

Vigilada **Mineducación**

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN

UNIVERSIDAD **EL BOSQUE**

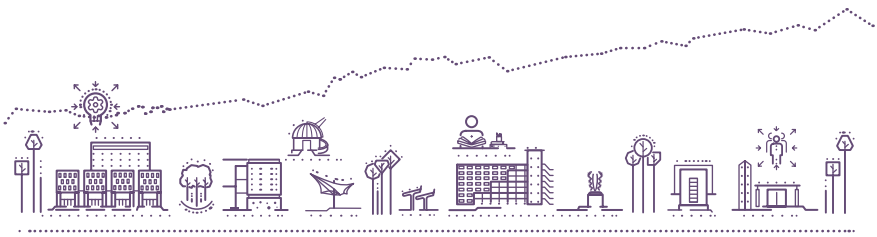
Por una cultura de la vida, su calidad y su sentido

UNIVERSIDAD
EL BOSQUE

Por una cultura de la vida,
su calidad y su sentido.

Vigilada **Mineducación**

POLÍTICA DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN



UNIVERSIDAD
EL BOSQUE

Por una cultura de la vida,
su calidad y su sentido

Publicación octubre de 2026

DIRECTIVOS (2025-2027)

Juan Carlos López Trujillo
Presidente de El Claustro

Juan Guillermo Marín Moreno
Presidente Consejo Directivo

Miguel Ruiz Rubiano
Rector

Juan Carlos Sánchez París
Vicerrector Académico

Carolina Vizcaíno Sarmiento
Vicerrectora de Investigaciones

Ricardo Enrique Gutiérrez Marín
Vicerrector Administrativo

Cristina Matiz Mejía
Secretaria General

ÁREA DE DISEÑO ENCARGADA

Centro de Diseño y Comunicación
Facultad de Creación y Comunicación
Universidad El Bosque

DISEÑO Y DIAGRAMACIÓN

Salomé Muñoz Gómez
Diseñadora editorial

© **UNIVERSIDAD EL BOSQUE**

Dirección: Carrera 7 B bis No. 132 - 25
Teléfono: (601) 648 9000, ext. 1453
www.unbosque.edu.co
Bogotá, D. C., Colombia, 2024

Universidad El Bosque | Vigilada Mineducación. Reconocimiento como universidad: Resolución 327 del 5 de febrero de 1997, MEN. Reconocimiento de personería jurídica: Resolución 11153 del 4 de agosto de 1978, MEN. Acreditación institucional de alta calidad mediante: Resolución 13172 del 17 de julio de 2020. Por seis (6) años, del Ministerio de Educación Nacional.

CONTENIDO

ACUERDO NUM. 18723 DE 2026 6

1 Glosario de siglas 7

2 Introducción 9

2.1 Propósito general y relación con el PEI 9

2.2 Resultado esperado y razones que sustentan la adopción 10

3 Estructura genera l2

4 Contexto institucional 14

4.1 Características internas 14

4.2 Características del entorno 15

4.3 Vínculo con la identidad institucional 15

4.4 Vínculo con los grupos de interés 16

5 Alcance de la política 17

5.1 Sujetos de aplicación 17

5.2 Objeto 17

5.3 Contenido 18

5.4 Exclusiones 18

6 Desarrollo de la política 19

6.1 Elementos sustantivos y articulación con el PEI 19

6.2 Declaración general de seguridad y privacidad de la informació 20

7 Principios rectores 21

8 Objetivos 23

8.1 Objetivo genera 23

8.2 Objetivos específicos 23

9 Gestión del riesgo de seguridad de la información 25

10 Dominios de políticas específicas 27

10.1 Controles organizacionales 27

10.2 Controles de personas 29

10.3 Controles físicos 29

10.4 Controles tecnológicos 30

11 Programa institucional de privacidad y protección de datos personales 32

11.1 Principios del tratamiento 32

11.2 Lineamientos del programa 33

12 Cultura y educación en seguridad de la información 35

13 Estrategias de implementación, acciones e instrumentos 37

13.1 Plan de Seguridad 37

13.2 Instrumentos derivados 38

14 Gobernanza de la política 39

14.1 Estructura organizacional relacionada 39

14.2 Roles y responsabilidades 40

14.3 Instancias de aprobación, actualización, seguimiento y evaluación 41

15 Evaluación y mejora continua 42

15.1 Mecanismos de medición 42

15.2 Ciclo de mejora continua 44

15.3 Criterios para el inicio de la actualización 44

16 Referencias 46

Normativa nacional 46

Documentos institucionales 47

Estándares y literatura técnica 48

Anexo A Mapa de dominios de control 50

Anexo B Controles del programa de privacidad 52

Anexo C Controles del programa de educación en seguridad 54

Anexo D Control de cambios 56

ACUERDO NÚM. 18723 DE 2026

(26 de agosto)

"Por el cual se aprueba la actualización de la Política de Seguridad y Privacidad de la Información de la Universidad El Bosque"

El Consejo Directivo, en uso de las atribuciones legales que le confiere el Estatuto de la Universidad El Bosque, en su sesión ordinaria del día 26 de agosto de 2026, Acta Núm. 1.353 y,

CONSIDERANDO

A. Que con fundamento en el literal d) del Artículo 19 de los Estatutos institucionales, el Consejo Directivo es competente para aprobar los reglamentos y políticas institucionales.

B. Que la Secretaria General, doctora Cristina Matiz Mejía, presentó a consideración del Consejo Directivo, previa recomendación del Consejo Académico, la actualización de la Política de Seguridad y Privacidad de la Información de la Universidad El Bosque.

C. Que el Consejo Directivo aprobó por unanimidad la solicitud.

Con base en lo anteriormente expuesto,

ACUERDA:

Artículo único. APROBAR la actualización de la Política de Seguridad y Privacidad de la Información de la Universidad El Bosque que se adjunta bajo el Anexo Núm. 1 a este Acuerdo.

Articulo segundo. DEROGAR el Acuerdo Núm. 15893 del 20 de febrero de 2019 expedido por este mismo órgano.

NOTIFÍQUESE Y CÚMPLASE

Dado en Bogotá D.C., a los veintiséis (26) días del mes de agosto del año (2026).

JUAN GUILLERMO MARÍN MORENO
Presidente

CRISTINA MATIZ MEJÍA
Secretaria

1 Glosario de siglas



Para efectos de la interpretación y aplicación de la presente política, se adoptan las siguientes siglas y abreviaturas:

Sigla	Significado
ANS	Acuerdo de Niveles de Servicio.
BPSyC	Enfoque Biopsicosocial y Cultural, sello institucional de la Universidad El Bosque.
BYOD	Bring Your Own Device – uso de dispositivos personales para acceder a servicios institucionales.
CESU	Consejo Nacional de Educación Superior.
CIS	Center for Internet Security.
CNA	Consejo Nacional de Acreditación.
COBIT	Control Objectives for Information and Related Technologies – marco de gobierno y gestión de la información y la tecnología de ISACA.
DLP	Data Loss Prevention – Prevención de fuga de información.
EIP	Evaluación de Impacto en la Privacidad – Análisis previo del riesgo para los derechos de los titulares de datos personales.

Sigla	Significado
IA	Inteligencia Artificial.
IoT	Internet of Things – Internet de las cosas; dispositivos conectados no convencionales.
ISO/ IEC	International Organization for Standardization / International Electrotechnical Commission.
ITIL	Information Technology Infrastructure Library – marco de gestión de servicios de TI. La Universidad adopta ITIL 4 como base de la gestión de servicios, peticiones e incidentes.
KGI	Key Goal Indicator – Indicador clave de logro de objetivos.
KPI	Key Performance Indicator – Indicador clave de desempeño.
MFA	Multi-Factor Authentication – Autenticación multifactor.
NIST	National Institute of Standards and Technology (Estados Unidos).
PDCM	Plan de Desarrollo, Consolidación y Mejoramiento 2025-2027.
PDI	Plan de Desarrollo Institucional 2022-2027.
PDS	Plan de Seguridad – Instrumento de planeación estratégica de la seguridad de la información.
PEI	Proyecto Educativo Institucional, versión 2025.
PHVA	Planear - Hacer - Verificar - Actuar (ciclo de mejora continua).
RACI	Responsible, Accountable, Consulted, Informed – Matriz de asignación de responsabilidades.
RNBD	Registro Nacional de Bases de Datos administrado por la Superintendencia de Industria y Comercio.
SGPI	Sistema de Gestión de Privacidad de la Información.
SGSI	Sistema de Gestión de Seguridad de la Información.
SIC	Superintendencia de Industria y Comercio.
SOC 2	System and Organization Controls 2 – Informe de atestación sobre controles de una organización de servicios, emitido conforme a los Trust Services Criteria del AICPA.
TIC	Tecnologías de la Información y las Comunicaciones.
UEB	Universidad El Bosque.
ZTNA	Zero Trust Network Access – Acceso bajo el principio de confianza cero.

2 Introducción



El Consejo Directivo mediante Acuerdo Núm. 18257 de 2025 actualizó el Proyecto Educativo Institucional de la Universidad El Bosque (en adelante, PEI). El nuevo PEI propone la consolidación de un modelo educativo centrado en el aprendizaje del estudiante, la formación integral a lo largo de la vida, la innovación y la transferencia del conocimiento, así como el fortalecimiento de la responsabilidad social y la sostenibilidad. En coherencia con lo anterior, la presente política incorpora enfoques contemporáneos que responden a los retos de la educación superior, las dinámicas del entorno, la transformación digital y el compromiso institucional con la cultura de la vida, su calidad y su sentido, garantizando que los lineamientos aquí establecidos se articulen con la misión, la visión, el buen gobierno institucional y los procesos de planeación y aseguramiento de la más alta calidad.

