RESOLUCION 367 (16-01-2026)
POR LA CUAL SE POR LA CUAL SE ADOPTA EL ESTATUTO DIGITAL INTEGRAL DE FUNDES Y SE DEROGA LA RESOLUCIÓN No. 165 DE 2014.

El rector en uso de sus atribuciones constitucionales, legales y en especial los conferidos por la ley 30 de 1992 y el artículo 15 del Estatuto General de la Fundación de Estudios Superiores "Monseñor Abraham Escudero Montoya" FUNDES, y

CONSIDERANDO

- Que el Artículo 67 de la Constitución Política, establece que la educación es responsabilidad del Estado, la sociedad y la familia. La Ley 30 de 1992, artículo 28 y literal "d", artículo 29, faculta a la Universidad para organizar sus labores formativas, académicas, científicas y culturales para el cumplimiento de su misión social y de su función Institucional.
- Que los artículos 15 y 20 de la Constitución Política consagran los derechos a la intimidad, al *habeas data* y a la libertad de información, y que la Ley Estatutaria 1581 de 2012, el Decreto Único Reglamentario 1074 de 2015, la Ley 1273 de 2009 y la Ley 1266 de 2008 conforman el marco legal de protección de datos personales y seguridad informática aplicable a las instituciones de educación superior.
- Que el CONPES 3995 de 2020 y el Decreto 1330 de 2019 exigen a las IES contar con políticas de gestión de la información, infraestructura tecnológica adecuada y gobernanza digital institucional.
- Que la evolución acelerada de las Tecnologías de la Información y la Comunicación (TIC), la proliferación de amenazas como el *ransomware*, el *phishing* avanzado y la suplantación de identidad mediante medios sintéticos (*deepfakes*), así como la irrupción de la Inteligencia Artificial generativa en los procesos académicos, exigen la actualización integral de los marcos normativos internos.
- Que FUNDES ofrece programas en modalidad presencial, virtual e híbrida, utiliza Google Workspace para Educación como plataforma tecnológica institucional, y ha adoptado la Política de Buen Uso de Inteligencia Artificial mediante Resolución Rectoral No. 352 de 2025, lo cual requiere un marco normativo integral que regule el ecosistema digital de la Institución.
- Que es necesario regular de manera integral el tratamiento de datos biométricos, el uso de imagen y voz, la auditoría de herramientas digitales institucionales y la preferencia de los canales oficiales de comunicación, para garantizar la seguridad, la transparencia y la protección de los derechos de toda la comunidad educativa.
- Que la Resolución No. 165 del 13 de febrero de 2014, sobre uso de correo electrónico, acceso a internet y protección de datos personales, requiere ser actualizada e integrada en un instrumento comprehensivo que responda a la realidad digital actual.
- Que es función del Rector de la Fundación expedir los procedimientos administrativos (Estatuto General articulo 15 literal i ratificado por Resolución 5607 del 12 Julio 2011 MEN)

Aprobada según Resolución 1495 del Ministerio de Educación Nacional, reformada según Resolución 5607 de Julio 12 de 2011 / Código ante el ICFES 2741 – NIT 809.008.799-7
(8)2485862 - 2488787 Carrera 7 No. 10 - 37 733520 / Espinal - Tolima - COL
3202254010 www.fundes.edu.co fundes@fundes.edu.co

EN MÉRITO DE LO EXPUESTO, EL RECTOR RESUELVE:

ARTÍCULO PRIMERO. Adoptar el Estatuto Digital Integral de FUNDES, cuyo texto completo forma parte integrante de la presente resolución como Anexo Único. El Estatuto regula: la protección de datos personales, el gobierno digital, el uso de recursos TIC, la ciberseguridad, la propiedad intelectual digital, el uso ético de la IA y el régimen disciplinario digital.

ARTÍCULO SEGUNDO. El Estatuto Digital aplica a todos los miembros de la comunidad educativa de FUNDES —estudiantes, docentes, personal administrativo, contratistas, proveedores y visitantes— y a toda persona que acceda a los recursos tecnológicos o instalaciones de la Institución.

ARTÍCULO TERCERO. El Estatuto Digital se integra al ordenamiento institucional como norma complementaria del Reglamento Estudiantil, el Reglamento Interno de Trabajo, la Política de Buen Uso de IA (Res. 352/2025) y los demás instrumentos normativos internos. La Política de Ingreso, Permanencia y Seguridad (Resolución 222-L de 2018) continúa vigente en materia de seguridad física; el tratamiento de datos personales captados por videovigilancia y control de ingreso se rige por el Estatuto Digital. Su aceptación será requisito para la matrícula, la vinculación laboral y la suscripción de contratos que impliquen acceso a recursos TIC.

