MANUAL DE LA POLÍTICA GENERAL DEL MODELO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Control de Cambios

Versión	Fecha	Descripción
1.0	20-09-2011	Versión Inicial
2.0	25-07-2018	Versión corregida

.

Tabla de Contenido

1. INTRODUCCIÓN

La información es un recurso que, como el resto de los activos, tiene valor para la Universidad Surcolombiana que permite el desarrollo continuo de la misión y el cumplimiento del objetivo de la misma, lo cual genera la necesidad de implementar reglas y medidas que permitan proteger la confidencialidad, integridad y disponibilidad en todo el ciclo de vida de la información.

El establecimiento, seguimiento, mejora continua y aplicación de la Política de Seguridad y Privacidad de la Información garantiza un compromiso ineludible de protección a la misma frente a una amplia gama de amenazas y contribuye a minimizar los riesgos asociados a pérdida de información y/o accesos no autorizados a la infraestructura tecnológica y asegurar el eficiente cumplimiento de las funciones sustantivas del ente territorial apoyadas en un correcto sistema de información.

El presente manual describe las políticas de seguridad y privacidad de la información definida por la Universidad Surcolombiana, estas se encuentran enfocadas al cumplimiento de la normatividad legal colombiana vigente y a las buenas prácticas de seguridad de la información, basadas en la norma ISO 27001/2013 y al modelo de seguridad y privacidad de la información de la estrategia Gobierno En Línea (GEL) del Ministerio de Tecnologías de la Información y las Comunicaciones de Colombia

La seguridad de la información es para la Universidad Surcolombiana, una labor prioritaria que exhorta a todos a velar por el cumplimiento de las políticas establecidas en el presente manual.

2. OBJETIVO

Establecer las políticas que regulan la seguridad y privacidad de la información de la Universidad Surcolombiana y presentar en forma clara y coherente los elementos que conforman la política de seguridad y privacidad que deben conocer y cumplir todos los directivos, funcionarios, contratistas, terceros, aprendices, practicantes, docentes, estudiantes y comunidad en general que tengan algún tipo de relación con la Universidad Surcolombiana.

3. ALCANCE

Las Políticas de seguridad y privacidad de la información son aplicables para todos los aspectos administrativos y de control que deben ser cumplidos por los directivos, funcionarios, contratistas, terceros, comunidad estudiantil y en general todos los usuarios de la información que tenga algún tipo de relación con la Universidad Surcolombiana para el cumplimiento de sus funciones y para conseguir un adecuado nivel de protección de las características de calidad y seguridad de la información, aportando con su participación en la toma de medidas preventivas y correctivas, siendo un punto clave para el logro del objetivo y la finalidad del presente manual.

Los usuarios tienen la obligación de dar cumplimiento a las presentes políticas emitidas y aprobadas por el Comité de Seguridad de la Información de la Universidad Surcolombiana.

4. MARCO NORMATIVO

- **Constitución Política de Colombia 1991**. Artículo 15. Reconoce como Derecho Fundamental el Habeas Data.
- **Artículo 20**. Libertad de Información.
- **Decreto 599 de 2000** - Código Penal Colombiano
- **Ley 906 de 2004**, Código de Procedimiento Penal.
- **Ley 87 de 1993**, por la cual se dictan Normas para el ejercicio de control interno en las entidades y organismos del Estado, y demás normas que la modifiquen.
- **Decreto 1599 de 2005**, por el cual se adopta el Modelo Estándar de Control Interno MECI para el Estado Colombiano.
- **Ley 734 de 2002**, del Congreso de la República de Colombia, Código Disciplinario Único.
- **Ley 23 de 1982** de Propiedad Intelectual - Derechos de Autor.
- **Ley 594 de 2000** - Ley General de Archivos.
- **Ley 80 de 1993, Ley 1150 de 2007** y decretos reglamentarios.
- **Ley 527 de 1999**, por la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales y se establecen las entidades de certificación y se dictan otras disposiciones.
- **Directiva presidencial 02 del año 2000**, Presidencia de la República de Colombia, Gobierno en línea.
- **Ley 1032 de 2006**, por el cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales. **Ley 1266 de 2007**, por la cual se dictan disposiciones generales del Habeas Data y se regula el manejo de la información contenida en base de datos personales.
- **Ley 1273 de 2009**, "Delitos Informáticos" protección de la información y los datos.
- **Ley 1437 de 2011**, "Código de procedimiento administrativo y de lo contencioso administrativo".

- **Ley 1581 de 2012**, "Protección de Datos personales".
- **Decreto 2609 de 2012**, por la cual se reglamenta la ley 594 de 200 y ley 1437 de 2011
- **Decreto 1377 de 2013**, por la cual se reglamenta la ley 1581 de 2012
- **Ley 1712 de 2014,** "De transparencia y del derecho de acceso a la información pública nacional"
- **Ley 962 de 2005**. "Simplificación y Racionalización de Trámite. Atributos de seguridad en la Información electrónica de entidades públicas;"
- **Ley 1150 de 2007**. "Seguridad de la información electrónica en contratación en línea"
- **Ley 1341 de 2009**. "Tecnologías de la Información y aplicación de seguridad".
- **Decreto 2952 de 2010**. "Por el cual se reglamentan los artículos 12 y 13 de la Ley 1266 de 2008"
- **Decreto 886 de 2014**. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012"
- **Decreto 1083 de 2015**. "Por el cual se reglamenta el artículo 25 de la Ley 1581 de 2012" • CONPES 3701 de 2011 Lineamientos de Política para Ciberseguridad y Ciberdefensa
- **CONPES 3854 de 2016** Política Nacional de Seguridad digital.

5. REQUISITOS TÉCNICOS

- Norma Técnica Colombiana NTC/ISO 27001:2013 Sistemas de gestión de la seguridad de la información
- Norma Técnica Colombiana NTC/ISO 27002: Buenas prácticas para gestión de la seguridad de la información
- Norma Técnica Colombiana NTC/ISO 17799 Código de práctica para la gestión de la seguridad de la información.
- ISO/IEC 27005 Information technology Systems- Security techniques- information security risk management.
- Modelo Estándar de Control Interno MECI 1000 2da versión "Subsistema:
- Control de Gestión; Componente: Actividades de Control; Elemento: Monitoreo y Revisión e Información"
- Norma Técnica Colombiana NTC - ISO 19011 "Directrices para la Auditoria de los Sistemas de Gestión de la Calidad y/o Ambiental"

6. POLÍTICAS, PROCEDIMIENTOS Y CONTROLES

6.1. Políticas de seguridad y privacidad de la información

6.1.1. Política general de seguridad de la información

La Universidad Surcolombiana, como institución de educación superior de orden nacional, establece que la información es un activo vital para el desarrollo de las actividades misionales, motivo por el cual, está comprometida a proteger los activos de información de la entidad (Empleados, información y entorno laboral), orientando sus esfuerzos a la preservación de la confidencialidad, integridad, disponibilidad, continuidad de las operaciones de gobernabilidad, administración y/o gestión de riesgos, la creación de cultura y conciencia de seguridad en los funcionarios, estudiantes, contratistas, proveedores y personas que hagan uso de los activos de información de la Universidad Surcolombiana, tomando como base que la efectividad de esta política depende finalmente del comportamiento de las personas, (por lo que saben, lo que sienten y de que estén dispuestos a realizar) y los controles establecidos en las políticas de seguridad descritas en el presente documento, fundamentados en la norma técnica colombiana NTC-ISO-27001:2013 y el modelo de seguridad y privacidad de la información.

Las Políticas de seguridad y privacidad de la información, surgen como una herramienta institucional de obligatorio cumplimiento por parte de cada uno de los directivos, funcionarios, estudiantes, contratistas y terceros que presten sus servicios o tengan algún tipo de relación con la Universidad Surcolombiana.

Objetivo**:**
Definir las pautas para asegurar una adecuada protección, seguridad y privacidad de la información de la Universidad Surcolombiana.

Directrices**:**

- Se debe verificar que se definan, implementen, revisen y actualicen las políticas de seguridad y privacidad de la información.
- Se debe establecer un programa que permita el fomento continuo de la creación de cultura y conciencia de seguridad en los funcionarios, estudiantes, contratistas, proveedores, personas, usuarios de los sistemas de información y telecomunicaciones de la Universidad Surcolombiana.
- Todos los usuarios de los sistemas de información y telecomunicaciones de la Universidad Surcolombiana, tienen la responsabilidad y obligación de cumplir con las políticas, normas, procedimientos y buenas prácticas de seguridad de la información establecidas en el presente manual de la política de seguridad y privacidad de la información.
- Diseñar, programar y realizar los programas de auditoría del sistema de gestión

de seguridad de la información, los cuales estarán a cargo de la Oficina de Control Interno.

- Los jefes de área o dependencia deben asegurarse que todos los procedimientos de seguridad y privacidad de la información dentro de su área de responsabilidad, se realizan correctamente para lograr el cumplimiento de las políticas y estándares de seguridad de la información de la Universidad Surcolombiana.
- La Universidad Surcolombiana debe mantener correspondencia y vínculos técnicos entre las normas NTC-IS0 9001:2015 y las normas , NTC-IS0 27001 y NTC-IS0 27002. Se utilizan los requisitos: 7.1.d Compromisos de la dirección y 5.6 Revisión por la dirección del Manual de la Política para la Seguridad de la Información de la Universidad Surcolombiana en intervalos planificados, para asegurar su conveniencia, eficiencia y eficacia continua
- El Comité de Seguridad de la Información de la Universidad Surcolombiana definirá de acuerdo a la clasificación de la información, las directrices necesarias para la implementación de los respectivos controles.

6.1.2. Política de estructura organizacional de seguridad de la información

Objetivo:

Definir el programa de seguridad y privacidad de la información en la Universidad Surcolombiana donde se describan roles y responsabilidades para operación, gestión y administración de seguridad de la información.

Directrices:

- Crear el Comité de Seguridad de la Información de la Universidad Surcolombiana, y asignar el rol de Oficial de seguridad de la información y su equipo de apoyo, junto con los roles, funciones y responsabilidades respectivamente.
- El Centro de Información, Tecnologías y Control Documental debe establecer los roles, funciones y responsabilidades de operación y administración de los sistemas de información de la Universidad Surcolombiana a los funcionarios disponibles en la Universidad Surcolombiana, estos roles, funciones y responsabilidades, deberán estar debidamente documentadas y distribuidas.
- El Comité de Seguridad de la Información de la Universidad Surcolombiana decidirá quién debe tomar contacto con las autoridades para reportar incidentes de seguridad que así lo ameriten.
- La Universidad Surcolombiana, establecerá acuerdos de cooperación de seguridad de información con entidades de seguridad del estado.
- El Oficial de seguridad, asistirá a capacitaciones, conversatorios, conferencias de interés especial en seguridad de la información.
- Los proyectos desarrollados por La Universidad Surcolombiana deberán incorporar dentro de la planeación y desarrollo, el cumplimiento de la política de seguridad y privacidad de la información, valoración de riesgos y los controles a estos.

6.1.3. Política para uso de dispositivos móviles

Objetivo:
Establecer las directrices de uso y manejo de dispositivos móviles (teléfonos móviles, teléfonos inteligentes "smart phones", tabletas), entre otros, suministrados por la entidad y personales que hagan uso de los servicios de información de la Universidad Surcolombiana.

Directrices:

- Los dispositivos móviles (teléfonos móviles, teléfonos inteligentes (smart phones) tabletas, entre otros) suministrados por la Universidad, son una herramienta de trabajo que se deben utilizar únicamente para facilitar las comunicaciones de los usuarios de la entidad.
- Los sistemas de mensajería instantánea para dispositivos móviles institucionales a implementar en la Universidad Surcolombiana debe incluir métodos de cifrado de extremo a extremo de la comunicación.
- Los dispositivos móviles institucionales deben tener únicamente la tarjeta sim asignada por la institución, de igual forma la tarjeta sim únicamente debe instalarse en los equipos asignados por la entidad.
- Es responsabilidad del usuario hacer buen uso del dispositivo suministrado por la Universidad Surcolombiana con el fin de realizar actividades propias de su cargo o funciones asignadas en la entidad.
- Los usuarios no están autorizados a cambiar la configuración, ni a la desinstalación de software de los equipos móviles institucionales posterior a su recibo; únicamente se deben aceptar y aplicar las actualizaciones.
- Los usuarios de dispositivos móviles asignados por la institución, deben evitar hacer uso de estos en lugares con algún riesgo de seguridad, evitando el extravío o hurto del equipo.
- Los usuarios de dispositivos móviles institucionales no deben conectarlos en computadores y/o puertos USB de uso público (Restaurantes, café internet, aeropuertos, etc.).
- Los usuarios de dispositivos móviles institucionales deben mantener desactivados las funciones de redes inalámbricas WiFi, puertos infrarrojos, puerto Bluetooth.

