Fecha de elaboración: 28/11/2025

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.
- 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. Algunas de estas situaciones obligaron incluso a suspender actividades durante semanas, generando afectaciones operativas, legales y reputacionales difíciles de contener; las noticias circularon ampliamente y dejaron claro que el sector educativo es un blanco cada vez más apetecido por los actores maliciosos. La razón es clara: manejan grandes volúmenes de datos personales, dependen profundamente de sus infraestructuras digitales y muchas veces no cuentan con equipos robustos de seguridad para salvaguardar esta información.

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.

El Plan Nacional de Desarrollo 2022-2026, por su parte, va en la misma línea. Cuando habla de “Colombia Potencia Mundial de la Vida” y se refiere a los habilitadores del bienestar, ahí está la seguridad digital como garante de las condiciones básicas para que todo lo demás funcione. Si no hay confianza digital, no hay desarrollo posible.

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; Privacidad de la Información, 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 seguridada, 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.

2.1 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 de la Información 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

Con el fin de garantizar la viabilidad a la Política de Seguridad Digital de la Institución Universitaria Digital de Antioquia, es fundamental situarse en la Constitución Política de

Colombia de 1991; específicamente en el Artículo 20, que trata de las garantías a la libertad de expresar y difundir el pensamiento y opiniones de toda persona, y el derecho a informar y recibir información veraz e imparcial; el Artículo 76 que establece el espectro electromagnético como un bien público inajenable e imprescriptible, sujeto a la gestión y control del Estado; y el Artículo 101 que incluye al espectro electromagnético como parte del territorio colombiano.

Así mismo, la presente Política se alinea con la Ley 1341 de 2009, también conocida como la "Ley TIC", la cual define el marco general para el desarrollo de las Tecnologías de la Información y las Comunicaciones en Colombia, estableciendo principios orientadores que buscan promover el acceso y uso eficiente de las TIC, incluyendo la seguridad como un elemento transversal para garantizar la confianza en el entorno digital. Esta normativa es esencial para la Institución Universitaria Digital de Antioquia, al ser un actor clave en la provisión de servicios educativos en un entorno fundamentalmente digital.

En el ámbito de la protección de datos personales, esta Política se enmarca rigurosamente en lo dispuesto por la Ley 1581 de 2012 – Ley General de Protección de Datos Personales, y su reglamentario el Decreto 1377 de 2013, que establece las disposiciones para el tratamiento de datos personales, los derechos de los titulares y los deberes de los responsables y encargados del tratamiento. De igual manera, se considera la Ley 1266 de 2008, o "Ley de Habeas Data", la cual regula el manejo de la información contenida en bases de datos personales, garantizando a las personas el derecho a conocer, actualizar y rectificar la información que sobre ellas repose en dichas bases de datos. Complementariamente, la Ley 1273 de 2009, que tipifica delitos informáticos y protege la información y los datos personales a través del establecimiento de sanciones penales, subraya la importancia de implementar medidas de seguridad robustas para prevenir y castigar conductas que atenten contra la seguridad digital.

Adicionalmente, la Política de Seguridad Digital de la Institución acoge los "Lineamientos de seguridad digital" establecidos en el CONPES 3854 de 2016. Este documento de política pública define la visión y los principios que deben guiar la gestión de la seguridad digital en el Estado colombiano, promoviendo un entorno digital confiable y resiliente. La adhesión a estos lineamientos asegura que la Institución Universitaria Digital de Antioquia no solo cumpla con estándares nacionales, sino que también contribuya al objetivo superior del país de fortalecer la seguridad en el ciberespacio.

También el Plan Nacional de Desarrollo “Colombia Potencia Mundial Para la Vida”, específicamente en el pilar denominado “Seguridad Humana y Justicia Social”, en el cual se encuentra el catalizador “Habilitadores que potencian la seguridad humana y las oportunidades de bienestar”, en el pilar "Seguridad Humana y Justicia Social" su numeral

octavo, “Seguridad digital confiable para la garantía de las libertades, la protección de la dignidad y el desarrollo integral de las personas”, se evidencia la apuesta del Gobierno Nacional por la protección de las personas, frente a las amenazas a sus derechos por el uso de las TIC. Este pilar es una respuesta que surge como contramedida a la amenaza actual que pone en riesgo los medios de vida y la dignidad de las personas, limitando sus libertades y su desarrollo integral. Una situación que, en caso de no cuidarse, puede producir nuevas condiciones de vulnerabilidad o profundizarlas en quienes ya las viven. Por esta razón, el Gobierno Nacional ha tomado medidas ante las posibles amenazas en pro de garantizar la seguridad y confiabilidad a toda la población.

Coherente con esa responsabilidad, la Institución Universitaria Digital de Antioquia, dentro de su Plan de Desarrollo, en su eje estratégico “Consolidación del modelo educativo de la IU Digital”, busca brindar todas las herramientas para contrarrestar las posibles amenazas a las que se vea enfrentada la Institución y quienes la componen. Así pues, se proyecta esta Política con el fin de brindar seguridad y confiabilidad a todos los integrantes de la comunidad universitaria.

Para garantizar el cumplimiento de la Política de Seguridad Digital de la Institución Universitaria Digital de Antioquia, es fundamental que ésta se enmarque en la legislación colombiana vigente en la materia, especialmente en cuanto a las regulaciones de protección de datos señaladas en la Ley 1581 del 2012. En este sentido, se hace necesario establecer una colaboración obligatoria con la entidad encargada de la protección y almacenamiento de datos, es decir, la Superintendencia de Industria y Comercio (SIC).

4.2 Marco Referencial

La presente política se fundamenta en un marco referencial integrado por mejores prácticas, estándares internacionales y modelos de gestión reconocidos, que proporcionan los lineamientos técnicos y metodológicos para la implementación, operación y mejora continua de la seguridad digital en la Institución.

- Normas Técnicas Internacionales de la Serie ISO/IEC 27000: La política adopta los principios y requisitos de las normas internacionales más relevantes en seguridad de la información. En particular:
    - ISO/IEC 27001: Proporciona los requisitos para establecer, implementar, mantener y mejorar un sistema de Gestión de Seguridad de la Información (SGSI).
    - ISO/IEC 27002: Sirve como guía de mejores prácticas para los controles de seguridad de la información, orientando la selección e implementación de medidas de protección.

- ISO/IEC 27005: Define las directrices para la gestión de riesgos de seguridad de la información, fundamentales para el proceso de identificación, análisis y tratamiento de riesgos digitales.
- ISO 22301: Establece los requisitos para un sistema de Gestión de Continuidad del Negocio, asegurando la capacidad de la Institución para responder y recuperarse de incidentes disruptivos.

- Modelo de Seguridad y Privacidad de la Información: Se recogen las mejores prácticas nacionales e internacionales para suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo de la seguridad y privacidad de la información en la Institución.
- Modelo Integrado de Planeación y Gestión (MIPG): Este marco de referencia, adoptado por la administración pública colombiana, es integrado para dirigir, planear, ejecutar, hacer seguimiento, evaluar y controlar la gestión de la seguridad digital, alineándose con los principios de integridad

4.3 Conceptos Clave

Gobierno, Estructura Humana y Concienciación

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:

1. 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.
2. 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.
3. 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

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 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.

4.4 Gestión de recursos humanos

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.
- 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.

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

6. **Respuesta y Recuperación ante Incidentes:**

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

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 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:

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

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 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 de riesgos 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)

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

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