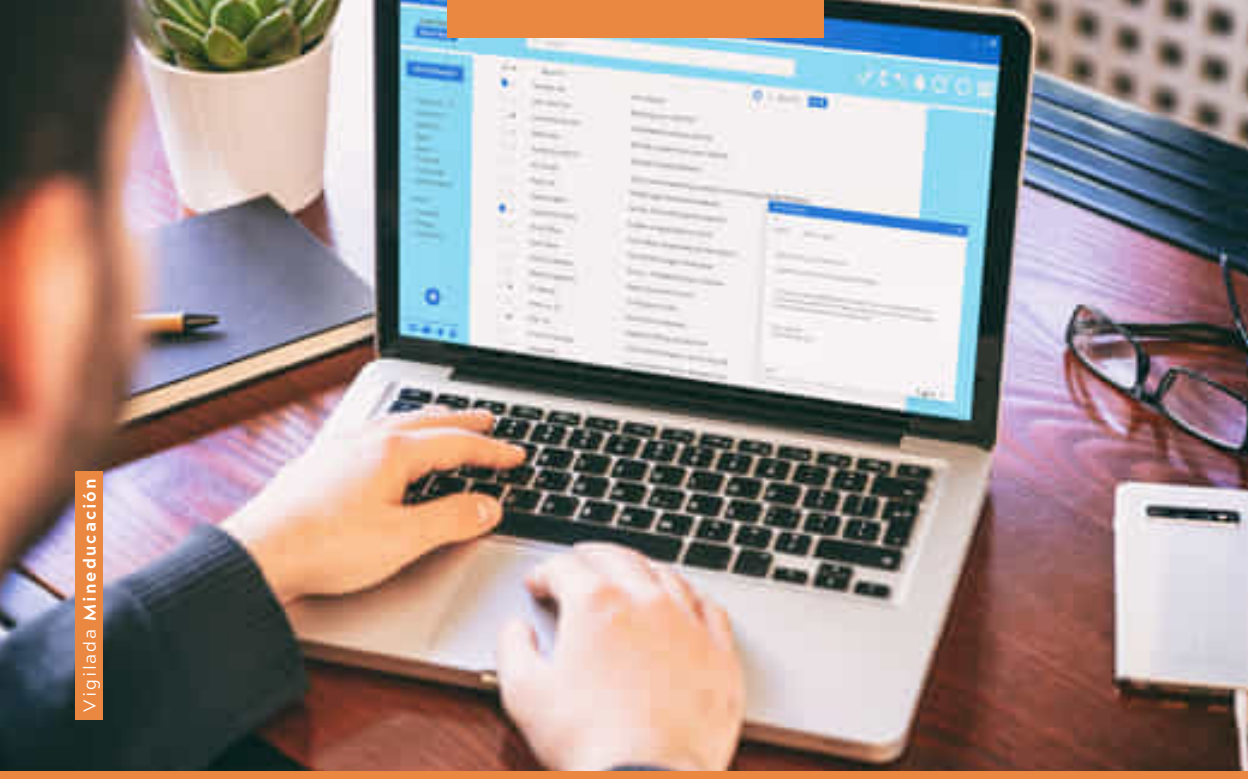


Vigilada **Mineducación**

POLÍTICA DE USO ADECUADO DEL CORREO INSTITUCIONAL

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 USO ADECUADO
DEL CORREO
INSTITUCIONAL



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. 18722 DE 2026 (26 DE AGOSTO) 6

1 Glosario de siglas 7

2 Introducción (justificación) 9

- 2.1 Propósito general y relación con el PEI 9
- 2.2 Resultado esperado y razones que sustentan la adopción 10

3 Estructura general 12

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 Objeto17
- 5.3 Contenido18
- 5.4 Exclusiones18

6 Desarrollo de la política 19

- 6.1 Elementos sustantivos y articulación con el PEI 19

7 Objetivos 21

- 7.1 Objetivo general 21
- 7.2 Objetivos específicos 21

8 Principios rectores 23

9 Ciclo de vida de la cuenta institucional 25

10 Lineamientos de uso 27

- 10.1 Responsabilidad del titular 27
- 10.2 Clasificación y manejo de la información 28
- 10.3 Prevención del fraude y verificación reforzada 28
- 10.4 Comunicaciones institucionalesy envíos masivos 29
- 10.5 Firma institucional y aviso legal 29
- 10.6 Conductas prohibidas 30

10.7 Uso de inteligencia artificial sobre el buzón institucional 31
10.8 Continuidad, respaldo y retención 31
10.9 Gestión de incidentes 32
10.10 Monitoreo, privacidad y debido proceso 32
10.11 Consecuencias del incumplimiento 33

11 Estrategias de implementación 34

12 Acciones e instrumentos 36

13 Gobernanza de la política 38

13.1 Estructura organizacional relacionada 38
13.2 Roles y responsabilidades 39
13.3 Instancias de aprobación, actualización, seguimiento y evaluación 40

14 Evaluación y mejora continua 41

14.1 Mecanismos de medición 41
14.2 Ciclo de mejora continua 42
14.3 Criterios para el inicio de la actualización 43

15 Referencias 44

Normativa nacional 44
Documentos institucionales 45
Estándares y literatura técnica 46

Anexo A Controles mínimos de gestión técnica del correo 47

Anexo B Firma institucional y aviso legal 49

Anexo C Control de cambios 50

ACUERDO NÚM. 18721 DE 2026

(26 de agosto)

"Por el cual se aprueba la actualización de la Política de Uso Adecuado del Correo Electrónico Institucional 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 Uso Adecuado del Correo Electrónico Institucional 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 Uso Adecuado del Correo Electrónico Institucional de la Universidad El Bosque que se adjunta bajo el Anexo Núm. 1 a este Acuerdo.

Artículo segundo. DEROGAR el Acuerdo Núm. 12923 del 15 de octubre de 2024 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.
BEC	Business Email Compromise – compromiso del correo corporativo; fraude basado en la suplantación de una identidad institucional legítima.
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.

Sigla	Significado
CSIRT	Computer Security Incident Response Team – equipo de respuesta a incidentes de seguridad informática.
DKIM	DomainKeys Identified Mail – firma criptográfica que acredita la autenticidad del remitente.
DLP	Data Loss Prevention – prevención de fuga de información.
DMARC	Domain-based Message Authentication, Reporting and Conformance.
DTI	Dirección de Tecnologías de la Información de la Universidad El Bosque.
IA	Inteligencia Artificial.
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.
MTA	Mail Transfer Agent – agente de transferencia de correo.
NIST	National Institute of Standards and Technology (Estados Unidos).
OSI	Oficial de Seguridad de la Información.
PDCM	Plan de Desarrollo, Consolidación y Mejoramiento 2025-2027.
PDI	Plan de Desarrollo Institucional 2022-2027.
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.
SGSI	Sistema de Gestión de Seguridad de la Información.
SPF	Sender Policy Framework.
TIC	Tecnologías de la Información y las Comunicaciones.
TLS	Transport Layer Security – protocolo de cifrado de las comunicaciones en tránsito.
UEB	Universidad El Bosque.