6.1.4. Política de seguridad para los recursos humanos

Objetivo:
Asegurar que los funcionarios, contratistas y demás colaboradores de la Universidad Surcolombiana, entiendan sus responsabilidades y las funciones de sus roles y usuarios, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información y de las instalaciones.

Directrices**:**

- Se debe asegurar que los funcionarios, contratistas y demás colaboradores de la Universidad Surcolombiana, adopten sus responsabilidades en relación con las políticas de seguridad y privacidad de la información y actúen de manera consistente frente a las mismas, con el fin de reducir el riesgo de hurto, fraude, filtraciones o uso inadecuado de la información o los equipos empleados para el tratamiento de la información
- Los aspirantes, estudiantes, funcionarios, contratistas y proveedores deben dar aprobación a la Universidad Surcolombiana para el tratamiento de sus datos personales de acuerdo a la Ley 1581 de 2012 y decretos reglamentarios que dictan disposiciones generales de Habeas Data, propiedad intelectual, y se regula el manejo de la información contenida en base de datos personales.
- El Área de Talento Humano deberá verificar la competencia necesaria de los candidatos o aspirantes a ocupar la vacante disponible al igual que los antecedentes disciplinarios, fiscales y judiciales y demás requisitos definidos en el Manual de Contratación.
- Se debe dar cumplimiento a la normatividad vigente que regula el empleo público, a los Entes Autónomos Universitarios y al Manual Específico de Funciones, Competencias Laborales y Requisitos de los empleos de la Planta de Personal de la Universidad Surcolombiana.
- A la firma del contrato laboral o posesión del cargo el funcionario debe firmar la autorización de tratamiento de datos, el Acuerdo de Confidencialidad y un Acuerdo de cumplimiento las Políticas de Seguridad y Privacidad de la Información para con la Universidad Surcolombiana.
- Se debe capacitar y sensibilizar a los funcionarios durante la inducción sobre las políticas de seguridad y privacidad de la información.
- Los funcionarios de la Universidad Surcolombiana deben cumplir con el Código de Buen Gobierno y Ética.
- En situaciones de incumplimiento y/o violaciones a las políticas de seguridad y privacidad de la información y la de Protección de Datos Personales, se deberá tramitar el cumplimiento de la ley 734 de 2013, Ley 1273 de 2009 y demás normas que reglamenten los procesos disciplinarios para los estudiantes, servidores públicos y contratistas que presten servicios al estado.

6.1.5. Política de gestión de activos de Información

Objetivo:
Establecer la forma en que se logra y mantiene la protección adecuada de los activos de información.

Directrices:

- Inventario de activos de información
  - La Universidad Surcolombiana mantendrá un inventario actualizado de sus activos de información, bajo la responsabilidad de cada propietario de

información.

- Propietarios de los activos de información
  - La Universidad Surcolombiana es la dueña de la propiedad intelectual de los avances tecnológicos e intelectuales desarrollados por los funcionarios y los contratistas, derivadas del objeto del cumplimiento de funciones y/o tareas asignadas, como las necesarias para el cumplimiento del objeto del contrato.
  - La Universidad Surcolombiana es propietaria de los activos de información y los administradores de estos activos son los funcionarios, contratistas o demás colaboradores de la Universidad (denominados "usuarios") que estén autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de Tecnología y Sistemas de Información (TIC).

6.1.6. Política de uso de los activos

Objetivo:
Lograr y mantener la protección adecuada de los activos de información mediante la asignación a los usuarios finales que deban administrarlos de acuerdo a sus roles y funciones.

Directrices**:**

- Los activos de información pertenecen a la Universidad Surcolombiana y el uso de los mismos debe emplearse exclusivamente con propósitos laborales.
- Los usuarios deberán utilizar únicamente los programas y equipos autorizados por el Centro de Información, Tecnologías y Control Documental.
- La Universidad Surcolombiana proporcionará al usuario, los equipos informáticos y los programas instalados en ellos; los datos/información creados, almacenados y recibidos, serán propiedad de la Universidad Surcolombiana, los funcionarios solo podrán realizar backup de sus archivos personales o de información pública.
- Para copiar cualquier tipo de información clasificada o reservada debe pedir autorización a su jefe inmediato, de acuerdo a las normas sobre clasificación dela información de acuerdo a los niveles de seguridad establecidos por la Universidad Surcolombiana; su copia, sustracción, daño intencional o utilización para fines distintos a las labores propias de la Institución, serán sancionadas de acuerdo con las normas y legislación vigentes.
- Periódicamente, el Centro de Información, Tecnologías y Control Documental efectuará la revisión de los programas utilizados en cada dependencia. La descarga, instalación o uso de aplicativos o programas informáticos NO autorizados será considerado como una violación a las Políticas de seguridad y privacidad de la información de la Universidad Surcolombiana.
- Todos los requerimientos de aplicativos, sistemas y equipos informáticos deben ser solicitados por el Jefe de la dependencia a través del aplicativo de Gestión Documental al Centro de Información, Tecnologías y Control Documental.

- Estarán bajo custodia del Centro de Información, Tecnologías y Control Documental los medios magnéticos/electrónicos (disquetes, cintas, CDs u otros) que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar el software de fabricantes de sus páginas web o sitios en internet y los passwords de administración de los equipos informáticos, sistemas de información o aplicativos.
- En caso de ser necesario y previa autorización del Comité de Seguridad de la Información de la Universidad Surcolombiana, los funcionarios de la Universidad Surcolombiana podrán acceder a revisar cualquier tipo de activo de información y material que los usuarios creen, almacenen, envíen o reciban, a través de Internet o de cualquier otra red o medio, en los equipos informáticos a su uso.
- Los recursos informáticos de la Universidad Surcolombiana no podrán ser utilizados, sin previa autorización escrita, para divulgar, propagar o almacenar contenido personal o comercial de publicidad, promociones, ofertas, programas destructivos (virus), propaganda política, material religioso o cualquier otro uso que no esté autorizado.
- Los usuarios no deben realizar intencionalmente actos que impliquen un mal uso de los recursos tecnológicos o que vayan en contravía de las políticas de seguridad y privacidad de la información entre ellos envíos o reenvíos masivos de correos electrónicos o spam, práctica de juegos en línea, uso permanente de redes sociales personales, conexión de periféricos o equipos que causen molestia a compañeros de trabajo, entre otros.
- Los usuarios no podrán efectuar ninguna de las siguientes labores sin previa autorización del Centro de Información, Tecnologías y Control Documental:
  - Instalar software en cualquier equipo de la Universidad Surcolombiana;
  - Bajar o descargar software No Licenciado, de Internet u otro servicio en línea en cualquier equipo de la Universidad Surcolombiana;
  - Modificar, revisar, transformar o adaptar cualquier software propiedad de la Universidad Surcolombiana;
  - Descompilar o realizar ingeniería inversa en cualquier software de propiedad de la Universidad Surcolombiana.
  - Copiar o distribuir cualquier software de propiedad de la Universidad Surcolombiana.
  - Cambiar la configuración de hardware de propiedad de la Universidad Surcolombiana
- El usuario deberá informar al Jefe Inmediato de cualquier violación de las políticas de seguridad y privacidad, uso indebido y debilidades de seguridad de la información de la Universidad Surcolombiana que tenga conocimiento y al Centro de Información, Tecnologías y Control Documental de la Universidad Surcolombiana.
- El usuario será responsable de todas las transacciones o acciones efectuadas con su “cuenta de usuario”.
- Ningún usuario deberá acceder a la red o a los servicios TIC de la Universidad Surcolombiana, utilizando una cuenta de usuario o clave de otro usuario.
- Todo archivo o material descargado o recibido a través de medio

magnético/electrónico o descarga de Internet o de cualquier red externa, deberá ser revisado para detección de virus y otros programas maliciosos antes de ser instalados en la infraestructura TIC de la Universidad Surcolombiana.

- Todo cambio a la infraestructura informática deberá estar controlado y será realizado de acuerdo con los procedimientos de Ingeniería de Software del Centro de Información, Tecnologías y Control Documental de la Universidad Surcolombiana (AP-TIC-PR-03 Ingeniería de Software, AP-TIC-PR-04 Administración Redes de Datos, AP-TIC-PR-05 Diseño implementación nueva red de datos).
- La información de la Universidad Surcolombiana debe ser respaldada de forma frecuente, debe ser almacenada en lugares apropiados en los cuales se pueda garantizar que la información este segura y podrá ser recuperada en caso de un desastre o de incidentes con los equipos de procesamiento. (AP-TIC-PR-08 Administración de copias de seguridad).
- Los funcionarios deberán realizar la devolución de todos los activos físicos y/o electrónicos asignados por la Universidad Surcolombiana en el proceso de desvinculación, de igual manera deberán documentar y entregar a la Universidad Surcolombiana los conocimientos importantes que posee de la labor que ejecutan.
- Se deben llevar control de la programación de los mantenimientos preventivos de los equipos de cómputo institucionales, revisar el sistema de detección y extinción de incendios y de los recursos informáticos del Centro de Datos y verificar su realización.

6.1.7. Política de uso de estaciones cliente

Objetivo:
Garantizar que la seguridad es parte integral de los activos de información y la correcta utilización por los usuarios finales.

Directrices**:**

- El Centro de Información, Tecnologías y Control Documental no prestará servicio de soporte técnico (revisión, mantenimiento, reparación, configuración y manejo e información) a equipos que no sean de propiedad de la Universidad Surcolombiana.
- La instalación de software en los computadores suministrados por la Universidad Surcolombiana y el soporte técnico de los mismos, es una función exclusiva del Centro de Información, Tecnologías y Control Documental.
- Los usuarios que hagan uso de equipos institucionales en préstamo, NO deberán almacenar información en estos dispositivos y deberán borrar aquellos que copien en estos al terminar su uso.
- Los usuarios no deben mantener almacenados en los discos duros de las estaciones cliente o discos virtuales de red, archivos de vídeo, música y fotos que no sean de carácter institucional.

- En el Disco C:\ de las estaciones cliente se tiene configurado el sistema operativo, aplicaciones y perfil de usuario. El usuario deberá abstenerse de realizar modificaciones a éstos archivos.

6.1.8. Política de uso de Internet

Objetivo:
Establecer unos lineamientos que garanticen la navegación segura y el uso adecuado de la red por parte de los usuarios finales, evitando errores, pérdidas, modificaciones no autorizadas o uso inadecuado de la información en las aplicaciones WEB.

Directrices**:**

- La infraestructura, servicios y tecnologías usados para acceder a internet son propiedad de la Universidad Surcolombiana, por lo tanto se reserva el derecho de monitorear el tráfico de internet y el acceso la información.
- La navegación en Internet debe realizarse de forma razonable y con propósitos laborales y académicos.
- No se permite la navegación a sitios con contenidos contrarios a la ley o a las políticas de la Universidad Surcolombiana o que representen peligro para la entidad como: pornografía, terrorismo, hacktivismo, segregación racial u otras fuentes definidas por la Universidad Surcolombiana. El acceso a este tipo de contenidos con propósitos de estudio de seguridad o de investigación, debe contar con la autorización expresa del Comité de Seguridad de la Información de la Universidad Surcolombiana.
- El Centro de Información, Tecnologías y Control Documental administrará autorización de navegación a los usuarios de la Universidad Surcolombiana, previa solicitud del Jefe de la dependencia.
- La descarga de archivos de Internet debe ser con propósitos laborales y académicos, de forma razonable para no afectar el servicio, en forma específica el usuario debe cumplir los requerimientos de la política de uso de internet descrita en este manual.

6.1.9. Política de clasificación de la información

Objetivo:
Asegurar que la información recibe el nivel de protección apropiado de acuerdo al tipo de clasificación establecido por la ley y la Universidad Surcolombiana.

Directrices**:**

- Se considera información toda forma de comunicación o representación de conocimiento o datos digitales, escritos en cualquier medio, ya sea magnético, papel, visual u otro que genere la Universidad Surcolombiana como por ejemplo:

  - Formularios / comprobantes propios o de terceros.
  - Información en los sistemas, equipos informáticos, medios magnéticos/electrónicos o medios físicos como papel.
  - Otros soportes magnéticos/electrónicos removibles, móviles o fijos.
  - Información o conocimiento transmitido de manera verbal o por cualquier otro medio de comunicación.
- Los usuarios responsables de la información de la Universidad Surcolombiana, deben identificar los riesgos a los que está expuesta la información de sus áreas, teniendo en cuenta que ésta pueda ser copiada, divulgada, modificada o destruida física o digitalmente por personal interno o externo.
- Un activo de información es un elemento definible e identificable que almacena registros, datos o información en cualquier tipo de medio y que es reconocida como "Valiosa" para la Universidad Surcolombiana; Independiente del tipo de activo, se deben considerar las siguientes características.
  - El activo de información es reconocido como valioso para la Universidad Surcolombiana.
  - No es fácilmente reemplazable sin incurrir en costos, habilidades especiales, tiempo, recursos o la combinación de los anteriores.
  - Forma parte de la identidad de la organización y sin el cual la Universidad Surcolombiana puede estar en algún nivel de riesgo.
  - Los niveles de clasificación de la información valiosa que se ha establecido son: INFORMACIÓN PÚBLICA RESERVADA, INFORMACIÓN PÚBLICA CLASIFICADA (PRIVADA Y SEMI-PRIVADA) e INFORMACIÓN PÚBLICA.

