UNIVERSIDAD SURCOLOMBIANA

.

MANUAL DE POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Control de Cambios

Versión	Fecha	Descripción	Elaboró	Vo Bo	Vo Bo
3.0	01/02/24	Versión Inicial	Martha Liliana Hermosa T. Nancy Catherine Molina S. Isabel Cristina Cleves R	German Andrés Sánchez Ortegón Asesor Seguridad de la Información	Erick Richard Rincón Cárdenas Asesor Privacidad de la Información

Contenido

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

1. OBJETIVO

El objetivo del presente documento es integrar todas las políticas de seguridad y privacidad de la información en un solo documento, con el fin de publicarlas a todos los funcionarios administrativos, docentes, estudiantes, contratistas y/o terceros de la Universidad Surcolombiana. Este manual de políticas se convertirá en la herramienta o canal de apropiación del Sistema de Gestión de Seguridad y Privacidad de la Información (SGSPI), a través de un proceso continuo de divulgación y concientización.

2. ALCANCE DE LAS POLÍTICAS DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Este Manual de Políticas de Seguridad y Privacidad de la Información es parte integral de todos los procesos de la Universidad Surcolombiana y es de obligatorio cumplimiento por parte de los funcionarios administrativos, docentes, estudiantes, contratistas y/o terceros.

3. TÉRMINOS Y DEFINICIONES DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

Los siguientes términos y definiciones están basados en los estándares NTC ISO IEC 27001 y NTC ISO IEC 27701 y son aplicables a la Universidad Surcolombiana y al Sistema de Gestión de Seguridad y Privacidad de la Información.

Política: es una declaración de las intenciones y dirección de una organización, como la expresa formalmente la alta dirección (véase la norma NTC ISO IEC 27000).

Aceptación de riesgo: decisión de asumir un riesgo.

Activo: cualquier elemento que represente valor para la organización.

Alta Dirección: se considera Alta Dirección a los directivos con cargo más alto en una organización; en el caso de la Universidad Surcolombiana se entiende como Alta Dirección a la integrada por el Consejo Superior, la Rectora, los Vicerrectores y los líderes de procesos.

Análisis de Riesgo: uso sistemático de la información para identificar fuentes y para estimar el riesgo.

4. CONDICIONES GENERALES

Marco de Políticas

El marco de políticas proporciona una estructura básica para gestionar la seguridad y privacidad de la información de manera efectiva y garantizar la protección de los activos de información y otros activos asociados, adaptado a las necesidades y contexto específico de la Universidad, considerando sus riesgos, recursos y requisitos legales y regulatorios.

La política de seguridad y privacidad de la información se sustenta en una variedad de

políticas específicas por temas relacionadas con aspectos de seguridad y privacidad de la información. Algunas de estas se presentan y describen en la NTC ISO IEC 27002.

Creación de Políticas

Las políticas de la Universidad Surcolombiana son creadas por los procesos responsables de las mismas, con el acompañamiento del proceso de Gestión de Seguridad de la Información.

Actualización de Políticas

Cualquier modificación a las políticas debe ser dirigida por los líderes de proceso, al Responsable de Seguridad de la Información y Oficial de Protección de datos personales.

Aprobación de Políticas

Las políticas de la Universidad son aprobadas por los líderes de proceso con base en las recomendaciones de las áreas técnicas responsables de los temas asociados y del Responsable de Seguridad de la Información y Oficial de Protección de datos personales quien posteriormente las presentará ante el Comité de Seguridad y Privacidad de la Información para su respectiva aprobación.

Nombre de las políticas

Se hará referencia a las políticas de seguridad y privacidad de la información relacionadas a los Anexos de la normas NTC IEC 27001 y NTC IEC 27701 y a todas aquellas que la Universidad necesite para lograr la eficacia del SGSPI.

Estructura de las Políticas

La estructura de las políticas de seguridad y privacidad de la información contiene los siguientes elementos:

- Título de la política
- Objetivo de la política
- Alcance de la política
- Definiciones
- Documentos de referencia
- Lineamientos
- Responsabilidades y autoridades
- Documentos relacionados y registros

5. POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

La política de seguridad y privacidad de la información de la Universidad describe la importancia estratégica del Sistema de Gestión de Seguridad y Privacidad de la Información, dirige y expresa cuáles son las necesidades de seguridad y privacidad de la información en el contexto real de la Universidad.

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

La Universidad establece como Política de seguridad y privacidad de la información el siguiente apartado:

"La alta dirección de la Universidad asume la responsabilidad de promover la protección y seguridad de la información de sus procesos garantizando la legalidad, confidencialidad, disponibilidad e integridad de los datos, promoviendo la gestión por procesos, la cultura y toma de conciencia en seguridad y privacidad de la información, estableciendo objetivos, controles y gestionando los riesgos a los que están expuestos los sistemas de información, garantizando su protección con el apoyo de tecnologías y prácticas humanas integras que contribuyan al cumplimiento de la misión institucional y la confianza de sus partes interesadas".

