

	UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE INFORMACIÓN TECNOLOGÍAS Y CONTROL DOCUMENTAL					   	
	DIRECTRICES PARA LA CRIPTOGRAFIA Y GESTIÓN DE CLAVES						
CÓDIGO	AP-TIC-DR-03	VERSIÓN	1	VIGENCIA	2026	Página	1 de 5

1. OBJETIVO

Asegurar el uso adecuado y efectivo del cifrado para proteger la confidencialidad, autenticidad e integridad de la información de acuerdo con los requisitos de seguridad y privacidad de la información de la Universidad y tomando en consideración los requisitos legales, estatutarios, reglamentarios y contractuales relacionados con el cifrado.

2. ALCANCE

Las presentes directrices aplican a todos los funcionarios administrativos, docentes, estudiantes, contratistas y/o terceros de la Universidad Surcolombiana, que por la naturaleza de sus funciones requieren uso de alguna técnica de protección de información mediante controles criptográficos o llaves criptográficas en la institución.

3. DEFINICIONES

Criptografía: práctica de proteger información mediante algoritmos que transforman datos legibles (texto plano) en un formato ilegible (texto cifrado) y viceversa, utilizando claves secretas. Su objetivo principal es garantizar la confidencialidad, integridad, autenticación y no repudio de la información.

Gestión de claves proceso de generar, almacenar, distribuir y proteger claves criptográficas para garantizar la seguridad de los datos cifrados.

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

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.

	UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE INFORMACIÓN TECNOLOGÍAS Y CONTROL DOCUMENTAL						
	DIRECTRICES PARA LA CRIPTOGRAFIA Y GESTIÓN DE CLAVES					Página	2 de 5
CÓDIGO	AP-TIC-DR-03	VERSIÓN	1	VIGENCIA	2026		

- 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

La Universidad Surcolombiana define directrices para proteger la confidencialidad, autenticidad e integridad de la información pertinente con base en los siguientes controles de acuerdo a las normas:

ISO/IEC 27001:2022

A.8.24 Uso de cifrado

ISO/IEC 27701:2025

A.3.26 Uso de criptografía

6. DIRECTRICES

Estas directrices describen las consideraciones generales para asegurar el uso apropiado y eficaz de la criptografía con la finalidad de proteger la confidencialidad, autenticidad e integridad de la información de la Universidad Surcolombiana.

El cifrado, debe tener en cuenta lo siguiente:

- a) el uso del cifrado para maximizar los beneficios y minimizar los riesgos de utilizar técnicas de cifrado y evitar un uso inapropiado o incorrecto de la

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.

	UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE INFORMACIÓN TECNOLOGÍAS Y CONTROL DOCUMENTAL					   	
	DIRECTRICES PARA LA CRIPTOGRAFIA Y GESTIÓN DE CLAVES						
CÓDIGO	AP-TIC-DR-03	VERSIÓN	1	VIGENCIA	2026	Página	3 de 5

información;

- b) identificar el nivel de protección requerido y la clasificación de la información y, en consecuencia, establecer el tipo, la fuerza y la calidad de los algoritmos cifrados necesarios;
- c) el uso del cifrado para la protección de la información contenida en dispositivos finales de usuario móvil o medios de almacenamiento y transmitida a través de redes a dichos dispositivos o medios de almacenamiento;
- d) el enfoque de la gestión de claves, incluidos los métodos para tratar la generación y protección de claves cifradas y la recuperación de información cifrada en caso de pérdida, compromiso o daño de claves;
- e) la implementación de las reglas para el uso efectivo del cifrado, la gestión de claves, incluida la generación de las mismas
- f) los estándares que se van a adoptar, así como los algoritmos cifrados, la fuerza del cifrado, las soluciones cifradas y las prácticas de uso aprobadas o requeridas para su uso en la Institución;
- g) el impacto del uso de información cifrada en controles que dependen de la inspección de contenido

Al implementar las reglas institucionales para el uso efectivo del cifrado, se tienen en cuenta las regulaciones y restricciones nacionales que pueden aplicarse al uso de técnicas de cifrado en diferentes partes del mundo, así como los temas del flujo transfronterizo de información cifrada

El contenido de los acuerdos de nivel de servicio o contratos con proveedores externos de servicios cifrados debe abarcar cuestiones de responsabilidad, fiabilidad de los servicios y tiempos de respuesta para la prestación de servicios.

5.1 GESTIÓN DE CLAVES

La gestión adecuada de claves requiere procesos seguros para generar, almacenar, archivar, recuperar, distribuir, retirar y destruir claves cifradas.

	UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE INFORMACIÓN TECNOLOGÍAS Y CONTROL DOCUMENTAL					 SC 7384-1SA-CER 987628DS-CER 987655		
	DIRECTRICES PARA LA CRIPTOGRAFIA Y GESTIÓN DE CLAVES							
	CÓDIGO	AP-TIC-DR-03	VERSIÓN	1	VIGENCIA	2026	Página	4 de 5

Un sistema de gestión de claves debe basarse en un conjunto acordado de normas, procedimientos y métodos seguros para:

- a) generar claves para diferentes sistemas de cifrado y diferentes aplicaciones;
- b) emitir y obtener certificados de clave pública;
- c) distribuir claves a las entidades previstas, incluido cómo activar las claves cuando se reciben;
- d) almacenamiento de claves, incluida la forma en que los usuarios autorizados obtienen acceso a ellas;
- e) cambiar o actualizar claves, incluidas las reglas sobre cuándo cambiar claves y cómo se hará esto;
- f) tratar con claves comprometidas;
- g) revocación de claves, incluido cómo retirar o desactivar claves;
- h) recuperar claves que se pierden o están dañadas;
- i) copia de seguridad o archivado de claves;
- j) destruir claves;
- k) registro y auditoría de actividades relacionadas con la gestión de claves;
- l) establecer las fechas de activación y desactivación de las claves para que solo se puedan utilizar durante el período de tiempo de acuerdo con las reglas institucionales sobre la gestión de claves;
- m) gestionar solicitudes legales de acceso a claves cifradas

Todas las claves cifradas deben estar protegidas contra modificaciones y pérdidas. Además, las claves secretas y privadas necesitan protección contra el uso no autorizado, así como la divulgación. El equipo utilizado para generar, almacenar y archivar claves debe estar físicamente protegido.

	UNIVERSIDAD SURCOLOMBIANA GESTIÓN DE INFORMACIÓN TECNOLOGÍAS Y CONTROL DOCUMENTAL					   	
	DIRECTRICES PARA LA CRIPTOGRAFIA Y GESTIÓN DE CLAVES						
CÓDIGO	AP-TIC-DR-03	VERSIÓN	1	VIGENCIA	2026	Página	5 de 5

6. RESPONSABILIDADES Y AUTORIDADES

Los funcionarios administrativos, docentes, estudiantes, pasantes, judicantes, contratistas y/o terceros deben cumplir con las políticas 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 presente 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.

7. DOCUMENTOS RELACIONADOS Y REGISTROS

MANUAL DE CIFRADO DE ARCHIVOS CON CLEOPATRA
INSTALACIÓN CERTIFICADO DIGITAL SSL EN APACHE

CONTROL DE CAMBIO		
VERSIÓN	DOCUMENTO Y FECHA DE APROBACIÓN	DESCRIPCION 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

Vigilada Mineducación

La versión vigente y controlada de este documento, solo podrá ser consultada a través del sitio web Institucional www.usco.edu.co, link Sistema Gestión de Calidad. La copia o impresión diferente a la publicada, será considerada como documento no controlado y su uso indebido no es de responsabilidad de la Universidad Surcolombiana.