2 Introducción (justificación)



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 actuales 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 Uso Adecuado del Correo Electrónico Institucional establece los principios, deberes y lineamientos que rigen la creación, el uso, la custodia y la disposición final de las cuentas y los mensajes de correo electrónico de la Universidad

El Bosque, con el fin de preservar la confidencialidad, la integridad y la disponibilidad de la información institucional, asegurar la validez probatoria y archivística de las comunicaciones oficiales y proteger los derechos de los titulares de los datos personales que circulan por este canal.

Su relación con el PEI es directa. El correo institucional es la plataforma de comunicación sobre la cual se materializan varios de los postulados fundamentales declarados en el PEI (2025): sostiene el **modelo centrado en el aprendizaje del estudiante,** al ser el canal formal de interacción entre estudiantes, profesores y unidades académicas; habilita la **formación integral a lo largo de la vida,** al mantener el vínculo con egresados y participantes de educación continuada; soporta la **investigación, la investigación-creación y la transferencia de conocimiento,** por cuanto a través de él circula información sensible, no publicada y sujeta a derechos de propiedad intelectual; y expresa la r**esponsabilidad social y la sostenibilidad,** al exigir un uso ético, respetuoso, austero y no discriminatorio de un recurso institucional compartido. Adicionalmente, la política operacionaliza los principios *éticos, sociales e institucionales* de la Misión, en tanto traduce el respeto por la dignidad de la persona humana en reglas concretas de trato, privacidad y debido proceso en el entorno digital.

2.2 Resultado esperado y razones que sustentan la adopción

El resultado esperado de esta política es que, al cierre del período del PDCM 2025–2027, la Universidad opere un canal de correo electrónico institucional **confiable, verificable y gobernado,** en el que la comunidad universitaria distinga entre una comunicación oficial y un intento de fraude, en el que la información clasificada circule con los controles que corresponden a su nivel, y en el que la Universidad pueda demostrar, ante organismos de inspección, vigilancia y control y ante los pares académicos, la trazabilidad y el debido proceso con que administra las comunicaciones institucionales.

La adopción de esta versión responde a cuatro razones. **Primera,** la obsolescencia técnica y normativa de la versión 1.0 (2014): fue formulada para un escenario de correo perimetral y hace referencia a estándares hoy superados (ISO/IEC 27001:2013) y a una cita normativa imprecisa (Ley 524 de 1999), mientras que el ecosistema actual es de nube, movilidad, identidad federada e integración con herramientas de inteligencia artificial. **Segunda,** la evolución del riesgo: el fraude por suplantación de identidad institucional (*phishing* dirigido y BEC), potenciado por IA generativa, es hoy el vector de intrusión más frecuente en el sector de educación superior, y la versión anterior no contemplaba controles de autenticación de dominio, autenticación multifactor, ni un procedimiento

formal de reporte y respuesta. **Tercera,** la exigencia normativa: el desarrollo del régimen de protección de datos personales, los deberes de conservación y valor probatorio de los mensajes de datos y las expectativas de gobierno de datos derivadas de la Política de Gobernanza de Datos (2024) imponen obligaciones que la política vigente no recogía.

Cuarta y determinante, la brecha identificada en el proceso de acreditación institucional. Las recomendaciones de los pares académicos señalaron la necesidad de actualizar el cuerpo de políticas institucionales, articularlas explícitamente con el PEI y dotarlas de mecanismos verificables de seguimiento. La versión 1.0 carecía de objetivos medibles, de indicadores y de criterios de actualización, lo que impedía evidenciar su eficacia. Esta versión corrige esa deficiencia mediante objetivos formulados bajo criterios SMART, un tablero de indicadores con líneas base y metas, y una gobernanza explícita, 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,** liderado por la Dirección de Tecnología.

3 Estructura general



Conceptualmente, esta política se apoya en tres líneas. La primera es la comprensión de la seguridad como un **proceso** y no como un producto o un estado estático (Schneier, 2000), lo que implica que sus disposiciones son revisables y que su valor depende de la operación sostenida de los controles. La segunda es la protección de la **tríada de seguridad de la información** —confidencialidad, integridad y disponibilidad— aplicada al correo electrónico como activo de información y como canal de tratamiento de datos personales. La tercera es la **jerarquía normativa** adoptada por la Universidad: la política define la dirección y el "por qué"; las normas técnicas derivadas definen el "qué"; los procedimientos determinan el "cómo"; las guías técnicas instruyen sobre sistemas concretos; y las líneas de base fijan los umbrales mínimos auditables. En consecuencia, este documento no detalla configuraciones tecnológicas, que corresponden a los instrumentos de nivel inferior relacionados en el numeral 6.7 y en el Anexo A.

En materia de estándares, la política se alinea con la familia ISO/IEC 27000 —en particular ISO/IEC 27001:2022 y su Enmienda 1:2024, ISO/IEC 27002:2022 para la selección de controles, ISO/IEC 27004:2016 para la medición del desempeño e ISO/IEC 27701:2025, que constituye la norma autónoma

de gestión de la privacidad—, con ISO 31000:2018 para el tratamiento del riesgo, con el NIST Cybersecurity Framework 2.0 para la organización de las funciones de gobierno, identificación, protección, detección, respuesta y recuperación, con los CIS Critical Security Controls v8.1 para la priorización de salvaguardas y con la *Email Management Policy* del SANS Institute (2026), cuyos controles se adoptan como norma técnica derivada en el Anexo A. Para el uso de asistentes de inteligencia artificial sobre buzones institucionales se toma como referencia ISO/IEC 42001:2023. En materia de gestión del servicio, la política se apoya en **ITIL 4,** marco adoptado por la Dirección de Tecnología de la Información como base de la operación de sus servicios; de él se toman las prácticas de *mesa de servicio, gestión de incidentes, gestión de peticiones de servicio,* habilitación del cambio y gestión de niveles de servicio, que estructuran la atención de solicitudes de cuentas y delegaciones, el reporte y escalamiento de incidentes de correo, y los tiempos de respuesta comprometidos con la comunidad universitaria. La articulación entre ambos cuerpos es deliberada: ISO/IEC 27001 define qué debe controlarse e ITIL 4 define *cómo* se opera y se mide el servicio que soporta esos controles.

En materia normativa, la política se enmarca en la Constitución Política de Colombia (artículos 15 y 20), en la Ley 527 de 1999 sobre validez probatoria de los mensajes de datos —que corrige la cita errónea a la "Ley 524 de 1999" contenida en la versión 1.0—, en la Ley 1273 de 2009 sobre delitos informáticos, en la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 sobre protección de datos personales, en la Ley 1266 de 2008, en la Ley 2300 de 2023 en lo relativo a comunicaciones no solicitadas, y en el Decreto 1330 de 2019 junto con el Acuerdo 02 de 2020 del CESU en cuanto a las condiciones de calidad institucional. Internamente, se subordina a los Estatutos institucionales y al Código de Buen Gobierno, y se articula con la Política de Seguridad y Privacidad de la Información, la Política de Tratamiento de Datos Personales, la Política de Gobernanza de Datos, la Política de Comunicación, la Política de Uso Adecuado de Internet, el Reglamento Estudiantil, el Estatuto Docente y el Reglamento Interno de Trabajo.

