Fecha de elaboración: 21/01/2026

1. INTRODUCCIÓN

La prosperidad económica y social actual están cada vez más ligadas a los ambientes digitales. En ese sentido, el continuo avance tecnológico y el aumento en la generación de información digital han traído consigo nuevos retos, entre ellos, la confidencialidad e integridad de los datos y la disponibilidad de servicios informáticos que, además de ser efectivos y eficientes, en entornos digitales. Superar estos desafíos es posible por medio de la seguridad digital, la cual consiste en el uso y apropiación de la tecnología para la protección de la información y los recursos digitales con los que dispone la organización. Debido a que la gestión, almacenamiento, procesamiento y transmisión de la información requieren del mayor cuidado posible, en la Institución Universitaria Digital de Antioquia se cuenta con una Política de Seguridad Digital. El propósito fundamental de la Política de Seguridad Digital en la Institución Universitaria Digital de Antioquia es garantizar la protección integral de esta, el equipo humano que la conforman y los grupos de interés con los que se relaciona, a través de la información y los recursos digitales institucionales, proporcionando un marco normativo sólido apoyado en cuatro pilares fundamentales:

a. Normatividad
b. Recursos humanos
c. Recursos financieros
d. Recursos tecnológicos

Se trata de cuatro pilares fundamentales e, interdependientes, que en conjunto promueven una gestión integral de la seguridad digital:

- El pilar de Normatividad constituye el cimiento de la política, dotando de legitimidad, alcance y alineación estratégica a todas las acciones de seguridad digital.
- El pilar de Recursos Humanos representa el núcleo de la estrategia, integrando tanto el talento especializado como a programas de formación y concientización, reconociendo que las personas son el factor crítico en la implementación y uso seguro de la tecnología.
- El pilar de Recursos Financieros actúa como el combustible que hace posible materializar los demás pilares, asegurando la inversión sostenible necesaria para su ejecución.

Elaboró	Revisó	Aprobó
Nombre: Juan Diego Rojas Tombe	Nombre: César Alexander Zapata	Nombre: Ana Paola Montoya Ríos
Cargo: Outsourcing	Cargo: Profesional especializado	Cargo: Directora de Tecnología
Fecha: 06-01-2026	Fecha: 15-01-2026	Fecha: 21-01-2026

- El pilar de Recursos Tecnológicos provee la infraestructura tangible sobre la cual se implementan los controles de seguridad, materializando técnicamente los principios de la política.

Esta estructura propende para que la Institución no solo aborde las capacidades técnicas ("el cómo"), sino que también promueva los fundamentos de gobierno, talento y sostenibilidad económica ("el con qué") para el éxito a largo plazo.
Asimismo, la Política de Seguridad Digital solo es posible con la articulación de todos los miembros de la comunidad universitaria que interactúan de manera continua con los sistemas, datos y recursos digitales.
Solo se garantiza la seguridad informática a partir de la implementación colaborativa de esta política, su divulgación pedagógica y su apropiación con la comunidad universitaria. Las actitudes de compromiso común son el principal eje para brindar confianza, asegurar la protección de la información, enfrentar los desafíos de la ciberseguridad y, por supuesto, garantizar las condiciones tecnológicas que desarrollen la misión educativa y de investigación de la Institución Universitaria Digital de Antioquia.

1.1 Antecedentes

En los últimos años, el mundo entero se ha sumergido en la tendencia de lo digital buscando apoyo en las nubes públicas y privadas, y dejando toda la información lista para ser consumida y procesada a la necesidad de quien las requiera. Cada vez son más las entidades públicas y privadas que trasladan sus procesos, servicios e interacciones al entorno digital. Esto, que por un lado representa avances importantes en términos de acceso, eficiencia y cobertura, también implica asumir nuevos riesgos que, aunque a veces invisibles, son cada vez más frecuentes y complejos. Desde ataques a infraestructuras críticas, hasta filtraciones de datos sensibles. La amenaza es real, y las consecuencias, profundas.
Las instituciones de educación superior no han estado al margen de estas amenazas. En los últimos años, varios casos han salido a la luz pública, con titulares en medios nacionales que alertaban sobre el secuestro de plataformas académicas, interrupciones prolongadas en sistemas de matrícula y clases virtuales, y la pérdida o exposición de información de estudiantes y profesores.
A nivel nacional, el país ha venido reaccionando a estas necesidades. La Estrategia Nacional Digital –que se viene fortaleciendo desde el Ministerio TIC– ha dejado claro que la seguridad digital y la confianza no son elementos decorativos en la transformación digital: son pilares fundamentales. El documento habla incluso de “seguridad humana”, dándole un enfoque que va más allá de los firewalls o las contraseñas robustas. Se trata de proteger derechos, libertades, dignidad. Es decir, personas.

