por el área de talento humano o dependencia autorizada, el grupo de recursos informáticos en

cabeza de funcionario/contratista autorizado por el coordinador generará la copia de seguridad de la información institucional almacenada en el equipo.

Al momento de generarse una nueva versión de un aplicativo sea desarrollado por la institución o adquirido a un tercero, antes de implementarse en la plataforma tecnológica, se debe generar una copia de seguridad del aplicativo y su base de datos completa si aplica.

La periodicidad y el tipo de copias de seguridad de las bases de datos, se debe definir de acuerdo a la criticidad, tecnología, tamaño e importancia, criterios que debe definir el grupo de recursos informáticos.

Toda copia de seguridad independiente del tipo, tamaño, si es sistema operativo, aplicativo, base de datos, se debe guardar en disco duro y dispositivo diferente al que contiene el origen de la información, se debe procurar respaldar la información en una ubicación física diferente.

Se creará una carpeta compartida para que funcionarios autorizados almacenen allí información institucional de su gestión, la periodicidad será dada por el funcionario quien en pleno conocimiento de su función clasificarán la información.

El grupo de recursos informáticos generará una copia semestral de la información de los usuarios que hayan dejado copia en la carpeta compartida.

Es responsabilidad de los usuarios que no están dentro de la red dominio o por fuera de la institucional, realizar la copia de seguridad de la información que dentro del desarrollo de su función institucional se genere, este indicará la periodicidad que de acuerdo a la importancia y relevancia de la información se clasifique.

Las UTS dispondrán de recursos físicos y tecnológicos para generar las copias de instaladores de software, licencias/claves y lenguajes de programación, bases de datos completas, recursos que se utilizan en la gestión institucional de la institución, su ubicación se ajustará a lo indicado en la presente política.

Las copias de respaldo se almacenarán de forma segura para garantizar que no sea manipulada por personas no autorizadas. A su vez, se deberán registrar todas las actividades desarrolladas frente al tratamiento y manipulación de las copias de respaldo para asegurar la trazabilidad de estas.

El responsable de las copias de respaldo deberá realizar las respectivas pruebas de restauración conforme a los propósitos para las cuales han sido recaudadas.

Las copias de respaldo deberán ser almacenadas en lugares que tengan los debidos controles de seguridad físicos y tecnológicos, que permitan limitar el acceso sólo a las personas autorizadas y garanticen la disponibilidad de la información.

Al cumplir el ciclo de vida útil de los medios de almacenamiento de las copias de respaldo deberán ser destruidos o eliminados de forma segura, evitando la recuperación de la información contenida y acceso por personas no autorizadas.

Los funcionarios, contratistas y terceros responsables de la infraestructura, sistemas de información y Bases de datos requeridos para la operación de las UTS, deberán generar las respectivas copias de respaldo, estableciendo la periodicidad, tipo de almacenamiento y registrando la información según lo establecido dentro de la presente política.

El(Los) encargado(s) de las copias de respaldo deben velar porque la información sea almacenada conforme a los lineamientos establecidos, de forma controlada y conforme a las necesidades de las UTS. Así mismo deberán realizar una prueba periódica de las copias con el fin validar el correcto funcionamiento y la efectiva restauración.

Los responsables de la información serán los encargados de velar porque las copias de respaldo se realicen de acuerdo con lo establecido y que las estrategias utilizadas se ajusten a las necesidades y requerimientos de las UTS.

7.10 POLÍTICA DE SEGURIDAD EN LAS COMUNICACIONES

Se implementarán controles para garantizar la seguridad de los datos y los servicios conectados en las redes, contra el acceso no autorizado, considerando la ejecución de las siguientes acciones:

a. Establecer los procedimientos para la administración de los equipos servidores, incluyendo los equipos en las áreas de usuarios.
b. Establecer controles especiales para salvaguardar la confidencialidad e integridad del procesamiento de los datos que pasan a través de Internet, y para proteger los sistemas conectados.
c. Implementar controles especiales para mantener la disponibilidad de los servicios de red y computadores conectados.
d. Garantizar mediante actividades de supervisión, que los controles se aplican uniformemente en toda la infraestructura de procesamiento de información.
e. Mantener instalados y habilitados sólo aquellos servicios y puertos que sean utilizados por los sistemas de información y software de la institución.
f. La infraestructura la institución estará separada por VLANs para garantizar la confidencialidad de los datos que se trasmitan.

Para controlar la seguridad en redes extensas, se podrán dividir en dominios lógicos separados y VLANs. Para esto se definirán y documentarán los perímetros de seguridad que sean convenientes, para filtrar el tráfico entre los dominios y para bloquear el acceso no autorizado.

El Grupo de Recursos Informáticos es el responsable de administrar y gestionar la red de las Unidades Tecnológicas de Santander.