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 2026 ofrece más de 140 programas de educación superior distribuidos en diez facultades y dos departamentos académicos, además de una amplia oferta de educación continuada. Esta configuración determina una población de usuarios de correo institucional heterogénea —estudiantes de pregrado y posgrado, residentes de especializaciones médico-quirúrgicas, profesores de planta y de cátedra, investigadores, personal administrativo, directivos, egresados y terceros vinculados— con necesidades, niveles de exposición al riesgo y competencias digitales muy distintos entre sí. Una parte relevante de la comunidad opera además desde escenarios de práctica externos, incluidos entornos clínicos, donde el correo transporta información sujeta a reserva.

En cuanto a capacidades, la Universidad presta el servicio sobre una plataforma de correo en la nube, administrada por la Dirección de Tecnología, con soporte de primer nivel a través de la Mesa de Servicio y con el acompañamiento

de la Coordinación de Seguridad de la Información en la definición y verificación de controles. El PDCM 2025–2027 refuerza estas capacidades al inscribir el correo dentro del ecosistema del **Campus Digital** (Proyecto 14), que articula infraestructura, transformación digital, inteligencia artificial y gestión estratégica de datos bajo criterios explícitos de retorno sobre la inversión y sostenibilidad. La política reconoce, no obstante, que la madurez de los controles es desigual y que su despliegue debe ser gradual, priorizado por riesgo y proporcional al valor del activo protegido, evitando controles cuyo costo de operación supere el valor de aquello que pretenden proteger.

4.2 Características del entorno

El entorno externo presenta tres presiones convergentes. La primera es tecnológica: la adopción acelerada de tecnologías disruptivas, en particular la inteligencia artificial generativa, ha reducido drásticamente el costo de producir mensajes fraudulentos verosímiles, personalizados y libres de los errores idiomáticos que históricamente permitían detectarlos. La segunda es regulatoria: el endurecimiento de las obligaciones sobre datos personales y la mayor exigencia de trazabilidad documental elevan el estándar de diligencia esperado de la Institución. La tercera es sectorial: el sector de educación superior concentra un volumen creciente de incidentes por compromiso de credenciales, dada la amplitud de sus comunidades, la rotación anual de usuarios y la cultura de apertura propia de la vida académica, que no puede ni debe suprimirse, pero sí acompañarse de controles inteligentes.

4.3 Vínculo con la identidad institucional

Esta política es una expresión operativa de la Misión. El **imperativo supremo de la promoción de la dignidad de la persona humana** se traduce aquí en la prohibición de todo uso del correo que hostigue, discrimine, difame o vulnere la intimidad de un miembro de la comunidad, y en la garantía de debido proceso frente a cualquier medida de monitoreo o restricción. Los **principios éticos** —que propenden a la formación de un ser libre, responsable, justo, pluralista y solidario— fundamentan el deber de veracidad y respeto en las comunicaciones. Los **principios sociales** sustentan la comprensión del correo como recurso común, cuyo uso desconsiderado afecta a terceros. Los **principios institucionales,** que afirman a la Universidad como comunidad autónoma, pluralista y librepensadora, exigen que los controles de seguridad se diseñen de modo que protejan sin restringir innecesariamente la libertad académica ni la deliberación. Finalmente, el **Enfoque BPSyC** obliga a considerar el impacto de las comunicaciones digitales sobre el bienestar de las personas, en articulación con la Política de Desconexión Laboral.

4.4 Vínculo con los grupos de interés

Grupo de interés	Vinculación con la política
Estudiantes (pregrado, posgrado)	Titulares de cuenta institucional; receptores de notificaciones académicas con efectos reglamentarios; sujetos de formación en ciudadanía digital.
Profesores e investigadores	Custodios de información académica, evaluativa y de investigación no publicada; responsables de la reserva sobre resultados y datos de estudio.
Personal administrativo y directivo	Tratan información financiera, contractual y de talento humano; población de mayor exposición a fraude por suplantación (BEC).
Egresados y graduados	Conservan vínculo institucional a través del correo; sujetos de reglas específicas de vigencia, uso y desvinculación.
Proveedores, acreedores y contratistas	Interlocutores en procesos de contratación y pago; destinatarios de verificación reforzada ante cambios de datos bancarios.
Instituciones de educación superior aliadas	Contrapartes en convenios, movilidad y proyectos conjuntos; requieren garantías de autenticidad del remitente institucional.
Organismos de inspección, vigilancia y control, y pares académicos	Destinatarios de la evidencia sobre gobierno, trazabilidad y mejora continua de la política.

5 Alcance de la política



5.1 Sujetos de aplicación

La presente política es de obligatorio cumplimiento para todas las personas a quienes la Universidad El Bosque asigne una cuenta de correo electrónico institucional o autorice el acceso a una de ellas, a saber: estudiantes de todos los niveles y modalidades; profesores de planta, de cátedra y visitantes; investigadores; personal administrativo y directivo; egresados y graduados con cuenta activa; participantes de educación continuada cuando se les asigne cuenta; y terceros —contratistas, practicantes, pasantes, personal en misión y aliados— que, por razón de su vínculo, requieran una cuenta institucional o funcional. La vinculación a la Universidad, la matrícula o la activación de la cuenta comportan la aceptación íntegra de esta política.

5.2 Objeto

Constituyen objeto de esta política: las cuentas de correo del dominio institucional y sus subdominios; las cuentas funcionales, genéricas, de área y de proyecto; los alias, listas de distribución y grupos; los mensajes, sus meta-

datos y sus archivos adjuntos; las firmas y avisos legales asociados; los buzones compartidos y las delegaciones de acceso; los clientes de correo y aplicaciones que accedan al buzón, incluidos los instalados en dispositivos personales bajo esquema BYOD; y los servicios conexos de la suite de productividad institucional en cuanto se integren con el correo, incluidas las funcionalidades de inteligencia artificial que operen sobre su contenido.

5.3 Contenido

La política desarrolla: los principios rectores del uso del correo; el ciclo de vida de las cuentas; los deberes de los usuarios; el tratamiento de la información según su clasificación; las reglas de comunicación institucional y de envíos masivos; el uso de asistentes de inteligencia artificial; las conductas expresamente prohibidas; el régimen de monitoreo, privacidad y debido proceso; la retención y disposición de los mensajes; la respuesta ante incidentes; y el esquema de gobernanza, medición y actualización.

5.4 Exclusiones

No son objeto de esta política las cuentas de correo personales de los miembros de la comunidad universitaria, salvo en cuanto se utilicen indebidamente para tramitar asuntos institucionales, hipótesis expresamente prohibida en el numeral 6.5.6. Tampoco regula los contenidos académicos ni las plataformas de aprendizaje, gobernadas por la Política para el Diseño y Apropiación de Entornos Digitales, ni sustituye las condiciones contractuales del proveedor del servicio de correo, que se entienden complementarias y de obligatoria observancia.

