



**Institución
Universitaria
Digital de
Antioquia**

digitalidad próxima

Plan de Seguridad y Privacidad de la Información

**Institución Universitaria Digital de Antioquia
Dirección de Tecnología
2026**

www.iudigital.edu.co

ORD No 74 de 2017 • Vigilada MinEducación

Historial de cambios

Versión	Fecha	Descripción del Cambio
01	30/01/2023	No aplica para la primera versión
02	26/01/2024	Se adecuaron las metas e indicadores al Plan de Desarrollo 2023-2026. Se actualizaron todos los componentes del plan.
03	05/12/2024	Se actualizaron las metas e indicadores al Plan de Desarrollo 2023-2026. Se actualizaron todos los componentes del plan.
04	15/12/2025	Se actualiza estructura y contenido del plan.

Contenido

1. Marco general	3
1.1. Marco institucional	3
1.2. Marco normativo y legal	4
2. Diagnóstico del institucional	5
2.1. Diagnóstico en el contexto nacional	5
2.2. Diagnóstico en el contexto institucional	6
3. Marco estratégico y programático	7
3.1. Objetivos del Plan	7
3.1.1. Objetivo general	7
3.1.2. Objetivos estratégicos	7
3.2. Principios del Plan	8
3.3. Resultados esperados	9
4. Desglose estratégico del Plan	9
4.1. Dimensión estratégica: Seguridad y privacidad de la información como habilitador de la transformación digital institucional	10
4.2. Eje estratégico: Gestión integral de la seguridad y privacidad de la información	11
4.3. Programas y proyectos	12
4.4. Mapa de ruta y seguimiento	13

1. Marco general

1.1. Marco institucional

La Institución Universitaria Digital de Antioquia es una institución de educación superior pública del orden departamental, creada con el propósito de ampliar el acceso a la educación superior mediante un ecosistema digital abierto, incluyente y con enfoque territorial. Su modelo institucional, basado en el concepto de “Digitalidad Próxima”, orienta la transformación educativa, administrativa y tecnológica, articulando la innovación digital con el sentido humano, la equidad y el compromiso con el territorio.

El Plan de Desarrollo Institucional 2023–2026 “Digitalidad Próxima” constituye el principal referente estratégico que orienta la gestión institucional a mediano plazo. En este se establecen los ejes estratégicos, proyectos e indicadores que permiten fortalecer la gobernabilidad, la gestión institucional y la prestación de servicios educativos en entornos digitales, reconociendo la información y las tecnologías como activos estratégicos para el cumplimiento de la misión institucional.

En este contexto, la gestión de la seguridad y privacidad de la información se configura como un habilitador transversal del quehacer institucional, al garantizar la confiabilidad, integridad, disponibilidad y protección de los datos que soportan los procesos académicos, administrativos y misionales. El Plan de Seguridad y Privacidad de la Información 2026 se articula con los lineamientos del Plan de Desarrollo Institucional, particularmente con aquellos asociados al fortalecimiento de la gestión institucional, la transformación digital, la transparencia y la continuidad de los servicios tecnológicos.

Las orientaciones estratégicas institucionales promueven una cultura organizacional basada en la gestión responsable de la información, el enfoque preventivo del riesgo, la mejora continua y la adopción de buenas prácticas en seguridad digital. En coherencia con lo anterior, este Plan se concibe como un instrumento de planificación que contribuye al logro de los objetivos institucionales y al fortalecimiento de la confianza de los grupos de valor en los entornos digitales de la IU Digital de Antioquia.

1.2. Marco normativo y legal

El Plan de Seguridad y Privacidad de la Información se fundamenta en un marco normativo nacional e institucional que orienta la gestión de la seguridad digital, la protección de datos personales y el uso responsable de las tecnologías de la información en las entidades públicas.

A nivel institucional, este se alinea con el Plan de Desarrollo Institucional 2023–2026 “Digitalidad Próxima”, aprobado mediante Acuerdo Directivo No. 128 de 2023, el cual establece los lineamientos estratégicos para la gestión institucional, la transformación digital y el fortalecimiento de la gobernanza universitaria. Asimismo, se articula con las políticas internas relacionadas con la gestión de la información, la arquitectura tecnológica y la continuidad de los servicios digitales.