ARTÍCULO CUARTO. La Secretaría General y la Dirección Administrativa dispondrán de seis (6) meses para adecuar los contratos de matrícula, contratos laborales y formularios de autorización de datos personales a las disposiciones del Estatuto Digital. Las autorizaciones otorgadas con anterioridad mantienen su vigencia conforme al artículo 10 del Decreto 1377 de 2013.

ARTÍCULO QUINTO. La Rectoría designará al Oficial de Protección de Datos dentro de los treinta (30) días hábiles siguientes a la expedición de la presente resolución, conforme al artículo 7 del Estatuto Digital.

ARTÍCULO SEXTO. La Administración TIC actualizará la señalización de videovigilancia dentro de los noventa (90) días siguientes, conforme al artículo 16, parágrafo 1, del Estatuto Digital y la Guía de Videovigilancia de la SIC.

ARTÍCULO SÉPTIMO. FUNDES socializará el Estatuto Digital a toda la comunidad educativa dentro de los primeros treinta (30) días de cada semestre. El texto estará disponible permanentemente en www.fundes.edu.co y en las plataformas institucionales.

ARTÍCULO OCTAVO. DEROGATORIA. Derógase integralmente la Resolución Rectoral No. 165 del 13 de febrero de 2014 y todas las disposiciones internas que resulten contrarias al Estatuto Digital.

ARTÍCULO NOVENO – VIGENCIA. La presente resolución rige a partir de su expedición y deroga todas las disposiciones que le sean contrarias.

Aprobada según Resolución 1495 del Ministerio de Educación Nacional, reformada según Resolución 5607 de Julio 12 de 2011 / Código ante el ICFES 2741 – NIT. 809.008.799-7
(8)2485862 - 2488787 Carrera 7 No. 10 - 37 733520 / Espinal - Tolima - COL
3202254010 www.fundes.edu.co fundes@fundes.edu.co

COMUNIQUESE Y CUMPLASE,

Dada en El Espinal, Tolima, a los dieciséis (16) días del mes de enero de 2026.

P. ROBERTO JOSE GUZMAN VILLANUEVA.
Rector.

VoBo **María Odette Amaya Aljure**
Dirección Administrativa y Financiera

Aprobada según Resolución 1495 del Ministerio de Educación Nacional, reformada según Resolución 5607 de Julio 12 de 2011 / Código ante el ICFES 2741 – NIT. 809.008.799-7
(8)2485862 - 2488787 Carrera 7 No. 10 - 37 733520 / Espinal - Tolima - COL
3202254010 www.fundes.edu.co fundes@fundes.edu.co

FUNDACIÓN DE ESTUDIOS SUPERIORES
«MONSEÑOR ABRAHAM ESCUDERO MONTOYA»
FUNDES

NIT: 809.008.799-7 Código ICFES: 2741
«Ciencia, Fe y Liderazgo»
Carrera 7 No. 10-37, El Espinal, Tolima

ESTATUTO DIGITAL INTEGRAL

Política Institucional de Protección de Datos Personales,
Uso Responsable de Tecnologías de la Información y la Comunicación,
Ciberseguridad e Inteligencia Artificial

Resolución No. 367 de 16 Enero 2026

(Deroga integralmente la Resolución No. 165 del 13 de febrero de 2014)

El Espinal, Tolima
[2026]