2.1 Propósito general y relación con el PEI

La Política de Seguridad y Privacidad de la Información es la **política marco** del cuerpo normativo de seguridad de la Universidad El Bosque. Establece la posición institucional frente a la protección de los activos de información,

define los dominios de control que la Universidad se obliga a mantener y fija las reglas que gobiernan el tratamiento de los datos personales de los que la Institución es responsable o encargada. De ella se derivan y a ella se subordinan las políticas específicas de la Universidad en materia de correo electrónico institucional, uso de internet y servicios de red, tratamiento de datos personales y gobernanza de datos, junto con las normas, procedimientos, guías técnicas y líneas de base que las desarrollan.

Su relación con el PEI es de doble naturaleza. Por una parte, la información es el sustrato material del quehacer misional: sin integridad de los registros académicos no hay fe pública en el título; sin confidencialidad de los datos de salud recogidos en los escenarios de práctica no hay ejercicio ético de la formación clínica; sin disponibilidad de las plataformas no hay continuidad del aprendizaje. Los datos que la Universidad custodia no son un activo abstracto: son la vida académica, la salud, la situación económica y la trayectoria personal de estudiantes, profesores, colaboradores y egresados. Protegerlos es una obligación ética antes que técnica, y así se asume en esta política.

2.2 Resultado esperado y razones que sustentan la adopción

El resultado esperado es que, al cierre del período del PDCM 2025–2027, la Universidad opere un Sistema de Gestión de Seguridad de la Información verificable, medible y gobernable, articulado con un Sistema de Gestión de Privacidad de la Información que permita demostrar —ante los titulares de los datos, ante la Superintendencia de Industria y Comercio, ante los pares académicos y ante los organismos de inspección, vigilancia y control— que el tratamiento de la información institucional y de los datos personales se realiza conforme a la ley, con controles proporcionados al riesgo y con trazabilidad de las decisiones.

La adopción de esta versión responde a cuatro razones. Primera, la obsolescencia normativa de la 1.ª edición (2019): su marco de referencia se apoya en ISO/IEC 27001:2013, ISO/IEC 27002 e ISO/IEC 27005 en ediciones hoy superadas, sin recoger la reestructuración de controles introducida por ISO/IEC 27002:2022 ni la Enmienda 1:2024 sobre acción climática. Segunda, una brecha de contenido: el documento se denomina Política de Seguridad y Privacidad de la Información, pero no desarrolla la privacidad. No define el programa de privacidad, no reconoce los derechos de los titulares, no regula las autorizaciones de tratamiento, las transferencias y transmisiones internacionales, las evaluaciones de impacto ni la notificación de incidentes que comprometan datos personales.

Tercera, se requiere ampliar la cobertura: las nueve políticas específicas de la edición anterior corresponden a un subconjunto de los dominios de control y omiten materias hoy indispensables —clasificación de activos, gestión de identidades, gestión de incidentes, continuidad del negocio, seguridad en servicios de nube, gestión de vulnerabilidades, registro y monitoreo, seguridad del personal, seguridad física, uso de inteligencia artificial y cultura de seguridad—. Cuarta, las recomendaciones de los pares académicos en la visita de acreditación institucional, que señalaron la necesidad de actualizar el cuerpo de políticas, articularlas con el PEI y dotarlas de mecanismos verificables de seguimiento. La edición de 2019 no incluye objetivos medibles, indicadores, matriz de responsabilidades y criterios de actualización, por lo que su eficacia no era demostrable. Esta versión corrige esas cuatro deficiencias, en cumplimiento del resultado clave del Proyecto 10 del PDCM 2025–2027 —políticas institucionales actualizadas y alineadas con servicios y productos, con meta del 100 % a 2027— y en articulación con el Proyecto 14, Desarrollo de campus, infraestructura y servicios digitales.

3 Estructura general



Conceptualmente, esta política se apoya en cuatro líneas. La primera es la comprensión de la seguridad como un proceso dinámico y no como un producto o un estado estático (Schneier, 2000), de lo que se sigue que sus disposiciones son revisables y que su valor depende de la operación sostenida y evidenciada de los controles. La segunda es la protección de la tríada de seguridad de la información —confidencialidad, integridad y disponibilidad—, entendida como el objetivo irrenunciable de todo el cuerpo normativo. La tercera es la gestión basada en riesgo: cada control existe porque mitiga un riesgo identificado sobre un activo valorado, y ningún control cuyo costo de operación supere el valor del activo que protege debe implantarse. La cuarta es la jerarquía normativa: la política define la dirección y el "por qué"; las normas definen el "qué"; los procedimientos, el "cómo"; las guías técnicas, la operación sobre sistemas concretos; y las líneas de base, los umbrales mínimos auditables

En materia de estándares, la política estructura el Sistema de Gestión de Seguridad de la Información conforme a ISO/IEC 27001:2022 y su Enmienda 1:2024, selecciona sus controles conforme a ISO/IEC 27002:2022, mide su desempeño conforme a ISO/IEC 27004:2016, gestiona el riesgo conforme a ISO/

IEC 27005:2022 e ISO 31000:2018, y establece el Sistema de Gestión de Privacidad de la Información conforme a ISO/IEC 27701:2025, norma autónoma en su segunda edición. Complementariamente adopta ISO/IEC 27017:2015 e ISO/IEC 27018:2019 para servicios de nube, ISO 22301:2019 para continuidad del negocio e ISO/IEC 42001:2023 para la gobernanza de la inteligencia artificial. Como marcos de referencia operativa se emplean el NIST Cybersecurity Framework 2.0, el NIST SP 800-53 Rev. 5 y el NIST SP 800-207 sobre arquitectura de confianza cero, los CIS Critical Security Controls v8.1 para la priorización de salvaguardas, las plantillas del SANS Institute (2026) para privacidad y educación en ciberseguridad, adoptadas como normas técnicas derivadas en los Anexos B y C, y COBIT 2019 como referencia para la alineación entre el gobierno de la información y el gobierno institucional. En materia de gestión del servicio, la política se apoya en ITIL 4, marco adoptado por la Dirección de Tecnología como base de la operación de sus servicios; de él se toman las prácticas de gestión de la seguridad de la información, mesa de servicio, gestión de incidentes, gestión de problemas, gestión de peticiones de servicio, habilitación del cambio, gestión de activos de TI, monitoreo y gestión de eventos, gestión de la continuidad del servicio, gestión de proveedores y gestión de niveles de servicio. La articulación entre los tres cuerpos es deliberada: COBIT orienta quién decide y rinde cuentas, ISO/IEC 27001 define qué debe controlarse e ITIL 4 determina cómo se opera y se mide el servicio que sostienen esos controles.

En materia normativa, la política se enmarca en la Constitución Política de Colombia (artículos 15, 20 y 61), en la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 —compilado en el Decreto Único Reglamentario 1074 de 2015— sobre protección de datos personales, en la Ley 1266 de 2008 sobre hábeas data financiero, en la Ley 1273 de 2009 sobre delitos informáticos, en la Ley 527 de 1999 sobre validez probatoria de los mensajes de datos, en la Ley 23 de 1982 y la Ley 1915 de 2018 sobre derecho de autor, en la Ley 2300 de 2023 en materia de comunicaciones no solicitadas, en la Ley 1978 de 2019 en materia de TIC, y en el Decreto 1330 de 2019 junto con el Acuerdo 02 de 2020 del CESU respecto de las condiciones de calidad institucional. Internamente, se subordina a los Estatutos institucionales (2020) y al Código de Buen Gobierno (2022), y constituye la política marco de la que se derivan la Política de Tratamiento de Datos Personales (2022), la Política de Gobernanza de Datos (2024), la Política de Uso Adecuado del Correo Electrónico Institucional, la Política de Uso Adecuado de Internet y de los Servicios de Red y la Política para el Diseño y Apropiación de Entornos Digitales (2023).

4 Contexto institucional



4.1 Características internas

La Universidad El Bosque es una institución de educación superior de carácter privado, acreditada institucionalmente en alta calidad, que a 2025 ofrece 140 programas distribuidos en diez facultades y dos departamentos académicos, además de una amplia oferta de educación continuada. Esta configuración determina un inventario de activos de información excepcionalmente diverso: registros académicos con efectos de fe pública, historias clínicas y datos de salud generados en escenarios de práctica, datos de investigación con seres humanos sujetos de aval en comités de ética, información financiera y de talento humano, propiedad intelectual e investigación no publicada, y datos personales de estudiantes, aspirantes, egresados, colaboradores, proveedores y participantes de proyectos de extensión.

Con lo anterior, la Universidad trata datos personales sensibles de manera ordinaria. Los datos de salud recogidos en la relación docencia-servicio, los datos biométricos de control de acceso, los datos de bienestar universitario y los datos de investigación biomédica se encuentran sujetos al régimen reforzado del artículo 5.º de la Ley 1581 de 2012. La edición anterior de esta política no reconocía esa condición. Esta versión la asume como premisa y estructura en consecuencia el programa de privacidad del numeral 6.7.

En cuanto a capacidades, la Universidad cuenta con una Dirección de Tecnología responsable de la infraestructura y los servicios digitales, con una Coordinación de Seguridad de la Información como instancia de definición y verificación de controles, y con un Comité de Tecnología como órgano de decisión táctica y estratégica. El PDCM 2025–2027 refuerza estas capacidades al inscribir la seguridad dentro del **Campus Digital** (Proyecto 14), que articula infraestructura física y tecnológica, transformación digital, inteligencia artificial y gestión estratégica de datos bajo criterios explícitos de retorno sobre la inversión, e incorpora entre sus propósitos el seguimiento y control integral de procesos clave y riesgos organizacionales. La política reconoce, no obstante, que la madurez de los dominios de control es desigual y que su despliegue debe ser gradual y priorizado por riesgo, conforme al Plan de Seguridad del numeral 6.9.