6 Desarrollo de la política



6.1 Elementos sustantivos y articulación con el PEI

El correo electrónico institucional es el **medio formal y oficial de comunicación** de la Universidad El Bosque. Toda notificación, citación, requerimiento o acto de comunicación dirigido a un miembro de la comunidad universitaria que sea remitido a su cuenta institucional se entiende válidamente comunicado, sin perjuicio de las formalidades especiales previstas en el Reglamento Estudiantil, el Estatuto Docente o la ley. Correlativamente, es deber del titular consultar su cuenta con la periodicidad que exige su vínculo con la Institución.

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

Postulado del PEI (2025)	Traducción en esta política
Formación integral a lo largo de la vida	Reglas de vigencia y uso de la cuenta para egresados y participantes de educación continuada; formación obligatoria y periódica en ciudadanía digital y seguridad.
Modelo centrado en el aprendizaje del estudiante	Reconocimiento del correo como canal oficial de notificación académica, con reglas de claridad, oportunidad y no saturación del estudiante.
Formación para la investigación y transferencia de conocimiento	Deber reforzado de reserva sobre resultados no publicados, datos de investigación y activos de propiedad intelectual transm tidos por correo.
Ecosistemas de innovación	Marco de uso responsable de asistentes de inteligencia artificial sobre el buzón institucional (numeral 6.5.7), habilitando la innovación con salvaguardas.
Responsabilidad social y sostenibilidad	Principios de austeridad en el envío masivo, uso racional del recurso compartido y proscripción de todo contenido discriminatorio u ofensivo.

7 Objetivos



7.1 Objetivo general

Establecer los principios, deberes y lineamientos que aseguren un uso adecuado, ético, seguro y trazable del correo electrónico institucional de la Universidad El Bosque, de modo que se protejan la confidencialidad, la integridad y la disponibilidad de la información institucional y los derechos de los titulares de datos personales, y se garantice la validez y confiabilidad del correo como canal oficial de comunicación.

7.2 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 14.1.

Tabla 2. Objetivos específicos formulados bajo criterios SMART.

N.º	Objetivo específico	Horizonte
OE-1	Garantizar que el 100 % de las cuentas institucionales activas opere con autenticación multifactor, priorizando los perfiles de mayor exposición al riesgo.	Diciembre de 2026
OE-2	Asegurar que el dominio institucional y sus subdominios autorizados cuenten con registros SPF, DKIM y DMARC en política de rechazo, y que el 100 % del correo entrante y saliente se transporte cifrado mediante TLS.	Diciembre de 2026
OE-3	Reducir la tasa de compromiso de credenciales por suplantación de identidad al menos un 50 % frente a la línea base de 2025, mediante filtrado, simulaciones controladas y formación.	Diciembre de 2027
OE-4	Lograr que al menos el 85 % de la comunidad universitaria complete anualmente la formación institucional en uso seguro del correo y ciudadanía digital.	Anual, desde 2026
OE-5	Implementar y mantener el procedimiento de reporte de correo sospechoso, con un tiempo medio de contención de incidentes confirmados inferior a cuatro horas hábiles.	Diciembre de 2026
OE-6	Formalizar el ciclo de vida de las cuentas –creación, modificación, delegación, suspensión y disposición final– con trazabilidad auditable del 100 % de las novedades.	Junio de 2027
OE-7	Definir y aplicar el marco de uso responsable de asistentes de inteligencia artificial sobre buzones institucionales, con criterios diferenciados por nivel de clasificación de la información.	Junio de 2027

8 Principios rectores



Estos principios se fundamentan en lo dispuesto por el PEI, 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.

- **Oficialidad.** El correo institucional es el canal formal de comunicación de la Universidad; los asuntos institucionales se tramitan por este medio y no por canales personales.
- **Titularidad** institucional y uso personal e intransferible. La cuenta es un recurso de la Universidad asignado nominalmente a una persona; su uso no es transferible y su titular responde por la actividad realizada desde ella.

- **Proporcionalidad y mínimo privilegio.** Los accesos, delegaciones y controles se otorgan y aplican en la medida estrictamente necesaria para la función o el estudio.
- **Dignidad, respeto y no discriminación.** Ninguna comunicación institucional puede hostigar, discriminar, difamar ni vulnerar la intimidad o el buen nombre de una persona.
- **Privacidad y debido proceso.** El monitoreo se realiza con finalidad legítima, de forma proporcionada y con las garantías del numeral 6.5.10; no se accede al contenido de un buzón sino en los supuestos y con las autorizaciones allí previstas.
- **Trazabilidad y valor probatorio.** Los mensajes de datos tienen la fuerza probatoria que les reconoce la Ley 527 de 1999; la Universidad preserva su integridad y trazabilidad.
- **Austeridad y uso racional del recurso compartido.** El envío innecesario o masivo indiscriminado consume recursos institucionales y tiempo de terceros.
- **Mejora continua.** Los controles se revisan periódicamente conforme al ciclo PHVA y a la evolución del riesgo.

9 Ciclo de vida de la cuenta institucional



Etapa	Lineamiento
Creación	La cuenta se crea a partir de la novedad formal registrada por Talento Humano, Registro y Control Académico o la unidad contratante, según el tipo de vínculo. La solicitud se tramita como petición de servicio conforme a la práctica de gestión de peticiones de ITIL 4, con los tiempos definidos en el acuerdo de niveles de servicio. No se crean cuentas por solicitud informal.
Activación	El titular acepta expresamente esta política, define credenciales conforme a la norma de contraseñas y activa la autenticación multifactor para el uso pleno del buzón.
Cuentas funcionales o de área	Toda cuenta no nominal debe tener un responsable designado por escrito, quien responde por su uso, sus accesos delegados y su revisión semestral. Se prohíbe compartir la contraseña; el acceso de varias personas se habilita mediante delegación registrada en la plataforma.
Modificación y delegación	Los cambios de vínculo, unidad o rol generan la revisión de accesos. Toda delegación de buzón se autoriza por escrito por el titular o el responsable, se registra y se revoca de forma automática al cesar la causa que la originó.

Etapa	Lineamiento
Inactividad y suspensión	La Dirección de Tecnología puede suspender preventivamente una cuenta ante indicios razonables de compromiso, uso indebido o riesgo inminente para la infraestructura, informando al titular y a su unidad en el término de un (1) día hábil.
Desvinculación	Al terminar el vínculo, el área encargada Talento Humano, Registro y Control Académico o la unidad contratante registra la inhabilitación del correo en la Mesa de Servicio o a través de mecanismos automatizados conforme a los plazos definidos en el procedimiento de gestión de identidades. La información de carácter institucional contenida en el buzón se transfiere al jefe inmediato o al responsable del proceso, con registro de la entrega.
Egresados y graduados	La vigencia, las funcionalidades y las condiciones de uso de la cuenta de egresado se rigen por el procedimiento específico definido por la Dirección de Tecnología en articulación con la Política de Egresados y Graduados, y su uso permanece sujeto a esta política.
Disposición final	La eliminación del buzón se realiza conforme a las tablas de retención documental y a las obligaciones legales de conservación, previa verificación de que no exista deber de preservación por proceso disciplinario, judicial o de auditoría en curso.