CONTENIDO

CONTENIDO 2
TÍTULO I – DISPOSICIONES GENERALES 3
TÍTULO II – GOBIERNO Y ORGANIZACIÓN DIGITAL 5
TÍTULO III – PROTECCIÓN DE DATOS PERSONALES 6
Capítulo 1. Generalidades del tratamiento 6
Capítulo 2. Datos sensibles y de menores de edad 8
Capítulo 3. Datos biométricos, imagen y voz 9
Capítulo 4. Derechos y procedimientos 11
Capítulo 5. Transferencia y transmisión de datos 12
TÍTULO IV – USO ACEPTABLE DE RECURSOS TIC 13
Capítulo 1. Correo electrónico institucional 14
Capítulo 2. Acceso a internet y redes 15
Capítulo 3. Plataformas educativas y herramientas digitales 16
Capítulo 4. Uso de redes sociales externas 18
Capítulo 5. Canales de comunicación institucional preferentes 18
Capítulo 6. Netiqueta y comunicación digital 19
Capítulo 7. Cumplimiento de condiciones de la plataforma tecnológica 20
Capítulo 8. Buenas prácticas de ciberseguridad para la comunidad educativa 21
TÍTULO V – CIBERSEGURIDAD 23
TÍTULO VI – RESPUESTA A INCIDENTES Y GESTIÓN DE BRECHAS 25
TÍTULO VII – USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL 26
TÍTULO VIII – PROPIEDAD INTELECTUAL EN ENTORNO DIGITAL 26
TÍTULO IX – CONVIVENCIA Y CIUDADANÍA DIGITAL 27
TÍTULO X – RÉGIMEN DISCIPLINARIO DIGITAL Y DISPOSICIONES FINALES 27
Capítulo 1. Clasificación de faltas 27
Capítulo 2. Sanciones 28
Capítulo 3. Disposiciones finales 29

TÍTULO I – DISPOSICIONES GENERALES

ARTÍCULO 1. ***Objeto.*** El presente Estatuto Digital tiene por objeto establecer el marco integral de políticas, principios, derechos, obligaciones y procedimientos que rigen la protección de datos personales —incluyendo datos biométricos, de imagen y de voz—, el uso responsable de los recursos tecnológicos y los canales de comunicación, la ciberseguridad, la propiedad intelectual en entornos digitales, el uso ético de la Inteligencia Artificial y la auditoría de las herramientas digitales en la Fundación de Estudios Superiores «Monseñor Abraham Escudero Montoya» – FUNDES.

ARTÍCULO 2. ***Ámbito de aplicación.*** Este Estatuto aplica a todas las personas que interactúen con los recursos tecnológicos, los sistemas de información o los datos personales administrados por FUNDES, incluyendo:

1. Estudiantes de todos los niveles y modalidades de formación.
2. Docentes, investigadores y personal académico.
3. Personal administrativo, directivo y operativo.
4. Contratistas, consultores, proveedores y terceros con acceso a recursos institucionales.
5. Egresados, aspirantes y miembros de la comunidad educativa extendida en cuanto interactúen con los servicios digitales de FUNDES.

Parágrafo. El presente Estatuto se aplica con independencia de la ubicación geográfica desde la cual se acceda a los recursos institucionales, de la modalidad —presencial, virtual o híbrida— y del tipo de dispositivo utilizado.

ARTÍCULO 3. ***Marco normativo de referencia.*** El presente Estatuto se fundamenta en la Constitución Política de Colombia, la legislación vigente en materia de protección de datos personales, delitos informáticos, comercio electrónico, derechos de autor y educación superior, las políticas nacionales de seguridad digital y de inteligencia artificial, los instrumentos internacionales adoptados por el Estado colombiano, los estándares técnicos de referencia y las demás disposiciones que modifiquen, sustituyan, complementen o desarrollen dicho marco.

Parágrafo. Las referencias específicas a normas contenidas en este Estatuto se entenderán hechas a las disposiciones vigentes al momento de su aplicación. Cualquier modificación legislativa o reglamentaria que afecte las materias aquí reguladas se entenderá automáticamente incorporada en lo que resulte favorable al cumplimiento de los fines institucionales y a la protección de los derechos de los titulares.

ARTÍCULO 4. ***Definiciones.*** Para los efectos del presente Estatuto, se adoptan las definiciones contenidas en la Ley Estatutaria 1581 de 2012 y sus normas reglamentarias, así como las siguientes definiciones complementarias:

Término	Definición	Referencia
Dato personal	Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.	Art. 3, Ley 1581/2012

