PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN – UNIVERSIDAD COLEGIO MAYOR DE CUNDINAMARCA

2026

1. INTRODUCCIÓN

En el contexto de la transformación digital y el uso intensivo de tecnologías de la información, la seguridad de la información y la protección de la privacidad se han consolidado como elementos estratégicos para las entidades del sector público. En Colombia, estos aspectos adquieren especial relevancia debido a la necesidad de cumplir estrictamente el marco normativo vigente y de preservar la confianza de la ciudadanía en la gestión estatal. En este sentido, el presente Plan de Seguridad y Privacidad de la Información define un conjunto de lineamientos, mecanismos y acciones orientadas a salvaguardar la confidencialidad, integridad y disponibilidad de los activos de información, en concordancia con las disposiciones legales y regulatorias aplicables en materia de ciberseguridad y protección de datos personales.

Las actividades propias de las entidades públicas implican el tratamiento permanente de información sensible y reservada, cuyo uso indebido, pérdida o alteración podría generar afectaciones significativas a los derechos de los ciudadanos, a la credibilidad institucional y al normal desarrollo de la función pública. Por ello, este plan trasciende el simple cumplimiento normativo y se concibe como una herramienta para consolidar una cultura organizacional orientada a la gestión responsable de la información y al respeto por la privacidad.

A lo largo de este documento se describen las acciones y medidas que permitirán a la Universidad Colegio Mayor de Cundinamarca anticiparse, identificar y responder de manera oportuna a los riesgos y amenazas que puedan comprometer la seguridad de la información. De igual forma, se promueve el tratamiento ético y adecuado de los datos personales, en armonía con los principios de legalidad, transparencia, responsabilidad demostrada y garantía de los derechos de los titulares.

La adopción e implementación de este plan reafirma el compromiso institucional con la protección de la información y los datos personales, asegurando que los procesos, sistemas y servicios estén diseñados para mitigar riesgos cibernéticos, dar cumplimiento a la legislación vigente y fortalecer la confianza de los ciudadanos que interactúan con la entidad.

2. OBJETIVO

Definir las actividades para incrementar el nivel de madurez de seguridad y privacidad de la Información en la Universidad Colegio Mayor de Cundinamarca para la vigencia 2026, el estándar internacional ISO/IEC 27001:2022, estrategias de Gobierno Digital, MIPG, requerimientos de la entidad y disposiciones legales vigentes; con el fin de garantizar la confidencialidad, disponibilidad, integridad y privacidad de los activos de información del Ministerio.

3. OBJETIVOS ESPECÍFICOS

- Establecer y divulgar las actividades para el fortalecimiento de la seguridad y privacidad de la información en la entidad.
- Incrementar el nivel de madurez de la Universidad frente a la gestión de la seguridad y privacidad de la información.
- Fortalecer y optimizar la gestión de seguridad y privacidad de la información en la Universidad.
- Gestionar los riesgos de seguridad y privacidad de la información, seguridad digital, ciberseguridad y continuidad del negocio que puedan afectar la integridad, confidencialidad, disponibilidad y privacidad de la información.
- Asegurar la protección de los activos de información de la Entidad, a través de la identificación, clasificación y/o actualización de los activos de información y sus riesgos asociados
- Gestionar de manera oportuna los eventos e incidentes de seguridad de la información que pongan en riesgo la integridad, confidencialidad, disponibilidad y privacidad, reduciendo su impacto y propagación.
- Fortalecer la cultura, el conocimiento y las habilidades de los colaboradores en los temas de seguridad y privacidad de la información en la Universidad.

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información de la Universidad, comprende la implementación del Sistema de Gestión de Seguridad de la Información en sus fases del modelo de mejora continua (Planear, Hacer, Verificar y Actuar) aplicable a los procesos institucionales, y a todos los usuarios internos, externos, proveedores y a la ciudadanía en general, mediante la implementación de una estrategia integral de seguridad de la información que parta desde las políticas, prácticas y aborde toda la cadena de valor, en torno a los objetivos estratégicos de la institución, con el fin de diagnosticar, planear e implementar de manera coordinada acciones que sean pertinentes para que la universidad cuente con un escenario donde se apliquen buenas prácticas en materia de seguridad

de la información, que conlleven a la seguridad de los sistemas, los procesos, las personas que los ejecutan y los datos, bajo el propósito de reducir las vulnerabilidades a las que se encuentran expuestos los activos de información institucionales.