6.1.10. Política de manejo disposición de información, medios y equipos.

Objetivo:
Contrarrestar las interrupciones en las actividades de la Universidad Surcolombiana, proteger sus procesos críticos contra los efectos de fallas importantes en los sistemas de información o contra desastres y propender por su recuperación oportuna, permitiendo la confidencialidad, integridad y disponibilidad de la información.

Directrices**:**

- Los medios y equipos donde se almacena, procesa o comunica la información, deben mantenerse con las medidas de protección físicas y lógicas, que permitan su monitoreo y correcto estado de funcionamiento, para ello se debe realizar los mantenimientos preventivos y correctivos que se requieran, la instalación de software en los computadores suministrados por la Universidad Surcolombiana y el soporte técnico de los mismos, es una función exclusiva del Centro de Información, Tecnologías y Control Documental.

6.1.11. Política de control de acceso.

Objetivo:
Definir las pautas generales para asegurar un acceso controlado, físico o lógico, a la información de la plataforma informática de la Universidad Surcolombiana.

Directrices**:**

- El área de Gestión de Servicios Generales, establecerá un programa de mantenimiento integral de los sistemas de control de acceso.
- El Centro de Información, Tecnologías y Control Documental establecerá el procedimiento para establecer los niveles de acceso para usuarios de los servicios y sistemas de información de la Universidad Surcolombiana.
- El Centro de Información, Tecnologías y Control Documental establecerá las configuraciones de las políticas en los sistemas de tecnología y comunicaciones para el control de acceso a los activos de información.
- La Universidad Surcolombiana proporcionará a los funcionarios, personal en comisión permanente y contratistas (personas naturales) todos los recursos tecnológicos necesarios para que puedan desempeñar las funciones para las cuales fueron contratados.
- La Universidad Surcolombiana suministrará a los usuarios las claves respectivas para el acceso a los servicios de red y sistemas de información a los que hayan sido autorizados, las claves son de uso personal e intransferible.
- Solo usuarios designados por el Centro de Información, Tecnologías y Control Documental estarán autorizados para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la Universidad Surcolombiana, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos, eliminar software malicioso.
- Todo trabajo a realizarse en los servidores de la Universidad Surcolombiana con información de la entidad, por parte de sus funcionarios o contratistas, se debe realizar en las instalaciones, no se podrá realizar ninguna actividad de tipo remoto sin la debida aprobación del Director del Centro de Información, Tecnologías y Control Documental de la Universidad Surcolombiana.
- El Centro de Información, Tecnologías y Control Documental debe generar el lineamiento para restringir y auditar el acceso a los códigos fuentes de los programas y elementos asociados como (diseños, especificaciones, librerías de fuentes de programas, planes de verificación y planes de validación).
- El Centro de Información, Tecnologías y Control Documental establecerá el procedimiento de registro, cancelación y periodicidad de revisión y ajuste a permisos de acceso a la red y servicios de red, asignados a los usuarios de los sistemas de información y comunicaciones de la Universidad Surcolombiana, tomando como base los múltiples factores de riesgo existentes en la seguridad de la información.
- Es responsabilidad del jefe de cada dependencia solicitar al Centro de Información, Tecnologías y Control Documental de la Universidad

Surcolombiana. la creación de usuarios en los aplicativos institucionales de los funcionarios y/o contratistas que pertenecen a la misma. De igual manera la modificación o cancelación de dichos usuarios al momento de que se desvincule de la Universidad.

- Los usuarios de los aplicativos institucionales de los funcionarios y/o contratistas serán inactivados un día después de la finalización del contrato o desvinculación de la Institución.
- El dominio oficial de la Universidad Surcolombiana es usco.edu.co

6.1.12. Política de establecimiento, uso y protección de claves de acceso.

Objetivo:
Controlar el acceso a la información.

Directrices:

- Se debe obligar y controlar a los usuarios para que apliquen buenas prácticas de seguridad en la selección, uso y protección de claves o contraseñas, las cuales constituyen un medio de validación de la identidad de un usuario y consecuentemente un medio para establecer derechos de acceso a las instalaciones, equipos o servicios informáticos.
- Se deben asignar nombres de usuario únicos a los usuarios de la Universidad Surcolombiana que lo requieran y éstos no deben compartir con otros usuarios.
- Para la creación de usuarios se define el siguiente lineamiento:

  - Usuarios aplicativos informáticos institucionales:
    - ✓ Docentes:
      Número de identificación del docente
    - ✓ Funcionario Administrativo:
      Letra a (minúscula) seguido de número de identificación del funcionarios
    - ✓ Estudiantes:
      Letra u + código de matrícula estudiante (año+periodo académico+número de inscripción)
      Ejemplo: U20152142110

  - Usuarios de correo electrónico:
    - ✓ Estudiantes:
      Letra u (minúscula) + código de matrícula estudiante (año+periodo académico+número de inscripción) @usco.edu.co
      Ejemplo: u20152142110@usco.edu.co
    - ✓ Funcionarios y contratistas:
      a. primer nombre + carácter punto (.) + primer apellido @usco.edu.co
      Ejemplo: lina.perez@usco.edu.co

      Excepciones:

1. Si existen dos usuarios con el primer nombre y primer apellido igual, el nombre de usuario estará compuesto por:
   Primer y segundo nombre + carácter punto (.) + primer apellido@usco.edu.co
   Ejemplo: linamaria.perez@usco.edu.co si existe dos usuarios con nombres y primer apellido igual y ya se usado el anterior caso, el nombre de usuario estará compuesto por:
   Primer nombre + primera letra del segundo nombre + carácter punto (.) + primer apellido @usco.edu.co
   Ejemplo: linam.perez@usco.edu.co
2. En el caso que existan dos cuentas de usuario con igual primer nombre, sin segundo nombre e igual primer apellido, el nombre de usuario estará compuesto por:
   Primer nombre + carácter punto (.) + primer y segundo apellido @usco.edu.co
   Ejemplo: lina.perezpinto@usco.edu.co
3. Si existen dos cuentas de usuario con los dos nombres y primer apellido iguales, el nombre de usuario se compone:
   Primer nombre + primera letra del segundo nombre, + carácter punto (.) + primer apellido + primera letra del segundo apellido @usco.edu.co
   Ejemplo: linam.perezp@usco.edu.co
4. En caso de que se presente un conflicto no contenido las reglas anteriores, éste será solucionado por la Dirección del Centro de Información, Tecnologías y Control Documental – CTIC.

✓ Institucionales:
Nombre Dependencia @usco.edu.co
Ejemplo: contabilidad@usco.edu.co
Nombre Sede @usco.edu.co
Ejemplo: sedepitalito@usco.edu.co

✓ Eventos (cuentas creadas:
Nombre Evento @usco.edu.co
Ejemplo: Evento@usco.edu.co

- Los usuarios son responsables del uso de las claves o contraseñas de acceso que se le asignen para la utilización de los equipos o servicios informáticos de la Entidad.
- Los usuarios deben tener en cuenta los siguientes aspectos:
  - No incluir contraseñas en ningún proceso de registro automatizado, por ejemplo almacenadas en un macro o en una clave de función.
  - El cambio de contraseña solo podrá ser solicitado por el titular de la cuenta o su jefe inmediato en los casos excepcionales.
  - Terminar las sesiones activas cuando finalice, o asegurarlas con el mecanismo de bloqueo cuando no estén en uso.

Las claves o contraseñas deben:

- Poseer un alto grado de complejidad y no deben ser palabras comunes que se puedan encontrar en diccionarios, ni tener información personal, ni productos a resaltar de su entidad, evite asociarla con fechas especiales, por ejemplo: fechas de cumpleaños, nombre de los hijos, placas de automóvil, etc.
- Nunca utilice sus contraseñas personales en el entorno laboral
- Tener mínimo ocho caracteres alfanuméricos, mínimo debe incluir una mayúscula, una minúscula, números y uno de los siguientes caracteres (punto, coma, dos puntos, guion bajo).
- Cambiarse obligatoriamente la primera vez que el usuario ingrese al sistema, y periódicamente por iniciativa del usuario.
- Cada vez que se cambie la contraseña debe ser distinta por lo menos de las últimas tres anteriores.
- Cambiar la contraseña si ha estado bajo riesgo o se ha detectado anomalía en la cuenta de usuario.
- No se deben usar caracteres idénticos consecutivos, ni que sean todos numéricos, ni tildes, ni eñes, entre otros.
- No debe ser visible en la pantalla, al momento de ser ingresada o mostrarse o compartirse.
- No ser reveladas a ninguna persona, incluyendo al personal del Centro de Información, Tecnologías y Control Documental.
- No regístralas en papel, archivos digitales o dispositivos manuales, a menos que se puedan almacenar de forma segura y el método de almacenamiento este aprobado.

6.1.13. Política de uso de puntos de red de datos (red de área local – LAN).

Objetivo:
Asegurar la operación correcta y segura de los puntos de red.

Directrices**:**

- Los usuarios deberán emplear los puntos de red, para la conexión de equipos informáticos Institucionales.
- Los equipos de uso personal, que no son de propiedad de la Universidad Surcolombiana, solo tendrán acceso a servicios limitados destinados a invitados o visitantes, estos equipos deben ser conectados a los puntos de acceso autorizados y definidos por el Centro de Información, Tecnologías y Control Documental de la Universidad Surcolombiana.
- La instalación, activación y gestión de los puntos de red es responsabilidad del Centro de Información, Tecnologías y Control Documental.
- No está permitido intervenir las redes de cableado, instalar cables no suministrados por Centro de Información, Tecnologías y Control Documental de

la Universidad Surcolombiana., cortar o empalmar cables, desprender marcaciones de tomas, puertas o ductos, golpear o forzar tubos y/o canaletas, así como cualquier otra acción que atente contra la integridad de las redes informáticas Institucionales

6.1.14. Política de uso de impresoras y del servicio de Impresión.

Objetivo:
Asegurar la operación correcta y segura de las impresoras y del servicio de impresión.

Directrices**:**

- Los documentos que se impriman en las impresoras de la Universidad Surcolombiana deben ser de carácter institucional.
- Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner y fotocopiado) para que no se afecte su correcto funcionamiento.
- Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras. En caso de presentarse alguna falla, esta se debe reportar al Centro de Información, Tecnologías y Control Documental mediante el correo electrónico a mantenimientopc@usco.edu.co.
- Los funcionarios en el momento de realizar impresiones de documentos con clasificación pública reservada o información pública clasificada (privada o semiprivada), debe mantener control de la impresora, por lo cual no la deberán dejar desatendida, preservando la confidencialidad de la información.

6.1.15. Política de controles criptográficos

Objetivo:
Implementar actividades para proteger activos de información clasificada, fortaleciendo la confidencialidad, disponibilidad e integridad, mediante el uso de herramientas criptográficas.

Directrices**:**

- El Centro de Información, Tecnologías y Control Documental debe verificar los sistemas o aplicaciones que realicen y/o permitan la transmisión de información pública reservada o información pública clasificada (privada o semiprivada), lo realicen mediante herramientas de cifrado de datos.
- La asignación de la clave para el cifrado de la información en la herramienta, debe ser establecida por el usuario que administra dicha información, teniendo siempre presente que en caso de olvidar la clave, la información cifrada no es recuperable.
- La contraseña de cifrado debe cumplir con la política de establecimiento, uso y protección de claves de acceso de la Universidad Surcolombiana.

- Asegurar que la información clasificada como pública reservada o información pública clasificada (privada o semiprivada), sea protegida por el usuario final generador de la información, con el uso de la herramienta de encripción para transferencias de archivos con esta clasificación, por medio de los sistemas de información y comunicaciones.
- El Centro de Información, Tecnologías y Control Documental debe transmitir y/o almacenar la información clasificada como pública reservada o información pública clasificada (privada o semiprivada) con técnicas de cifrado.
- El Centro de Información, Tecnologías y Control Documental establecerá los lineamientos de administración, protección y ciclo de vida de las llaves criptográficas.
- Los usuarios de la Universidad Surcolombiana que usen las herramientas criptográficas, deben dar cumplimiento a los acuerdos y legislación existente Nacional y/o Internacional.