En el ámbito nacional, el Plan se soporta principalmente en los lineamientos de la estrategia de Gobierno Digital, el Modelo de Privacidad y Seguridad de la Información (MSPI) del Ministerio de Tecnologías de la Información y las Comunicaciones, y el Modelo Integrado de Planeación y Gestión (MIPG), los cuales promueven la gestión integral de riesgos, la protección de la información y la mejora continua de los servicios digitales en el sector público.

De manera complementaria, el Plan incorpora las disposiciones normativas vigentes relacionadas con la protección de datos personales, la seguridad de la información y la ciberseguridad, entre las que se destacan la Ley 1581 de 2012, los decretos reglamentarios asociados, así como las resoluciones y lineamientos expedidos por el Ministerio TIC que orientan la implementación de controles, la gestión de incidentes y la relación con terceros y proveedores tecnológicos.

Adicionalmente, el Plan adopta como referentes las buenas prácticas y estándares internacionales en seguridad de la información, en particular la Norma Técnica Colombiana NTC ISO/IEC 27001, como marco para la gestión sistemática de los riesgos y la protección de los activos de información institucionales.

2. Diagnóstico del institucional

2.1. Diagnóstico en el contexto nacional

El contexto nacional presenta un escenario de transformación digital acelerada que incide directamente en la gestión de la seguridad y privacidad de la información de las entidades públicas. La consolidación de la estrategia de Gobierno Digital, el fortalecimiento de los servicios en línea y la creciente dependencia de plataformas tecnológicas han incrementado la exposición a riesgos asociados a la ciberseguridad, la protección de datos personales y la continuidad de los servicios digitales.

En esta dinámica, se evidencia un aumento sostenido de amenazas cibernéticas, incidentes de seguridad de la información y vulnerabilidades derivadas del uso intensivo de tecnologías emergentes, la tercerización de servicios tecnológicos y la interoperabilidad entre sistemas de información. Este contexto exige a las instituciones públicas el fortalecimiento integral de sus capacidades de prevención, detección y respuesta, adoptando enfoques articulados de gestión del riesgo y de protección de los activos de información.

De manera complementaria, el marco normativo nacional ha evolucionado para responder a estos desafíos, estableciendo mayores responsabilidades para las entidades públicas en materia de seguridad digital, tratamiento de datos personales, gestión de proveedores tecnológicos y aseguramiento de la información. Lineamientos como el Modelo de Privacidad y Seguridad de la Información (MSPI), el Modelo Integrado de Planeación y Gestión (MIPG) y las disposiciones asociadas a la estrategia de Gobierno Digital refuerzan la necesidad de contar con planes estructurados, medibles y alineados con la planeación institucional.

En el sector educativo, y particularmente en la educación superior con modalidades digitales, estos retos se intensifican debido al manejo de grandes volúmenes de información académica, administrativa y personal, así como a la prestación de servicios educativos en entornos virtuales. En este contexto, el Plan de Seguridad y Privacidad de la Información se constituye en un instrumento clave para responder a las tendencias nacionales y garantizar la confianza de los ciudadanos en los servicios digitales institucionales, en coherencia con los objetivos del desarrollo educativo y la transformación digital del país.

2.2. Diagnóstico en el contexto institucional

La IU Digital de Antioquia desarrolla su quehacer académico y administrativo en un entorno altamente digitalizado, lo que posiciona a la información y a las tecnologías como activos estratégicos para el cumplimiento de su misión institucional. La operación de procesos misionales, académicos y de apoyo a través de plataformas digitales implica una alta dependencia de los sistemas de información, infraestructuras tecnológicas y servicios en la nube.

En coherencia con el Plan de Desarrollo Institucional 2023–2026 “Digitalidad Próxima”, la Institución ha avanzado en la consolidación de su modelo educativo digital, el fortalecimiento de la gestión institucional y la ampliación de su cobertura territorial mediante el uso intensivo de tecnologías de la información. Este avance, si bien genera oportunidades en términos de innovación y acceso, también incrementa los riesgos asociados a la seguridad de la información, la privacidad de los datos personales y la continuidad de los servicios tecnológicos.