En el plano regional, Antioquia 2040 marca una hoja de ruta de largo aliento. La tecnología es parte del tejido de ese futuro proyectado. Pero no cualquier tecnología: una que sea segura, ética, confiable. Una que garantice que las brechas no se amplíen, y que las oportunidades no terminen siendo vulnerabilidades. De nuevo, se habla de habilitadores, y la seguridad digital es uno de ellos.

Ahora bien, dentro de la Institución Universitaria Digital de Antioquia –que no sólo vive en lo digital, sino que fue concebida de esta forma, el desafío es todavía mayor. No se trata solo de adoptar tecnologías, sino de blindar un modelo educativo que, por diseño, depende de entornos virtuales, plataformas, datos, redes, sistemas distribuidos, y comunidades que se conectan desde distintos lugares, con distintos niveles de conocimiento y de riesgo.

Es por lo que esta Política de Seguridad Digital no parte de cero. Viene a integrarse con otras políticas existentes en la institución: Transformación Digital, que define los caminos del cambio tecnológico; Protección de datos, que garantiza el manejo ético y legal de los datos. Por lo anterior, esta política se articula con las existentes, se suma a los esfuerzos institucionales y, sobre todo, protege los derechos y la seguridad digital de la comunidad universitaria.

La idea no es tener una política por cumplimiento normativo sino tener una postura institucional clara frente al riesgo, frente a las amenazas, frente a la responsabilidad de cuidar los activos digitales que, en este caso, además, son parte esencial de la vida universitaria. Por eso, esta política responde a las tendencias y marcos regulatorios nacionales, a la Ley 1581 sobre protección de datos personales, al CONPES 3854 sobre seguridad digital, al CONPES 3995 de política nacional de confianza y seguridad, CONPES 4144 Política Nacional de Inteligencia Artificial y a todo ese entramado de normas y estrategias que Colombia ha venido consolidando, con el fin de regular y promover la seguridad Digital en el país.

2. OBJETIVO

2.1 Objetivo general

Promover la protección de la información y de los recursos digitales de la Institución Universitaria Digital de Antioquia, por medio de acciones que potencien la seguridad digital como base para impulsar la competitividad, productividad y funcionamiento continuo de la Institución.

2.2 Objetivos Específicos

- Promover una cultura de seguridad digital consciente y responsable en la comunidad universitaria, mediante programas de capacitación continua y

campañas de sensibilización, con el fin de fortalecer la protección de la información y los recursos digitales institucionales.

- Gestionar los riesgos e incidentes de la seguridad digital mediante la definición y aplicación de lineamientos claros que permitan la identificación, medición del impacto y el establecimiento de alternativas de tratamiento, asegurando la continuidad de la operación institucional
- Preservar la integridad y confidencialidad de la información, los datos sensibles y los activos digitales del equipo humano que conforma la Institución y los grupos de interés con los que se relaciona.
- Mantener la alta disponibilidad de los recursos digitales institucionales a las personas y comunidades que sostienen un vínculo con la Institución.
- Cumplir con las regulaciones colombianas aplicables en torno a la seguridad digital, buscando así salvaguardar los derechos humanos y los valores fundamentales de la ciudadanía.
- Implementar mecanismos de mejora continua en las prácticas de seguridad de los actores institucionales de modo que estos puedan desarrollar sus actividades en el entorno digital de forma libre, confiable y segura.
- Mantener actualizada, vigente y operativa la Política de Seguridad Digital de manera que pueda ser auditada de acuerdo con los riesgos identificados por la Institución, con el fin de conservar su nivel de eficacia y aplicabilidad.

3. ALCANCE DE LA POLÍTICA

La Política de Seguridad Digital de la Institución Universitaria Digital de Antioquia adopta un enfoque basado en mitigar, controlar y dar respuesta a incidentes en sitio, que comprometa a toda la comunidad universitaria. Su logro será el producto colectivo que permita a cada individuo el libre, confiable y seguro desarrollo de sus actividades en el entorno digital, con el fin de alcanzar la Misión y Visión Institucional. Se consideran sujetos activos de esa política los siguientes actores:

- Estudiantes
- Profesores
- Empleados
- Contratistas
- Proveedores
- Ciudadanos

Se destaca en esta Política la inclusión de los activos digitales, datos, sistemas, redes,

aplicaciones y servicios utilizados por la Institución. Además, aplica a todas las ubicaciones y entornos en los que se utilizan activos digitales institucionales, ya sea dentro o fuera de las instalaciones físicas.
El cumplimiento de esta Política es un requisito inquebrantable y de responsabilidad compartida. La seguridad de la información es una prioridad institucional y una parte integral de la cultura universitaria.