El Grupo de Recursos Informáticos es el responsable de establecer los controles lógicos para el acceso a los diferentes recursos informáticos, con el fin de mantener los niveles de seguridad apropiados.

Las UTS proporciona a los funcionarios, contratistas y terceros todos los recursos tecnológicos de conectividad necesarios para que puedan desempeñar las funciones y actividades laborales en el desarrollo de su gestión, por lo cual no es permitido conectar a

las estaciones de trabajo o a los puntos de acceso de la red institucional, elementos de red (tales como Switch, enrutadores, módems, firewall, etc.) que no sean autorizados por el Grupo de Recursos Informáticos.

Los funcionarios, contratistas y terceros que realicen conexión desde las diferentes redes de la institución no deben ingresar a páginas de temas pornográficos, con contenido que vulnere la integridad de los colaboradores o represente riesgos a los activos de información institucionales.

El acceso a internet desde las redes y subredes diferentes a las de acceso público se debe hacer desde un host debidamente registrado o autorizado.

El acceso a la red por parte de terceros deberá ser gestionado a través de los canales dispuestos y autorizado por el grupo de recursos informáticos, lo cual deberá ser solicitado por el competente.

El Grupo de Recursos Informáticos a través del área de redes generará subredes en la infraestructura de telecomunicación, con el fin de controlar el acceso a los diferentes segmentos de red y garantizar la confidencialidad, integridad y disponibilidad de la información, las subredes estarán divididas de acuerdo a su función y contarán con la protección en el borde de red de un firewall con funciones de IDS e IPS, las directivas de configuración y administración serán definidas por el coordinador del grupo de recursos informáticos.

Por defecto las reglas en el firewall para acceder a la red desde puntos externos están deshabilitadas, se permitirá acceso restringido a aplicaciones y redes de acuerdo a necesidad propias de la Institución, estas deben estar autorizadas por el coordinador del grupo de recursos informáticos y se deben establecer herramientas para controlar, registrar y supervisar la conexión.

Se deben establecer parámetros técnicos para la conexión segura de la red con los servicios de red.

Se deben establecer mecanismos de autenticación seguros para el acceso a la red.

Se deben separar las redes inalámbricas de las redes internas, para garantizar los principios de la seguridad de la información.

7.11 POLÍTICA DE TRANSFERENCIA DE INFORMACIÓN

En la medida de lo posible, el intercambio de información entre entidades y/o organizaciones se deberá realizar a través de los protocolos de interoperabilidad, en todo caso, la transmisión de la información perteneciente a las UTS se deberá controlar según los niveles de clasificación de la información establecidos y las políticas de seguridad de las UTS. En caso de que se requiera intercambiar información sensible o confidencial, se deberán adoptar controles de cifrado de información de acuerdo con lo establecido en la política descrita en el presente documento.

Los intercambios de información sensible o confidencial, con otras instituciones o partes interesadas externas deberán ser justificados cuando así se requiera. El uso de la información transmitida o intercambiada deberá realizarse exclusivamente para los fines pactados, en todo caso se deberá tratar como información confidencial y no podrá ser compartida con terceros no autorizados siguiendo los lineamientos de la política de protección de datos personales.

La transmisión de la información se desarrollará teniendo en cuenta la normatividad colombiana vigente, especialmente la relativa a la Ley de Habeas Data (Ley 1266 de 2008), la Ley de Protección de Datos Personales (Ley 1581 de 2012 y decretos reglamentarios) y Ley de Transparencia (Ley 1712 de 2014).

La información deberá protegerse de divulgación no autorizada conforme a los Procedimientos de Clasificación de la Información definidos en las UTS, así como a los mecanismos y controles establecidos para el tratamiento de la información.

Para el intercambio de información se deberán definir las responsabilidades y procedimientos para la transferencia segura de la información, el responsable y proceso a seguir en caso de presentarse un incidente de seguridad, los niveles de clasificación de la información a ser intercambiada.

7.12 POLÍTICA DE DESARROLLO DE SOFTWARE

Para el desarrollo de software dentro de las Unidades Tecnológicas de Santander se deberá realizar un proceso de planeación en donde se determine la respectiva metodología a utilizar; las etapas de desarrollo; la estructura de desglose de trabajo, con sus respectivos responsables, criterios de aceptación y las pruebas de funcionalidad y seguridad teniendo en cuenta los requerimientos y el cumplimiento de los objetivos estratégicos de las UTS.

La identificación de las necesidades y requisitos de funcionalidad, calidad y seguridad se realizará entre el área solicitante y el grupo de Recursos Informáticos, y los mismos deberán ser validados durante el proceso de aprobación del desarrollo de software.