Desde la perspectiva institucional, se identifican como factores relevantes la necesidad de fortalecer la cultura organizacional en seguridad y privacidad de la información, la gestión integral de riesgos digitales, la actualización permanente de controles de seguridad y la articulación de estos esfuerzos con los procesos de planeación, evaluación y mejora continua. Asimismo, la interacción con proveedores tecnológicos, aliados estratégicos y plataformas externas exige mecanismos claros para la gestión de riesgos asociados a terceros.

El Plan de Seguridad y Privacidad de la Información 2026 responde a este diagnóstico institucional, consolidando un enfoque preventivo y estratégico que permite proteger los activos de información, asegurar la disponibilidad y confiabilidad de los servicios digitales y fortalecer la gobernanza de la seguridad de la información. De esta manera, el Plan se integra como un componente transversal que apoya la sostenibilidad institucional, la transparencia y la confianza de los grupos de valor en el ecosistema digital de la Institución.

3. Marco estratégico y programático

3.1. Objetivos del Plan

3.1.1. Objetivo general

Fortalecer la gestión de la seguridad y privacidad de la información de la IU Digital de Antioquia, mediante la implementación de lineamientos, controles y acciones articuladas al modelo institucional de transformación digital, que permitan proteger los activos de información, gestionar los riesgos asociados y garantizar la confidencialidad, integridad, disponibilidad y privacidad de los datos que soportan los procesos misionales, académicos y administrativos.

3.1.2. Objetivos estratégicos

- Implementar y consolidar un modelo de gestión de seguridad y privacidad de la información alineado con el Modelo de Privacidad y Seguridad de la Información (MSPI), la estrategia de Gobierno Digital y los lineamientos institucionales.
- Identificar, evaluar y gestionar los riesgos asociados a la seguridad de la información y la protección de datos personales, priorizando aquellos que impactan la continuidad de los servicios digitales institucionales.
- Fortalecer la gobernanza y la cultura organizacional en materia de seguridad y privacidad de la información, promoviendo la corresponsabilidad de los servidores, contratistas y terceros.
- Fortalecer la protección de los datos personales y la información institucional en los entornos digitales, plataformas tecnológicas y relaciones con proveedores y aliados estratégicos.
- Contribuir a la mejora continua de los procesos institucionales mediante el seguimiento, evaluación y actualización permanente de los controles de seguridad de la información.

3.2. Principios del Plan

El Plan de Seguridad y Privacidad de la Información se orienta por los siguientes principios, en coherencia con los principios constitucionales, sectoriales e institucionales:

- **Enfoque estratégico:** la seguridad y privacidad de la información se conciben como habilitadores del cumplimiento de la misión institucional y del logro de los objetivos del Plan de Desarrollo Institucional.
- **Gestión del riesgo:** las decisiones y acciones del Plan se fundamentan en la identificación, análisis y tratamiento de los riesgos que afectan los activos de información.
- **Responsabilidad y corresponsabilidad:** todos los actores institucionales comparten responsabilidades en la protección de la información y el uso adecuado de los recursos tecnológicos.
- **Prevención y mejora continua:** el Plan promueve acciones preventivas, correctivas y de mejora permanente frente a las amenazas y vulnerabilidades del entorno digital.
- **Legalidad y transparencia:** la gestión de la seguridad y privacidad de la información se realiza en estricto cumplimiento del marco normativo vigente y con criterios de transparencia institucional.
- **Protección de la información y los datos personales:** se prioriza la confidencialidad, integridad, disponibilidad y privacidad de la información institucional y de los datos de los grupos de valor.
- **Alineación institucional:** las acciones del Plan se articulan con la planeación institucional, los procesos misionales y los modelos de gestión adoptados por la IU Digital de Antioquia.