4.2 Características del entorno

El entorno externo presenta cuatro presiones convergentes. La de riesgo: el sector de educación superior se ha consolidado como blanco preferente de campañas de *ransomware* y de compromiso de credenciales, por la amplitud de sus comunidades, la rotación anual de usuarios, la heterogeneidad de sus sistemas y la cultura de apertura propia de la vida académica, que no puede ni debe suprimirse. La regulatoria: el desarrollo del régimen de protección de datos personales, las exigencias de registro y actualización ante el RNBD y el escrutinio creciente sobre el tratamiento de datos sensibles elevan el estándar de diligencia exigible. La tecnológica: la migración a servicios de nube, la desaparición del perímetro de red y la irrupción de la inteligencia artificial generativa desplazan el control desde la infraestructura hacia la identidad, el dato y el proveedor. Y la de cadena de suministro: una parte creciente del riesgo institucional reside hoy en terceros que procesan información de la Universidad, lo que obliga a trasladar exigencias de control a la relación contractual.

4.3 Vínculo con la identidad institucional

Esta política es una expresión operativa de la Misión. Los principios antropológicos, que sitúan la dignidad de la persona como imperativo supremo, fundamentan la comprensión del dato personal como extensión de la persona y no como recurso disponible; de ahí que la política subordine cualquier finalidad institucional al respeto de los derechos del titular. Los principios éticos sustentan el deber de veracidad, transparencia y responsabilidad en el tratamiento de la información, y el rechazo del uso encubierto o desviado de los datos. Los principios epistemológicos, que promueven la libertad de pensamiento y la actitud crítica, imponen que los controles de seguridad se diseñen de modo que protejan sin restringir la libertad académica ni la circulación legítima del conocimiento; la seguridad no puede convertirse en un obstáculo para la investigación ni en un

instrumento de censura. Los principios sociales fundamentan la corresponsabilidad: la seguridad es una construcción colectiva en la que cada miembro de la comunidad tiene un deber propio. Y el Enfoque BPSyC exige atender el impacto humano de los incidentes, en particular cuando comprometen datos sensibles o afectan la intimidad de las personas.

4.4 Vínculo con los grupos de interés

Grupo de interés	Vinculación con la política
Estudiantes, aspirantes y egresados	Titulares de datos personales y, en muchos casos, de datos sensibles; destinatarios de las garantías de confidencialidad, exactitud y ejercicio de derechos.
Profesores e investigadores	Custodios de información académica, evaluativa y de investigación; responsables del tratamiento de datos de participantes en estudios y de la reserva sobre resultados no publicados.
Personal administrativo y directivo	Propietarios de activos de información en sus procesos; responsables de clasificar la información y de autorizar los accesos que la afectan.
Pacientes y usuarios de escenarios de práctica	Titulares de datos de salud tratados en la relación docencia-servicio, sujetos al régimen reforzado de datos sensibles.
Proveedores, contratistas y encargados del tratamiento	Sujetos de obligaciones contractuales de seguridad y privacidad, de evaluación previa y de verificación periódica.
Superintendencia de Industria y Comercio y demás autoridades	Destinatarias del registro de bases de datos, de los reportes de incidentes y de la evidencia de cumplimiento.
Organismos de inspección, vigilancia y control, y pares académicos	Destinatarios de la evidencia sobre gobierno, medición y mejora continua del SGSI y del SGPI.

5 Alcance de la política



5.1 Sujetos de aplicación

La presente política es de obligatorio cumplimiento para todos los procesos institucionales de la Universidad El Bosque y para todas las personas que accedan, traten, custodien o dispongan de información institucional o de datos personales bajo responsabilidad de la Institución, a saber: estudiantes de todos los niveles y modalidades; aspirantes; profesores de planta, de cátedra y visitantes; investigadores; personal administrativo y directivo; egresados; contratistas, practicantes, pasantes y personal en misión; proveedores y encargados del tratamiento; y, en general, cualquier tercero vinculado por contrato o convenio que trate información de la Universidad.

5.2 Objeto

Constituyen objeto de esta política todos los activos de información de la Universidad, cualquiera que sea su formato, soporte o ubicación: la información en medio digital, físico o verbal; las bases de datos y los sistemas de información académicos, administrativos, financieros, de investigación y de salud; la infraestructura tecnológica, las redes y los servicios de nube contratados; los equipos

de cómputo, dispositivos móviles y dispositivos personales que accedan a información institucional; los dispositivos IoT, biomédicos y de laboratorio conectados; el software desarrollado interna o externamente; los servicios de inteligencia artificial que traten información institucional; las instalaciones físicas donde reside o se procesa información; y los datos personales de los que la Universidad sea responsable o encargada del tratamiento.

5.3 Contenido

La política desarrolla: la declaración general de seguridad y privacidad de la alta dirección; los principios rectores; los objetivos del sistema de gestión; los dominios de políticas específicas organizados en controles organizacionales, de personas, físicos y tecnológicos; el programa institucional de privacidad y protección de datos personales; el programa de cultura y educación en seguridad; el modelo de gestión del riesgo; las estrategias de implementación y los instrumentos derivados; la gobernanza del sistema; y los mecanismos de medición, evaluación y actualización.

5.4 Exclusiones

No son objeto de esta política la información y los sistemas de terceros sobre los cuales la Universidad no ejerce responsabilidad ni encargo, ni los dispositivos personales que no accedan a información institucional. La política tampoco sustituye las obligaciones específicas derivadas de la habilitación de servicios de salud en los escenarios de práctica propios, que se rigen adicionalmente por la normativa sectorial aplicable, ni las condiciones contractuales pactadas con proveedores, que se entienden complementarias y de obligatoria observancia.

6 Desarrollo de la política



6.1 Elementos sustantivos y articulación con el PEI

La Universidad El Bosque reconoce la información como un activo de alta importancia que sustenta sus funciones misionales de docencia, investigación y extensión, y los procesos de apoyo que las hacen posibles. En consecuencia, establece, implementa, mantiene y mejora de manera continua un **Sistema de Gestión de Seguridad de la Información** y un **Sistema de Gestión de Privacidad de la Información,** integrados entre sí y articulados con el sistema de gestión institucional.

Tabla 1. Articulación entre los postulados fundamentales del PEI (2025) y el desarrollo de la política.

Postulado del PEI (2025)	Traducción en esta política
Dignidad de la persona humana como imperativo supremo	El dato personal se trata como extensión de la persona: régimen reforzado para datos sensibles y derechos del titular garantizados.
Modelo centrado en el aprendizaje del estudiante	Integridad y disponibilidad de los registros académicos y de las plataformas de aprendizaje como condición de continuidad del proceso formativo.
Formación para la investigación y transferencia de conocimiento	Protección de la investigación no publicada y de la propiedad intelectual; tratamiento de datos de participantes en estudios conforme a los avales de los comités de ética.
Ecosistemas de innovación	Marco de gobernanza de la inteligencia artificial conforme a ISO/IEC 42001:2023, que habilita la adopción con salvaguardas de datos y supervisión humana.
Comunidad autónoma, pluralista, crítica y librepensadora	Los controles de seguridad protegen sin restringir la libertad académica corresponsable; su aplicación no puede convertirse en instrumento de censura ni de vigilancia individual injustificada.
Responsabilidad social y sostenibilidad	Consideración del cambio climático como factor del contexto del SGSI, conforme a la Enmienda 1:2024 de ISO/IEC 27001, y continuidad de los servicios esenciales.

6.2 Declaración general de seguridad y privacidad de la información

La alta dirección de la Universidad El Bosque declara:

La Universidad El Bosque, como institución de educación superior, gestiona la seguridad y la privacidad de la información mediante la incorporación, el seguimiento y la mejora continua de los controles necesarios, sustentados en una adecuada gestión de los riesgos, que aseguren la preservación de la confidencialidad, la integridad y la disponibilidad de la información bajo su responsabilidad, así como el respeto de los derechos de los titulares de los datos personales que trata, en concordancia con los marcos legales, normativos, regulatorios y contractuales que le apliquen, y en coherencia con el imperativo de la dignidad de la persona humana que orienta su Misión. Este compromiso se extiende a la asignación de los recursos necesarios, a la exigencia de su cumplimiento a toda la comunidad universitaria y a terceros vinculados, y a la rendición de cuentas periódica sobre sus resultados.

7 Principios rectores



Los principios que orientan la presente política se fundamentan en lo dispuesto por el PEI (2025), el cual define los principios fundamentales de la misión como el marco axiológico e institucional que rige la actuación universitaria. En consecuencia, esta política se estructura conforme a los principios antropológicos, éticos, epistemológicos, estéticos, sociales, biológicos, institucionales y psicológicos, entendidos como criterios rectores para garantizar la formación integral desde el enfoque biopsicosocial y cultural, la promoción de la dignidad humana, la responsabilidad social universitaria, la construcción crítica del conocimiento, la convivencia pluralista, la protección de la vida y los ecosistemas, así como el aseguramiento de una cultura institucional orientada a la excelencia, la calidad y la mejora continua.

- **Dignidad y protección de la persona.** La finalidad última de la seguridad es proteger a las personas cuyos datos y actividad representa la información, no únicamente a los sistemas que la contienen.
- **Gestión basada en riesgo.** Todo control responde a un riesgo identificado, valorado y priorizado; el costo de operación de una salvaguarda no debe superar el valor del activo que protege.