6.1.16. Política de Seguridad Física

Objetivo:
Implementar el programa de seguridad física de para el acceso a las instalaciones, centros de datos y centros de cableado que permita fortalecer la integridad, disponibilidad e integridad la información

Directrices**:**

- El área de Gestión de Servicios Generales debe implementar un sistema de seguridad física para las instalaciones de la Universidad Surcolombiana.
- El área de Gestión de Servicios Generales definirá el procedimiento de acceso físico (Altos Directivos, Directivos, Funcionarios, visitantes, contratistas, proveedores, estudiantes) a las instalaciones de la Universidad Surcolombiana.
- El Centro de Información, Tecnologías y Control Documental debe implementar barreras y sistemas de control de acceso a las instalaciones, centros de datos y centros de cableado de la Universidad Surcolombiana, así como la asignación de niveles de acceso.
- El Centro de Información, Tecnologías y Control Documental debe implementar alarmas de detección de intrusos a los centros de datos y centros de cableado de la Universidad Surcolombiana.
- El área de Gestión de Servicios Generales informará las debilidades que encuentren a nivel de barreras físicas al Comité de Seguridad de la Información de la Universidad Surcolombiana para aprobación e implementación de soluciones.
- El área de Gestión de Servicios Generales de la Universidad Surcolombiana, implementará y mantendrá en operación sistemas de control de incendio, así como planes integrales a las instalaciones para prevenir inundaciones o humedad en los centros de datos y centros de cableado.
- El Centro de Información, Tecnologías y Control Documental, deberá

implementar protecciones que eviten o mitiguen daños causados por incendios, inundaciones y otros desastres naturales o generados por el hombre a los centros de datos y centros de cableado.

6.1.17. Políticas de seguridad del centro de datos y centros de cableado.

Objetivo:
Asegurar la protección de la información en las redes y la protección de la infraestructura de soporte.

Directrices**:**

- No se permite el ingreso al centro de datos, al personal que no esté expresamente autorizado. Se debe llevar un control de ingreso y salida del personal que visita el centro de datos. En el centro de datos debe disponerse de una planilla para el registro, la cual debe ser diligenciada en lapicero de tinta al iniciar y finalizar la actividad a realizar.
- El Centro de Información, Tecnologías y Control Documental debe garantizar que el control de acceso al centro de datos de la Universidad Surcolombiana, exija autenticación para aprobación de acceso con dispositivos electrónicos.
- El Centro de Información, Tecnologías y Control Documental deberá garantizar que todos los equipos de los centros de datos cuenten con un sistema alterno de respaldo de energía
- La limpieza y aseo del centro de datos debe efectuarse en presencia de un funcionario y/o contratista del Centro de Información, Tecnologías y Control Documental de la Universidad Surcolombiana. El personal de limpieza debe ser ilustrado con respecto a las precauciones mínimas a seguir durante el proceso de limpieza. Debe prohibirse el ingreso de personal de limpieza con maletas o elementos que no sean estrictamente necesarios para su labor de limpieza y aseo.
- En las instalaciones del centro de datos o de los centros de cableado, no se debe fumar, comer o beber; de igual forma se debe eliminar la permanencia de papelería y materiales inflamables o combustibles que generen riesgo de propagación de fuego, así como mantener el orden y limpieza en todos los equipos y elementos que se encuentren en este espacio.
- El centro de datos debe estar provisto de:
  - Señalización adecuada de todos y cada uno de los diferentes equipos y elementos, así como luces de emergencia y de evacuación, cumpliendo las normas de seguridad industrial y de salud ocupacional.
  - Pisos elaborados con materiales no combustibles.
  - Sistema de refrigeración por aire acondicionado de precisión. Este equipo debe ser redundante para que en caso de falla se pueda continuar con la refrigeración.
  - Unidades de potencia ininterrumpida UPS, que proporcionen respaldo al mismo, con el fin de garantizar el servicio de energía eléctrica durante una

falla momentánea del fluido eléctrico de la red pública.
- Alarmas de detección de humo y sistemas automáticos de extinción de fuego, conectada a un sistema central. Los detectores deberán ser probados de acuerdo a las recomendaciones del fabricante o al menos una vez cada 6 meses y estas pruebas deberán estar previstas en los procedimientos de mantenimiento y de control.
- Extintores de incendios o un sistema contra incendios debidamente probados y con la capacidad de detener el fuego generado por equipo eléctrico, papel o químicos especiales.

- El cableado de la red debe ser protegido de interferencias por ejemplo usando canaletas que lo protejan.
- Los cables de potencia deben estar separados de los de comunicaciones, siguiendo las normas técnicas.
- No está permitido el uso de equipo fotográfico, de video, audio u otro dispositivo de grabación de audio o video al interior del centro de datos, centros de cableados, centros de control, salvo en los casos que se a necesarios.
- Las actividades de soporte y mantenimiento dentro del centro de datos siempre deben ser supervisadas por un funcionario y/o contratista autorizado de la Universidad Surcolombiana.
- Las puertas del centro de datos deben permanecer cerradas. Si por alguna circunstancia se requiere ingresar y salir del centro de datos, el funcionario responsable de la actividad se ubicará dentro del centro de datos.
- Cuando se requiera realizar alguna actividad sobre algún armario (rack), este debe quedar ordenado, cerrado y con llave, cuando se finalice la actividad.
- Mientras no se encuentre personal dentro de las instalaciones del centro de datos, las luces deben permanecer apagadas.
- Los equipos del centro de datos que lo requieran, deben estar monitoreados para poder detectar las fallas que se puedan presentar.

6.1.18. Políticas de seguridad de los Equipos

Objetivo:
Asegurar la protección de la información en los equipos.

Directrices**:**

- **Instalación de equipos de procesamiento y almacenamiento**
- Los equipos de procesamiento y almacenamiento deben ser instalados en las áreas de trabajo seguras definidas por el Centro de Información, Tecnologías y Control Documental.

- **Protecciones en el suministro de energía**
- A la red de energía regulada de los puestos de trabajo solo se pueden conectar equipos como computadores, pantallas; los otros elementos deberán conectarse a la red no regulada.

- La Dirección de la Universidad Surcolombiana debe garantizar que se puedan implementar sistemas redundantes de alimentación eléctrica, como por ejemplo: plantas generadoras de energía que permita soportar la operación de los sistemas de información durante una falta de suministro de un proveedor de energía.

- **Seguridad del cableado**
  - Los cables deben estar claramente marcados para identificar fácilmente los elementos conectados y evitar desconexiones erróneas.
  - Deben existir planos que describan las conexiones del cableado.
  - El acceso a los centros de cableado (Racks), debe estar protegido.
  - El Centro de Información, Tecnologías y Control Documental establecerá un programa de revisiones y/o inspecciones físicas al cableado, con el fin de detectar dispositivos no autorizados.

- **Mantenimiento de los Equipos**
  - Ningún usuario debe realizar labores de reparación o mantenimiento de los equipos de cómputo propiedad de la Universidad Surcolombiana.
  - Solo usuarios designados por el Centro de Información, Tecnologías y Control Documental estarán autorizados para instalar software y/o hardware en los equipos, servidores e infraestructura de telecomunicaciones de la Universidad Surcolombiana, así como el uso de herramientas que permitan realizar tareas de mantenimiento, revisión de software, recuperar datos perdidos, eliminar software malicioso.
  - En caso de presentarse alguna falla, esta se debe reportar al Centro de Información, Tecnologías y Control Documental mediante el correo electrónico a mantenimientopc@usco.edu.co.
  - La Universidad Surcolombiana debe mantener contratos de soporte y mantenimiento de los equipos críticos.
  - Las actividades de mantenimiento tanto preventivo como correctivo deben registrarse para cada elemento.
  - Las actividades de mantenimiento de los servidores, elementos de comunicaciones, energía o cualquiera que pueda ocasionar una suspensión en el servicio, deben ser realizadas y programadas.
  - Los equipos que requieran salir de las instalaciones de la Universidad Surcolombiana para reparación o mantenimiento, deben estar debidamente autorizados por el responsable del equipo y se debe garantizar que en dichos elementos no se encuentra información clasificada de acuerdo a los niveles de clasificación de la información pública reservada o información pública clasificada (privada o semiprivada).
  - Los equipos retirados de la institución deben ser protegidos, no se deben dejar sin vigilancia en lugares públicos, de igual forma se debe continuar con las recomendaciones de uso de los fabricantes de estos y la conexión con los sistemas de información de la Universidad Surcolombiana debe cumplir con la política de control acceso.
  - Cuando un dispositivo vaya a ser reasignado o retirado de servicio debe

garantizarse la eliminación de toda información residente en los elementos utilizados para el almacenamiento, procesamiento y transporte de la información.

- **Ingreso y retiro de activos de información de terceros.**

- El retiro e ingreso de todo activo de información de propiedad de los usuarios de la Universidad Surcolombiana, utilizados para fines personales, se realizará mediante los procedimientos establecidos por el sistema de seguridad física. La Universidad Surcolombiana no se hace responsable de los bienes o los problemas que se presenten al conectarse a la red eléctrica de la Universidad.
- El retiro e ingreso de todo activo de información de los visitantes que presten servicios a la Universidad Surcolombiana (consultores, pasantes, visitantes, etc.) será registrado e inspeccionado en los controles de accesos de las instalaciones de la Entidad. El personal de seguridad y vigilancia en los controles de acceso verificarán y registrarán las características de identificación del activo de información.

- **Normas de protección**

- Los funcionarios que hagan uso de los equipos de la Universidad Surcolombiana, no deben dejar desatendidos los equipos de cómputo en sitios públicos y deben transportarlos en lugares visibles bajo medidas que le provean seguridad física.
- Los computadores portátiles siempre deben ser transportados como equipaje de mano, evitando golpes, exponerlo a líquidos, y prevenir la perdida y/o hurto.

6.1.19. Política de escritorio y pantalla limpia

Objetivo:
Definir las pautas generales para reducir el riesgo de acceso no autorizado, pérdida y daño de la información durante y fuera del horario de trabajo normal de los usuarios.

Directrices:

- El personal de la Universidad Surcolombiana debe conservar su escritorio libre de información, propia de la entidad, que pueda ser alcanzada, copiada o utilizada por terceros o por personal que no tenga autorización para su uso o conocimiento.
- El personal de la Universidad Surcolombiana debe bloquear la pantalla de su computador con el protector de pantalla, en los momentos que no esté utilizando el equipo o cuando por cualquier motivo deba dejar su puesto de trabajo.
- Los usuarios de los sistemas de información y comunicaciones de la Universidad Surcolombiana deberán cerrar las aplicaciones y servicios de red cuando ya no los necesite.
- Los usuarios a los que la Universidad Surcolombiana les asigne equipos móviles como computadores, teléfonos inteligentes, tablets, deben activar el bloqueo de teclas o pantalla, que permita evitar el acceso no autorizado a estos dispositivos.
- Al imprimir documentos con información pública reservada y/o pública clasificada

(semi-privada o privada), deben ser retirados de la impresora inmediatamente y no se deben dejar en el escritorio sin custodia.

6.1.20. Política de adquisición, desarrollo y mantenimiento de sistemas de información

Objetivo:
Garantizar que la seguridad es parte integral de los sistemas de información.

Directrices**:**

- Asegurar que los sistemas de información o aplicativos informáticos incluyan controles de seguridad y cumplan con las políticas de seguridad y privacidad de la información.
- En caso de desarrollos propios el Centro de Información, Tecnologías y Control Documental debe separar los ambientes de desarrollo, prueba y producción, en diferentes procesadores y dominios.
- El Centro de Información, Tecnologías y Control Documental deberá realizar pruebas de funcionamiento y de seguridad a los nuevos sistemas, actualizaciones y/o aplicaciones en ambiente de pruebas, para validar la necesidad y operatividad de estos, previo a la aprobación e implementación.
- El Centro de Información, Tecnologías y Control Documental desarrollará y/o adquirirá el software requerido por la Universidad Surcolombiana de manera coordinada con el área que manifieste de manera justificada la necesidad del software. El Centro de Información, Tecnologías y Control Documental establecerá claramente los requerimientos funcionales, operacionales y especificaciones técnicas para la adquisición o desarrollo de sistemas de información y/o comunicaciones, contemplando requerimientos de seguridad de la información.
- Se debe verificar que los desarrollos de la entidad estén completamente documentados, igualmente todas las versiones de los desarrollos se deben preservar adecuadamente en varios medios y guardar copia de respaldo externa a la entidad.
- Desarrollar estrategias para analizar la seguridad en los sistemas de información, como no usar datos sensibles en ambientes de prueba y usar diferentes perfiles para pruebas y producción.
- La compra de una licencia de un programa permitirá a la Universidad Surcolombiana realizar una copia de seguridad, para ser utilizada en caso de que el medio se averíe.
- Cualquier otra copia del programa original será considerada como una copia no autorizada y su utilización conlleva a las sanciones administrativas y legales pertinentes.
- El Centro de Información, Tecnologías y Control Documental será la única dependencia autorizada para realizar copia de seguridad del software original.
- La instalación del software en los activos informáticos de la Universidad

Surcolombiana, se realizará únicamente solicitando al Centro de Información, Tecnologías y Control Documental.

