1. OBJETIVO

Definir las directrices para:

a) Asegurar la seguridad y privacidad en el uso de los servicios de red.
b) Proteger la información de las redes y sus instalaciones de procesamiento de información de apoyo frente a riesgos a través de la red.
c) Dividir la red en límites de seguridad y privacidad y controlar el tráfico entre ellos en función de las necesidades de la Universidad.

2. ALCANCE

Las presentes directrices aplican a todos los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros de la Universidad Surcolombiana.

3. DEFINICIONES

Red: Es un conjunto de dispositivos (de red) interconectados físicamente (ya sea vía alámbrica o vía inalámbrica) que comparten recursos y que se comunican entre sí a través de reglas (protocolos) de comunicación

4. MARCO DE REFERENCIA

La gestión de riesgos y oportunidades en la Universidad Surcolombiana considera para su labor, los lineamientos definidos en las directrices y políticas institucionales, además de las consideraciones definidas en:

- La norma ISO 31000:2018– Gestión del riesgo. Principios y directrices.
- La norma ISO IEC 27005:2022 – Gestión de riesgos para la seguridad de la información.
- Los lineamientos definidos en los documentos del Sistema de Gestión de Seguridad y Privacidad de la Información.

- Los requisitos aplicables a la gestión del riesgo, detallados en el estándar ISO IEC 27001:2022 y la ISO IEC 27701:2025
- Código de Práctica para Controles de Seguridad de la Información - GTC ISO IEC 27002:2022 Tecnología de la Información. Técnicas de Seguridad.
- Modelo de Seguridad y Privacidad de la Información, Ministerio de Tecnologías y Sistemas de Información.
- Guía de Administración de riesgos y el diseño de controles en entidades públicas
- CONPES de Seguridad Digital (CONPES 3854 de 2016 y actualizaciones)
- Modelo de Seguridad y Privacidad de la Información – MSPI (MinTIC)
- Política de Gobierno Digital (Decreto 1078 de 2015 y actualizaciones)
- Modelo Integrado de Planeación y Gestión – MIPG (DAFP)
- FURAG (Formulario Único de Reporte de Avance de la Gestión)
- Ley 1581 de 2012 y Decreto 1377 de 2013
- Lineamientos y guías de la Superintendencia de Industria y Comercio.

5. GENERALIDADES

Estas directrices son la declaración general que establece la Universidad para la administración de las redes, seguridad, privacidad y servicios, con base en los siguientes controles de acuerdo a la norma:

ISO/IEC 27001:2022

A.8.20 Seguridad y privacidad de las redes
A.8.21 Seguridad y privacidad de los servicios de red
A.8.22 Segregación de redes

6. DIRECTRICES

El Centro de Información, Tecnología y Gestión Documental debe 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.

6.1. SEGURIDAD Y PRIVACIDAD DE LAS REDES

El Centro de Información, Tecnologías y Gestión Documental implementa controles para garantizar la seguridad y privacidad de la información en las redes y proteger los servicios conectados del acceso no autorizado, considerando los siguientes factores:

a) el tipo y el nivel de clasificación de la información que se transmite a través de la red;

b) establecer responsabilidades y procedimientos para la gestión de equipos y dispositivos de red;

c) mantener documentación actualizada, incluidos diagramas de red y archivos de configuración de dispositivos (por ejemplo, switches, controladores de wifi);

d) Separar la responsabilidad operativa de las redes de las operaciones de los sistemas de TIC;

e) establecer controles para salvaguardar la confidencialidad e integridad de los datos que pasan a través de redes públicas o redes inalámbricas y proteger los sistemas y aplicaciones conectados, a través del firewall de red y de código (F5), token, VPN entre otros;

f) mantener la disponibilidad de los servicios de red y de los computadores conectados a la red;

g) monitoreo, registro y supervisión adecuados para permitir la detección de acciones que puedan afectar o sean relevantes para la seguridad y privacidad de la información;