- **Responsabilidad demostrada.** No basta con cumplir: la Universidad debe poder evidenciar que cumple, mediante registros, indicadores y auditorías.
- **Privacidad y seguridad desde el diseño y por defecto.** Los proyectos, sistemas y contratos incorporan requisitos de seguridad y privacidad desde su concepción, no como añadido posterior.
- **Minimización y limitación de la finalidad.** Se trata únicamente la información necesaria para la finalidad informada y por el tiempo que esa finalidad justifique.
- **Mínimo privilegio y segregación de funciones.** Los accesos se otorgan en la medida estrictamente necesaria y las funciones críticas se separan para evitar concentración de riesgo.
- **Libertad académica.** Los controles protegen sin restringir la investigación, la deliberación ni la circulación legítima del conocimiento.
- **Corresponsabilidad.** Cada miembro de la comunidad universitaria es responsable de la información que trata y gestiona; la seguridad no se delega íntegramente en la Coordinación de Seguridad de la Información o la Dirección de Tecnología.
- **Transparencia.** La comunidad conoce qué se controla, con qué finalidad y cómo ejercer sus derechos.
- **Mejora continua.** El sistema se revisa conforme al ciclo PHVA y a la evolución del contexto y de las amenazas.

8 Objetivos



8.1 Objetivo general

Establecer la posición institucional y los lineamientos que rigen la seguridad y la privacidad de la información en la Universidad El Bosque, orientando el tratamiento de los riesgos que afectan la confidencialidad, la integridad y la disponibilidad de la información, garantizando el respeto de los derechos de los titulares de los datos personales, mediante un sistema de gestión medible, gobernado y sujeto a mejora continua.

8.2 Objetivos específicos

Los objetivos específicos se formulan bajo criterios SMART —específicos, medibles, alcanzables, realistas y acotados en el tiempo— y se miden mediante los indicadores del numeral 15.1.

Tabla 2. Objetivos específicos formulados bajo criterios SMART.

N.º	Objetivo específico	Horizonte
OE-1	Mantener actualizado el inventario de activos de información con propietario asignado y clasificación vigente para el 100 % de los procesos institucionales.	Diciembre de 2027
OE-2	Mantener el perfil de riesgo residual de seguridad de la información en niveles bajo o moderado, con plan de tratamiento formal para el 100 % de los riesgos que superen el nivel aceptable.	Permanente, desde 2026
OE-3	Implementar el programa institucional de privacidad, con registro y actualización de las bases de datos ante el RNBD y trazabilidad del 100 % de las solicitudes de ejercicio de derechos.	Diciembre de 2026
OE-4	Atender el 100 % de las solicitudes de ejercicio de derechos de los titulares dentro de los términos legales, con tiempo medio de respuesta inferior a diez (10) días hábiles.	Permanente, desde 2026
OE-5	Lograr que al menos el 85 % de la comunidad universitaria complete anualmente la formación institucional en seguridad y protección de datos personales.	Anual, desde 2027
OE-6	Reducir el tiempo medio de detección y contención de incidentes de seguridad de alto impacto por debajo de cuatro (4) horas hábiles.	Diciembre de 2027
OE-7	Someter el 100 % de los proveedores críticos que traten información institucional a evaluación previa de seguridad y privacidad y a cláusulas contractuales específicas.	Diciembre de 2027
OE-8	Ejecutar anualmente el programa de auditoría interna del SGSI y cerrar el 100 % de los hallazgos críticos dentro de los plazos comprometidos.	Anual, desde Diciembre de 2026
OE-9	Realizar evaluación de impacto en la privacidad al 100 % de los tratamientos nuevos que involucren datos sensibles, decisiones automatizadas o inteligencia artificial.	Diciembre de 2027

9 Gestión del riesgo de seguridad de la información



El análisis de riesgos justifica cada control de esta política. La Universidad mantiene una metodología formal de gestión del riesgo de seguridad de la información, conforme a ISO/IEC 27005:2022 e ISO 31000:2018, integrada al sistema institucional de administración de riesgos y articulada con el seguimiento de riesgos organizacionales previsto en el Proyecto 14 del PDCM 2025–2027.

- La identificación del riesgo parte del inventario de activos de información y de la relación amenaza – vulnerabilidad – activo – impacto.
- La valoración considera la probabilidad de ocurrencia y el impacto sobre la confidencialidad, la integridad y la disponibilidad, así como el impacto sobre los derechos de los titulares cuando intervienen datos personales.
- El tratamiento adopta una de cuatro vías: evitar la actividad que genera el riesgo, reducir mediante salvaguardas, compartir con terceros o aseguradores, o aceptar de forma informada y documentada cuando el costo de mitigación no se justifica.

- La aceptación de un riesgo residual por encima del nivel definido como aceptable requiere autorización expresa del Comité de Seguridad de la Información, motivación escrita, vigencia máxima de doce (12) meses y registro en el inventario de excepciones.
- El registro de riesgos se revisa al menos semestralmente y ante todo cambio significativo del contexto, incluidos los efectos del cambio climático sobre la continuidad de los servicios, conforme a la Enmienda 1:2024 de ISO/IEC 27001.

10 Dominios de políticas específicas



Los siguientes dominios constituyen el desarrollo temático de la política. Se organizan conforme a los cuatro temas de control de ISO/IEC 27002:2022 y sustituyen, ampliándolas, las nueve políticas específicas de la edición de 2019. El detalle de implementación de cada dominio corresponde a las normas, procedimientos y guías relacionados en el numeral 6.9 y mapeados en el Anexo A.

10.1 Controles organizacionales

- **Gestión de activos de información.** Todo activo de información tiene un propietario formalmente designado, responsable de determinar su nivel de protección. La Universidad mantiene un inventario actualizado y una escala institucional de clasificación, y exige el etiquetado de la información conforme a dicha escala antes de su uso, transferencia o publicación.

- **Control de acceso y gestión de identidades.** El acceso a la información institucional se concede únicamente a las personas autorizadas conforme a las funciones de su rol en los procesos formalmente definidos, bajo los principios de mínimo privilegio y necesidad de conocer. La Universidad gestiona el ciclo de vida completo de las identidades —altas, modificaciones, revisiones periódicas y bajas— y exige autenticación multifactor para los accesos privilegiados, remotos y a sistemas que traten datos sensibles.
- **Seguridad en la relación con proveedores y en la cadena de suministro.** Toda relación con proveedores que involucre activos de información se formaliza en un acuerdo que establezca expresamente la protección de la confidencialidad, la integridad y la disponibilidad de dichos activos. Los proveedores críticos y los encargados del tratamiento de datos personales se someten a evaluación previa de seguridad y privacidad, a cláusulas contractuales específicas y a verificación periódica; la Universidad podrá exigir evidencia independiente de control, tal como certificación ISO/IEC 27001 o informe SOC 2 Tipo II, cuando el riesgo lo justifique.
- **Gestión de incidentes de seguridad de la información.** La Universidad mantiene un procedimiento formal de detección, registro, clasificación, escalamiento, contención, erradicación, recuperación y análisis posterior de incidentes. Todo miembro de la comunidad universitaria tiene el deber de reportar los incidentes y las sospechas de incidente que conozca; el reporte oportuno y de buena fe no dará lugar por sí solo a medidas sancionatorias.
- **Continuidad del negocio y de los servicios de información.** Los procesos críticos deben contar con análisis de impacto, objetivos de tiempo y punto de recuperación definidos, y planes de continuidad y recuperación probados periódicamente, conforme a ISO 22301:2019.
- **Cumplimiento legal, regulatorio y contractual.** La Universidad identifica y mantiene actualizado el conjunto de obligaciones legales, regulatorias y contractuales aplicables a la seguridad y la privacidad, incluidas las relativas a propiedad intelectual, licenciamiento de software, protección de datos personales y conservación documental.
- **Gobernanza de la inteligencia artificial.** La adquisición, el desarrollo y el uso de sistemas de inteligencia artificial que traten información institucional se deben sujetar a evaluación previa de riesgos, a la prohibición de exponer información clasificada o datos personales en servicios no autorizados, a la exigencia de supervisión humana en decisiones con efectos académicos, disciplinarios, laborales o contractuales, y a los lineamientos de ISO/IEC 42001:2023.

10.2 Controles de personas

- **Seguridad en el ciclo de vida del vínculo.** Los procesos de selección, vinculación, cambio de rol y desvinculación incorporan controles de seguridad: verificación proporcional al nivel de acceso, suscripción de acuerdos de confidencialidad, entrega formal de activos y revocación oportuna de accesos.
- **Cláusulas de confidencialidad.** Los colaboradores, contratistas y terceros que accedan a información clasificada se obligación al cumplimiento de cláusulas de confidencialidad en los contratos que suscriben con la Universidad.
- **Cultura y educación en seguridad.** La Universidad debe mantener un programa permanente de formación y sensibilización, desarrollado en el numeral 6.8 y en el Anexo C.
- **Teletrabajo y trabajo remoto.** El teletrabajo se autoriza cuando se cumplen los requisitos administrativos, técnicos, de seguridad de la información y de ley aplicables a esa modalidad. El trabajo remoto se aprueba por la Dirección de Talento Humano, con solicitud del responsable del área y se avala por la Dirección de Tecnología de previa verificación de que las condiciones de acceso cumplen los requisitos institucionales de seguridad.
- **Escritorio y pantalla limpios.** Los miembros de la comunidad universitaria deben conservar sus puestos de trabajo libres de información institucional susceptible de ser alcanzada, copiada o utilizada por personas no autorizadas, y bloquean la pantalla de sus equipos cuando no los estén utilizando.
- **Régimen disciplinario.** El incumplimiento de esta política da lugar a las medidas académicas, administrativas, disciplinarias, contractuales o legales que correspondan, conforme al Reglamento Estudiantil, el Estatuto Docente, el Reglamento Interno de Trabajo, los contratos aplicables y la ley. Las medidas se adoptan por la instancia competente, de manera consistente e imparcial, y su severidad guarda proporción con la gravedad de la conducta, el daño causado y la reincidencia.

10.3 Controles físicos

- **Seguridad de las áreas y las instalaciones.** Las áreas que albergan infraestructura crítica o información clasificada cuentan con perímetros definidos, control de acceso físico registrado, y protección frente a amenazas ambientales y fallos de suministro.