Término	Definición	Referencia
Dato sensible	Dato que afecta la intimidad del titular o cuyo uso indebido puede generar discriminación: origen racial, orientación política, convicciones religiosas, salud, vida sexual, datos biométricos.	Art. 5, Ley 1581/2012
Dato biométrico	Dato sensible obtenido mediante el tratamiento técnico de características físicas o fisiológicas de una persona (huella dactilar, reconocimiento facial, iris, voz) que permita su identificación unívoca.	Art. 5, Ley 1581/2012; SIC
Responsable del tratamiento	FUNDES, en su condición de persona jurídica que decide sobre la base de datos y el tratamiento de los datos.	Art. 3, Ley 1581/2012
Encargado del tratamiento	Persona natural o jurídica que realiza el tratamiento de datos por cuenta de FUNDES (proveedores de nube, plataformas LMS, etc.).	Art. 3, Ley 1581/2012
Recurso TIC	Cualquier equipo, red, sistema, plataforma, aplicación, cuenta o servicio tecnológico provisto o administrado por FUNDES.	Definición institucional
Canal institucional	Todo medio de comunicación oficial provisto por FUNDES: correo @fundes.edu.co, plataforma Q10, Google Workspace institucional, LMS y demás herramientas administradas por la Institución.	Definición institucional
Inteligencia Artificial (IA)	Sistema basado en máquinas que puede generar predicciones, recomendaciones, contenido o decisiones a partir de datos, influyendo en entornos reales o virtuales.	OCDE, 2024
Incidente de seguridad	Evento que compromete o amenaza la confidencialidad, integridad o disponibilidad de la información o los sistemas de FUNDES.	CONPES 3995/2020
Auditoría digital	Proceso sistemático de revisión, verificación y evaluación del uso de las herramientas y recursos tecnológicos institucionales con fines de seguridad, cumplimiento y mejora.	Definición institucional

ARTÍCULO 5. ***Principios rectores.*** El tratamiento de datos personales y el uso de recursos TIC en FUNDES se rigen por los siguientes principios, sin perjuicio de los demás consagrados en la legislación vigente:

a) Legalidad. Toda actividad de tratamiento de datos y uso de recursos TIC se sujeta a la Constitución, la ley y el presente Estatuto.
b) Finalidad. El tratamiento de datos obedece a finalidades legítimas, explícitas e informadas al titular.
c) Libertad. El tratamiento de datos requiere el consentimiento previo, expreso e informado del titular, salvo excepciones legales.
d) Veracidad. La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada y comprobable.
e) Transparencia. El titular tiene derecho a conocer en todo momento la existencia y las características del tratamiento.
f) Seguridad. FUNDES adopta medidas técnicas, humanas y administrativas para proteger los datos contra acceso no autorizado, pérdida, alteración o destrucción.

g) Confidencialidad. Las personas que intervienen en el tratamiento están obligadas a guardar reserva, incluso después de finalizar su vinculación con FUNDES.
h) Responsabilidad demostrada. FUNDES implementa medidas apropiadas y efectivas, y está en capacidad de demostrar su cumplimiento ante la autoridad de protección de datos.
i) Proporcionalidad. Las restricciones al uso de recursos TIC y las actividades de auditoría son proporcionadas a los fines legítimos de seguridad, operatividad y misión institucional.
j) Autonomía universitaria. Las disposiciones de este Estatuto se expiden en ejercicio de la autonomía institucional, con respeto a los derechos fundamentales de la comunidad educativa.

TÍTULO II – GOBIERNO Y ORGANIZACIÓN DIGITAL

ARTÍCULO 6. ***Gobernanza Digital.*** La dirección estratégica del ecosistema tecnológico de FUNDES corresponde a la Rectoría, con el apoyo operativo de la Administración TIC y la supervisión en materia de datos personales del Oficial de Protección de Datos. Cuando la complejidad de un asunto lo requiera, la Rectoría podrá convocar mesas de trabajo con los actores pertinentes de la comunidad educativa.

ARTÍCULO 7. ***Oficial de Protección de Datos Personales.*** FUNDES designará un Oficial de Protección de Datos Personales, quien ejercerá las siguientes funciones:

1. Velar por el cumplimiento de la legislación vigente en materia de protección de datos.
2. Atender las consultas y reclamos de los titulares dentro de los plazos legales.
3. Coordinar la actualización del registro de bases de datos cuando la normativa lo exija.
4. Supervisar la implementación de medidas de seguridad para la protección de la información personal, incluyendo los datos biométricos y de imagen y voz.
5. Articular la capacitación periódica de la comunidad educativa en protección de datos.
6. Reportar a la Rectoría las novedades, incidentes y recomendaciones pertinentes en materia de protección de datos personales.

ARTÍCULO 8. ***Administración TIC.*** La administración operativa de los recursos tecnológicos, incluyendo el correo electrónico institucional, los servidores, las redes, las plataformas educativas y los sistemas de información, recae en el área de Sistemas de Información y Tecnología. Dentro de esta área, los roles de *PostMaster* y *WebMaster* son los únicos autorizados para realizar envíos masivos de correo electrónico a la comunidad educativa en nombre de la Institución.