4. DESARROLLO DE LA POLÍTICA

4.1 Marco normativo

La Política de Seguridad Digital de la Institución Universitaria Digital de Antioquia se fundamenta en un marco normativo nacional e internacional que define las competencias, principios y obligaciones en materia de seguridad digital, gestión de riesgos tecnológicos, protección de datos personales y confianza en el entorno digital.
Este marco normativo se articula con las políticas públicas de transformación digital del Estado colombiano, garantizando que la gestión institucional de la seguridad digital se desarrolle conforme a los principios de gobernanza digital, protección de derechos fundamentales, transparencia y resiliencia tecnológica.
Dada la naturaleza de la Institución Universitaria Digital de Antioquia como entidad pública de educación superior cuyo modelo educativo se soporta principalmente en entornos digitales, la adopción de políticas de seguridad digital constituye un elemento estratégico para proteger la información institucional, garantizar la continuidad de los servicios académicos y administrativos, y salvaguardar los derechos de los miembros de la comunidad universitaria.
En este sentido, la presente política se estructura respetando la jerarquía normativa del ordenamiento jurídico colombiano y establece la relación entre las disposiciones constitucionales, legales, reglamentarias y de política pública que orientan la gestión de la seguridad digital en la Institución.

4.1.1 Normas de Nivel Constitucional y Legal

Constitución Política de Colombia de 1991: La presente política se fundamenta en los principios constitucionales que garantizan la protección de los derechos fundamentales en el entorno digital. En particular:

- Artículo 15, que consagra el derecho a la intimidad personal y familiar y al buen nombre, así como el derecho de las personas a conocer, actualizar y rectificar la información que sobre ellas repose en bases de datos o archivos, principio que sustenta el régimen de protección de datos personales en Colombia.

- Artículo 20, que garantiza la libertad de expresión y el derecho a informar y recibir información veraz e imparcial, derechos que deben desarrollarse en entornos digitales seguros que garanticen la integridad, disponibilidad y confiabilidad de la información.

Ley 1341 de 2009 – Ley de Tecnologías de la Información y las Comunicaciones (TIC) y su modificación mediante la Ley 1978 de 2019: Estas normas establecen el marco general para la organización del sector TIC en Colombia y promueven el acceso, uso eficiente y apropiación de las tecnologías de la información y las comunicaciones.
En particular, el artículo 2 de la Ley 1341 establece principios orientadores para el desarrollo del ecosistema digital del país, dentro de los cuales se reconoce la importancia de fortalecer la confianza en el entorno digital y promover el aprovechamiento de las tecnologías en la gestión pública.
Para la Institución Universitaria Digital de Antioquia, estas disposiciones resultan especialmente relevantes al sustentar el desarrollo de servicios educativos y administrativos en entornos digitales seguros.
Ley 1581 de 2012 – Régimen General de Protección de Datos Personales: Esta norma establece el marco jurídico para el tratamiento de datos personales en Colombia, definiendo los principios, derechos y deberes que deben observar las entidades públicas y privadas que administran información personal.
La presente política se alinea con los principios de legalidad, finalidad, libertad, veracidad, seguridad y confidencialidad establecidos en dicha ley, garantizando que los procesos institucionales que involucren la recolección, almacenamiento, uso o circulación de datos personales se realicen bajo condiciones adecuadas de seguridad y protección de la información.
Ley 1273 de 2009 – Delitos Informáticos: Esta ley modifica el Código Penal colombiano e incorpora nuevos tipos penales relacionados con la protección de la información y los sistemas informáticos, tales como el acceso abusivo a sistemas informáticos, la interceptación de datos informáticos, la violación de datos personales y el daño informático.
La inclusión de esta norma en el marco normativo de la presente política resalta la importancia de implementar controles técnicos, administrativos y humanos que prevengan la materialización de conductas que atenten contra la confidencialidad, integridad y disponibilidad de la información institucional.
Ley 1712 de 2014 – Ley de Transparencia y Acceso a la Información Pública: Esta ley establece el derecho fundamental de acceso a la información pública y las obligaciones de las entidades del Estado en materia de transparencia y gestión de la información.
La Política de Seguridad Digital contribuye al cumplimiento de esta normativa al establecer mecanismos que garantizan la disponibilidad y confiabilidad de la información

pública institucional, asegurando al mismo tiempo su adecuada protección frente a accesos no autorizados, alteraciones o pérdidas.