- **Seguridad de los equipos y de los soportes.** Los equipos y soportes de almacenamiento se protegen durante su uso, traslado y disposición final.
- **Dispositivos móviles y dispositivos personales.** La información creada, procesada, almacenada o accedida desde dispositivos móviles institucionales se protege con los mismos controles que corresponderían a cualquier otro equipo de la Universidad, según su clasificación. El uso de dispositivos personales para fines institucionales está permitido, salvo cuando permita el acceso a información clasificada en los niveles más altos de criticidad, caso en el cual se exigen las condiciones mínimas de seguridad definidas en la guía institucional aplicable.
- **Dispositivos conectados no convencionales.** Los dispositivos IoT, biomédicos y de laboratorio conectados a la red institucional se registran, se asignan a segmentos aislados y cuentan con un responsable funcional designado.

10.4 Controles tecnológicos

- **Controles criptográficos.** Se aplican controles criptográficos, en almacenamiento y en tránsito, a la información clasificada como confidencial o valorada con la criticidad más alta en la dimensión de integridad, empleando algoritmos vigentes y catalogados como fuertes. Las llaves de cifrado se gestionan bajo un procedimiento formal que garantiza su protección durante todo su ciclo de vida.
- **Copias de respaldo y recuperación.** Se generan copias de respaldo, como mínimo, de todos los activos de información clasificados en el nivel alto de criticidad para la disponibilidad, con una estrategia que contemple los puntos y tiempos de recuperación adecuados y que mantenga durante el tránsito y el almacenamiento los mismos requisitos de seguridad de los activos originales. La consistencia, la integridad y la capacidad de recuperación se deben verificar mediante pruebas periódicas documentadas.
- **Transferencia de información.** La transferencia de información, interna o externa, se realiza únicamente a través de los medios definidos y suministrados por la Universidad, o por un cliente o proveedor cuando así se acuerde, aplicando los controles que correspondan a la clasificación del activo. Todo activo debe haber pasado por el procedimiento de clasificación y etiquetado antes de ser transferido.

- **Desarrollo seguro de software.** Las aplicaciones y sistemas desarrollados por equipos internos o por proveedores para uso en actividades institucionales incorporan criterios de seguridad a lo largo del ciclo de vida del desarrollo, proporcionales a la clasificación de los datos que procesarán, incluyendo separación de ambientes, gestión de secretos, pruebas de seguridad y control de cambios.
- **Gestión de vulnerabilidades y configuración segura.** La Universidad identifica, evalúa y remedia las vulnerabilidades técnicas de su infraestructura y aplicaciones dentro de plazos definidos según criticidad, y mantiene líneas base de configuración segura para sus plataformas.
- **Registro, monitoreo y detección.** Se generan y conservan registros de auditoría de los eventos relevantes de seguridad, protegidos frente a alteración, por los períodos definidos en el procedimiento de gestión de trazas, y se opera un esquema de monitoreo y detección de actividad anómala.
- **Protección frente a código malicioso.** Los sistemas y dispositivos que traten información institucional deben contar con protección actualizada frente a código malicioso y con mecanismos de detección y respuesta en el punto final.
- S**eguridad en servicios de nube.** La adopción de servicios de nube se sujeta a evaluación previa, a la definición explícita del modelo de responsabilidad compartida y a los lineamientos de ISO/IEC 27017:2015 e ISO/IEC 27018:2019 cuando traten datos personales.
- **Seguridad de las redes y del correo institucional.** Los lineamientos específicos se desarrollan en la Política de Uso Adecuado de Internet y de los Servicios de Red y en la Política de Uso Adecuado del Correo Electrónico Institucional, derivadas de la presente política.

11 Programa institucional de privacidad y protección de datos personales



La Universidad El Bosque establece un programa de privacidad transparente y verificable, que desarrolla el componente que la edición anterior de esta política enunciaba en su título sin desarrollarlo en su articulado. El programa se estructura conforme a ISO/IEC 27701:2025 y a la Ley 1581 de 2012, y sus controles operativos se detallan en el Anexo B. La Política de Tratamiento de Datos Personales (2022) desarrolla los procedimientos de este programa y se subordina a la presente política.

11.1 Principios del tratamiento

El tratamiento de datos personales por parte de la Universidad se rige por los principios de legalidad, finalidad, libertad, veracidad o calidad, transparencia, acceso y circulación restringida, seguridad y confidencialidad, consagrados en la Ley 1581 de 2012, complementados por los principios de minimización, exactitud, limitación del plazo de conservación y responsabilidad demostrada.

11.2 Lineamientos del programa

- **Registro de tratamientos.** La Universidad mantiene un inventario de las bases de datos personales bajo su responsabilidad, con indicación de finalidad, categorías de titulares y de datos, base de legitimación, encargados, transferencias y plazos de conservación, y lo mantiene registrado y actualizado ante el RNBD conforme a la normativa aplicable.
- **Autorización y bases de legitimación.** El tratamiento requiere autorización previa, expresa e informada del titular, salvo en los casos exceptuados por la ley. La Universidad mantiene prueba de la autorización otorgada y de la información suministrada al titular, y se debe definir un procedimiento para el otorgamiento y la revocatoria.
- **Datos sensibles y de menores de edad.** El tratamiento de datos sensibles —incluidos los datos de salud tratados en la relación docencia-servicio, los datos biométricos y los datos de investigación con seres humanos— se sujeta al régimen reforzado del artículo 5.º de la Ley 1581 de 2012, exige autorización explícita con advertencia de su carácter facultativo, y se limita a las finalidades expresamente informadas. El tratamiento de datos de menores de edad se realiza únicamente cuando responde a su interés superior y con las garantías correspondientes.
- **Derechos de los titulares.** La Universidad garantiza el ejercicio de los derechos a conocer, actualizar, rectificar y suprimir los datos, a revocar la autorización, a solicitar prueba de esta y a presentar quejas ante la autoridad competente. Mantiene canales accesibles de atención de consultas y reclamos, y responde dentro de los términos legales, con registro trazable de cada solicitud y de su respuesta.
- **Aviso de privacidad y transparencia.** La Universidad informa a los titulares, en lenguaje claro y accesible, las finalidades del tratamiento, sus derechos y los canales para ejercerlos, y publica su aviso de privacidad en los puntos de recolección.
- **Encargados, transferencias y transmisiones.** La entrega de datos personales a terceros se formaliza en un contrato de transmisión que establezca las obligaciones del encargado. Las transferencias internacionales se realizan a países que garanticen niveles adecuados de protección o bajo alguno de los mecanismos autorizados por la ley.

- **Evaluación de impacto en la privacidad.** Todo tratamiento nuevo o modificado que involucre datos sensibles, tratamiento masivo, elaboración de perfiles, decisiones automatizadas o uso de inteligencia artificial se somete a evaluación previa de impacto en la privacidad, con concepto de la Coordinación de Seguridad de la Información y de la Secretaría General.
- **Privacidad desde el diseño y por defecto.** Los proyectos, sistemas y contratos incorporan requisitos de privacidad desde su concepción, con configuraciones que por defecto minimicen la recolección y la exposición de datos personales.
- **Conservación y disposición final.** Los datos personales se conservan únicamente por el tiempo que justifique la finalidad informada y las obligaciones legales de retención, y se mantienen de forma segura al término de dicho plazo, conforme a las tablas de retención documental.
- **Incidentes que afecten datos personales**. Todo incidente que comprometa datos personales activa, además del procedimiento general de incidentes, la evaluación del riesgo para los derechos de los titulares, el reporte a la autoridad competente cuando proceda y la comunicación a los titulares afectados en los casos que lo requieran.

12 Cultura y educación en seguridad de la información



La Universidad debe mantener un programa permanente de formación y sensibilización en seguridad de la información y protección de datos personales, cuyos controles se detallan en el Anexo C y cuya ejecución se articula con la Vicerrectoría Académica, la Dirección de Talento Humano y la División de Innovación Digital en Educación con las siguientes características.

- Programa diferenciado por perfil de riesgo: contenidos distintos para estudiantes, profesores, personal administrativo, personal directivo, desarrolladores y usuarios privilegiados.
- Obligatorio y periódico, con al menos una activación anual por persona y refuerzos dirigidos a los grupos de mayor exposición.
- Se apoya en una plataforma institucional que permita entregar la formación y registrar su cumplimiento de manera auditable.
- Incluye actividades de validación —simulaciones controladas, ejercicios y evaluaciones— cuyos resultados se emplean con finalidad formativa y se reportan de forma agregada.

- Sus resultados se miden y reportan a las instancias de gobierno mediante los indicadores del numeral 8.1.
- La comunicación se realiza en lenguaje claro y orientado al valor.

13 Estrategias de implementación, acciones e instrumentos



13.1 Plan de Seguridad

La implementación de esta política se planifica mediante un Plan de Seguridad con horizonte alineado al PDCM 2025–2027, desarrollado en seis fases: definición del modelo, a partir de los objetivos institucionales, la gestión de riesgos y el marco legal; análisis de la situación actual mediante auditorías, entrevistas y revisión de indicadores; análisis de brecha frente al estado objetivo; plan de acción con proyectos priorizados, presupuesto y responsables; aprobación por la alta dirección e inicio de la ejecución; y seguimiento de desviaciones en costo, tiempo y grado de cumplimiento.

13.2 Instrumentos derivados

Tabla 3. Instrumentos derivados de la política, según la jerarquía del cuerpo normativo de seguridad.