10 Lineamientos de uso



10.1 Responsabilidad del titular

- El titular es responsable de todas las actividades realizadas desde su cuenta institucional.
- La cuenta es de uso personal e intransferible. La contraseña no se comparte, no se reutiliza en servicios externos y se gestiona conforme a la norma institucional de contraseñas.
- El acceso se protege con autenticación multifactor. Ningún usuario debe aprobar una solicitud de segundo factor que no haya iniciado.
- El titular debe reportar de inmediato a la Mesa de Servicio cualquier indicio de acceso no autorizado, pérdida de credenciales, actividad anómala o extravío de un dispositivo con acceso al buzón.
- El acceso desde dispositivos personales (BYOD) exige bloqueo de pantalla, cifrado del dispositivo y capacidad de borrado remoto del perfil institucional; el titular acepta estas condiciones al configurar el buzón en dicho dispositivo.

- El titular debe verificar la exactitud, la pertinencia y la corrección idiomática de los mensajes que remite, y validar la necesidad de incluir a todos los destinatarios, el historial y los adjuntos antes de responder o reenviar.

10.2 Clasificación y manejo de la información

- La información transmitida por correo se maneja conforme a los niveles de clasificación definidos en la Política de Seguridad y Privacidad de la Información y en la Política de Gobernanza de Datos.
- Los mensajes que contengan información clasificada deben rotularse en el asunto con la etiqueta correspondiente y, cuando el nivel lo exija, cifrarse o transmitirse mediante el portal institucional de transferencia segura de archivos, y no como adjunto ordinario.
- El tratamiento de datos personales por correo se sujeta a la Política de Tratamiento de Datos Personales. Se prohíbe remitir bases de datos personales a destinatarios externos sin autorización del responsable del tratamiento y sin los controles de protección exigidos.
- Se prohíbe copiar o reenviar mensajes clasificados como reservados o confidenciales sin autorización expresa del remitente original o del propietario de la información.
- La información de carácter institucional contenida en el buzón es de propiedad de la Universidad. La Universidad no responde por la información de carácter estrictamente personal que el usuario decida almacenar en su cuenta institucional.

10.3 Prevención del fraude y verificación reforzada

- Ante cualquier mensaje que solicite credenciales, pagos, cambios de datos bancarios, compra de bonos, transferencias urgentes o información sensible, el usuario debe abstenerse de actuar y verificar la solicitud por un canal distinto del correo, aun cuando el remitente aparente ser una autoridad institucional.
- Todo cambio de datos bancarios de un proveedor o de un colaborador requiere verificación por doble canal y registro documental, con independencia de la aparente legitimidad del correo que lo solicita.

- No se deben abrir enlaces ni archivos adjuntos de origen desconocido o inesperado. Se recomienda digitar directamente en el navegador la dirección del servicio que se desea consultar.
- Todo correo sospechoso debe reportarse mediante el mecanismo institucional de reporte y no simplemente eliminarse, a fin de permitir la contención del incidente para el resto de la comunidad.
- La Universidad realizará simulaciones controladas de suplantación de identidad con finalidad exclusivamente formativa. Sus resultados son agregados y no serán utilizados como fundamento de medidas disciplinarias individuales.

10.4 Comunicaciones institucionales y envíos masivos

- La Dirección de Comunicaciones es la instancia autorizada para el envío de comunicados masivos institucionales, conforme a la Política de Comunicación. Las unidades que requieran un envío masivo deben solicitarlo por el canal establecido, con la antelación definida en el procedimiento respectivo.
- Los envíos masivos deben identificar claramente al emisor institucional, guardar relación con los fines misionales y respetar los principios de pertinencia, oportunidad y austeridad.
- Las comunicaciones dirigidas a titulares de datos personales con fines distintos de los estrictamente académicos o contractuales observarán lo dispuesto en la Ley 2300 de 2023 y en la Política de Tratamiento de Datos Personales, incluyendo mecanismos accesibles de exclusión.
- Se prohíbe compartir con terceros externos los contactos o las listas de distribución de la Universidad.
- Las comunicaciones enviadas fuera de la jornada laboral atenderán lo previsto en la Política de Desconexión Laboral.

10.5 Firma institucional y aviso legal

Todos los usuarios deben emplear la firma institucional unificada y el aviso legal definidos en el **Anexo B,** cuya versión vigente publica la Dirección de Comunicaciones. No se admite el uso de imágenes, lemas, avisos o elementos gráficos ajenos a la identidad institucional en la firma del correo.

10.6 Conductas prohibidas

Sin perjuicio de otras conductas que resulten contrarias a la ley, a los reglamentos institucionales o a los principios de esta política, se prohíbe expresamente:

- Enviar mensajes que contravengan las normas legales, el orden público, la intimidad o el buen nombre de las personas, o que contengan material irrespetuoso, difamatorio, discriminatorio, de acoso, intimidación o violencia, así como contenidos ilegales, extorsivos, obscenos o de carácter sexual.
- Utilizar cuentas de correo personales para establecer, tramitar o transferir información institucional.
- Suplantar la identidad de otra persona o unidad, alterar las cabeceras del mensaje o hacerse pasar por una instancia institucional.
- Emplear el correo institucional para propaganda, ofertas, negocios personales, avisos publicitarios, proselitismo político-electoral o cualquier actividad ajena a las funciones académicas o laborales.
- Reenviar o propagar cadenas, rumores, correo basura o mensajes de procedencia desconocida hacia cuentas institucionales.
- Utilizar el correo institucional como herramienta de mensajería instantánea, existiendo canales institucionales dispuestos para ese fin.
- Configurar el reenvío automático y permanente del buzón institucional hacia cuentas externas, salvo autorización expresa de la Dirección de Tecnología por razones justificadas y documentadas.
- Extraer o exportar de manera masiva el contenido del buzón institucional sin autorización, especialmente con ocasión de la terminación del vínculo.
- Eludir, desactivar o intentar vulnerar los controles de seguridad del servicio de correo, incluidos los filtros de contenido, la autenticación multifactor y los mecanismos de prevención de fuga de información.

10.7 Uso de inteligencia artificial sobre el buzón institucional

La Universidad promueve la adopción de la inteligencia artificial como palanca de innovación y eficiencia, en coherencia con el PEI (2025) y con el Proyecto 14 del PDCM 2025–2027. Su uso sobre el correo institucional se sujeta a las siguientes reglas:

- Solo se permite el uso de asistentes de inteligencia artificial **aprobados y contratados institucionalmente,** cuyos términos garanticen que la información no se emplea para el entrenamiento de modelos de terceros.
- Se prohíbe copiar, cargar o exponer información institucional clasificada, datos personales sensibles, resultados de investigación no publicados o información sujeta a acuerdos de confidencialidad en herramientas de inteligencia artificial no autorizadas.
- Toda comunicación oficial generada con asistencia de inteligencia artificial debe ser revisada y validada por una persona antes de su envío. La responsabilidad por el contenido recae siempre en el titular de la cuenta.
- No se admite el uso de inteligencia artificial para automatizar respuestas en procesos que impliquen decisiones con efectos académicos, disciplinarios, laborales o contractuales, sin intervención humana explícita.
- La Dirección de Tecnología, con el acompañamiento de la Coordinación de Seguridad de la Información, mantendrá y publicará el listado de herramientas autorizadas y sus condiciones de uso, tomando como referencia ISO/IEC 42001:2023.