6. POLÍTICAS SOBRE CONTROLES ORGANIZACIONALES

6.1. Política de activos de la información

Dentro de las responsabilidades de la Universidad Surcolombiana se encuentra la custodia sobre todo tipo de información generada por la institución misma o sobre aquella que le ha sido entregada y que genere un impacto para la misma. Dado lo anterior, se establecen lineamientos enfocados en:

- Inventario de información y otros activos asociados
- Uso aceptable de la información y otros activos asociados
- Devolución de activos
- Clasificación de la información
- Etiquetado de la información

6.2. Política de transferencia de la información

Es de vital importancia la transmisión de información desde y hacia la Universidad, por tal razón se deben establecer ciertos parámetros que garanticen la confidencialidad e integridad de la información transmitida, se debe evitar el envío de información confidencial o sensible de la Universidad a personal externo, sin autorización previa. Se debe proteger la transferencia de información a través todo tipo de sistema de comunicaciones, en concordancia con la normatividad vigente. La transferencia estará regida bajo los criterios de:

- Transferencia electrónica
- Transferencia física
- Transferencia verbal

6.3. Política de control de acceso

Para la Universidad Surcolombiana debe ser prioritario definir el personal que va a tener acceso a información sensible, por lo cual debe limitar el acceso a las aplicaciones computarizadas a los funcionarios y demás personal tanto interno como externo que tengan que ver directamente con sus responsabilidades, obligaciones y funciones a cargo. Así

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

mismo es necesario restringir el acceso a las instalaciones donde dicha información se encuentra resguardada, garantizando así la confidencialidad e integridad de la misma.

La Universidad Surcolombiana establece lineamientos con respecto a:

- Control de acceso.
- Gestión de identidad.
- Información de autenticación.
- Derechos de acceso.
- Derechos de acceso privilegiados.
- Restricción del acceso a la información.
- Acceso al código fuente.
- Autenticación de seguridad.

6.4. Política de Seguridad de la información Proveedores

Los proveedores deben asegurar la confidencialidad e integridad de la información a la cual tengan acceso durante la permanencia con la Institución. Se deben aplicar lineamientos de seguridad y privacidad de la información pertinentes con cada proveedor que pueda acceder, procesar, almacenar, comunicar o suministrar información; dado lo anterior, se establecen lineamientos enfocados en:

- Seguridad de la información en las relaciones con los proveedores.
- Prohibiciones.
- Vulnerabilidades, eventos e incidentes de seguridad de información con Proveedores.
- Abordar la seguridad de la información dentro de los acuerdos con los proveedores.
- Gestión de la seguridad de la información en la cadena de suministro de las TIC.
- Seguimiento, revisión y gestión de cambios de los servicios de los proveedores.

6.5. Política seguridad la información para el uso de servicios en la Nube

La Universidad debe gestionar los procesos de adquisición, uso, gestión y salida de los servicios en la nube, estableciendo los requisitos de seguridad de la información de la Institución, para ello establece lineamientos enfocados en:

- Seguridad de la información para el uso de servicios en la nube.

6.6. Política de gestión de eventos e incidentes de seguridad y privacidad de la información

La Universidad Surcolombiana debe gestionar los incidentes de seguridad y privacidad de manera eficaz y eficiente, de tal forma que se disminuya el impacto que estos pudieran generar a la Institución. Debe establecer acciones que mitiguen el impacto asociado a los incidentes que se presentan, por tal razón se establecen los lineamientos para la gestión de los incidentes de seguridad de la información, incluyendo:

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

- Planificación y preparación de la gestión de incidentes de seguridad de la información.
- Evaluación y decisión sobre eventos de seguridad de la información
- Respuesta a los incidentes de seguridad de la información
- Aprendizaje de los incidentes de seguridad de la información
- Recopilación de evidencias
- Informes de eventos de seguridad de la información

6.7. Política de continuidad del negocio

La Universidad implementa un proceso de continuidad de negocio con la finalidad de mitigar el impacto de acciones como desastres naturales, accidentes, fallas de los equipos y acciones deliberadas de terceros en los cuales la Universidad Surcolombiana no tiene injerencia directa, pero establece acciones para poder recuperarse rápidamente y que su operación no se vea comprometida.

La Universidad determina sus requisitos para la seguridad y privacidad de la información y la continuidad de la gestión de la seguridad de la información en situaciones adversas, y establece lineamientos enfocados en:

- Seguridad de la información durante la interrupción
- Preparación de las TIC para la continuidad del negocio
- Redundancia de las instalaciones de procesamiento de información

6.8. Política de derechos de propiedad intelectual

La Universidad Surcolombiana regula las relaciones que en materia de propiedad intelectual se desarrollen entre esta y sus docentes, investigadores, estudiantes, empleados administrativos, contratistas, y en general sus servidores; así como derechos reservados sobre los contenidos publicados en el sitio web institucional, licencias de software y las actividades de carácter académico, laboral o contractual que tengan por objeto la creación de obras intelectuales protegibles por los derechos asociados a la propiedad intelectual.