5. MARCO NORMATIVO

Marco Normativo	Descripción
Ley Estatutaria 1266 de 2008	Por la cual se dictan las disposiciones generales del hábeas data y se regula el manejo de la información contenida en bases de datos personales.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos.
Ley 2012 Estatutaria 1581 de	Por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 2609 de 2012	Por el cual se reglamenta el Título V de la Ley 594 de 2000 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado".
Decreto 1377 de 2013	Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Ley 1712 de 2014	Por medio de la cual se crea la Ley de Transparencia ydel derecho de acceso a la Información pública nacional y se dictan otras disposiciones
Decreto 2573 de 2014	Por el cual se establecen los lineamientos generales de la Estrategia de Gobierno en línea, se reglamenta parcialmente la Ley 1341 de 2009 y se dictan otras disposiciones.
Decreto 103 de 2015	Por el cual se reglamenta parcialmente la Ley 1712 de2014 y se dictan otras disposiciones
Decreto 1078 de 2015	Modificado por el Decreto 1008 de 2018 - Política de Gobierno Digital que contiene el Modelo de seguridad y Privacidad - MSPI de MINTIC.
CONPES 3854 de 2016	Política de Seguridad Digital del Estado Colombiano
Decreto 1499 de 2017	El cual modificó el Decreto 1083 de 2015 – Modelo Integrado de Planeación y Gestión.
Ley 1928 de 2018	Por medio de la cual se aprueba el “Convenio sobre La Ciberdelincuencia”, adoptado el 23 de noviembre de 2001, en Budapest
CONPES 3995 de 2020	Política Nacional De Confianza y Seguridad Digital
Resolución 1519 de 2020	Por la cual se definen los estándares y directrices para publicar la información señalada en la Ley 1712 del 2014 y se definen los requisitos Materia de acceso a la Información pública, accesibilidad web, seguridad digital, y datos abiertos.
Resolución 746 de 2022	Por la cual se fortalece el Modelo de Seguridad y Privacidad de la Información y se definen lineamientos adicionales a los establecidos en la Resolución 500 de 2021.
Resolución 02277 de 2025	Por la cual se actualiza el Anexo 1 de la Resolución 500 de 2021 y se derogan otras disposiciones relacionadas con la materia

6. DESARROLLO DEL PLAN DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

ACTIVIDAD HITO	ACTIVIDADES	PRODUCTO	RESPONSABLE	FECHA
Mantenimiento al Modelo de Seguridad y Privacidad de la Información	Elaborar la Declaración de Aplicabilidad del nuevo MSPI	Declaración de Aplicabilidad en SIAC	Oficial de seguridad de la información	Abril 2026
	Actualizar el Manual de Políticas de Seguridad de la Información	Documento del Manual actualizado en el SIAC	Oficial de seguridad de la información	Agosto 2026
	Socializar el Manual de Políticas de Seguridad de la Información	Asistencia de la Socialización	Oficial de seguridad de la información	Octubre 2026
Gestión de vulnerabilidades técnicas de la plataforma tecnológica	Elaborar la programación de los análisis de vulnerabilidades para el primer semestre	Cronograma de los análisis de vulnerabilidades	Oficial de seguridad de la información	Marzo 2026
	Mitigar vulnerabilidades encontradas durante el primer semestre	Informe de Gestión de Vulnerabilidades	Oficial de seguridad de la información	Junio 2026
	Elaborar la programación de los análisis de vulnerabilidades para el segundo semestre	Cronograma de los análisis de vulnerabilidades	Oficial de seguridad de la información	Julio 2026
	Mitigar vulnerabilidades encontradas durante el segundo semestre	Informe de Gestión de Vulnerabilidades	Oficial de seguridad de la información	Diciembre 2026
Mantenimiento del Programa de Protección de Datos Personales	Actualizar Manual Interno de Políticas y Procedimientos de Datos Personales	Documento del Manual actualizado en el SIAC	Oficial de seguridad de la información	Agosto 2026
	Socializar el Manual Interno de Políticas y Procedimientos de Datos Personales	Asistencia de la Socialización	Oficial de seguridad de la información	Octubre 2026
Plan de Capacitaciones de Seguridad y Privacidad de la Información	Elaborar plan anual de capacitaciones de seguridad y privacidad de la información	Plan de capacitaciones aprobado	Oficial de seguridad de la información	Febrero 2026
	Ejecutar el plan de capacitaciones de seguridad y privacidad de la información	Soportes de las sesiones de capacitación	Oficial de seguridad de la información	Marzo 2026 a Diciembre 2026