- El Centro de Información, Tecnologías y Control Documental implementará reglas y herramientas que restrinjan la instalación de software no autorizado en los activos de información de la Universidad Surcolombiana.
- El software proporcionado por la Universidad Surcolombiana no puede ser copiado o suministrado a terceros.
- En los equipos de la Universidad Surcolombiana se podrá utilizar el software licenciado por el Centro de Información, Tecnologías y Control Documental y el adquirido o licenciado por los proyectos o programas que se encuentran en la Universidad Surcolombiana.
- El software que se adquiera a través de proyectos o programas, debe quedar licenciado a nombre de la Universidad Surcolombiana.
- Se encuentra prohibido el uso e instalación de juegos en los computadores de la Universidad Surcolombiana.
- El Centro de Información, Tecnologías y Control Documental debe implementar actividades para la protección contra códigos maliciosos y de reparación.
- El Centro de Información, Tecnologías y Control Documental debe implementar métodos y/o técnicas para el desarrollo de software seguro, estas deben incluir definiciones y requerimientos de seguridad, buenas prácticas para desarrollo de software seguro, que le permita a los desarrolladores aplicarlas de manera clara y eficiente.
- Se debe implementar el procedimiento de control de cambios de los sistemas de información de la Universidad Surcolombiana, basados en el ciclo de vida, asegurando la integridad desde las primeras etapas de diseño, pasando por mantenimiento.

6.1.21. Política de respaldo y restauración de información

Objetivo**:**

Proporcionar medios de respaldo adecuados para asegurar que toda la información esencial y el software, se pueda recuperar después de una falla.

Directrices:

- Los administradores de los servidores, los sistemas de información o los equipos de comunicaciones, son los responsables de definir la frecuencia de respaldo y los requerimientos de seguridad de la información (codificación); de igual manera el administrador del sistema de respaldo, es el responsable de realizar los respaldos periódicos.
- Todas las copias de información crítica deben ser almacenadas en un área adecuada y con control de acceso.
- Las copias de respaldo se guardaran únicamente con el objetivo de restaurar el sistema luego de la infección de un virus informático, defectos en los discos de almacenamiento, problemas de los servidores o computadores, materialización

de amenazas, catástrofes y por requerimiento legal.

- Debe ser desarrollado un plan de emergencia para todas las aplicaciones que manejen información crítica; el dueño de la información debe asegurar que el plan es adecuado, frecuentemente actualizado y periódicamente probado y revisado.
- Ningún tipo de información institucional puede ser almacenada en forma exclusiva en los discos duros de las estaciones de trabajo; por lo tanto, es obligación de los usuarios finales realizar las copias en las carpetas destinadas para este fin.
- La restauración de copias de respaldo en ambientes de producción debe estar debidamente aprobada por el propietario de la información.
- El Centro de Información, Tecnologías y Control Documental debe mantener un inventario actualizado de las copias de respaldo de la información y los aplicativos o sistemas de la Universidad Surcolombiana.
- Los medios que vayan a ser eliminados deben surtir un proceso de borrado seguro[1] y posteriormente serán eliminados o destruidos de forma adecuada.

6.1.22. Política para realización de copias en estaciones de trabajo de usuario final

Objetivo:
Asegurar la operación de realización de copias de información en estaciones de trabajo de usuario final.

Directrices**:**

- De acuerdo a lo previsto por el artículo 91 de la Ley 23 de 1982, los derechos de autor sobre las obras creadas por los empleados y funcionarios en virtud de su vinculación a la Entidad pública correspondiente, en este caso a la Universidad Surcolombiana, son de propiedad de ésta con las excepciones que la misma ley han señalado.
- Ningún usuario final debe realizar copias de la información contenida en la estación de trabajo a medios extraíbles de información.
- En caso de presentarse alguna falla en los equipos de cómputo, se debe reportar al correo mantenimientopc@usco.edu.co del Centro de Información, Tecnologías y Control Documental y en caso de requerirse copia de la información, ésta se realizará de manera temporal durante las diferentes labores de reparación o mantenimiento.
- Ningún usuario debe utilizar equipo diferente al asignado para copiar algún tipo de archivo, excepto al autorizado por jefe inmediato.

[1] El borrado seguro se ejecuta cuando al borrar un archivo o formatear un dispositivo de almacenamiento, alguna utilidad de borrado escribe ceros (o) sobre el archivo, no permitiendo que éste se pueda recuperar posteriormente. Tomado de: http://es.wikipedia.org/wiki/Borrado_de_archivos

6.1.23. Política de registro y seguimiento de eventos de sistemas de información y comunicaciones

Objetivo:
Preservar la integridad, confidencialidad y disponibilidad de los registros de eventos (logs) generados por los sistemas de información y comunicaciones de la Universidad Surcolombiana.

Directrices**:**

- El Centro de Información, Tecnologías y Control Documental debe implementar los lineamientos para elaborar, preservar y revisar los registros de actividades (logs) de los usuarios de los sistemas de la Universidad Surcolombiana.
- Los profesionales del Centro de Información, Tecnologías y Control Documental, no están facultados para modificar, borrar o desactivar registros (logs) de sus actividades propias, ni de los usuarios de los sistemas de información y telecomunicaciones, de igual forma se deben realizar las configuraciones de seguridad necesarias para evitar la eliminación o cambios no autorizados a los registros de información.
- El acceso a los registros (logs) es restringido, por lo cual su consulta por usuarios se debe realizar con previa autorización del Centro de Información, Tecnologías y Control Documental.
- La consulta y copia de la información de registros que se requiera con fines probatorios debe ser solicitada por autoridad judicial a la Oficina Jurídica.
- El Centro de Información, Tecnologías y Control Documental deberá realizar copias de respaldo de los registros de auditoria.
- El Centro de Información, Tecnologías y Control Documental debe proteger y auditar periódicamente los registros de actividades (logs) de los administradores de los sistemas de información y telecomunicaciones

6.1.24. Política de control de software operacional de la Universidad Surcolombiana

Objetivo:
Generar acciones que permitan preservar la integridad de los sistemas operativos pertenecientes la Universidad Surcolombiana.

Directrices**:**

- El Centro de Información, Tecnologías y Control Documental definirá e implementará el procedimiento de instalación y actualización de software sobre los sistemas operativos de la Universidad Surcolombiana, dentro del cual se debe prever una estrategia de retroceso, registros de auditoria, control y copia de versiones, control de cambio, pruebas en su respectivo ambiente y configuraciones de seguridad.

- Las transacciones de los sistemas de información adquiridos a terceros y/o contratistas que generen errores de software, omisiones y problemas de seguridad deben ser identificadas y la evidencia de dichos errores debe ser documentada, para ser enviada al proveedor del sistema de información o software. Así mismo, errores de software, omisiones y problemas de seguridad que son atribuibles a los sistemas de información desarrollados al interior de la Universidad se deben retornar a los diseñadores y desarrolladores internos para que sean revisados y corregidos.

6.1.25. Política de seguridad de las comunicaciones

Objetivo:
Implementar mecanismos de control que permitan mantener la disponibilidad de las redes de datos, sistemas de comunicaciones e instalaciones de procesamiento de la Universidad Surcolombiana.

Directrices**:**

- El Centro de Información, Tecnologías y Control Documental de la Universidad Surcolombiana, es el área responsable de realizar el aseguramiento de los accesos a internet, acceso a redes de terceros y a las redes de la institución; esta responsabilidad incluye, pero no se limita a prevenir que intrusos tengan acceso a los recursos informáticos y a prevenir la introducción y propagación de virus.
- El Centro de Información, Tecnologías y Control Documental debe implementar medidas para asegurar la disponibilidad de los recursos y servicios de red de la Universidad Surcolombiana.
- El Centro de Información, Tecnologías y Control Documental debe crear los estándares técnicos de configuración de la red de la Universidad Surcolombiana y configuración de seguridad y de dispositivos de seguridad.
- El Centro de Información, Tecnologías y Control Documental debe interconectar las instalaciones de las facultades y sedes bajo el cumplimiento los estándares de técnicos de configuración y de seguridad de las redes y servicios de la Universidad Surcolombiana.
- El Centro de Información, Tecnologías y Control Documental debe implementar sistemas de protección entre las redes de la Universidad Surcolombiana y las redes externas no administradas por la entidad.
- El Centro de Información, Tecnologías y Control Documental debe identificar y documentar los servicios, protocolos y puertos autorizados en las redes de datos e inhabilitar o eliminar los servicios, protocolos y puertos no utilizados.
- La Universidad Surcolombiana debe contar con un firewall o dispositivos de seguridad perimetral para la conexión a Internet o cuando sea inevitable para la conexión a otras redes en outsourcing o de terceros.
- La conexión remota a la red de área local de la Universidad Surcolombiana debe realizarse a través de una conexión VPN segura suministrada por la entidad, la

cual debe ser aprobada, registrada y auditada, por el Centro de Información, Tecnologías y Control Documental.

- El Centro de Información, Tecnologías y Control Documental debe segmentar la red, de modo que permita separar los grupos de servicios de información.
- Los usuarios no están autorizados para hacer uso de redes externas a través de dispositivos personales en las instalaciones de la entidad (modem USB, router, wifi público, etc.), esto compromete la seguridad de los recursos informáticos de la Universidad Surcolombiana.

6.1.26. Política para la Transferencia de Información

Objetivo:
Proteger la información transferida al interior y exterior de la Universidad Surcolombiana.

Directrices:

- El Centro de Información, Tecnologías y Control Documental debe implementar las herramientas necesarias para asegurar la transferencia de información al interior y exterior de la Universidad Surcolombiana, contra interceptación, copiado, modificación, enrutado y destrucción.
- El Centro de Información, Tecnologías y Control Documental, deberá controlar las acciones para reenvío automático de correo electrónico a direcciones de correo externo.
- Los funcionarios de la Universidad Surcolombiana que traten temas o información clasificada como información pública reservada o información pública clasificada (privada o semiprivada), lo deberán hacer en lugares seguros y/o por medios de comunicación seguros.
- Se debe establecer el procedimiento para la transferencia de información en medios físicos a nivel interno, externo de la Universidad Surcolombiana y a terceros.

6.1.27. Políticas de Creación y uso de correo electrónico

Objetivo:
Definir las pautas generales para asegurar una adecuada protección de la información de la Universidad Surcolombiana, en el servicio y uso del servicio de correo electrónico por parte de los usuarios autorizados.

Directrices:

- Esta política define y distingue el uso de correo electrónico aceptable/apropiado e inaceptable/inapropiado y establece las directrices para el uso seguro del servicio.
- Los funcionarios de la Universidad Surcolombiana deberán hacer uso del correo electrónico institucional suministrado por el Centro de Información, Tecnologías

y Control Documental, para desarrollar las actividades oficiales inherentes al cargo asignado.

- La cuenta de correo oficial para el cumplimiento de las funciones desempeñadas para la Universidad Surcolombiana, es la cuenta de correo electrónico institucional suministrada por el Centro de Información, Tecnologías y Control Documental.

El servicio de correo electrónico:

- Permite a los usuarios de la Universidad Surcolombiana, el intercambio de mensajes, a través de una cuenta de correo electrónico institucional, que facilita el desarrollo de sus funciones.
- Los usuarios del correo electrónico corporativo son responsables de evitar prácticas o usos del correo que puedan comprometer la seguridad de la información.
- Los servicios de correo electrónico corporativo se emplean para servir a una finalidad operativa y administrativa en relación con la institución. Todos los correos electrónicos procesados por los sistemas, redes y demás infraestructura TIC de la Universidad Surcolombiana se consideran bajo el control de la entidad.
- Este servicio debe utilizarse exclusivamente para las tareas propias de la función desarrollada en la Universidad Surcolombiana y no debe utilizarse para ningún otro fin.
- No está autorizado el envío de correos con contenido que atenten contra la integridad y dignidad de las personas y el buen nombre, imagen y reputación de la Universidad.
- No está autorizado enviar o reenviar cadenas de correo, mensajes ajenos al quehacer institucional (por ejemplo mensajes con contenido racista, sexista, pornográfico, publicitario no institucional) o cualquier otro tipo de mensajes que atenten contra la dignidad de las personas, mensajes mal intencionados que puedan afectar los sistemas internos o de terceros, mensajes que vayan en contra de las leyes, la moral, las buenas costumbres y mensajes que incite a realizar prácticas ilícitas o promuevan a violencia.
- No está autorizado el envío de correos masivos con archivos adjuntos de gran tamaño que puedan congestionar la red.
- El uso de la correspondencia en forma electrónica, permite disminuir costos, por lo cual no se debe imprimir lo recibido por e-mail mientras no sea necesario o autorizado, pues esto genera un costo adicional para la Institución.
- Las cuentas de correo electrónico de los funcionarios y/o contratistas serán inactivadas un día después de la finalización del contrato o desvinculación de la Institución.
- Las cuentas de correo electrónico de los estudiantes que no sean usadas durante dos años consecutivos serán eliminadas de manera automática y sin consentimiento alguno por parte del usuario.
- Las cuentas de correo electrónico de los graduados serán eliminadas de manera automática tres meses después de su graduación.