Parágrafo. El área de Administración TIC definirá y ejecutará los planes de mantenimiento preventivo y correctivo, las políticas de respaldo, la ejecución periódica de antivirus y la monitorización del desempeño de los servicios tecnológicos.

ARTÍCULO 9. ***Política de seguridad de la información.*** FUNDES adopta una política de seguridad de la información orientada a preservar la confidencialidad, integridad y disponibilidad de todos los activos de información institucionales. Esta política se alinea con los estándares técnicos nacionales e internacionales aplicables y se

implementa bajo un ciclo de mejora continua que comprende las fases de planificación, implementación, evaluación y mejora.

TÍTULO III – PROTECCIÓN DE DATOS PERSONALES

Capítulo 1. Generalidades del tratamiento

ARTÍCULO 10. ***Responsable del tratamiento.*** FUNDES, identificada con NIT 809.008.799-7, con domicilio en la Carrera 7 No. 10-37, El Espinal (Tolima), actúa como responsable del tratamiento de los datos personales contenidos en sus bases de datos físicas y digitales.

Parágrafo 1. De conformidad con el Decreto 090 del 18 de enero de 2018 (compilado en el DUR 1074 de 2015), la obligación de inscribir las bases de datos en el Registro Nacional de Bases de Datos (RNBD) ante la Superintendencia de Industria y Comercio aplica a las sociedades y entidades sin ánimo de lucro cuyos activos totales superen las cien mil (100.000) Unidades de Valor Tributario (UVT) y a las personas jurídicas de naturaleza pública. Dado que FUNDES es una entidad sin ánimo de lucro de naturaleza privada, la obligación de registro en el RNBD se determinará en función de que sus activos totales superen o no el umbral señalado, conforme a la información contable certificada del ejercicio fiscal correspondiente. Con independencia de que FUNDES esté o no obligada al registro en el RNBD, la Institución cumplirá la totalidad de las obligaciones previstas en la Ley 1581 de 2012 y sus normas reglamentarias en materia de tratamiento de datos personales, incluyendo: contar con una Política de Tratamiento de Datos publicada y accesible; obtener autorización previa, expresa e informada; atender consultas y reclamos en los plazos legales; implementar medidas de seguridad; designar al Oficial de Protección de Datos; y adoptar el principio de responsabilidad demostrada. Si en algún ejercicio fiscal los activos de FUNDES superan el umbral legal, la Administración TIC, bajo la supervisión del Oficial de Protección de Datos, procederá a inscribir las bases de datos en el RNBD dentro de los dos (2) meses siguientes y a mantener actualizada anualmente la información registrada.

Parágrafo 2. En cumplimiento del principio de responsabilidad demostrada (*accountability*), FUNDES implementará un programa integral de gestión de datos personales que incluya, como mínimo: (i) políticas internas de protección de datos efectivas y aplicables; (ii) procedimientos de atención de consultas y reclamos; (iii) un sistema de gestión de autorizaciones; (iv) evaluaciones periódicas de impacto en la privacidad; (v) auditorías internas de cumplimiento; (vi) un plan de formación continua para el personal que trate datos personales; y (vii) mecanismos de respuesta ante incidentes de seguridad de datos personales. El Oficial de Protección de Datos coordinará la implementación y el seguimiento de este programa.

Parágrafo 3. Cuando se presente un incidente de seguridad que comprometa datos personales (acceso no autorizado, pérdida, destrucción, alteración o divulgación indebida), FUNDES activará de inmediato su protocolo de respuesta, que incluirá: (i) contención técnica del incidente; (ii) evaluación del impacto y de los riesgos para los titulares afectados; (iii) notificación a los titulares cuando el incidente pueda afectar significativamente sus derechos; (iv) reporte a la Superintendencia de Industria y Comercio conforme a los plazos y procedimientos vigentes; y (v) documentación del incidente, las medidas adoptadas y las lecciones aprendidas. Toda persona que detecte o

sospeche de un incidente de seguridad de datos personales deberá reportarlo de manera inmediata al Oficial de Protección de Datos o a la Administración TIC.