Instrumento	Nivel	Responsable de su expedición
Metodología de gestión del riesgo de seguridad de la información	Norma	Coordinación de Seguridad de la Información
Norma de clasificación y etiquetado de la información	Norma	Coordinación de Seguridad de la Información
Norma de control de acceso y gestión de identidades	Norma	Vicerrectoría Administrativa y Dirección de Tecnología
Norma de seguridad en la relación con proveedores	Norma	Coordinación de Seguridad de la Información / Vicerrectoría Administrativa
Programa institucional de privacidad y protección de datos personales (Anexo B)	Norma	Coordinación de Seguridad de la Información / Secretaría General
Programa de cultura y educación en seguridad (Anexo C)	Norma	Coordinación de Seguridad de la Información / Talento Humano
Procedimiento de gestión de incidentes de seguridad de la información	Procedimiento	Coordinación de Seguridad de la Información
Procedimiento de atención de derechos de los titulares	Procedimiento	Secretaría General
Procedimiento de evaluación de impacto en la privacidad	Procedimiento	Coordinación de Seguridad de la Información
Procedimiento de gestión de vulnerabilidades y parches	Procedimiento	Dirección de Tecnología
Procedimiento de copias de respaldo y pruebas de restauración	Procedimiento	Dirección de Tecnología
Catálogo de servicios y acuerdos de niveles de servicio (ANS)	Norma	Dirección de Tecnología
Plan de continuidad y recuperación de los servicios de información	Plan	Dirección de Tecnología
Guías técnicas de configuración segura y de uso de IA	Guía técnica	Dirección de Tecnología
Líneas base de configuración de plataformas críticas	Baseline	Dirección de Tecnología
Plan de Seguridad	Plan	Coordinación de Seguridad de la Información / Dirección de Tecnología
Tablero de indicadores del SGSI y del SGPI	Instrumento de medición	Coordinación de Seguridad de la Información

14 Gobernanza de la política



14.1 Estructura organizacional relacionada

La gobernanza de esta política se inscribe en la estructura de gobierno institucional descrita en el PEI (2025) y en el Código de Buen Gobierno (2022), y adopta la distinción entre gobierno y gestión propia de COBIT 2019: el gobierno evalúa, orienta y supervisa; la gestión planifica, construye, opera y monitorea. La estructura se organiza en cuatro niveles: un nivel de dirección estratégica, integrado por El Claustro, el Consejo Directivo y la Rectoría, que aprueba la política, asigna recursos y responde por su vigencia; un nivel de orientación y decisión táctica, conformado por el Comité de Tecnología y el Comité de Seguridad de la Información, que aprueba el Plan de Seguridad, acepta riesgos residuales, autoriza excepciones y revisa indicadores; un nivel de ejecución, encabezado por la Dirección de Tecnología de la Información y la Coordinación de Seguridad de la Información, esta última como instancia de definición, verificación y supervisión con independencia funcional respecto de la operación; y un nivel de aplicación distribuida, compuesto por las vicerrectorías, facultades, direcciones y unidades administrativas, los propietarios de los activos de información y cada miembro de la comunidad universitaria en su condición de corresponsable.

14.2 Roles y responsabilidades

Tabla 4. Matriz de responsabilidades. R: responsable de ejecutar · A: aprueba y rinde cuentas · C: consultado · I: informado.

Instancia o rol	Responsabilidad principal	RACI
El Claustro y Rectoría	Planeación institucional y procesos de autoevaluación; asignación de recursos y respaldo explícito al sistema de gestión.	A
Consejo Directivo	Aprobar la política y sus actualizaciones sustanciales; conocer los resultados de su evaluación.	A
Consejos Académico y Administrativo	Desarrollo y seguimiento de las políticas institucionales en sus ámbitos.	C
Comité de Tecnología / Comité de Seguridad de la Información	Aprobar el Plan de Seguridad, revisar el registro de riesgos e indicadores, aceptar riesgos residuales, autorizar excepciones y recomendar actualizaciones.	C / I
Coordinación de Seguridad de la Información	Diseñar, mantener y verificar el SGSI y el SGPI; liderar la gestión del riesgo, la respuesta a incidentes, el programa de privacidad y el de cultura; reportar a las instancias de gobierno.	R
Dirección de Tecnología de la Información	Unidad responsable de la operación: implantar y sostener los controles tecnológicos, expedir guías y líneas de base, y mantener el tablero de indicadores.	R
Secretaría General	Custodia documental, concepto jurídico, atención de derechos de los titulares, registro ante el RNBD y articulación con retención documental.	R
Vicerrectoría Académica y Vicerrectoría Administrativa	Implementación, ejecución, evaluación y seguimiento de la política en los programas y procesos a su cargo.	R
Vicerrectoría de Investigaciones	Articular la protección de los datos de investigación y los avales de los comités de ética con los controles de esta política.	C
Dirección de Talento Humano	Controles de seguridad en el ciclo de vida del vínculo laboral, acuerdos de confidencialidad, inducción y régimen disciplinario.	R
Propietarios de activos de información	Clasificar sus activos, determinar la protección necesaria y autorizar los accesos correspondientes.	R

Instancia o rol	Responsabilidad principal	RACI
Auditoría Interna	Evaluación independiente del sistema de gestión y verificación del cierre de hallazgos.	R
Miembros de la comunidad universitaria	Corresponsabilidad: cumplir la política, proteger la información que tratan y reportar incidentes.	R

14.3 Instancias de aprobación, actualización, seguimiento y evaluación

- **Aprobación y derogatoria:** Consejo Directivo, por recomendación de la Rectoría.
- **Actualización sustancial:** propuesta por la Coordinación de Seguridad de la Información y la Dirección de Tecnología, con concepto de la Secretaría General, revisión del Comité de Tecnología y aprobación del Consejo Directivo.
- **Actualización de instrumentos derivados (normas, procedimientos, guías y líneas de base):** Coordinación de Seguridad de la Información y Dirección de Tecnología según corresponda; se informa al Comité de Tecnología.
- **Seguimiento:** La Coordinación de Seguridad de la Información, con reporte trimestral al Comité de Seguridad de la Información, semestral al Comité de Tecnología y anual a la Rectoría y a la Dirección de Planeación y Prospectiva, en el marco del seguimiento al PDCM 2025–2027.
- **Evaluación independiente:** Auditoría Interna y División de Calidad, mediante el programa anual de auditoría interna del SGSI y en el marco de los procesos de autoevaluación institucional.
- **Revisión por la dirección:** al menos una vez al año, conforme al requisito 9.3 de ISO/IEC 27001:2022, con evaluación de los resultados del sistema, el estado de los riesgos y las oportunidades de mejora.
- **Excepciones:** toda excepción a un lineamiento debe solicitarse por escrito, motivarse, contar con concepto de la Coordinación de Seguridad de la Información, ser aprobada por el Comité de Seguridad de la Información, tener vigencia máxima de doce (12) meses y quedar registrada en el inventario de excepciones.
- **Revisión por capítulos:** por su extensión y complejidad, la política puede revisarse como un todo o por dominios, según consideración del Consejo Directivo.

15 Evaluación y mejora continua



15.1 Mecanismos de medición

La eficacia del sistema se mide mediante indicadores construidos conforme a ISO/IEC 27004:2016, que distingue entre indicadores de desempeño de los procesos (KPI) e indicadores de logro de los objetivos institucionales (KGI). El tablero se actualiza mensualmente y se reporta con la periodicidad establecida en el numeral 7.3. Cada indicador cuenta con nombre inequívoco, tipo, propósito, escala, método de cálculo, frecuencia, propietario, fuente de datos y fecha de validez, documentados en la ficha técnica que administra la Coordinación de Seguridad de la Información.

Tabla 5. Tablero de indicadores del SGSI y del SGPI. Las líneas base se establecen con corte a diciembre de 2025.

Código	Indicador	Tipo	Fórmula	Frecuencia	Meta 2026	Meta 2027
KPI-01	Cobertura del inventario de activos	Cumplimiento	Procesos con activos inventariados y clasificados / Total de procesos	Anual	≥ 50 %	100 %
KPI-02	Riesgos con plan de tratamiento	Cumplimiento	Riesgos sobre el nivel aceptable con plan formal / Total de riesgos sobre el nivel aceptable	Trimestral	50 %	100 %
KPI-03	Riesgo residual dentro del apetito	Eficacia	Riesgos con residual bajo o moderado / Total de riesgos valorados	Semestral	≥ 65 %	≥ 95 %
KPI-04	Bases de datos registradas y actualizadas ante el RNBD	Cumplimiento	Bases registradas y vigentes / Bases identificadas	Semestral	100 %	100 %
KPI-05	Oportunidad en la atención de derechos de titulares	Eficiencia	Solicitudes atendidas en término legal / Total de solicitudes	Mensual	100 %	100 %
KPI-06	Evaluaciones de impacto en la privacidad	Cumplimiento	Tratamientos de alto riesgo con EIP realizada / Total de tratamientos de alto riesgo	Semestral	≥ 50 %	100 %
KPI-07	Cobertura de formación	Cumplimiento	Personas que completan la formación anual / Población objetivo	Semestral	≥ 30 %	≥ 60 %
KPI-08	Tiempo medio de detección y contención	Eficiencia	Promedio de horas hábiles entre detección y contención de incidentes de alto impacto	Mensual	≤ 8 h	≤ 4 h
KPI-09	Proveedores críticos evaluados	Cumplimiento	Proveedores críticos con evaluación y cláusulas vigentes / Total de proveedores críticos	Semestral	≥ 50 %	100 %
KPI-10	Remediación de vulnerabilidades críticas	Eficiencia	Vulnerabilidades críticas remediadas en plazo / Total de vulnerabilidades críticas	Mensual	≥ 80 %	≥ 95 %
KGI-01	Madurez del sistema de gestión	Impacto	Nivel de madurez evaluado del SGSI y del SGPI frente al modelo de referencia adoptado	Anual	Nivel 2	Nivel 3

Código	Indicador	Tipo	Fórmula	Frecuencia	Meta 2026	Meta 2027
KGI-02	Confianza de la comunidad	Impacto	Percepción favorable sobre la protección de la información y los datos personales (encuesta anual)	Anual	≥ 50 %	≥ 85 %
KGI-03	Cumplimiento del compromiso del PDCM	Impacto	Estado de actualización e implementación de la política frente al Proyecto 10	Anual	En Implementación	Implementada

15.2 Ciclo de mejora continua

El sistema se gestiona bajo el ciclo PHVA. En la fase de planeación se actualizan el contexto, el análisis de riesgos, el Plan de Seguridad y las metas anuales; en la de ejecución se implantan los controles, el programa de privacidad y el de formación; en la de verificación se revisan los indicadores, las auditorías internas y externas, los resultados de las pruebas de continuidad y de restauración, los hallazgos de la autoevaluación institucional y las lecciones aprendidas de los incidentes; y en la de actuación se ajustan los instrumentos derivados, se corrigen las desviaciones y, cuando corresponde, se propone la actualización de la política. Este ciclo se articula con los procesos de autoevaluación y con los planes de mejoramiento del Sistema Interno de Aseguramiento de la Calidad, atendiendo los principios de calidad, transparencia y adaptabilidad, e involucra desde El Claustro hasta cada miembro de la comunidad universitaria en su corresponsabilidad.