4.1.2 Normas Reglamentarias y de Política Pública Nacional

Decreto 1078 de 2015 – Decreto Único Reglamentario del Sector TIC: Este decreto compila la normativa del sector de tecnologías de la información y las comunicaciones y establece, entre otros aspectos, la Política de Gobierno Digital para las entidades públicas colombianas.
La presente política institucional se articula con dicha política pública, particularmente con el Modelo de Seguridad y Privacidad de la Información (MSPI), el cual constituye el marco metodológico adoptado por el Estado colombiano para orientar la gestión de la seguridad de la información y la privacidad en las entidades públicas.
Decreto 338 de 2022 – Gobernanza de la Seguridad Digital: El Decreto 338 de 2022 adiciona el Título 21 al Decreto 1078 de 2015 y establece los lineamientos generales para fortalecer la gobernanza de la seguridad digital en Colombia.
Entre sus disposiciones más relevantes se destacan:

- **Artículo 2.2.21.1.1.4,** que establece la obligación de las entidades públicas de adoptar medidas técnicas, humanas y administrativas para garantizar la gestión de riesgos de seguridad digital.
- **Artículo 2.2.21.1.2.1,** que establece la adopción del modelo de gobernanza de la seguridad digital como marco para la gestión institucional de la ciberseguridad.
- **Artículo 2.2.21.1.5.7**, que promueve el desarrollo de capacidades institucionales y la apropiación de la cultura de seguridad digital.
- **Artículo 2.2.21.1.5.8**, que establece la necesidad de articular la gestión de incidentes de seguridad digital con las disposiciones de protección de datos personales.

La presente política adopta estos lineamientos como base para el desarrollo de la estrategia institucional de seguridad digital.
Decreto 1083 de 2015 – Decreto Único Reglamentario del Sector Función Pública: Este decreto establece el marco normativo del Modelo Integrado de Planeación y Gestión (MIPG), el cual orienta la gestión institucional de las entidades públicas colombianas.
En este contexto, la seguridad digital se integra como parte de las políticas de gestión institucional, permitiendo articular la gestión de riesgos tecnológicos, la protección de la información y la continuidad de los servicios digitales con los procesos de planeación, seguimiento y mejora continua de la entidad.

Documento CONPES 3995 de 2020 – Política Nacional de Confianza y Seguridad Digital: Este documento de política pública establece la estrategia nacional para fortalecer la seguridad digital en Colombia, promoviendo el desarrollo de capacidades institucionales para la gestión de riesgos digitales, la protección de la infraestructura tecnológica y la generación de confianza en el entorno digital.
La Política de Seguridad Digital de la Institución Universitaria Digital de Antioquia se alinea con los objetivos establecidos en este documento, contribuyendo al fortalecimiento de la cultura de seguridad digital, la gestión integral de riesgos y la protección de la información en el sector público.
Documento CONPES 4144 de 2024 – Política Nacional de Inteligencia Artificial: Este documento establece los lineamientos para el desarrollo y uso responsable de la inteligencia artificial en Colombia, reconociendo tanto sus beneficios como los riesgos asociados a su implementación.
La presente política contempla la necesidad de integrar consideraciones de seguridad digital en la adopción futura de soluciones basadas en inteligencia artificial dentro de la Institución, con el fin de garantizar el uso responsable, seguro y ético de estas tecnologías emergentes.

4.1.3 Normativa Institucional y Contexto Estratégico

Plan de Desarrollo Institucional: La presente política se articula con el Plan de Desarrollo de la Institución Universitaria Digital de Antioquia, particularmente con el eje estratégico orientado a la consolidación del modelo educativo digital.
La seguridad digital se reconoce como un habilitador fundamental para garantizar la continuidad de los servicios académicos, la protección de los activos de información institucionales y la confianza de la comunidad universitaria en los entornos tecnológicos utilizados para el desarrollo de las actividades misionales.
Planeación Regional: En coherencia con los procesos de planeación territorial y regional orientados al fortalecimiento de las capacidades tecnológicas y digitales del departamento de Antioquia, la Institución promueve la adopción de prácticas responsables y seguras en el uso de las tecnologías de la información, contribuyendo al desarrollo de un ecosistema digital confiable, ético y sostenible.
Políticas Institucionales Complementarias: La presente Política de Seguridad Digital se integra con otras políticas institucionales relacionadas con la gestión de tecnologías de la información, la transformación digital y la protección de datos personales, conformando un marco institucional coherente que fortalece la gobernanza digital y la gestión integral de riesgos tecnológicos en la Institución.