- Los correos electrónicos deben contener el siguiente disclaimer:

  "NOTA CONFIDENCIAL:
  Su dirección de correo electrónico fue suministrada a través de autorización consentida emitida a la UNIVERSIDAD SURCOLOMBIANA, para el desarrollo de una finalidad específica correspondiente a una función reglada. Este mensaje puede contener información confidencial o de uso interno de la UNIVERSIDAD SURCOLOMBIANA. Si usted no es el destinatario autorizado, por favor notifique de forma inmediata al emisor, borre y destruya este mensaje, junto con la información adjunta. Cualquier divulgación, distribución, copia o uso no autorizado podrá ser considerado ilegal. Por favor tenga en cuenta que los comentarios u opiniones presentados en este correo no son necesariamente en representación de la UNIVERSIDAD SURCOLOMBIANA. / El presente mensaje se ajusta a lo establecido por la Ley 1581 DE 2012 emitida por el Congreso de la República de Colombia.

  "CONFIDENTIAL NOTE:
  Your e-mail address was supplied through the consented authorization issued to UNIVERSIDAD SURCOLOMBIANA, in order to develop a specific achievement regarding a regulated function. This message may contain confidential or only-internal-use information of UNIVERSIDAD SURCOLOMBIANA. If you happen not to be the authorized addressee, please notify the transmitter, erase, and destroy this message altogether with the attached information. Any disclosure, distribution, copy, or unauthorized use of this information can be considered as illegal. Please, take into account that all the comments or opinions presented in this email are not necessarily in the representation of UNIVERSIDAD SURCOLOMBIANA. / This message is adjusted according to what is established by Law 1581 of 2012 emitted by the Congress of the Republic of Colombia.

- El tamaño del buzón de correo electrónico está definido por google apps es ilimitado y está sujeto a cambios por el mismo.
- Es responsabilidad del jefe de cada dependencia solicitar al Centro de Información, Tecnologías y Control Documental de la Universidad Surcolombiana. la creación de las cuentas de correo institucional de los funcionarios y/o contratistas que pertenecen a la misma. De igual manera la modificación o cancelación de dichas cuentas al momento de que se desvincule de la Universidad.
- Las cuentas de correo electrónico son propiedad de la Universidad Surcolombiana, las cuales son asignadas a personas que tengan algún tipo de vinculación con la institución, ya sea como personal de planta, en comisión permanente, contratistas, consultores, personal temporal, docente o estudiante, quienes deben utilizar este servicio única y exclusivamente para las tareas propias de la función desarrollada en la universidad y no debe utilizarse para ningún otro fin.

- Cada usuario es responsable del contenido del mensaje enviado y de cualquier otra información adjunta al mismo, de acuerdo a la clasificación de la información establecida por la Universidad Surcolombiana.
- Todos los mensajes pueden ser sujetos a análisis y conservación permanente por parte de la Institución.
- Todo usuario es responsable por la destrucción de los mensajes cuyo origen sea desconocido y por lo tanto asumirá la responsabilidad y las consecuencias que puede ocasionar la ejecución de cualquier archivo adjunto. En estos casos no se debe contestar dichos mensajes, ni abrir los archivos adjuntos y se debe reenviar el correo a mantenimientopc@usco.edu.co con la frase "correo sospechoso" en el asunto.
- El único servicio de correo electrónico autorizado en la Universidad Surcolombiana, es el asignado por el Centro de Información, Tecnologías y Control Documental.

6.1.28. Políticas específicas para Webmaster

Objetivo:
Proteger la integridad de las páginas Web institucionales, el software y la información contenida.

Directrices**:**

- Las claves de acceso de los responsables de los contenidos de las páginas Web (webmasters), son estrictamente confidenciales, personales e intransferibles.
- Los contenidos deben ser vigentes, relevantes, verificables y completos
- Los contenidos deben ser entendibles, agradables y de fácil uso
- No se deben usar abreviaturas. Si se necesita utilizar abreviaturas, éstas deben ir referenciadas después de que son utilizadas por primera vez, entre paréntesis, inmediatamente después del texto al que hacen referencia.
- No se deben usar siglas sin que al pie se especifique qué significan.
- No se deben usar tecnicismos. Si es estrictamente necesario utilizarlos, se debe explicar el significado del mismo inmediatamente después de que es utilizado por primera vez, incluyendo la explicación dentro de paréntesis.
- Cuando se publique información en forma de artículos, la información debe provenir de fuentes totalmente confiables. Si la fuente no es totalmente confiable o si no se tiene certeza de la fuente de donde proviene, la información debe ser corroborada al menos con tres (3) fuentes adicionales, identificando las fuentes al final del artículo.
- Cuando se publique información en archivos para descargar, se debe indicar la fecha de publicación o de su última actualización.
- Las imágenes, dibujos, fotos y cualquier otro material gráfico que se utilice, deben estar acordes con los textos. Cuando este tipo de material sufre algún tipo de tratamiento técnico (por ejemplo: montajes, composición, transparencias, etc.), se debe indicar claramente en el pie del material que éste ha sido tratado y ha sufrido modificaciones de su versión original.

- Los contenidos provistos por medios electrónicos por la Universidad Surcolombiana de ninguna forma pueden ser considerados como ofensivos, sexistas, racistas, discriminatorios, obscenos, en la medida que contenidos ofensivos atentan contra derechos fundamentales de los particulares. En todo momento se debe tener presente que se trata de la imagen de la Universidad.
- No se deben ofrecer contenidos que revelen aspectos confidenciales de las personas o entidades, que afecten el buen nombre o que puedan generar efectos legales adversos a las entidades que publiquen la información, conforme a las disposiciones contenidas en la Ley 1581 de 2012.
- Las obras protegidas por el derecho de autor que se encuentren dentro de los sitios Web hacen parte del patrimonio de la entidad pública y por lo tanto son considerados bienes fiscales, razón por la cual su utilización debe estar expresamente autorizada y así mismo se debe informar claramente al ciudadano qué puede hacer y qué no con el material alojado.
- El desconocimiento de las normas vigentes en materia de derechos de autor, derechos de propiedad intelectual y de propiedad industrial puede generar acciones civiles o penales.
- El portal web debe dar cumplimiento a la norma NTC 5854 la cual establece los requisitos de accesibilidad y usabilidad que se deben implementar en las páginas web en los niveles de conformidad A, AA y AAA.

6.1.29. Políticas específicas para funcionarios y contratistas del Centro de Información, Tecnologías y Control Documental

Objetivo**:**
Definir las pautas generales para asegurar una adecuada protección de la información de la Universidad Surcolombiana por parte de los funcionarios y contratistas de TI de la entidad.

Directrices:

- El personal del Centro de Información, Tecnologías y Control Documental no debe dar a conocer su clave de usuario a terceros de los sistemas de información, sin previa autorización del Director del Centro de Información, Tecnologías y Control Documental.
- Los usuarios y claves de los administradores de sistemas y del personal del Centro de Información, Tecnologías y Control Documental son de uso personal e intransferible.
- El personal del Centro de Información, Tecnologías y Control Documental debe emplear obligatoriamente las claves o contraseñas con un alto nivel de complejidad y utilizar los servicios de autenticación fuerte que posee la universidad de acuerdo al rol asignado.
- Los administradores de los sistemas de información deben seguir las políticas de cambio de clave y utilizar procedimiento de salvaguarda o custodia de las claves o contraseñas en un sitio seguro. A este lugar solo debe tener acceso el

Director del Centro de Información, Tecnologías y Control Documental o el oficial de Seguridad de la Información.

- Los documentos y en general la información de procedimientos, seriales, software etc. deben mantenerse custodiados en todo momento para evitar el acceso a personas no autorizadas.
- Para el cambio o retiro de equipos de funcionarios, se deben seguir políticas de saneamiento, es decir llevar a cabo mejores prácticas para la eliminación de la información de acuerdo al software disponible en la entidad. Ej.: Formateo seguro, destrucción total de documentos o borrado seguro de equipos electrónicos.
- Los funcionarios encargados de realizar la instalación o distribución de software, sólo instalarán productos con licencia y software autorizado.
- Los funcionarios del Centro de Información, Tecnologías y Control Documental no deben otorgar privilegios especiales a los usuarios sobre las estaciones de trabajo, sin la autorización correspondiente del Director del Centro de Información, Tecnologías y Control Documental y el registro en el sistema de gestión documental o correo a ctic@usco.edu.co.
- Los funcionarios del Centro de Información, Tecnologías y Control Documental se obligan a no revelar a terceras personas, la información a la que tengan acceso en el ejercicio de sus funciones de acuerdo con la guía de clasificación de la información según sus niveles de seguridad. En consecuencia, se obligan a mantenerla de manera confidencial y privada y a protegerla para evitar su divulgación.
- Los funcionarios del Centro de Información, Tecnologías y Control Documental no utilizarán la información para fines comerciales o diferentes al ejercicio de sus funciones.
- Toda licencia de software o aplicativo informático y sus medios, se deben guardar y relacionar de tal forma que asegure su protección y disposición en un futuro.
- Las copias licenciadas y registradas del software adquirido, deben ser únicamente instaladas en los equipos y servidores de la entidad. Se deben hacer copias de seguridad en concordancia con las políticas del proveedor y de la entidad.
- La copia de programas o documentación, requiere tener la aprobación escrita de la Universidad Surcolombiana y del proveedor si éste lo exige.
- El personal del Centro de Información, Tecnologías y Control Documental debe velar por que se cumpla con el registro en la bitácora de acceso al datacenter, de las personas que ingresen y que hayan sido autorizadas previamente por la Dirección del área o por quien ésta delegue.
- Por defecto deben ser bloqueados, todos los protocolos y servicios que no se requieran en los servidores; no se debe permitir ninguno de ellos, a menos que sea solicitado y aprobado oficialmente por la universidad a través del Comité de Seguridad de la Información de la Universidad Surcolombiana.
- El acceso a cualquier servicio, servidor o sistema de información debe ser autenticado y autorizado.

- Todos los servidores deben ser configurados con el mínimo de servicios necesarios y obligatorios para desarrollar las funciones designadas.

6.1.30. Política de Tercerización u Outsourcing

Objetivo:
Mantener la seguridad de la información y los servicios de procesamiento de información, a los cuales tienen acceso terceras partes, entidades externas o que son procesados, comunicados o dirigidos por estas.

Directrices**:**

- Se deben establecer criterios de selección que contemplen la experiencia y reputación de terceras partes, certificaciones y recomendaciones de otros clientes, estabilidad financiera de la compañía, seguimiento de estándares de gestión de calidad y de seguridad y otros criterios que resulten de un análisis de riesgos de la selección y los criterios establecidos por la entidad.
- Se deben establecer mecanismos de control en las relaciones contractuales, con el objetivo de asegurar que la información a la que tengan acceso o servicios que sean provistos por los proveedores o contratistas, cumplan con las políticas de seguridad y privacidad de la información de la Universidad Surcolombiana, política de tratamiento de datos, las cuales deben se divulgadas por los funcionarios responsables de la realización y/o firma de contratos o convenios.
- En los contratos o acuerdos con los proveedores y/o contratistas se debe incluir una causal de terminación del acuerdo o contrato de servicios, por el no cumplimiento de las políticas de seguridad y privacidad de la información
- Los contratistas, oferentes y/o proveedores deben aceptar y firmar el acuerdo de confidencialidad establecido por la Universidad Surcolombiana.
- El Centro de Información, Tecnologías y Control Documental deberá mitigar los riesgos de seguridad con referencia al acceso de los proveedores y/o contratistas a los sistemas de información de la Universidad Surcolombiana.
- Se debe identificar y monitorear los riesgos relacionados con los contratistas o proveedores en relación a los objetos contractuales, incluyendo la cadena de suministro de los servicios de tecnología y comunicación.
- Los funcionarios de la Universidad Surcolombiana que fungen como supervisores de contratos relacionados con sistemas de información deberán realizar seguimiento, control y revisión de los servicios suministrados por los proveedores y/o contratistas.

6.1.31. Política de Gestión de los Incidentes de la Seguridad de la Información

Objetivo:
Asegurar que los eventos e incidentes de seguridad que se presenten con los activos de información, sean comunicados y atendidos oportunamente, empleando los procedimientos definidos, con el fin de que se tomen oportunamente las acciones correctivas

Directrices**:**

- La Universidad Surcolombiana establecerá responsables y procedimientos de gestión para el tratamiento de incidentes de seguridad de la información asegurando una respuesta rápida, eficaz y eficiente, quienes investigarán y solucionarán los incidentes presentados, implementando las acciones necesarias para evitar su repetición, así mismo debe escalar los incidentes de acuerdo con la criticidad del mismo.
- El Comité de Seguridad de la Información de la Universidad Surcolombiana designa al equipo de respuesta a incidentes de seguridad informática y al Centro de Información, Tecnologías y Control Documental para responder a los eventos o incidentes de seguridad de la información; debe generarse el procedimiento de respuesta.
- Se debe establecer la implementación de lecciones aprendidas al término del análisis y solución de incidentes de seguridad de la información, estos deben ser socializados a los interesados conservando la confidencialidad de estas, así mismo, estas deben ser utilizadas como herramienta para la toma de decisiones y revisiones de la política de seguridad.
- El equipo de respuesta a incidentes de seguridad informática debe establecer el procedimiento para la recolección de evidencia, siguiendo los lineamientos jurídicos vigentes en Colombia y estándares internacionales.