Para el desarrollo y puesta de producción del software, se deberán tener presente tres ambientes separados así: i) de desarrollo (puede ser en los equipos asignados a los colaboradores), ii) de pruebas y iii) de producción, evitando así las alteraciones o modificaciones no autorizadas del código fuente.

Los cambios requeridos sobre el software de las UTS se llevarán a cabo a través del Procedimiento de Control de Cambios, el cual permite que se documenten y establezcan los requerimientos y los niveles de aceptación del cambio. Dentro de los requerimientos que se establezcan será necesario analizar los riesgos asociados a la seguridad de la información y la identificación de los controles a implementar para su aseguramiento.

Se establecerán acuerdos en procesos de desarrollo que establezcan con claridad la propiedad de las licencias y derechos intelectuales de los códigos fuentes, así como sus condiciones de usabilidad.

Para el caso que se considere la tercerización del desarrollo de software, se establecerán acciones que contemplen los siguientes puntos:

a. Acuerdos de licencias, propiedad de código y derechos conferidos (Derechos de Propiedad Intelectual).
b. Requerimientos contractuales con respecto a la calidad del código y la existencia de garantías.
c. Procedimientos de certificación de la calidad y precisión del trabajo llevado a cabo por el proveedor, que incluyan auditorías, revisión de código para detectar código malicioso, verificación del cumplimiento de los requerimientos de seguridad del software establecidos, etc.

Antes de iniciar el desarrollo de software, el grupo de recursos informáticos y las áreas de las UTS implicadas deberán acordar una metodología; una estructura de trabajo, con los respectivos responsables; así como el cronograma de desarrollo, determinando el alcance, los procesos afectados y los requerimientos.

El área solicitante validará los criterios de aceptación correspondientes a la funcionalidad y calidad para dar la aceptación formal del desarrollo de software.

El grupo de recursos informáticos en apoyo del Oficial de Seguridad validará los criterios de aceptación técnicos: interoperabilidad, buenas prácticas de programación y seguridad, para dar la aceptación formal del desarrollo de software. La aceptación de los criterios estará determinada por los resultados de las pruebas planteadas, las cuales tendrán dentro de sus objetivos detectar, entre otras vulnerabilidades, los códigos maliciosos, las puertas traseras, etc.

Los datos de pruebas con los que se llevarán a cabo las pruebas del software no deben utilizar datos reales de producción.

En el desarrollo de software es necesario establecer controles que permitan conservar la seguridad y privacidad de la información; por lo tanto, es importante tener en cuenta los mecanismos de acceso a la información, autenticación, detección de intrusos, cifrado de datos, salvaguarda de confidencialidad, integridad, disponibilidad y protección de los datos personales.

La metodología de desarrollo de software debe contemplar una etapa de gestión de riesgos.

El grupo de recursos informáticos deberá llevar a cabo revisiones periódicas a los desarrollos realizados, con el propósito de garantizar que se estén desplegando los controles conforme a lo establecido dentro de la fase de planeación.

En el desarrollo de software se llevará a cabo un control de versiones con los respectivos documentos de soporte, con el objeto de verificar el buen funcionamiento del software y el respectivo control de su ciclo de vida.

7.13 POLÍTICA PARA RELACIONES CON PROVEEDORES

Cuando se requiera otorgar acceso a los activos de información a los proveedores de las UTS, el responsable del activo, con apoyo del Oficial de seguridad, deberá realizar un análisis de riesgos con el fin de determinar los controles de seguridad que preserven la confidencialidad, disponibilidad e integridad, así como la finalidad del uso de los datos y el respectivo consentimiento en los casos que aplique conforme a los procedimientos legales y administrativos.

Antes de conceder los permisos de acceso se determinarán por parte del responsable del activo: las necesidades del acceso, el acceso requerido (físico o lógico), el nivel de clasificación de la información a acceder, la finalidad de uso, los controles mínimos para tener en cuenta frente al tratamiento de la información y el manejo de incidentes de seguridad de la información. En ningún caso se otorgará acceso a la información, sistemas de información o áreas seguras de las UTS a proveedores, hasta no haber realizado la adecuada gestión de los riesgos, formalizado la relación contractual.

Dentro de los acuerdos, contratos o convenios formalmente firmados entre las partes se deberán definir claramente los requerimientos de seguridad y privacidad controles a tener en cuenta antes, durante y después del tratamiento de los datos por parte del proveedor, con el respectivo consentimiento por parte de los titulares en los casos que aplique; así como las responsabilidades de las partes conforme a los lineamientos de las UTS y a la legislación vigente.

Siempre que se otorgue acceso a la información de las UTS a terceros, se establecerán acuerdos de confidencialidad que tengan como principio el cumplimiento de las políticas de seguridad de la información de las UTS y cláusulas requeridas para proteger la información a acceder.