- Política derechos de propiedad intelectual

6.9. Política de tratamiento de la información de datos personales

La Universidad Surcolombiana asegura la privacidad y la protección de la información de datos personales, como se exige en la ley 1581de 2012, el decreto 1377 de 2013 y la demás normatividad aplicable. Establece lineamientos enfocados en:

- Tratamiento de datos personales
- Finalidad del tratamiento y de la recolección de los datos personales.
- Autorización
- Información sobre el tratamiento de los datos
- Derechos de los titulares de la información
- Deberes de la Universidad
- Procedimiento para la atención de consultas, reclamos y peticiones
- Rectificación, actualización y supresión de datos personales
- Registro nacional de bases de datos personales

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

- Medidas de seguridad de la información
- Designación
- Disposiciones generales para la protección de datos personales

7. POLÍTICA SOBRE CONTROLES DE PERSONAS

7.1. Política Controles de Personas

Es de vital importancia concientizar a los funcionarios administrativos, docentes, estudiantes, contratistas y/o terceros de la Universidad Surcolombiana sobre la necesidad de generar las condiciones propicias para garantizar la confidencialidad, integridad y disponibilidad de la información, por tal razón se deberán tener en cuenta los lineamientos enfocados en:

- Selección
- Términos y condiciones de empleo
- Conciencia de seguridad de la información, educación y formación
- Proceso disciplinario
- Responsabilidades después de la terminación o cambio de empleo
- Acuerdos de confidencialidad o no divulgación
- Informes de eventos de seguridad de la información

7.2. Trabajo remoto

La Universidad implementa medidas de seguridad cuando el personal trabaja de forma remota para proteger la información a la que se accede, procesa o almacena fuera de las instalaciones de la institución para ello define lineamientos referentes a:

- Trabajo remoto

8. POLÍTICA SOBRE CONTROLES FÍSICOS

8.1. Política de controles físicos

La seguridad física y del entorno protege la información que se custodia o se procesa dentro de la Universidad y permite disminuir el acceso no autorizado de personas con la intención de alterar o modificar la información.

Para evitar el acceso no autorizado a ciertos espacios considerados como críticos se deben tener perímetros de seguridad para proteger áreas que contengan información confidencial y/o sensible, por medio de los controles de acceso físico, siendo estos definidos así:

- Perímetros de seguridad física
- Entrada física a las instalaciones de la Universidad Surcolombiana
- Protección de oficinas, salas e instalaciones
- Monitoreo de la seguridad física

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722

- Protección contra las amenazas físicas y ambientales
- Trabajo en zonas seguras
- Escritorio limpio y pantalla limpia
- Ubicación y protección de equipos
- Seguridad de los activos fuera de las instalaciones
- Medios de almacenamiento
- Servicios públicos de apoyo
- Seguridad del cableado
- Mantenimiento del equipo
- Disposición o reutilización segura de los equipos

9. POLÍTICAS SOBRE CONTROLES TECNOLÓGICOS

9.1. Política de criptografía y gestión de claves

Con el fin de garantizar la confidencialidad e integridad de algunos documentos designados como sensibles, la Universidad debe utilizar sistemas y técnicas criptográficas para la protección de la información, que cumplan con la reglamentación y estándares aplicables en la legislación colombiana. Establece lineamientos enfocados en:

- Directrices de uso de cifrado
- Métodos de protección de llaves
- Gestión de claves

9.2. Política de seguridad en las redes

El acceso a las redes de la Universidad Surcolombiana debe estar limitado a los servidores públicos de la entidad y demás personas autorizadas por la misma por medio de claves de acceso a los sistemas de información, con la finalidad de disminuir el acceso no autorizado de personal ajeno a la entidad. Establece lineamientos enfocados en:

- Seguridad en las redes
- Seguridad de los servicios de red
- Segregación de redes

9.3. Política de desarrollo seguro

Se deben aplicar reglas para el desarrollo de software y de sistemas, a los desarrolladores ya sea dentro de la Institución o externos. Establece lineamientos enfocados en:

- Arquitectura
- Planificación, análisis y diseño de sistemas de información
- Desarrollo y despliegue
- Desarrollo tercerizado

Sede Central / Av. Pastrana Borrero - Cra. 1
Sede Administrativa / Cra. 5 No. 23 - 40
www.usco.edu.co / Neiva - Huila
PBX: 875 4753
PBX: 875 3686
Línea Gratuita Nacional: 018000 968722