15.3 Criterios para el inicio de la actualización

- La política se revisa de manera ordinaria cada tres (3) años. Procede su revisión extraordinaria, dentro de los tres (3) meses siguientes a la ocurrencia del hecho, cuando se presente cualquiera de las siguientes circunstancias:
- Modificación del PEI, del Plan de Desarrollo Institucional o del PDCM que afecte los fundamentos o el alcance de la política.
- Expedición o modificación de normas legales aplicables a la protección de datos personales, los delitos informáticos, el derecho de autor, las TIC, la conservación documental o la calidad de la educación superior.
- Actualización sustancial de los estándares de referencia adoptados, en particular de ISO/IEC 27001, ISO/IEC 27002 o ISO/IEC 27701.

- Recomendaciones de pares académicos, del Consejo Nacional de Acreditación, de la Superintendencia de Industria y Comercio o de organismos de inspección, vigilancia y control que involucren esta política.
- Materialización de un incidente de seguridad de alto impacto, de una brecha que comprometa datos personales, o de una tendencia sostenida de incidentes que evidencie insuficiencia de los controles vigentes.
- Cambio sustancial en la arquitectura tecnológica, en el modelo de identidad institucional, en los proveedores críticos o en la adopción de nuevas categorías de servicios de nube o de inteligencia artificial.
- Incumplimiento sostenido de las metas de dos (2) o más indicadores durante dos (2) períodos consecutivos de medición.
- Modificación de la estructura organizacional que altere las responsabilidades definidas en el numeral 7.2.
- Resultados de la revisión por la dirección que evidencien la necesidad de ajustar el alcance, los objetivos o los dominios de control del sistema.

16 Referencias



Normativa nacional

Congreso de la República de Colombia. (1982). *Ley 23 de 1982. Sobre derechos de autor.* Diario Oficial n.º 35.949.

Congreso de la República de Colombia. (1999). *Ley 527 de 1999. Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales.* Diario Oficial n.º 43.673.

Congreso de la República de Colombia. (2008). *Ley 1266 de 2008. Por la cual se dictan las disposiciones generales del hábeas data.* Diario Oficial n.º 47.219.

Congreso de la República de Colombia. (2009). *Ley 1273 de 2009. Por medio de la cual se modifica el Código Penal y se crea un nuevo bien jurídico tutelado denominado "de la protección de la información y de los datos".* Diario Oficial n.º 47.223.

Congreso de la República de Colombia. (2012). *Ley 1581 de 2012. Por la cual se dictan disposiciones generales para la protección de datos personales.* Diario Oficial n.º 48.587.

Congreso de la República de Colombia. (2018). *Ley 1915 de 2018. Por la cual se modifica la Ley 23 de 1982 y se establecen otras disposiciones en materia de derecho de autor y derechos conexos.* Diario Oficial n.º 50.652.

Congreso de la República de Colombia. (2019). *Ley 1978 de 2019. Por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones.* Diario Oficial n.º 51.025.

Congreso de la República de Colombia. (2023). *Ley 2300 de 2023. Por medio de la cual se establecen medidas para la protección del consumidor frente a la utilización de datos personales en comunicaciones no solicitadas.* Diario Oficial.

Consejo Nacional de Educación Superior. (2020). *Acuerdo 02 de 2020. Por el cual se actualiza el modelo de acreditación en alta calidad.* CESU.

Ministerio de Comercio, Industria y Turismo. (2015). *Decreto 1074 de 2015. Decreto Único Reglamentario del Sector Comercio, Industria y Turismo* (Libro 2, Parte 2, Título 2, Capítulo 25).

Ministerio de Educación Nacional. (2019). *Decreto 1330 de 2019. Por el cual se sustituye el Capítulo 2 y se suprime el Capítulo 7 del Título 3 de la Parte 5 del Libro 2 del Decreto 1075 de 2015.*

Presidencia de la República de Colombia. (2013). *Decreto 1377 de 2013. Por el cual se reglamenta parcialmente la Ley 1581 de 2012.*

Documentos institucionales

Universidad El Bosque. (2019). *Política de seguridad y privacidad de la información* (1.ª ed.).

Universidad El Bosque. (2020). *Estatutos institucionales.*

Universidad El Bosque. (2022). *Código de Buen Gobierno.*

Universidad El Bosque. (2022). *Plan de Desarrollo Institucional 2022–2027: transformaciones oportunas para un futuro cambiante.* **https://www.unbosque.edu.co**

Universidad El Bosque. (2022). *Política de Tratamiento de Datos Personales.*

Universidad El Bosque. (2023). *Política para el Diseño y Apropiación de Entornos Digitales.* **https://www.unbosque.edu.co**

Universidad El Bosque. (2024). *Política de Gobernanza de Datos.*

Universidad El Bosque. (2025). *Plan de Desarrollo, Consolidación y Mejoramiento 2025–2027.*

Universidad El Bosque. (2025). *Proyecto Educativo Institucional* (Acuerdo n.º 18257 de 2025 del Consejo Directivo).

Estándares y literatura técnica

AXELOS. (2019). *ITIL foundation: ITIL 4 edition.* The Stationery Office.

Center for Internet Security. (2024). *CIS critical security controls, version 8.1.* CIS.

International Organization for Standardization. (2016). *ISO/IEC 27004:2016. Information technology — Security techniques — Information security management — Monitoring, measurement, analysis and evaluation.* ISO/IEC.

International Organization for Standardization. (2015). *ISO/IEC 27017:2015. Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services.* ISO/IEC.

International Organization for Standardization. (2018). *ISO 31000:2018. Risk management — Guidelines.* ISO.

International Organization for Standardization. (2019). ISO 22301:2019. *Security and resilience — Business continuity management systems — Requirements.* ISO.

International Organization for Standardization. (2019). *ISO/IEC 27018:2019. Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors.* ISO/IEC.

International Organization for Standardization. (2022). *ISO/IEC 27001:2022. Information security, cybersecurity and privacy protection — Information security management systems — Requirements.* ISO/IEC.

International Organization for Standardization. (2022). *ISO/IEC 27002:2022. Information security, cybersecurity and privacy protection — Information security controls.* ISO/IEC.

International Organization for Standardization. (2022). *ISO/IEC 27005:2022. Information security, cybersecurity and privacy protection — Guidance on managing information security risks.* ISO/IEC.

International Organization for Standardization. (2023). I*SO/IEC 42001:2023. Information technology — Artificial intelligence — Management system.* ISO/IEC.

International Organization for Standardization. (2024). I*SO/IEC 27001:2022/Amd 1:2024. Information security management systems — Requirements — Amendment 1: Climate action changes.* ISO/IEC.

International Organization for Standardization. (2025). *ISO/IEC 27701:2025. Information security, cybersecurity and privacy protection — Privacy information management systems — Requirements and guidance (2.ª ed.).* ISO/IEC.

ISACA. (2018). C*OBIT 2019 framework: Governance and management objectives.* ISACA.

National Institute of Standards and Technology. (2020). *Security and privacy controls for information systems and organizations* (NIST SP 800-53 Rev. 5). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology. (2020). *Zero trust architecture* (NIST SP 800-207). U.S. Department of Commerce. https://doi.org/10.6028/NIST.SP.800-207

National Institute of Standards and Technology. (2024). *The NIST cybersecurity framework (CSF) 2.0* (NIST CSWP 29). U.S. Department of Commerce. **https://doi.org/10.6028/NIST.CSWP.29**

SANS Institute. (2026). *Education management policy* [Plantilla de política]. SANS Institute.

SANS Institute. (2026). *Privacy management policy* [Plantilla de política]. SANS Institute.

Schneier, B. (2000). *Secrets and lies: Digital security in a networked world.* John Wiley & Sons.

Anexo A Mapa de dominios de control

El siguiente mapa relaciona los dominios desarrollados en el numeral 6.6 con los temas de control de ISO/IEC 27002:2022 y con las políticas y normas derivadas. Es administrado por la Coordinación de Seguridad de la Información y se revisa anualmente; su actualización no requiere modificar la política.