6.1.32. Política para la Gestión de la Continuidad de Seguridad de la Información

Objetivo:

Asegurar la continuidad de la seguridad de la información en situaciones de crisis o desastres

Directrices**:**

- La Universidad Surcolombiana establecerá el Plan de Continuidad del Negocio para la entidad, este debe incluir el plan de recuperación de desastres.
- Se debe generar el plan de continuidad de seguridad de la información, documentado e implementando procesos y procedimientos para asegurar la continuidad requerida por la Entidad.
- El Centro de Información, Tecnologías y Control Documental elaborará el plan de recuperación de desastres para los sistemas de información y comunicación de la Universidad Surcolombiana, el cual debe incluir mínimo procedimientos, condiciones de seguridad, recuperación y retorno a la normalidad.
- El plan de continuidad del negocio de la Universidad Surcolombiana se debe verificar, revisar y evaluar, por la Oficina de Control Interno durante el desarrollo del plan anual de auditorías.
- El Centro de Información, Tecnologías y Control Documental debe analizar y establecer los requerimientos mínimos de redundancia para los sistemas de

información críticos de la Universidad Surcolombiana junto con la plataforma tecnológica que los soporta, de igual forma deberá investigar, evaluar y probar las soluciones de tecnología que suplan la necesidad de la universidad.

- La Universidad Surcolombiana propenderá por la implementación de una plataforma tecnológica redundante que satisfaga los requerimientos de disponibilidad necesarios para la universidad, así como programación y ejecución de pruebas de funcionalidad de esta.

6.1.33. Política de cumplimiento de requisitos legales y contractuales

Objetivo:
Prevenir el incumplimiento de obligaciones legales relacionadas con seguridad de la información.

Directrices**:**

- La Universidad Surcolombiana respeta y acata las normas legales existentes relacionadas con seguridad de la información, para lo cual realizará una continua revisión, identificación, documentación y cumplimiento de la legislación y requisitos contractuales aplicables para la entidad, relacionada con la seguridad de la información.
- El Centro de Información, Tecnologías y Control Documental deberá garantizar que todo el software que se ejecute los activos de información de la Universidad Surcolombiana esté protegido por derechos de autor y requiera licencia de uso o, sea software de libre distribución y uso.
- Los usuarios y/o funcionarios de la Universidad Surcolombiana deben cumplir con las leyes de derechos de autor y acuerdos de licenciamiento de software, se recuerda que es ilegal duplicar software, duplicar documentación sin la autorización del propietario bajo los principios de derechos de autor y, la reproducción no autorizada es una violación a la ley.
- La Universidad Surcolombiana protegerá y retendrá los registros de información de acuerdo con la clasificación pública reservada o información pública clasificada (privada o semiprivada),
- El Centro de Información, Tecnologías y Control Documental realizará el procedimiento de back up los registros alojados en los sistemas de información.
- La Universidad Surcolombiana implementará los lineamientos para asegurar la privacidad y protección de datos personales, definiendo claramente los deberes en las actividades de recolección, procesamiento y transmisión de los mismos.
- Las Dependencias de la Universidad Surcolombiana que tratan con datos personales de funcionarios, proveedores, contratistas, u otras personas deben obtener la autorización para el tratamiento de datos personales que permita recolectar, transferir, almacenar, usar, circular, suprimir, compartir, actualizar y transmitir dichos datos personales en el desarrollo de las actividades de la Entidad, así mismo los Jefes de dependencias deben asegurar que tendrán acceso a los datos personales únicamente los funcionarios que tengan una necesidad laboral legitima.

- La Universidad Surcolombiana a través del Centro de Información, Tecnologías y Control Documental debe implementar métodos y herramientas que permitan proteger la información personal de los funcionarios, proveedores u otras terceras partes almacenada en bases de datos o cualquier otro tipo de almacenamiento o repositorio previniendo su divulgación, alteración o eliminación sin la autorización.

6.1.34. Política de Revisiones de Seguridad de la Información

Objetivo:
Garantizar el funcionamiento del sistema de gestión de seguridad de la información de acuerdo a las políticas y procedimientos implementados en la Universidad Surcolombiana.

Directrices:

- La Universidad Surcolombiana planeará y realizará auditorías internas y externas al sistema de gestión de seguridad de la información para la verificación y cumplimiento de objetivos, controles, políticas y procedimientos de seguridad de la Información.
- La Dirección de la Universidad, Directores de Centro, Jefes de Oficina, Jefes de Área, deben verificar y supervisar el cumplimiento de las políticas de seguridad y privacidad de la información en su área de responsabilidad.
- El Centro de Información, Tecnologías y Control Documental debe establecer el procedimiento para revisar periódicamente los sistemas de información con el herramientas automáticas y especialistas técnicos.

6.1.35. Políticas específicas para usuarios de la Universidad Surcolombiana.

Objetivo:
Definir las pautas generales para asegurar una adecuada protección de la información de la Universidad Surcolombiana por parte de los usuarios de la institución.

Directrices:

- La Universidad Surcolombiana instalará copia de los programas que han sido adquiridos legalmente en los equipos asignados en las cantidades requeridas para suplir las necesidades. El uso de programas sin su respectiva licencia y autorización de la Universidad Surcolombiana (imágenes, vídeos, software o música), obtenidos a partir de otras fuentes (internet, dispositivos de almacenamiento externo), puede implicar amenazas legales y de seguridad de la información para la entidad, por lo que ésta práctica no está autorizada.
- Todo el software usado en la plataforma tecnológica de la Universidad Surcolombiana debe tener su respectiva licencia y acorde con los derechos de autor.

- La Universidad Surcolombiana no se hace responsable por las copias no autorizadas de programas instalados o ejecutados en los equipos asignados a sus funcionarios o contratistas.
- El uso de dispositivos de almacenamiento externo (dispositivos móviles, DVD, CD, memorias USB, agendas electrónicas, celulares, etc.) pueden ocasionalmente generar riesgos para la universidad al ser conectados a los computadores, ya que son susceptibles de transmisión de virus informáticos o pueden ser utilizados para la extracción de información no autorizada.
- Los programas instalados en los equipos, son de propiedad de la Universidad Surcolombiana, la copia no autorizada de programas o de su documentación, implica una violación a la política general de la Universidad Surcolombiana. Aquellos funcionarios, contratistas o demás colaboradores que utilicen copias no autorizadas de programas o su respectiva documentación, quedarán sujetos a las acciones disciplinarias establecidas por la Universidad Surcolombiana o las sanciones que especifique la ley.
- La Universidad Surcolombiana se reserva el derecho de proteger su buen nombre y sus inversiones en hardware y software, fomentando controles internos para prevenir el uso o la realización de copias no autorizadas de los programas de propiedad de la entidad. Se incluirá valoraciones periódicas del uso de los programas, auditorías anunciadas y no anunciadas.
- Los recursos tecnológicos y de software asignados a los funcionarios de la Universidad Surcolombiana son responsabilidad de cada funcionario.
- Los usuarios son los responsables de la información que administran en sus equipos personales y deben abstenerse de almacenar en ellos información institucional.
- Los usuarios solo tendrán acceso a los datos y recursos autorizados por la Universidad Surcolombiana, y serán responsables disciplinaria y legalmente de la divulgación no autorizada de esta información.
- Es responsabilidad de cada usuario proteger la información que está contenida en documentos, formatos, listados, etc., los cuales son el resultado de los procesos informáticos; adicionalmente se deben proteger los datos de entrada de estos procesos.
- Los dispositivos electrónicos (computadores, impresoras, fotocopiadoras, escáner, etc.) solo deben utilizarse para los fines autorizados por la entidad.
- Cualquier evento o posible incidente que afecte la seguridad de la información, debe ser reportado inmediatamente al Centro de Información, Tecnologías y Control Documental o al equipo de respuesta a incidentes de seguridad informática.
- Los jefes de las diferentes áreas de la Universidad Surcolombiana, en conjunto con el Comité de Seguridad de la Información de la Universidad Surcolombiana propiciarán actividades para concienciar al personal sobre las precauciones necesarias que deben realizar los usuarios finales, para evitar revelar información confidencial.
- Los datos de los sistemas de información y aplicaciones no deben intercambiarse utilizando archivos compartidos en los computadores, discos

virtuales, CD, DVD, medios removibles; deben usarse los mismos servicios del sistema de información, los cuales están controlados y auditados.

6.1.36. Política de retención y archivo de datos.

Objetivo:
Mantener la integridad y disponibilidad de la información y de los servicios de procesamiento de información.

Directrices**:**

- La política de retención de archivos debe establecer cuánto tiempo se deben mantener almacenados los archivos en la Universidad Surcolombiana de acuerdo a las tablas de retención documental y demás normas relacionadas con el Archivo de la Universidad.
- Las reglas y los principios generales que regulan la función archivística del Estado, se encuentran definidos por la Ley, la cual es aplicable a la administración pública en sus diferentes niveles producidos en función de su misión y naturaleza.
- La ley prevé el uso de las tecnologías de la información y las comunicaciones en la administración, conservación de archivos y en la elaboración e implantación de programas de gestión de documentos.

6.1.37. Política de uso de mensajería instantánea y redes sociales

Objetivo:
Definir las pautas generales para asegurar una adecuada protección de la información de la Universidad Surcolombiana, en el uso del servicio de mensajería instantánea y de las redes sociales, por parte de los usuarios autorizados.

Directrices**:**

- El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.
- No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.
- La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, contratista o colaborador de la Universidad Surcolombiana, que sea creado a nombre personal en redes sociales como: twitter®, facebook®, youtube® likedink®, blogs, instaram, etc, se considera fuera del alcance del Sistema General de Seguridad y Privacidad de la Información y por lo tanto su confiabilidad, integridad y disponibilidad y los daños y perjuicios que pueda llegar a causar serán de completa responsabilidad de la persona que las haya generado.

- Toda información distribuida en las redes sociales institucionales deben cumplir con los protocolos establecidos por la Oficina de Comunicaciones de la Universidad.
- No se debe utilizar el nombre de la Universidad Surcolombiana en las redes sociales para difamar o afectar la imagen y reputación de los seguidores cuando responden comentarios en contra de la filosofía de la institución.

6.1.38. Política de tratamiento de datos personales

Objetivo:
Establecer los lineamientos para administración y tratamiento de datos personales en la Universidad Surcolombiana.

Directrices:

- Finalidades y tratamiento al cual serán sometidos los datos personales: Los datos personales que la Universidad Surcolombiana recolecte, almacene, use, circule y suprima, serán utilizados para alguna de las siguientes finalidades:
- En relación con la naturaleza y las funciones propias de la Universidad Surcolombiana. El Tratamiento de los datos se realizará con la finalidad de obtener y generar datos históricos, estadísticas en cumplimiento a la naturaleza de las funciones de la Universidad Surcolombiana.
- En relación con el funcionamiento de la Universidad Surcolombiana
    - Recurso Humano:

  El Tratamiento de los datos se realizará para la vinculación, desempeño de funciones o prestación de servicios, retiro o terminación, (incluye, entre otros, funcionarios, contratistas, exfuncionarios, judicantes, practicantes y aspirantes a cargos).
    - Proveedores y Contratistas:

  El Tratamiento de los datos se realizará para los fines relacionados con el desarrollo el proceso de gestión contractual de productos o servicios que la entidad requiera para su funcionamiento de acuerdo a la normatividad vigente.
    - Seguridad en instalaciones de la Universidad Surcolombiana

  El Tratamiento se realizará para seguridad de las personas, los bienes e instalaciones de gobierno bajo la responsabilidad de la Universidad Surcolombiana.
    - Comunidad educativa

  El Tratamiento de los datos se realizará con la finalidad de acceder de servicios académicos, educativos y accesorios a estos, definidos en las normas de la educación superior.

- Datos sensibles:

  El Titular tiene derecho a optar por no suministrar cualquier información sensible solicitada por la Universidad Surcolombiana, relacionada, entre

otros, con datos sobre su origen racial o étnico, la pertenencia a sindicatos, organizaciones sociales o de derechos humanos, convicciones políticas, religiosas, de la vida sexual, biométricos o datos de salud.

- Datos de menores de edad:
  El suministro de los datos personales de menores de edad es facultativo y debe realizarse con autorización de los padres de familia o representantes legales del menor.
- Autorización del titular:
  Sin perjuicio de las excepciones previstas en la ley, en el Tratamiento de datos se requiere la autorización previa, expresa e informada del Titular, la cual deberá ser obtenida por cualquier medio que pueda ser objeto de consulta y verificación posterior.
- Casos en que no se requiere la autorización:
  La autorización del Titular no será necesaria cuando se trate de:
  - Información requerida por la Universidad Surcolombiana en ejercicio de sus funciones legales o por orden judicial.
  - Datos de naturaleza pública.
  - Casos de urgencia médica o sanitaria.
  - Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
  - Datos relacionados con el Registro Civil de las Personas.