4.2 Gestión de Recursos Humanos

La efectiva aplicación de la Política de Seguridad Digital en la Institución Universitaria Digital de Antioquia requiere de una estructura de gobierno sólida, un equipo humano especializado y un programa continuo de concienciación que involucre a toda la comunidad universitaria.

Gobierno y Alta Dirección

La Alta Dirección es la máxima responsable de la seguridad digital, asignando los recursos estratégicos y respaldando la implementación de esta política. Su compromiso se materializa en la supervisión de la gestión de riesgos, la aprobación de la estrategia de seguridad y la garantía del cumplimiento normativo.

Equipo de Seguridad Digital: Estructura y Capacidad Mínima

La responsabilidad operativa, técnica y de gestión de la seguridad digital recae en la línea de operación de Seguridad Digital. Dada la naturaleza crítica de las operaciones digitales de la Institución y el volumen y sensibilidad de la información manejada, se requiere una capacidad de respuesta especializada y proactiva.
Para garantizar la operatividad básica, la gestión de riesgos y la respuesta a incidentes, se establece como capacidad mínima indispensable la conformación inicial de un equipo con los siguientes roles fundamentales:

- Líder de Seguridad Digital (CISO): Responsable de la estrategia, el gobierno, la gestión de riesgos, el cumplimiento normativo y la relación con la alta dirección.
- Ingeniero de Seguridad de la Información: responsable del diseño, implementación y mantenimiento de los controles técnicos (firewalls, SIEM, IDS/IPS), la gestión de vulnerabilidades y la arquitectura segura.
- Analista de Operaciones de Seguridad (SOC): responsable del monitoreo continuo, la detección de amenazas, la investigación y la respuesta inicial a incidentes de seguridad.

Esta estructura de tres (3) roles es el punto de partida crítico para establecer un programa de seguridad digital viable. El crecimiento futuro de este equipo (la incorporación de especialistas en ciber seguimiento, auditoría forense, o seguridad de aplicaciones) será determinado por la evolución del panorama de amenazas, los requisitos normativos y la expansión de los servicios digitales de la Institución, tal como se evalúe en las revisiones anuales de esta política.

Formación y Concienciación de la Comunidad

Son funciones del Equipo de Seguridad Digital, en coordinación con la Dirección de Recursos Humanos a través del Plan Institucional de Capacitación (PIC), la ejecución de un plan anual de formación y concienciación en seguridad digital. Este programa abordará desde conceptos básicos hasta amenazas complejas, e incorporará evaluaciones, simulacros de ciberseguridad y campañas de sensibilización continuas, como simulacros de phishing personalizados para diferentes audiencias.

Responsabilidades de los Sujetos Activos

Los Sujetos Activos (estudiantes, profesores, empleados, contratistas) son corresponsables en la protección del entorno digital. Su deber es cumplir con las normas establecidas en
esta política, notificar de inmediato cualquier incidente o actividad sospechosa, y participar activamente en los programas de formación y concienciación.

Compromisos con Terceros

La Dirección Jurídica velará por que los acuerdos de confidencialidad y cláusulas de seguridad digital sean parte integral de los contratos laborales y de prestación de servicios.
Los Proveedores y Contratistas que accedan a los activos tecnológicos institucionales estarán obligados a cumplir con esta política y a proporcionar evidencia de sus prácticas seguras, colaborando en la resolución de incidentes relacionados con sus servicios.

4.3 Gestión de recursos Financieros

La Institución Universitaria Digital de Antioquia reconoce que la seguridad digital es una inversión estratégica y un facilitador esencial para el cumplimiento de su misión. En este sentido, se compromete a garantizar la asignación eficiente y oportuna de los recursos financieros necesarios dentro de su presupuesto anual para la implementación, mantenimiento y mejora continua de las medidas de seguridad digital.
La priorización de las inversiones se realizará con base en un análisis riguroso de riesgos y plan anual que garantice que los recursos se destinen a la protección de los activos digitales más críticos y a las iniciativas que generen el mayor impacto en la postura de seguridad institucional. Esto incluye, pero no se limita a:

- La adquisición, actualización y mantenimiento de tecnologías y herramientas de seguridad.