Todos los funcionarios, contratistas y proveedores que tengan acceso a la información deberán cumplir con las políticas de seguridad y privacidad de la información, así mismo, en caso de que identifiquen una amenaza que pueda llegar a vulnerar la información, deberán reportarla a través de los conductos establecidos.

El responsable del activo de información no permitirá el acceso a la información hasta no tener firmados y formalizados, por medio de un contrato o acuerdo con los proveedores, los fines de uso, condiciones de tratamiento, así como la debida implementación de los controles requeridos para preservar las características de confidencialidad, integridad y disponibilidad de la información.

Antes de brindar acceso a los activos de información, los proveedores deben aceptar formalmente el cumplimiento de las políticas de seguridad y privacidad de la información de las UTS.

7.14 GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN

El grupo de Recursos Informáticos, aplicará el procedimiento para gestionar el tratamiento de las situaciones de seguridad de la información “Procedimiento de Gestión de Incidentes de Seguridad de la Información”, con el fin de mitigar el impacto y disminuir la probabilidad de ocurrencia de incidentes futuros de seguridad de la información.

Se deberá designar un responsable para responder los incidentes de seguridad de la información, definiendo los tipos de responsabilidades.

Los funcionarios y contratistas de la institución deberán reportar los eventos y debilidades de seguridad de la información, tan pronto como sea posible al área encargada.

Una vez se reciba el incidente se deberá clasificar cada evento de seguridad de la información usando la escala de clasificación.

Se deberá priorizar el incidente, lo que puede ayudar a identificar el impacto del incidente y la urgencia.

Cuando el incidente se resuelva se deberá notificar al usuario sobre el incidente cerrado.

Se deberá definir y aplicar procedimientos para la identificación y recolección de información que pueda servir como evidencia; teniendo en cuenta:

- Evidencia de la incidencia.
- Cadena de Custodia.
- Escalar a las instancias superiores.
- Tratar las debilidades que ocasionan el incidente de seguridad de la Información.
- Competencia del personal.
- Roles y Responsabilidades.
- Registrar y cerrar formalmente el incidente se seguridad de la Información.

7.15 ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO

Se define como requisito de seguridad de la institución, que en situaciones adversas o de interrupción no se debe disminuir el nivel de protección para los activos de información, para lo cual, la institución debe disponer los medios alternos necesarios que permitan cumplir los objetivos de recuperación de TI, sin afectar la confidencialidad o integridad de los activos de información.

Las UTS definirá su estrategia de gestión de la continuidad de TI a partir de las necesidades operativas y misionales asociadas a la razón de ser de la institución.

Se deberá proporcionar los recursos suficientes para dar una respuesta efectiva de funcionarios, contratistas y procesos en caso de contingencia o eventos catastróficos que se presenten en la institución, y afecten la continuidad de la operación.

El Plan de Continuidad de Servicios TI de la institución debe derivar en la implementación de los controles y medidas pertinentes, para gestionar incidentes de interrupción a la operación.

Se deberá mantener canales de comunicación adecuados hacia los funcionarios, contratistas, proveedores y partes interesadas, con el fin de responder de manera efectiva ante los eventos catastróficos.

Se debe monitorear la efectividad de los controles definidos en el Plan de Continuidad de Servicios TI establecido e implementado, con el fin de identificar oportunidades de mejora al desempeño, buscando siempre el cumplimiento de los objetivos de continuidad de la institución.

7.16 IDENTIFICACIÓN DE LEGISLACIÓN APLICABLE Y REQUISITOS CONTRACTUALES

Se deberá identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables a la institución y relacionados con seguridad de la información.

Los funcionarios y contratistas deberán cumplir con los acuerdos de licenciamiento de software.

Todo el software que se utilice en los equipos de cómputo de la institución debe ser autorizado y debe contar con su respectiva licencia. En ninguna circunstancia, se permite el uso de software que incumpla el tipo de licencia especificada por el fabricante.
Se deberá proteger las creaciones intelectuales de software cuando se realicen con terceros, incluyendo en los contratos la obligación de transferir a la institución los derechos patrimoniales sobre los productos desarrollados.

8 INCUMPLIMIENTO

El incumplimiento de esta Política del Sistema de Gestión de Seguridad de la Información traerá consigo las consecuencias legales que apliquen a la normativa de la Institución, incluyendo lo establecido en las normas que competen al Gobierno Nacional y Territorial en cuanto a seguridad y privacidad de la información se refiere.

9 HISTORIAL DE CAMBIOS

VERSIÓN	DESCRIPCIÓN	NUMERO DE SOLICITUD DE CAMBIO	FECHA
01	Emisión inicial	N/A	Noviembre de 2021
02	Actualización		Noviembre de 2023