7. DOCUMENTOS ASOCIADOS

Pueden ser consultados en el Sistema de Gestión de Calidad (SGC) - https://www.usco.edu.co/contenido/SGC-USCO/

8. RESPONSABLE DEL DOCUMENTO

Profesional de Gestión Responsable de Seguridad de la Información y Oficial de Protección de Datos Personales.

TÉRMINOS Y DEFINICIONES

Activo: Según [ISO/IEC 13335-12004]: Cualquier cosa que tiene valor para la organización. También se entiende por cualquier información o sistema relacionado con el tratamiento de la misma que tenga valor para la organización. Es todo activo que contiene información, la cual posee un valor y es necesaria para realizar los procesos misionales y operativos de la Entidad. Se pueden clasificar de la siguiente manera:

- **Datos:** Son todos aquellos elementos básicos de la información (en cualquier formato) que se generan, recogen, gestionan, transmiten y destruyen,
- **Aplicaciones:** Es todo el software que se utiliza para la gestión de la información.
- **Personal:** Es todo el personal, el personal subcontratado, los clientes, usuarios y en general, todos aquellos que tengan acceso de una manera u otra a los activos de información de la Universidad.
- **Servicios:** Son tanto los servicios internos, aquellos que una parte de la organización suministra a otra, como los externos, aquellos que la organización suministra a clientes y usuarios.
- **Tecnología:** Son todos los equipos utilizados para gestionar la información y las comunicaciones.
- **Instalaciones:** Son todos los lugares en los que se alojan los sistemas de información.
- **Equipamiento auxiliar:** Son todos aquellos activos que dan soporte a los sistemas de información y que no se hallan en ninguno de los tipos anteriormente definidos.

Administración de riesgos: Gestión de riesgos, es un enfoque estructurado para manejar la incertidumbre relativa a una amenaza, a través de una secuencia de actividades humanas que incluyen evaluación de riesgo, estrategias de desarrollo para manejarlo y mitigación del riesgo utilizando recursos gerenciales. Las estrategias incluyen transferir el riesgo a otra parte, evadir el riesgo, reducir los efectos negativos del riesgo y aceptar algunas o todas las consecuencias de un riesgo particular.

Administración de incidentes de seguridad: Procedimientos, estrategias y herramientas de control, enfocados a una correcta evaluación de las amenazas existentes, en este caso hacia toda la infraestructura de TI, se basa en un análisis continuo y mejorado del desempeño de todos los activos y recursos gerenciales que tiene la entidad.Su objetivo principal es atender y orientar las acciones inmediatas para solucionar cualquier situación que cause una interrupción de los diferentes servicios que presta la entidad, de manera rápida y eficaz

Alcance: Ámbito de la organización que queda sometido al Sistema de Gestión de Seguridad de la Información - SGSI. Debe incluir la identificación clara de las

dependencias, interfaces y límites con el entorno, sobre todo si sólo incluye una parte de la organización.

Alerta: Una notificación formal de que se ha producido un incidente relacionado con la seguridad de la información que puede evolucionar hasta convertirse en desastre.

Amenaza: Según [ISO/IEC 13335-1:2004): causa potencial de un incidente no deseado, el cual puede causar el daño a un sistema o la organización.

Análisis de riesgos: Según [ISO/IEC Guía 73:2002): Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Auditabilidad: Los activos de información deben tener controles que permitan su revisión. Permitir la reconstrucción, revisión y análisis de la secuencia de eventos.

Auditor: Persona encargada de verificar, de manera independiente, la calidad e integridad del trabajo que se ha realizado en un área particular.

Auditoria: Proceso planificado y sistemático en el cual un auditor obtiene evidencias objetivas que le permitan emitir un juicio informado sobre el estado y efectividad del SGSI de una organización.

Autenticación: Proceso que tiene por objetivo asegurar la identificación de una persona o sistema.

Características de la Información: las principales características desde enfoque de seguridad de información son: confidencialidad, disponibilidad e integridad.

Compromiso de la Dirección: Alineamiento firme de la Dirección de la organización con el establecimiento, implementación, operación, monitorización, revisión, mantenimiento y mejora del SGSI - Sistema de Gestión de la Seguridad de la Información.

Confiabilidad: Se puede definir como la capacidad de un producto de realizar su función de la manera prevista, De otra forma, la confiabilidad se puede definir también como la probabilidad en que un producto realizará su función prevista sin incidentes por un período de tiempo especificado y bajo condiciones indicadas.

Confidencialidad: Acceso a la información por parte únicamente de quienes estén autorizados, Según [ISO/IEC 13335-1:2004]:" característica/propiedad por la que la información no está disponible o revelada a individuos, entidades, o procesos no autorizados.

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

Control preventivo: Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

Declaración de aplicabilidad: Documento que enumera los controles aplicados por el SGSI de la organización -tras el resultado de los procesos de evaluación y tratamiento de riesgos- además de la justificación tanto de su selección como de la exclusión de controles incluidos en el anexo A de la norma.

Denegación de servicios: Acción iniciada por agentes externos (personas, grupos, organizaciones) con el objetivo de imposibilitar el acceso a los servicios y recursos de una organización durante un período indefinido de tiempo.

Desastre: Cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización durante el tiempo suficiente como para verse afectada de manera significativa.

Directiva: Según [ISO/IEC 13335-1: 2004): una descripción que clarifica qué debería ser hecho y cómo, con el propósito de alcanzar los objetivos establecidos en las políticas.

Disponibilidad: Según [ISO/IEC 13335-1: 2004): característica o propiedad de permanecer accesible y disponible para su uso cuando lo requiera una entidad autorizada.

Evaluación de riesgos: Según [ISO/IEC Guía 73:2002]: proceso de comparar el riesgo estimado contra un criterio de riesgo dado con el objeto de determinar la importancia del riesgo.

Evento: Según [ISO/IEC TR 18044:2004]: Suceso identificado en un sistema, servicio o estado de la red que indica una posible brecha en la política de seguridad y privacidad de la información o fallo de las salvaguardas, o una situación anterior desconocida que podría ser relevante para la seguridad.

Gestión de claves: Controles referidos a la gestión de claves criptográficas.

Gestión de riesgos: Proceso de identificación, control y minimización o eliminación, a un coste aceptable, de los riesgos que afecten a la información de la organización. Incluye la valoración de riesgos y el tratamiento de riesgos. Según [ISO/IEC Guía 73:2002]: actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Impacto: Resultado de un incidente de seguridad de la información.

Incidente: Según [ISO/IEC TR 18044:2004]: Evento único o serie de eventos de seguridad de la información inesperados o no deseados que poseen una

probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información.

Información: La información constituye un importante activo, esencial para las actividades de una organización y, en consecuencia, necesita una protección adecuada. La información puede existir de muchas maneras, es decir puede estar impresa o escrita en papel, puede estar almacenada electrónicamente, ser transmitida por correo o por medios electrónicos, se la puede mostrar en videos, o exponer oralmente en conversaciones.

Integridad: Mantenimiento de la exactitud y completitud de la información y sus métodos de proceso. Según [ISOIIEC 13335-1: 2004]: propiedad/característica de salvaguardar la exactitud y completitud de los activos.

Inventario de activos: Lista de todos aquellos recursos (físicos, de información, software, documentos, servicios, personas, reputación de la organización, etc.) dentro del alcance del SGSI, que tengan valor para la organización y necesiten por tanto ser protegidos de potenciales riesgos.

ISO: Organización Internacional de Normalización, con sede en Ginebra (Suiza). Es una agrupación de organizaciones nacionales de normalización cuyo objetivo es establecer, promocionar y gestionar estándares.

ISO 17799: Código de buenas prácticas en gestión de la seguridad de la información adoptado por ISO transcribiendo la primera parte de BS7799. A su vez, da lugar a ISO 27002 por cambio de nomenclatura el 1 de julio de 2007. No es certificable.

ISO 19011: "Guidelines for quality and/or environmental management systems auditing". Guía de utilidad para el desarrollo de las funciones de auditor interno para un SGSI.

ISO 27001: Estándar para sistemas de gestión de la seguridad de la información adoptado por ISO transcribiendo la segunda parte de BS 7799. Es certificable. Primera publicación en 2005, segunda publicación en 2013.

ISO 27002: Código de buenas prácticas en gestión de la seguridad de la información (transcripción de ISO 17799). No es certificable. Cambio oficial de nomenclatura de ISO 17799:20005 a ISO 27002:20005 el 1 de julio de 2007.

ISO 9000: Normas de gestión y garantía de calidad definidas por la ISO.

ISO/IEC TR 13335-3: "Information technology. Guidelines for the management of IT Security. Techniques for the management of IT Security." Guía de utilidad en la aplicación de metodologías de evaluación del riesgo.

ISO/IEC TR 18044: "Information technology. Security techniques. Information

security incident management". Guía de utilidad para la gestión de incidentes de seguridad de la información.

ITIL IT Infrastructure Library: Un marco de gestión de los servicios de tecnologías de la información.

Legalidad: El principio de legalidad o Primacía de la ley es un principio fundamental del Derecho público conforme al cual todo ejercicio del poder público debería estar sometido a la voluntad de la ley de su jurisdicción y no a la voluntad de las personas (ej. el Estado sometido a la constitución o al Imperio de la ley). Por esta razón se dice que el principio de legalidad establece la seguridad jurídica, Seguridad de Información, Seguridad informática y garantía de la información.

No conformidad: Situación aislada que, basada en evidencias objetivas, demuestra el incumplimiento de algún aspecto de un requerimiento de control que permita dudar de la adecuación de las medidas para preservar la confidencialidad, integridad o disponibilidad de información sensible, o representa un riesgo menor.

Plan de continuidad del negocio (Bussines Continuity Plan): Plan orientado a permitir la continuación de las principales funciones de la Entidad en el caso de un evento imprevisto que las ponga en peligro.

Plan de tratamiento de riesgos (Risk treatment plan): Documento de gestión que define las acciones para reducir, prevenir, transferir o asumir los riesgos de seguridad de la información inaceptables e implantar los controles necesarios para proteger la misma.

Política de seguridad: Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información. Según [ISO/IEC 27002:20005): intención y dirección general expresada formalmente por la Dirección.

Protección a la duplicidad: La protección de copia, también conocida como prevención de copia, es una medida técnica diseñada para prevenir la duplicación de información.

Riesgo: Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información. Según [ISO Guía 73:2002]: combinación de la probabilidad de un evento y sus consecuencias.

Seguridad de la información: Según [ISO/IEC 27002:20005]: Preservación de la confidencialidad, integridad y disponibilidad de la información; además, otras propiedades como autenticidad, responsabilidad, no repudio, trazabilidad y fiabilidad pueden ser también consideradas.

Selección de controles: Proceso de elección de los controles que aseguren la reducción de los riesgos a un nivel aceptable.

SGSI Sistema de Gestión de la Seguridad de la Información: Según [ISO/lEC 27001: 20005]: la parle de un sistema global de gestión que, basado en el análisis de riesgos, establece, implementa, opera, monitoriza, revisa, mantiene y mejora la seguridad de la información. (Nota: el sistema de gestión incluye una estructura de organización, políticas, planificación de actividades, responsabilidades, procedimientos, procesos y recursos.)

Servicios de tratamiento de información: Según [ISO/lEC 27002:20005]: cualquier sistema, servicio o infraestructura de tratamiento de información o ubicaciones físicas utilizados para su alojamiento.

Tratamiento de riesgos: Según [ISO/IEC Guía 73:2002]: Proceso de selección e implementación de medidas para modificar el riesgo.

Trazabilidad: Propiedad que garantiza que las acciones de una entidad se puede rastrear únicamente hasta dicha entidad.

Usuario: en el presente documento se emplea para referirse a directivos, funcionarios, contratistas, terceros y otros colaboradores de la Universidad Surcolombiana, debidamente autorizados para usar equipos, sistemas o aplicativos informáticos disponibles en la red de la Universidad Surcolombiana y a quienes se les otorga un nombre de usuario y una clave de acceso.

Valoración de riesgos: Según [ISO/lEC Guía 73:2002]: Proceso completo de análisis y evaluación de riesgos.

Virus: Programas informáticos de carácter malicioso, que buscan alterar el normal funcionamiento de una red de sistemas o computador personal, por lo general su acción es transparente al usuario y este tarda tiempo en descubrir su infección; buscan dañar, modificar o destruir archivos o datos almacenados.

Vulnerabilidad: Debilidad en la seguridad de la información de una organización que potencialmente permite que una amenaza afecte a un activo. Según [ISOIlEC 13335-1:2004]: debilidad de un activo o conjunto de activos que puede ser explotado por una amenaza.