Elaboró	Revisó	Aprobó
Nombre: Juan Diego Rojas Tombe	Nombre: César Alexander Zapata	Nombre: Ana Paola Montoya Ríos
Cargo: Outsourcing	Cargo: Profesional especializado	Cargo: Directora de Tecnología
Fecha: 06-01-2026	Fecha: 15-01-2026	Fecha: 21-01-2026

- La conformación y sostenimiento de un equipo de seguridad digital competente y dedicado.
- Los programas de formación, capacitación y concienciación para toda la comunidad universitaria.
- La contratación de servicios especializados de auditoría, consultoría y respuesta a incidentes cuando se requiera.

Cada solicitud de inversión en seguridad digital deberá estar respaldada por una justificación técnica y financiera que demuestre su alineación con los objetivos de esta política y su contribución a la gestión integral de riesgos digitales de la Institución.

4.4 Gestión de Recursos Tecnológicos:

La Institución Universitaria Digital de Antioquia establece que la protección de sus activos digitales se sustentará en una arquitectura de seguridad moderna, defensiva y resiliente. Dado el panorama dinámico de las amenazas, los recursos tecnológicos se seleccionarán, implementarán y mantendrán bajo los principios de eficacia, integración y mejora continua, garantizando que sean acordes a los riesgos identificados.
Para ello, la Institución implementará y mantendrá capacidades tecnológicas en las siguientes categorías estratégicas de control:

1. **Protección Perimetral y de Red:** Implementación de controles de red segmentados y de última generación para filtrar el tráfico, gestionar accesos y prevenir intrusiones, aplicando el principio de menor privilegio.
2. **Protección de Endpoints y Estaciones de Trabajo:** Despliegue de soluciones centralizadas de protección (antimalware, EDR - Detección y Respuesta en Endpoints) en todos los dispositivos con acceso a la red institucional, con capacidades de detección proactiva de amenazas.
3. **Protección de Datos y Aplicaciones:** Implementación de mecanismos de cifrado para información sensible en reposo y en tránsito. Adopción de controles de seguridad en el ciclo de desarrollo de software y en las aplicaciones web para prevenir vulnerabilidades comunes. Establecimiento de sistemas de prevención de pérdida de datos (DLP).
4. **Gestión de Identidades y Accesos:** Implementación de un sistema centralizado y robusto de gestión de identidades y accesos que garantice la autenticación multifactor (MFA) y el cumplimiento del principio de "acceso mínimo necesario".
5. **Monitoreo Continuo y Detección de Amenazas:** Despliegue de una capacidad centralizada de monitoreo (ej., una plataforma SIEM - Sistema de Gestión de Eventos

Elaboró	Revisó	Aprobó
Nombre: Juan Diego Rojas Tombe	Nombre: César Alexander Zapata	Nombre: Ana Paola Montoya Ríos
Cargo: Outsourcing	Cargo: Profesional especializado	Cargo: Directora de Tecnología
Fecha: 06-01-2026	Fecha: 15-01-2026	Fecha: 21-01-2026

e Información de Seguridad) para la correlación de logs, detección de anomalías y respuesta rápida ante incidentes.

6. **Respuesta y Recuperación ante Incidentes:** Mantenimiento de una infraestructura de respaldo (backup) automatizada, resiliente y periódicamente testeada, que garantice la recuperación de la información y la continuidad del negocio.

    - Establecimiento de herramientas forenses para la investigación de incidentes.

7. **Gestión de Vulnerabilidades:** Implementación de programas y herramientas periódicas para la identificación, clasificación y remediación de vulnerabilidades en sistemas, aplicaciones y redes. La selección, adquisición y renovación de estas tecnologías será responsabilidad del Equipo de Seguridad Digital, en coordinación con la Dirección de Tecnología, y deberá estar alineada con el Marco de Referencia de Seguridad (ej., ISO 27001, NIST) adoptado por la Institución y justificada mediante un análisis continuo de riesgos.

5. SEGUIMIENTO, MONITOREO Y EVALUACIÓN:

5.1. Seguimiento y Monitoreo.

El seguimiento del cumplimiento y la eficacia de esta política será continuo y estará a cargo de la Dirección de Tecnología. Para ello, se implementará una metodología de ciclo cerrado, basada en los principios de mejora continua y gestión por indicadores, que comprende las siguientes fases:

- Planificación (Plan): Definición anual de objetivos, actividades e Indicadores Clave de Desempeño (KPIs) para el Programa de Seguridad Digital, alineados con los riesgos institucionales. Estos KPIs medirán aspectos como tiempos de detección y respuesta, tasas de remediación de vulnerabilidades y cumplimiento de planes de capacitación. Dicha Planificación se verá reflejada en un plan anual.
- Ejecución y Verificación (Do - Check): Implementación de las actividades y monitoreo continuo de los KPIs mediante mecanismos como:
    - Análisis continuo de registros y eventos de seguridad.
    - Revisión periódica de accesos y privilegios.
    - Documentación y evaluación sistemática de todos los incidentes de seguridad.
    - Ejecución de auditorías programadas sobre procesos y sistemas.
- Análisis y Mejora (Act): Análisis trimestral de la información recopilada para generar