h) coordinar las actividades de gestión de la red para optimizar el servicio a la Institución al igual que asegurar que los controles se aplican de forma coherente en toda la infraestructura de procesamiento de la información;

i) restringir y filtrar la conexión de los sistemas a la red mediante firewalls y

sistemas de detección de intrusiones;

j) detectar, restringir y autenticar la conexión de equipos y dispositivos a la red;

k) separar los canales de administración de red de otro tráfico de red;

l) aislar temporalmente subredes críticas si la red está siendo atacada;

m) desactivar los protocolos de red vulnerables;

n) aplicar controles de seguridad y privacidad adecuados al uso de redes virtualizadas.

6.2. SEGURIDAD Y PRIVACIDAD DE LOS SERVICIOS DE RED

La Universidad identifica y verifica que los proveedores de servicios de la red implementen las medidas de seguridad y privacidad necesarias para determinados servicios, como las características de seguridad, los niveles de servicio y los requisitos de servicio, tales como:

a) las redes y los servicios de red a los que se puede acceder;

b) requisitos de autenticación para acceder a diversos servicios de red;

c) procedimientos de autorización para determinar quién puede acceder a qué redes y servicios en red;

d) gestión de redes y controles y procedimientos tecnológicos para proteger el acceso a las conexiones de red y a los servicios de red;

e) Los medios utilizados para acceder a las redes y los servicios de red, el uso de la red privada virtual (VPN) o la red inalámbrica;

f) monitoreo del uso de los servicios de red;

g) el derecho a la auditoría;

h) procedimientos para el uso del servicio de red para restringir el acceso a servicios o aplicaciones de red, cuando sea necesario.

6.3. SEGREGACIÓN DE REDES

El dominio oficial de la Universidad Surcolombiana es **usco.edu.co**

El Centro de Información, Tecnologías y Control Documental debe segmentar la red, de modo que permita separar los grupos de servicios de información, en función de los niveles de confianza, criticidad y sensibilidad

Todo cambio a la infraestructura de redes deberá estar controlado y será realizado de acuerdo con los procedimientos de AP-TIC-PR-04 ADMINISTRACIÓN REDES DE DATOS, AP-TIC-PR-05 DISEÑO IMPLEMENTACIÓN NUEVA RED DE DATOS.

7. RESPONSABILIDADES Y AUTORIDADES

El Centro de Información, Tecnología y Gestión Documental debe 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

Los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros deben cumplir con la política y directrices de seguridad y privacidad de la información definidas por la Universidad Surcolombiana; así mismo, deben reportar a los propietarios de la información y otros activos asociados las violaciones a la política, directrices y/o cualquier inconsistencia o irregularidad que pueda ser generada por los usuarios.

Los líderes de procesos y propietarios de la información y otros activos de la información deben revisar periódicamente los riesgos que se identifiquen sobre el uso inadecuado de los activos.

8. DOCUMENTOS RELACIONADOS Y REGISTROS

AP-TIC-PR-04 ADMINISTRACIÓN REDES DE DATOS
AP-TIC-PR-05 DISEÑO E IMPLEMENTACIÓN DE NUEVAS REDES DE DATOS
GUÍA PARA CONFIGURACIÓN DE ACCESO POR VPN

CONTROL DE CAMBIO		
VERSIÓN	DOCUMENTO Y FECHA DE APROBACIÓN	DESCRIPCIÓN DE CAMBIO
01	EV-CAL-FO-17 del 1 de septiembre de 2026	Creación documento

ELABORÓ	REVISÓ	APROBÓ
MARTHA LILIANA HERMOSA TRUJILLO Gestión Seguridad y Privacidad de la Información **Elaboró** DIEGO ANDRES CARVAJAL RUIZ Director Centro de Tecnología Información y Control Documental **Aprobó**	ALVARO TORRENTE LÓPEZ Profesional de apoyo SGC	MAYRA ALEJANDRA BERMEO Coordinador SGC