Dominio de la política	Tema ISO/IEC 27002:2022	Instrumento derivado
Gestión de activos de información	Organizacional	Norma de clasificación y etiquetado
Control de acceso y gestión de identidades	Organizacional / Tecnológico	Norma de control de acceso
Relación con proveedores y cadena de suministro	Organizacional	Norma de seguridad con proveedores
Gestión de incidentes	Organizacional	Procedimiento de gestión de incidentes
Continuidad del negocio	Organizacional	Plan de continuidad y recuperación

Dominio de la política	Tema ISO/IEC 27002:2022	Instrumento derivado
Cumplimiento legal y contractual	Organizacional	Matriz de requisitos legales
Gobernanza de la inteligencia artificial	Organizacional	Guía de uso responsable de IA
Seguridad en el ciclo de vida del vínculo	Personas	Procedimientos de Talento Humano
Cultura y educación en seguridad	Personas	Programa de educación (Anexo C)
Teletrabajo y trabajo remoto	Personas	Guía de acceso remoto
Escritorio y pantalla limpios	Personas / Físico	Guía de puesto de trabajo seguro
Seguridad de áreas, equipos y soportes	Físico	Norma de seguridad física
Dispositivos móviles y personales	Físico / Tecnológico	Guía BYOD
Controles criptográficos	Tecnológico	Norma de criptografía y gestión de llaves
Copias de respaldo y recuperación	Tecnológico	Procedimiento de respaldos
Transferencia de información	Tecnológico	Procedimiento de transferencia segura
Desarrollo seguro de software	Tecnológico	Norma de desarrollo seguro
Gestión de vulnerabilidades y configuración	Tecnológico	Procedimiento de vulnerabilidades y líneas de base
Registro, monitoreo y detección	Tecnológico	Procedimiento de gestión de trazas
Protección frente a código malicioso	Tecnológico	Línea base de protección de punto final
Seguridad en servicios de nube	Tecnológico	Norma de adopción de servicios de nube
Seguridad de redes y correo institucional	Tecnológico	Políticas derivadas de internet y correo
Programa de privacidad	Transversal (ISO/IEC 27701:2025)	Programa de privacidad (Anexo B)

Anexo B Controles del programa de privacidad

Los siguientes controles constituyen la norma técnica derivada del numeral 6.7. Se adoptan a partir de la Privacy Management Policy del SANS Institute (2026) y se adaptan al régimen colombiano de protección de datos personales y a ISO/IEC 27701:2025. Su implementación corresponde a la Coordinación de Seguridad de la Información en articulación con la Secretaría General.

Código	Control	Verificación
PRV-01	Mantener un programa de privacidad documentado y transparente que consolide las salvaguardas institucionales en materia de datos personales.	Anual
PRV-02	Definir el proceso de otorgamiento, mantenimiento y revocatoria de las autorizaciones de tratamiento, con prueba conservada de cada autorización.	Anual
PRV-03	Definir el proceso de consulta, transferencia, transmisión, divulgación, modificación y supresión de datos personales en los sistemas institucionales.	Anual

Código	Control	Verificación
PRV-04	Registrar y mantener las preferencias de privacidad manifestadas por los titulares.	Anual
PRV-05	Registrar, mantener y revisar las expectativas de los grupos de interés en materia de privacidad.	Anual
PRV-06	Evaluar el uso institucional de datos para detectar sesgos, en particular en sistemas de inteligencia artificial y decisiones automatizadas.	Anual
PRV-07	Sustituir valores de atributos por referencias en los sistemas de información cuando la finalidad lo permita.	Anual
PRV-08	Permitir a los titulares solicitar la actualización y rectificación de sus datos, con trazabilidad de la solicitud y su respuesta.	Semestral
PRV-09	Permitir a los titulares solicitar la supresión de sus datos y la revocatoria de la autorización, dentro de los límites legales de conservación.	Anual
PRV-10	Compartir con terceros únicamente los datos pertinentes a la finalidad, mediante contrato de transmisión que fije las obligaciones del encargado.	Anual
PRV-11	Mantener el registro y la actualización de las bases de datos personales ante el RNBD, conforme a la normativa aplicable.	Anual

Anexo C Controles del programa de educación en seguridad

Los siguientes controles constituyen la norma técnica derivada del numeral 6.8. Se adoptan a partir de la Education Management Policy del SANS Institute (2026) y se adaptan al contexto universitario, ampliando la población objetivo más allá de los colaboradores para incluir a estudiantes y terceros vinculados.

Código	Control	Verificación
EDU-01	Garantizar que todos los miembros de la comunidad universitaria tengan acceso a la documentación que define las salvaguardas asociadas a su rol.	Anual
EDU-02	Mantener una plataforma tecnológica para impartir la formación en seguridad y protección de datos personales.	Anual
EDU-03	Mantener el registro auditable de la formación impartida y completada por cada persona.	Anual
EDU-04	Impartir formación diferenciada a los perfiles técnicos –desarrolladores, administradores y usuarios privilegiados– sobre las salvaguardas propias de su rol.	Anual
EDU-05	Impartir formación general de sensibilización a toda la comunidad universitaria, incluidos estudiantes y terceros vinculados.	Anual

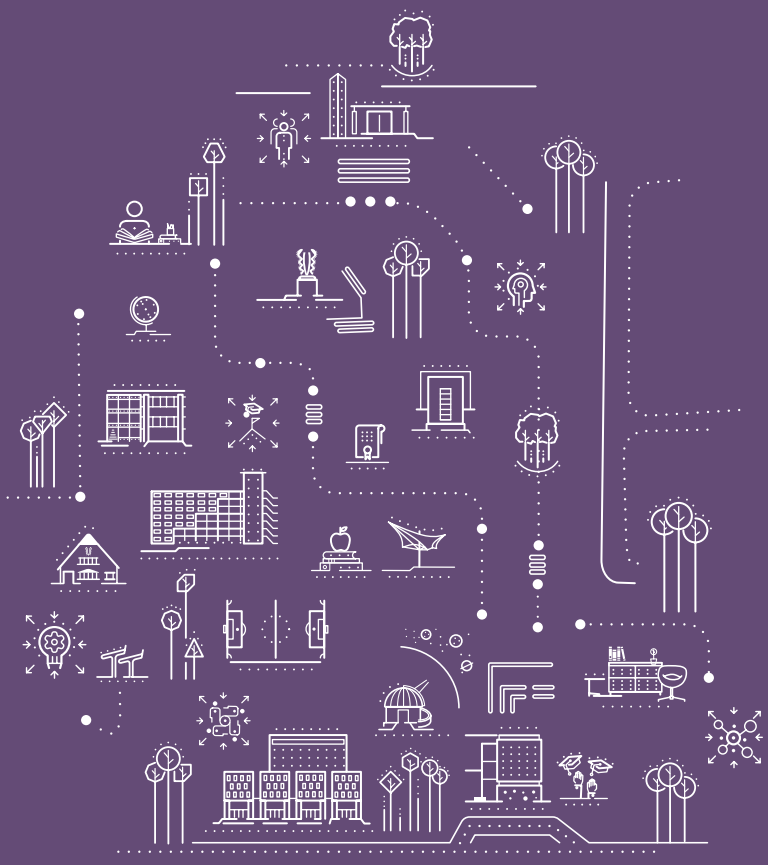
Código	Control	Verificación
EDU-06	Educar sobre autenticación segura a los sistemas de información, incluida la autenticación multifactor.	Anual
EDU-07	Educar sobre comunicación segura a través de redes no confiables.	Anual
EDU-08	Educar sobre el manejo seguro de la información y las causas más frecuentes de exposición de datos.	Anual
EDU-09	Educar sobre identificación y manejo de técnicas de ingeniería social, incluido el fraude por suplantación de identidad.	Anual
EDU-10	Educar sobre el reporte de fallas en las salvaguardas de seguridad.	Anual
EDU-11	Educar sobre el reporte oportuno de incidentes potenciales, promoviendo una cultura de reporte sin temor a represalias.	Anual

Anexo D Control de cambios

Versión	Fecha	Naturaleza del cambio
1.ª edición	Marzo de 2019	Expedición original. Estructura basada en introducción, justificación, marco general, objetivo, alcance, desarrollo, responsables y evaluación. Nueve políticas específicas. Marco de referencia: ISO/IEC 27001:2013, ISO/IEC 27002 e ISO/IEC 27005 en ediciones anteriores.
2.0	2026	Actualización integral. Adopción de la estructura de política institucional definida por la Secretaría General. Articulación explícita con el PEI (2025) y con los Proyectos 10 y 14 del PDCM 2025-2027. Cierre de la brecha de privacidad: incorporación del programa institucional de privacidad y protección de datos personales (numeral 6.7 y Anexo B). Ampliación de los dominios de control, organizados conforme a los cuatro temas de ISO/IEC 27002:2022 (Anexo A). Nuevos contenidos: gestión formal del riesgo, gestión de incidentes, continuidad del negocio, gestión de identidades, gestión de vulnerabilidades, registro y monitoreo, seguridad en servicios de nube, gobernanza de la inteligencia artificial, cadena de suministro, y programa de cultura y educación (Anexo C). Incorporación de objetivos SMART, tablero de indicadores KPI/KGI, Plan de Seguridad, matriz de gobernanza RACI, régimen de excepciones y criterios de actualización. Actualización de estándares: ISO/IEC 27001:2022 y Amd 1:2024, 27002:2022, 27004:2016, 27005:2022, 27017:2015, 27018:2019, 27701:2025, 42001:2023, ISO 22301:2019, ISO 31000:2018, NIST CSF 2.0, SP 800-53 Rev. 5, SP 800-207, CIS v8.1, COBIT 2019 e ITIL 4 como marco de gestión del servicio.

Elaboró	Revisó	Aprobó
Dirección de Tecnología de la Información _____	Secretaría General _____	Consejo Directivo Acta n. _____° _____

UNIVERSIDAD
EL BOSQUE



- **Edificio Fundadores**
  Av. Cra. 9 Nº. 131 A - 02,
  Bogotá, D.C., Colombia

- **Contacto**
  PBX (57) 601 + 6489000
  Línea Gratuita 018000 113033

POR UNA CULTURA DE LA VIDA, SU CALIDAD Y SU SENTIDO