10.8 Continuidad, respaldo y retención

- La Universidad define y mantiene los períodos de retención de los mensajes conforme a las tablas de retención documental y a las obligaciones legales aplicables, en articulación con la Secretaría General.
- Cuando exista un proceso disciplinario, judicial, de auditoría o de investigación en curso, la Universidad podrá disponer la preservación del buzón involucrado, suspendiendo su eliminación.

- El usuario es responsable de organizar y conservar la información propia de su gestión, y de solicitar oportunamente el respaldo o la migración que requiera ante cambios de rol o terminación del vínculo.

10.9 Gestión de incidentes

- Todo incidente que afecte la confidencialidad, la integridad o la disponibilidad del correo institucional debe reportarse de inmediato a la Mesa de Servicio, punto único de contacto conforme a la práctica de mesa de servicio de ITIL 4.
- La Mesa de Servicio registra, categoriza y prioriza el caso según impacto y urgencia, y lo escala a la Coordinación de Seguridad de la Información conforme a la práctica de *gestión de incidentes* de ITIL 4 y al procedimiento institucional de gestión de incidentes de seguridad. Los incidentes recurrentes o de causa desconocida se derivan a la práctica de *gestión de problemas* para su análisis de causa raíz.
- Los tiempos de respuesta, contención y resolución se rigen por el acuerdo de niveles de servicio publicado en el catálogo de servicios de la Dirección de Tecnología, y se miden conforme a la práctica de *gestión de niveles de servicio*.
- El reporte oportuno y de buena fe de un incidente, incluso cuando se derive de un error del propio usuario, no dará lugar por sí solo a medidas sancionatorias. La Universidad promueve una cultura de reporte sin temor a la represalia, por ser condición necesaria de una detección temprana.
- Cuando el incidente comprometa datos personales, se activarán los deberes de notificación previstos en la normativa aplicable y en la Política de Tratamiento de Datos Personales.

10.10 Monitoreo, privacidad y debido proceso

La Universidad realiza monitoreo automatizado del tráfico de correo con la finalidad exclusiva de proteger la infraestructura y la información institucional. Este monitoreo opera sobre metadatos, patrones de tráfico y contenido en tránsito procesado por los sistemas de filtrado; no constituye lectura sistemática de las comunicaciones.

El acceso al contenido del buzón de un usuario identificado únicamente procede en los siguientes supuestos: (i) autorización expresa y escrita del titular; (ii) requerimiento de autoridad judicial o administrativa competente; (iii) inves-

tigación disciplinaria o de seguridad formalmente abierta, con autorización conjunta de la Coordinación de Seguridad de la Información y de la Secretaría General; o (iv) necesidad institucional imperiosa derivada de ausencia prolongada o desvinculación del titular, limitada a la información estrictamente necesaria para la continuidad del proceso y con registro documental de la actuación. En todos los casos se dejará constancia del acceso, de su motivación y de su alcance, y se informará al titular, salvo prohibición legal expresa.

La Universidad se reserva el derecho de suspender, modificar o eliminar cuentas en las que se evidencie uso inadecuado o incumplimiento de esta política, previa aplicación de las garantías procesales que correspondan según el vínculo de la persona.

10.11 Consecuencias del incumplimiento

El uso inadecuado del correo institucional o el incumplimiento de esta política dará lugar a la aplicación de 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 adoptarán por la instancia competente, de manera consistente e imparcial, y su severidad guardará proporción con la gravedad de la conducta, el daño causado y la reincidencia. Cuando la conducta pueda constituir un delito de los tipificados en la Ley 1273 de 2009, la Universidad pondrá los hechos en conocimiento de las autoridades competentes.

11 Estrategias de implementación



1. **Fortalecimiento técnico del canal.** Despliegue y sostenimiento de los controles del Anexo A, con prioridad en autenticación de dominio (SPF, DKIM, DMARC), cifrado en tránsito, filtrado antimalware y antisuplantación, y análisis de adjuntos en entorno aislado.
2. **Identidad y acceso.** Universalización de la autenticación multifactor, aplicación del principio de mínimo privilegio y automatización del ciclo de vida de las cuentas a partir de las fuentes autoritativas de vinculación.
3. **Cultura y formación.** Programa anual de formación en ciudadanía digital y seguridad, diferenciado por perfil de riesgo, con simulaciones controladas de suplantación y refuerzo dirigido a los grupos con mayor exposición.
4. **Comunicación institucional.** Publicación de la política en los canales oficiales, incorporación al proceso de inducción de estudiantes, profesores y colaboradores, y divulgación mediante piezas de comunicación breves y accionables.

5. **Gestión del riesgo.** Inclusión del correo electrónico en el registro institucional de riesgos, con tratamiento definido conforme a ISO 31000 y revisión periódica ante cambios del contexto.
6. **Integración al Campus Digital.** Articulación de las acciones con el Proyecto 14 del PDCM 2025–2027, asegurando que cada inversión tecnológica asociada demuestre retorno medible.

12 Acciones e instrumentos



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

Instrumento	Nivel	Responsable de su expedición
Norma de Gestión Técnica del Correo Electrónico (controles mínimos, Anexo A)	Norma	Dirección de Tecnología / Coordinación de Seguridad de la Información
Procedimiento de gestión del ciclo de vida de cuentas e identidades	Procedimiento	Dirección de Tecnología
Procedimiento de reporte y respuesta a incidentes de correo (alineado a ITIL 4)	Procedimiento	Coordinación de Seguridad de la Información
Catálogo de servicios y acuerdo de niveles de servicio (ANS) del servicio de correo	Norma	Dirección de Tecnología

Instrumento	Nivel	Responsable de su expedición
Procedimiento de solicitud y aprobación de envíos masivos	Procedimiento	Dirección de Comunicaciones
Guía de clasificación y etiquetado de la información en el correo	Guía técnica	Coordinación de Seguridad de la Información
Guía de configuración segura del correo en dispositivos personales (BYOD)	Guía técnica	Dirección de Tecnologías
Guía de uso responsable de asistentes de inteligencia artificial	Guía técnica	Dirección de Tecnología / Coordinación de Seguridad de la Información
Línea base de configuración de la plataforma de correo	Baseline	Dirección de Tecnología
Plan anual de formación en ciudadanía digital y seguridad	Plan	Dirección de Tecnologías / Talento Humano / DIDE
Tablero de indicadores de la política	Instrumento de medición	Dirección de Tecnología

13 Gobernanza de la política

13.1 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. La línea de autoridad y responsabilidad se organiza en cuatro niveles: un **nivel de dirección estratégica,** integrado por el Consejo Directivo y la Rectoría, que aprueba la política 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 prioriza inversiones, aprueba excepciones y revisa indicadores; un **nivel de ejecución,** encabezado por la Dirección de Tecnología de la Información como unidad responsable, con Coordinación de Seguridad de la Información como instancia de supervisión y verificación independiente; y un **nivel de aplicación distribuida,** compuesto por las facultades, departamentos y unidades administrativas, sus líderes TIC y cada usuario en su condición de titular de cuenta.