Elaboró	Revisó	Aprobó
Nombre: Juan Diego Rojas Tombe	Nombre: César Alexander Zapata	Nombre: Ana Paola Montoya Ríos
Cargo: Outsourcing	Cargo: Profesional especializado	Cargo: Directora de Tecnología
Fecha: 06-01-2026	Fecha: 15-01-2026	Fecha: 21-01-2026

reportes de avance a la Alta Dirección, identificar desviaciones e implementar las acciones correctivas y de mejora necesarias.

5.2. Monitoreo y evaluación.

Para garantizar la objetividad y la mejora continua, se realizará de forma periódica ejercicios de monitoreo y evaluación independiente del Sistema de Gestión de Seguridad Digital y de la Política de Seguridad Digital. Dichas acciones tendrán como fin verificar la eficacia global de la política, la idoneidad de los controles y el manejo de los riesgos.
Entre los mecanismos para el monitoreo y la evaluación se encuentran los siguientes, los cuales serán liderados y consolidados por la Dirección de Planeación y la Oficina Asesora de Auditoría Interna.

- Auditorías de Cumplimiento y Desempeño: Evaluaciones programadas que verifiquen la adherencia a esta política y la efectividad de los controles.
- Análisis de Indicadores de Gestión (KPIs): Revisión y contraste de las métricas reportadas para validar su exactitud y el progreso real.
- Revisiones Post-Incidente de Alto Impacto: Análisis exhaustivo de incidentes significativos para evaluar la respuesta y extraer lecciones aprendidas a nivel estratégico.
- Verificación de Conformidad Legal y Normativa: Revisión del cumplimiento de los marcos legales y regulatorios aplicables.

La Oficina Asesora de Auditoría Interna como instancia evaluadora generará un informe formal con las observaciones y recomendaciones dirigidas a la Alta Dirección, el cual servirá como base para la actualización y el refinamiento de esta política y de las estrategias de seguridad institucionales.

6. DIVULGACIÓN, SOCIALIZACIÓN Y APROPIACIÓN

Para garantizar que la presente Política de Seguridad Digital sea conocida, comprendida y aceptada por toda la comunidad universitaria, la Institución Universitaria Digital de Antioquia implementará un plan integral de divulgación y socialización con las siguientes acciones:

6.1 Estrategias de comunicación y canales

- Comunicación Oficial: La política será publicada oficialmente en el portal web

institucional, en la sección de normatividad y gobierno, asegurando su acceso permanente para toda la comunidad.

- Lanzamiento Interno: Se realizará un lanzamiento formal dirigido por la Alta Dirección, dirigido a todos los líderes de dependencias, para transmitir su importancia y obtener su compromiso como voceros.
- Campañas de Sensibilización: Se desarrollarán campañas periódicas a través de los correos electrónicos institucionales, intranet, pantallas internas y redes sociales oficiales, utilizando un lenguaje claro y accesible que resalte los beneficios de la política y las responsabilidades individuales.
- Material de Apoyo: Se crearán y distribuirán materiales gráficos y multimedia (por ejemplo, infografías, videos explicativos, cartillas) que sinteticen los puntos clave, los deberes de los usuarios y los procedimientos para reportar incidentes.

6.2 Programas de capacitación y formación

- Sesiones de Socialización Obligatorias: Se implementarán sesiones de socialización virtuales y presenciales, segmentadas para los diferentes grupos de la comunidad universitaria (empleados, contratistas, profesores y estudiantes), explicando el alcance, los principios y los procedimientos establecidos en la política.
- Módulos de Formación Virtual: Se integrarán módulos específicos sobre la Política de Seguridad Digital en las plataformas de aprendizaje virtual de la institución, los cuales serán de cumplimiento obligatorio para el personal nuevo como parte de su proceso de inducción.
- Talleres Prácticos: El Equipo de Seguridad Digital, en coordinación con la Dirección de Talento Humano, organizará talleres prácticos enfocados en las amenazas más comunes (como phishing o ingeniería social) y en las buenas prácticas de seguridad.