3.3. Resultados esperados

Como resultado de la ejecución del Plan de Seguridad y Privacidad de la Información 2026, se espera alcanzar, entre otros, los siguientes resultados:

- Un modelo de seguridad y privacidad de la información implementado y alineado con el MSPI y la estrategia de Gobierno Digital.
- Riesgos de seguridad de la información identificados, evaluados y gestionados de manera sistemática.
- Mayor nivel de apropiación y cultura organizacional en seguridad y privacidad de la información.
- Protección efectiva de los datos personales tratados por la Institución.
- Mejora continua en la confiabilidad y disponibilidad de los servicios tecnológicos articulados con la gestión efectiva en la gestión de la seguridad de la información institucional.

4. Desglose estratégico del Plan

El Plan de Seguridad y Privacidad de la Información 2026 se estructura a partir de un enfoque estratégico que permite materializar los objetivos definidos mediante resultados concretos orientados a la gestión del riesgo, la protección de los activos de información y el fortalecimiento de la gobernanza institucional en entornos digitales. La ejecución del Plan busca consolidar capacidades institucionales para prevenir, detectar y responder a incidentes de seguridad de la información, garantizar la protección de los datos personales y asegurar la continuidad de los servicios tecnológicos que soportan los procesos misionales, académicos y administrativos.

Este desglose estratégico articula los resultados esperados con dimensiones, ejes, programas y actividades que facilitan su implementación, seguimiento y evaluación, en coherencia con el ciclo de mejora continua definido en el Plan de Seguridad y Privacidad de la Información y con los objetivos del Plan de Desarrollo Institucional 2023–2026.

4.1. Dimensión estratégica: Seguridad y privacidad de la información como habilitador de la transformación digital institucional

Esta dimensión estratégica reconoce la seguridad y privacidad de la información como un componente transversal y habilitador del modelo de transformación digital de la Institución Universitaria Digital de Antioquia. Su sentido radica en garantizar que el uso intensivo de tecnologías de la información, plataformas digitales y servicios en línea se desarrolle bajo criterios de confianza, protección de datos, gestión del riesgo y continuidad operativa, asegurando la sostenibilidad de los procesos misionales, académicos y administrativos.

En el marco del Plan de Desarrollo Institucional 2023–2026 “Digitalidad Próxima”, esta dimensión se articula directamente con el objetivo de fortalecer la gestión institucional y consolidar un ecosistema digital confiable, incluyente y orientado al ciudadano. La información se entiende como un activo estratégico que soporta la toma de decisiones, la prestación de servicios educativos y la relación con los grupos de valor, por lo cual su protección resulta fundamental para el cumplimiento de la misión institucional.

El principal reto que plantea esta dimensión consiste en integrar de manera efectiva la gestión de la seguridad y privacidad de la información en la planeación, ejecución y evaluación de los procesos institucionales, superando un enfoque meramente técnico y promoviendo una visión estratégica, preventiva y de mejora continua. Esto implica fortalecer la gobernanza, la cultura organizacional y la corresponsabilidad de todos los actores involucrados en el tratamiento de la información.

De esta forma, la dimensión de Seguridad y Privacidad de la Información se vincula directamente con el Objetivo General del Plan de Desarrollo Institucional, al contribuir al fortalecimiento de la transformación digital, la transparencia, la confianza institucional y la sostenibilidad de los servicios digitales que ofrece la IU Digital de Antioquia.

4.2. Eje estratégico: Gestión integral de la seguridad y privacidad de la información

Este eje estratégico se orienta a la consolidación de un enfoque integral para la gestión de la seguridad y privacidad de la información en la IU Digital de Antioquia, articulando aspectos organizacionales, normativos, tecnológicos y culturales. Su propósito es garantizar que los activos de información sean protegidos de manera sistemática durante todo su ciclo de vida, en coherencia con los lineamientos del Modelo de Privacidad y Seguridad de la Información (MSPI) y la estrategia de Gobierno Digital.