13.2 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
Consejo Directivo	Aprobar la política y sus actualizaciones sustanciales; conocer los resultados de su evaluación.	A
Rectoría	Impartir las directrices para su implementación y asegurar la asignación de recursos.	A
Comité de Tecnología / Comité de Seguridad de la Información	Revisar indicadores, priorizar inversiones, aprobar excepciones formales y recomendar actualizaciones.	C / I
Dirección de Tecnología	Unidad responsable: expedir los instrumentos derivados, operar los controles, gestionar el ciclo de vida de las cuentas, mantener el tablero de indicadores y liderar la actualización de la política.	R
Coordinación de Seguridad de la Información	Definir y verificar los controles, gestionar el riesgo asociado, coordinar la respuesta a incidentes y emitir concepto sobre excepciones y accesos a buzones.	R
Secretaría General	Custodia documental de la política, concepto jurídico, autorización conjunta de accesos a buzones en investigaciones y articulación con retención documental.	C
Dirección de Comunicaciones	Administrar los envíos masivos institucionales y mantener vigente la firma y el aviso legal.	R
Departamento de Talento Humano	Reportar oportunamente las novedades de vinculación y desvinculación; incorporar la política a la inducción y aplicar el régimen disciplinario laboral.	R
Vicerrectoría Académica y Registro y Control Académico	Reportar novedades de la población estudiantil y asegurar la coherencia con las notificaciones académicas.	C

Instancia o rol	Responsabilidad principal	RACI
Decanaturas, direcciones de unidad y líderes TIC	Difundir y hacer cumplir la política en su ámbito; validar accesos y delegaciones; reportar incidentes.	R
Usuario titular de la cuenta	Cumplir la política, custodiar sus credenciales y reportar incidentes.	R

13.3 Instancias de aprobación, actualización, seguimiento y evaluación

- **Aprobación y derogatoria:** Consejo Directivo, por recomendación de la Rectoría.
- **Actualización sustancial:** propuesta por la Dirección de Tecnología, con concepto de la Coordinación de Seguridad de la Información y de la Secretaría General, revisión del Comité de Tecnología y aprobación del Consejo Directivo.
- **Actualización de instrumentos derivados (normas, procedimientos, guías y líneas base):** Dirección de Tecnología, con concepto de la Coordinación de Seguridad de la Información; se informa al Comité de Tecnología.
- **Seguimiento:** Dirección de Tecnología, con reporte semestral al Comité de Tecnología y anual a la Rectoría, en el marco del seguimiento al PDCM 2025–2027.
- **Evaluación independiente:** Auditoría Interna y División de Calidad, en el marco de los procesos de autoevaluación institucional y aseguramiento de la calidad.
- **Excepciones:** toda excepción a un lineamiento debe solicitarse por escrito, motivarse, contar con concepto de la Coordinación de Seguridad de la Información, tener vigencia máxima de doce (12) meses y quedar registrada en el inventario de excepciones.

14 Evaluación y mejora continua



14.1 Mecanismos de medición

La eficacia de la política se mide mediante un conjunto de 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 Dirección de Tecnología.

Tabla 5. Tablero de indicadores de la política. Las líneas base se establecen con corte a diciembre de 2025.

Código	Indicador	Tipo	Fórmula	Frecuencia	Meta 2026	Meta 2027
KPI-01	Cobertura de autenticación multifactor	Cumplimiento	Cuentas activas con MFA / Total de cuentas activas	Mensual	100 %	100 %
KPI-02	Autenticación de dominio y cifrado en tránsito	Cumplimiento	Dominios con SPF, DKIM y DMARC en rechazo / Dominios autorizados	Trimestral	100 %	100 %
KPI-03	Tasa de compromiso de credenciales	Eficacia	N.º de cuentas comprometidas / Total de cuentas activas	Mensual	–30 % vs. 2025	–50 % vs. 2025
KPI-04	Cobertura de formación	Cumplimiento	Personas que completan la formación anual / Población objetivo	Semestral	≥ 75 %	≥ 85 %
KPI-05	Tasa de reporte en simulaciones controladas	Eficacia	Correos simulados reportados / Correos simulados enviados	Semestral	≥ 30 %	≥ 50 %
KPI-06	Tiempo medio de contención de incidentes	Eficiencia	Promedio de horas hábiles entre el reporte y la contención	Mensual	≤ 6 h	≤ 4 h
KPI-07	Trazabilidad del ciclo de vida de cuentas	Cumplimiento	Novedades con registro auditable / Total de novedades	Trimestral	≥ 90 %	100 %
KPI-08	Oportunidad en la desvinculación de cuentas	Eficiencia	Cuentas inhabilitadas dentro del plazo / Total de desvinculaciones	Mensual	≥ 90 %	≥ 98 %
KPI-09	Vigencia de excepciones	Cumplimiento	Excepciones vigentes dentro de plazo / Total de excepciones	Semestral	100 %	100 %
KPI-10	Cumplimiento del ANS de la Mesa de Servicio	Eficiencia	Casos de correo atendidos dentro del ANS / Total de casos de correo	Mensual	≥ 90 %	≥ 95 %
KGI-01	Confiabilidad del canal oficial	Impacto	Percepción favorable sobre confiabilidad del correo institucional (encuesta anual)	Anual	≥ 75 %	≥ 85 %
KGI-02	Cumplimiento del compromiso del PDCM	Impacto	Estado de actualización e implementación de la política frente al Proyecto 10	Anual	Imple-men-tada	100 %

14.2 Ciclo de mejora continua

La política se gestiona bajo el ciclo PHVA. En la fase de **planeación** se actualizan el análisis de riesgos y las metas anuales; en la de **ejecución** se despliegan los controles, la formación y las campañas de comunicación; en la de **verificación** se revisan los indicadores, los resultados de las simulaciones, las auditorías internas y externas, 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.

14.3 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 mensajes de datos, los delitos informáticos o la calidad de la educación superior.
- Recomendaciones de pares académicos, del Consejo Nacional de Acreditación o de organismos de inspección, vigilancia y control que involucren esta política.
- Materialización de un incidente de seguridad de alto impacto sobre el correo institucional, o de una tendencia sostenida de incidentes que evidencie insuficiencia de los controles vigentes.
- Cambio sustancial en la plataforma tecnológica de correo, en el proveedor del servicio o en el modelo de identidad institucional.
- Incumplimiento sostenido de las metas de dos (2) o más indicadores durante dos (2) períodos consecutivos de medición.
- Adopción institucional de nuevas capacidades de inteligencia artificial que operen sobre el contenido del correo.
- Modificación de la estructura organizacional que altere las responsabilidades definidas en el numeral 7.2.

15 Referencias



Normativa nacional

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. (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 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. (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 Desconexión Laboral.*

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 Comunicación.*

Universidad El Bosque. (2024). *Política de Egresados y Graduados.*

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).*

Universidad El Bosque. (s. f.). *Política de Seguridad y Privacidad de la Información.*

Estándares y literatura técnica

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

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

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

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

International Organization for Standardization. (2024). *ISO/IEC 27001:2022/Amd 1:2024. Information security management systems — Requirements — Amendment 1: Climate action changes.* 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. (2023). *ISO/IEC 42001:2023. Information technology — Artificial intelligence — Management system.* 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.

