

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



2025

1. INTRODUCCIÓN

En el entorno digital actual, la protección de la información y la privacidad se han convertido en aspectos fundamentales para las entidades públicas, especialmente en un país como Colombia, donde el cumplimiento normativo y la confianza de los ciudadanos son pilares esenciales de la gestión pública. Este **Plan de Seguridad y Privacidad de la Información** tiene como propósito establecer las directrices, estrategias y acciones necesarias para garantizar la protección de la confidencialidad, integridad y disponibilidad de los activos de información conforme a las normativas aplicables vinculantes relacionadas con ciberseguridad y privacidad del marco normativo colombiano

La naturaleza de las funciones que desempeñan las entidades públicas implica la gestión de datos sensibles y confidenciales que, de ser comprometidos, podrían impactar negativamente la confianza pública, la integridad institucional y los derechos fundamentales de los ciudadanos. Por esta razón, este plan no solo busca cumplir con las obligaciones legales, sino también fortalecer la cultura institucional en torno a la seguridad de la información y la privacidad.

En este documento se detallan las actividades que permitirán a la Universidad Colegio Mayor de Cundinamarca prevenir, detectar y responder eficazmente a las amenazas que puedan afectar la confidencialidad, integridad y disponibilidad de la información. Adicionalmente, este plan promueve una gestión responsable y ética de los datos personales, alineada con los principios de transparencia, responsabilidad proactiva y respeto a los derechos de los titulares.

Con la implementación de este plan, nuestra entidad reafirma su compromiso con la protección de la información, garantizando que los procesos y sistemas estén diseñados para resistir riesgos cibernéticos, cumplir con la legislación vigente y preservar la confianza de los ciudadanos que dependen de nuestros servicios.

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 2025, 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 UNICOLMAYOR 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 entidad.
- 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 UNICOLMAYOR.
-

4. ALCANCE

El Plan de Seguridad y Privacidad de la Información de la UNICOLMAYOR, 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 y del 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 de 2014 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 500 de 2021	Por la cual se establecen los lineamientos y estándares para la estrategia de seguridad digital y se adopta el modelo de seguridad y privacidad como habilitador de la política de Gobierno Digital.
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.

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

ACTIVIDAD HITO	ACTIVIDADES	PRODUCTO	RESPONSABLE	FECHA
Transición a la nueva norma ISO 27001:2022 y preparación para la certificación	Elaborar y socializar del plan de trabajo para la transición de la Norma ISO-IEC 27001:2022.	Plan de trabajo aprobado y socializado	Oficial de seguridad de la información	Marzo 2025
	Planear y aprobar los cambios en el SGSI conforme a lo establecido en el SIG	Documento con la planeación de los cambios aprobado	Oficial de seguridad de la información	Mayo 2025
	Implementar el plan de trabajo para la transición de la Norma ISO-IEC 27001:2022.	Seguimientos a la implementación del plan de trabajo	Oficial de seguridad de la información Todos los procesos	Diciembre 2025
Consultoría de Ingeniería Social y Transferencia de Conocimiento en Seguridad de la Información	Elaborar y radicar estudio de necesidad de contratación previa aprobación presupuestal para el proyecto	Estudio de necesidad radicado	Oficial de seguridad de la información	Abril 2025
	Ejecución Contrato de Consultoría en Ingeniería Social y Capacitación en Seguridad de la Información	Acta de finalización del contrato	Oficial de seguridad de la información	Septiembre 2025
	Elaborar el Plan de mejoramiento a partir de las recomendaciones entregadas por la consultoría	Plan de implementación de las recomendaciones de la consultoría	Oficial de seguridad de la información	Noviembre 2025

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	Febrero 2025
	Mitigar vulnerabilidades encontradas durante el primer semestre	Informe de Gestión de Vulnerabilidades	Oficial de seguridad de la información	Junio 2025
	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 2025
	Mitigar vulnerabilidades encontradas durante el segundo semestre	Informe de Gestión de Vulnerabilidades	Oficial de seguridad de la información	Diciembre 2025
Mantenimiento del Programa de Protección de Datos Personales	Actualizar inventario de bases de datos personales y sus finalidades	Inventario actualizado de las bases de datos con información personal	Oficial de seguridad de la información	Mayo 2025
	Elaborar y Socializar Procedimiento de Gestión de Datos Personales	Procedimiento publicado en el SIG	Oficial de seguridad de la información	Junio 2025
	Actualizar la Política de Tratamiento de la Información (PTI)	PTI Actualizada	Oficial de seguridad de la información	Septiembre 2025
	Cumplir con el calendario de actualizaciones y reportes de novedades en el Registro nacional de Bases de Datos (RNBD)	Radicados de actualizaciones en el Registro Nacional de Bases de Datos (RNBD)	Oficial de seguridad de la información	Diciembre 2025