6.3 Responsables

La Dirección de Tecnología, será la responsable de liderar la elaboración del contenido técnico y las sesiones de capacitación especializada. La Oficina de Comunicaciones será responsable del diseño, la estrategia de difusión masiva y la producción de los materiales de apoyo. Los líderes de cada dependencia serán corresponsables de promover la política dentro de sus equipos y de velar por su cumplimiento.

6.4 Metas y seguimiento

El éxito del plan de divulgación se medirá a través de métricas como el porcentaje de la comunidad que ha completado los módulos de formación, el número de miembros de la comunidad impactados, el número de incidentes reportados de forma proactiva y los resultados de las encuestas de percepción sobre cultura de seguridad digital, entre otros. La Dirección de Tecnología reportará periódicamente estos indicadores a la Alta Dirección.

Glosario de términos

- **Activo digital:** Elemento digital con valor para la organización, que puede incluir sistemas, datos, aplicaciones, configuraciones o contenido almacenado o transmitido electrónicamente. (ISO/IEC 27001:2022, NIST SP 800-53)
- **Acceso no autorizado:** Ingreso o uso de información, sistemas o recursos digitales por parte de personas o entidades sin los permisos correspondientes. (ISO/IEC 27002:2022)
- **Amenaza:** Causa potencial de un incidente no deseado que puede resultar en daño para un sistema o la organización. (ISO/IEC 27000:2018, definición 3.74)
- **Ciberseguridad:** Preservación de la confidencialidad, integridad y disponibilidad de la información en el ciberespacio. (ISO/IEC 27032:2012, definición 4.3)
- **Confidencialidad:** Propiedad que determina que la información solo está disponible para individuos, entidades o procesos autorizados. (ISO/IEC 27000:2018, definición 3.10)
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una persona natural identificada o identificable. (Ley 1581 de 2012, artículo 3 literal c)
- **Disponibilidad:** Propiedad de que la información esté accesible y utilizable por una entidad autorizada cuando se requiera. (ISO/IEC 27000:2018, definición 3.27)
- **Incidente de seguridad:** Evento que compromete o tiene el potencial de comprometer la confidencialidad, integridad o disponibilidad de un activo de información. (ISO/IEC 27035-1:2016, NIST SP 800-61 rev.2)
- **Integridad:** Propiedad que asegura que la información no ha sido alterada o destruida de manera no autorizada. (ISO/IEC 27000:2018, definición 3.28)
- **Política de seguridad digital:** Directriz institucional que establece los lineamientos, responsabilidades y controles para la protección de los recursos digitales y la información. (ISO/IEC 27001, Estrategia Nacional Digital – MinTIC)
- **Responsabilidad compartida:** Principio según el cual todos los actores involucrados en el uso y gestión de la información tienen obligaciones en la protección de la seguridad digital. (ISO/IEC 27014:2020)
- **Riesgo:** Efecto de la incertidumbre sobre los objetivos, en este contexto, asociado

Elaboró	Revisó	Aprobó
Nombre: Juan Diego Rojas Tombe	Nombre: César Alexander Zapata	Nombre: Ana Paola Montoya Ríos
Cargo: Outsourcing	Cargo: Profesional especializado	Cargo: Directora de Tecnología
Fecha: 06-01-2026	Fecha: 15-01-2026	Fecha: 21-01-2026

al impacto negativo que una amenaza puede generar sobre los activos de información. (ISO/IEC 27000:2018, definición 3.61)

- **Seguridad de la información:** Preservación de la confidencialidad, integridad y disponibilidad de la información. (ISO/IEC 27000:2018, definición 3.52)
- **Seguridad digital:** Abordaje integral que incluye la ciberseguridad, la protección de datos y la gestión deriesgos en entornos digitales, centrado también en la protección de derechos humanos y confianza institucional. (CONPES 3854 de 2016, Estrategia Nacional Digital – MinTIC)
- **Titular de la información:** Persona natural cuyos datos personales son objeto de tratamiento. (Ley 1581 de 2012, artículo 3 literal e)
- **Tratamiento de datos:** Cualquier operación sobre datos personales, como recolección, almacenamiento, uso, circulación o supresión. (Ley 1581 de 2012, artículo 3 literal g)
- **Vulnerabilidad:** Debilidad de un activo o control que puede ser explotada por una o más amenazas. (ISO/IEC 27000:2018, definición 3.94)

Elaboró	Revisó	Aprobó
Nombre: Juan Diego Rojas Tombe	Nombre: César Alexander Zapata	Nombre: Ana Paola Montoya Ríos
Cargo: Outsourcing	Cargo: Profesional especializado	Cargo: Directora de Tecnología
Fecha: 06-01-2026	Fecha: 15-01-2026	Fecha: 21-01-2026