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). *Email management policy* [Plantilla de política]. SANS Institute.

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

UNESCO. (2025). *Lifelong learning frameworks.* Instituto de la UNESCO para el Aprendizaje a lo Largo de Toda la Vida.

Anexo A Controles mínimos de gestión técnica del correo



Los siguientes controles constituyen la norma técnica derivada de esta política. Se adoptan a partir de la *Email Management Policy* del SANS Institute (2026) y se armonizan con ISO/IEC 27002:2022 y los CIS Critical Security Controls v8.1. Su implementación, verificación y evidencia corresponden a la Dirección de Tecnologías de la Información, con supervisión del Oficial de Seguridad de la Información.

Código	Control	Verificación
CE-01	Mantener el inventario actualizado de los dominios institucionales autorizados para el envío y la recepción de correo.	Semestral
CE-02	Mantener el inventario de los agentes de transferencia de correo (MTA) autorizados para cada dominio institucional.	Semestral
CE-03	Mantener registros DNS correctos y vigentes (SPF, DKIM y DMARC) para cada dominio institucional autorizado, con DMARC en política de rechazo.	Trimestral

Código	Control	Verificación
CE-04	Exigir conexiones cifradas mediante TLS entre todos los servidores de correo, internos y externos.	Trimestral
CE-05	Bloquear el correo proveniente de dominios que no dispongan de los registros de autenticación apropiados.	Trimestral
CE-06	Aplicar filtrado de contenido no deseado (spam) a todo el correo entrante y saliente.	Continua
CE-07	Aplicar filtrado de código malicioso a todo el correo entrante y saliente.	Continua
CE-08	Aplicar filtrado de contenido antisuplantación de identidad a todo el correo entrante y saliente.	Continua
CE-09	Aplicar filtrado de URL antisuplantación de identidad a todo el correo entrante y saliente.	Continua
CE-10	Aplicar filtrado de contenido de datos (DLP) sobre el correo, conforme a los niveles de clasificación institucionales.	Continua
CE-11	Aplicar filtrado de archivos adjuntos, incluyendo su detonación en entornos aislados (sandbox) para validar su comportamiento.	Continua
CE-12	Mantener un portal institucional de transferencia de archivos, independiente del sistema de correo, para el envío de archivos de gran tamaño a destinatarios externos.	Semestral
CE-13	Exigir autenticación multifactor para el acceso al buzón institucional desde cualquier cliente o dispositivo.	Mensual
CE-14	Registrar y conservar las trazas de auditoría de acceso y administración del servicio de correo, conforme a los períodos de retención definidos.	Trimestral
CE-15	Verificar y restringir la creación de reglas de reenvío automático hacia dominios externos.	Mensual

Anexo B Firma institucional y aviso legal



Todos los usuarios deben emplear el siguiente modelo de firma. La Dirección de Comunicaciones mantiene y publica la versión gráfica vigente.

Nombre y apellidos

Cargo o vínculo

Unidad académica o administrativa

Universidad El Bosque

PBX: (601) 648 9000 – Ext.

Av. Cra. 9 n.º 131 A - 02, Bogotá D. C., Colombia

www.unbosque.edu.co

Aviso legal: Este mensaje y sus archivos adjuntos son confidenciales y están dirigidos exclusivamente a su destinatario. Su distribución, reenvío, impresión o copia no autorizada está prohibida. Si usted recibió este mensaje por error, por favor notifíquelo al remitente y elimínelo. Las opiniones expresadas corresponden al autor y no representan necesariamente la posición institucional de la Universidad El Bosque. La Universidad trata los datos personales conforme a su Política de Tratamiento de Datos Personales, disponible en www.unbosque.edu.co.

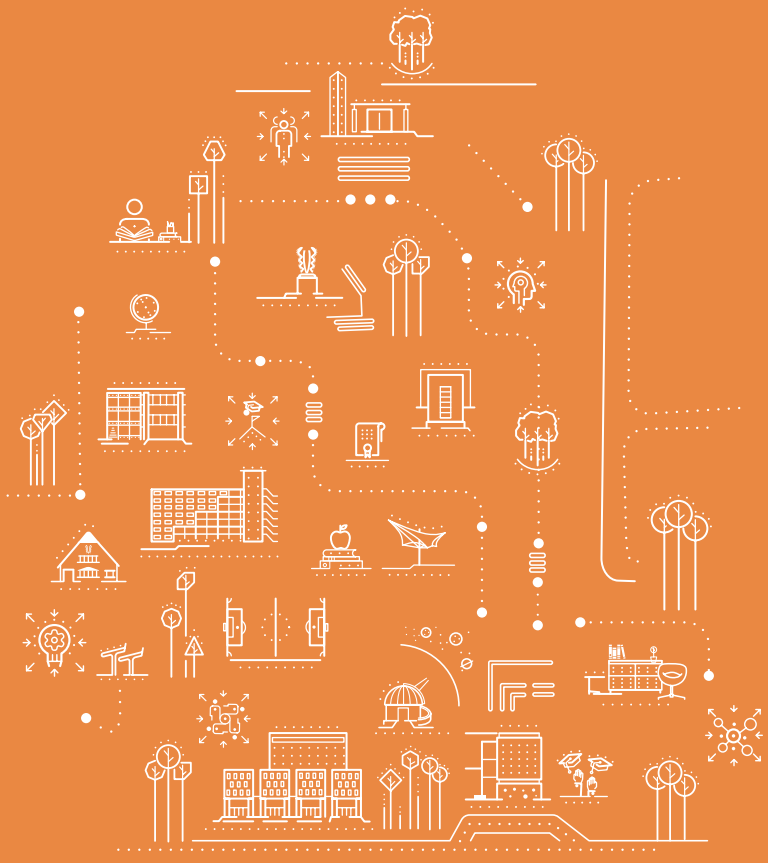
Antes de imprimir este mensaje, considere su responsabilidad con el ambiente.

Anexo C Control de cambios

Versión	Fecha	Naturaleza del cambio
1.0	Septiembre de 2014	Expedición original. Estructura basada en introducción, justificación, marco general, objetivo, alcance, desarrollo, responsables y evaluación.
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. Incorporación de objetivos SMART, tablero de indicadores KPI/KGI, criterios de actualización y matriz de gobernanza. Nuevos contenidos: ciclo de vida de cuentas, autenticación multifactor y de dominio, clasificación de la información, prevención de fraude por suplantación y BEC, uso de inteligencia artificial sobre el buzón, retención y preservación, monitoreo con debido proceso y anexo de controles técnicos derivados de SANS (2026). Actualización de estándares (ISO/IEC 27001:2022 y Amd 1:2024, 27002:2022, 27004:2016, 27701:2025, 42001:2023, ISO 31000:2018, NIST CSF 2.0, CIS v8.1) e incorporación de ITIL 4 como marco de gestión del servicio. Corrección de la referencia normativa a la Ley 527 de 1999.

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

UNIVERSIDAD
EL BOSQUE



- **Edificio Fundadores**
  Av. Cra. 9 N°. 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