El sentido de este eje radica en pasar de una gestión reactiva a una gestión preventiva y planificada de los riesgos asociados a la información y a los servicios digitales institucionales. Esto implica la identificación, evaluación y tratamiento continuo de riesgos, el fortalecimiento de los controles de seguridad, la protección de los datos personales y la definición de responsabilidades claras frente al uso y manejo de la información.

El principal reto de este eje consiste en integrar la seguridad y privacidad de la información en los procesos institucionales y en la cultura organizacional, asegurando la apropiación de buenas prácticas por parte de los servidores, contratistas y terceros. Asimismo, plantea el desafío de mantener los controles de seguridad actualizados frente a la evolución tecnológica, la tercerización de servicios y las amenazas emergentes del entorno digital.

Este eje se vincula directamente con los objetivos específicos del Plan, en tanto permite fortalecer el sistema de gestión de seguridad y privacidad de la información, promover una cultura institucional en ciberseguridad, gestionar de manera integral los riesgos digitales, asegurar la protección de los activos de información y contribuir a la continuidad y confiabilidad de los servicios tecnológicos de la IU Digital de Antioquia.

4.3. Programas y proyectos

Tabla 1. Programas y proyectos.

Programa / Proyecto	Descripción	Actores involucrados
Implementación del MSPI	Adopción y fortalecimiento del Modelo de Privacidad y Seguridad de la Información conforme a los lineamientos del MinTIC.	Dirección de Tecnología, Dirección de Planeación, áreas misionales
Gestión de riesgos de seguridad de la información	Identificación, análisis y tratamiento de riesgos asociados a los activos de información institucionales.	Dirección de Tecnología, líderes de proceso
Protección de datos personales	Fortalecimiento de controles y prácticas para el adecuado tratamiento de datos personales.	Dirección de Tecnología, Jurídica, áreas responsables
Gestión de incidentes de seguridad	Implementación de mecanismos para la detección, reporte y atención de incidentes de seguridad de la información.	Dirección de Tecnología, Mesa de Servicios
Sensibilización y cultura en seguridad de la información	Desarrollo de acciones de capacitación y apropiación institucional.	Talento Humano, Dirección de Tecnología

4.4. Mapa de ruta y seguimiento

Tabla 2. Actividades, indicadores y metas.

Línea	% Meta establecida	Unidad de medida Número/Porcentaje	Descripción del producto y/o resultado alcanzado
Actualizar el análisis de riesgos de seguridad de la información	1	Unidad	Un informe de análisis de riesgos de seguridad de la información identificados.
Implementar controles definidos en el Modelo de Seguridad y Privacidad de la Información	$\geq 80\%$	(Número de controles implementados / Número de controles programados) * 100	Cumplimiento de controles definidos en el Modelo de Seguridad y Privacidad de la Información evidenciados en el informe global.
Implementar espacios formativos de sensibilización institucional en seguridad y privacidad de la información	≥ 4 espacios	(Cantidad de espacios formativos realizados / Número de espacios formativos programados) * 100	Evidencias de los espacios formativos realizados.
Elaborar procedimiento de gestión de incidentes de seguridad y privacidad de la información	1	Unidad	Un procedimiento de gestión de incidentes.

Línea	% Meta establecida	Unidad de medida Número/Porcentaje	Descripción del producto y/o resultado alcanzado
Establecer controles para la protección de datos personales	1	Unidad	Un informe de los controles definidos e implementados para la protección de datos personales.

En este contexto, el Plan de Seguridad y Privacidad de la Información será objeto de **un (1) seguimiento semestral**, de acuerdo con los formatos establecidos en el Modelo de Operación por Procesos de la institución, con el fin de garantizar su correcta implementación, evaluación y ajuste conforme a los cambios y necesidades que puedan surgir.

Acción	Nombre	Fecha
Proyectó y Elaboró:	César Alexander Zapata Jiménez	15/12/2025
Revisó:	John Esteban Galeano Ríos	28/12/2025
Revisó y Aprobó:	Ana Paola Montoya Ríos	19/01/2026
Los anteriores, declaramos que hemos revisado el documento y lo encontramos ajustado a las normas y disposiciones legales y, por lo tanto, bajo nuestra responsabilidad presentamos para firma.		