ARTÍCULO 11. ***Finalidades del tratamiento.*** FUNDES tratará los datos personales de sus grupos de interés para las siguientes finalidades de carácter general:

1. Gestionar los procesos de admisión, matrícula, registro académico, certificación y seguimiento a egresados.
2. Administrar las relaciones laborales, contractuales y de prestación de servicios con docentes, personal administrativo, contratistas y proveedores.
3. Comunicar información sobre servicios educativos, eventos académicos, empresariales y publicaciones asociadas a la formación.
4. Cumplir obligaciones legales, incluyendo los reportes al SNIES, HECAA, el SPADIES y demás entidades de vigilancia y control.
5. Realizar análisis prospectivo de las necesidades de los grupos de interés para innovar en la prestación de servicios.
6. Garantizar la seguridad física y lógica de las instalaciones, redes y sistemas de información, incluyendo el control de acceso mediante datos biométricos.
7. Registrar en imagen y voz actividades académicas, eventos institucionales, y elaborar material de identificación y promoción.
8. Realizar auditorías digitales sobre las herramientas institucionales con fines de seguridad, cumplimiento normativo y mejora continua.
9. Recopilar, almacenar, analizar y procesar datos personales, académicos, laborales y de desempeño mediante sistemas de inteligencia artificial con fines de mejora de procesos educativos, análisis predictivo, sistemas de alerta temprana, evaluación institucional e investigación en educación superior.
10. Las demás que se deriven de la relación académica, laboral o contractual y que resulten compatibles con la misión institucional.

Parágrafo. Cualquier nueva finalidad de tratamiento que no se encuentre prevista en este artículo requerirá la actualización de la autorización por parte del titular, salvo que la ley disponga lo contrario.

ARTÍCULO 12. ***Autorización del titular.*** FUNDES recogerá la autorización previa, expresa e informada del titular para el tratamiento de sus datos personales. Dicha autorización podrá otorgarse por escrito, de forma oral, mediante conductas inequívocas, o a través de mecanismos electrónicos que permitan su posterior consulta. FUNDES conservará copia o prueba de la autorización otorgada.

Parágrafo 1. La autorización para el tratamiento de datos personales se integrará a los formularios de matrícula, contratos laborales, contratos de prestación de servicios y demás instrumentos contractuales que vincule FUNDES con sus grupos de interés. Dichos instrumentos contendrán cláusulas específicas y diferenciadas de autorización que cubran, según corresponda: datos personales y de contacto; datos biométricos; uso de imagen y voz; monitoreo y auditoría digital; tratamiento de datos para sistemas de IA; consulta de antecedentes; y datos de salud.

Parágrafo 2. Para los datos personales recolectados con anterioridad a la expedición del presente Estatuto, FUNDES podrá mantener el tratamiento conforme a las finalidades previamente informadas, siempre que el titular haya tenido la oportunidad de ejercer sus derechos en los términos de la ley aplicable.

Capítulo 2. Datos sensibles y de menores de edad

ARTÍCULO 13. ***Tratamiento de datos sensibles.*** El tratamiento de datos sensibles está prohibido, salvo que concurra alguna de las excepciones previstas en la ley, entre ellas: la autorización explícita del titular; el tratamiento necesario para salvaguardar un interés vital; el tratamiento referido a datos manifiestamente públicos; o el tratamiento necesario para fines históricos, estadísticos o científicos con disociación de la información. Cuando FUNDES requiera tratar datos sensibles, informará al titular de forma explícita el carácter facultativo de la respuesta y la naturaleza sensible de los datos solicitados.

ARTÍCULO 14. ***Datos de niños, niñas y adolescentes.*** De conformidad con el artículo 7 de la Ley 1581 de 2012 y el artículo 2.2.2.25.2.9 del Decreto Único Reglamentario 1074 de 2015, el tratamiento de datos personales de niños, niñas y adolescentes está prohibido, salvo que se trate de datos de naturaleza pública y que el tratamiento cumpla acumulativamente los siguientes requisitos: (i) que responda y respete el interés superior del menor; (ii) que asegure el respeto de sus derechos fundamentales; y (iii) que se cuente con la autorización del representante legal.

Parágrafo 1. FUNDES trata datos personales de estudiantes menores de dieciocho (18) años matriculados en sus programas académicos, en las mismas categorías previstas en el artículo 20 del presente Estatuto (datos personales y de contacto, datos biométricos, imagen y voz, monitoreo digital, tratamiento para sistemas de IA). La autorización para dicho tratamiento será otorgada por el representante legal (padre, madre o acudiente) al momento de la matrícula, mediante la firma conjunta del contrato de matrícula que incluye las cláusulas de autorización diferenciada. Previamente al otorgamiento de la autorización, el menor de edad ejercerá su derecho a ser escuchado, y su opinión será valorada teniendo en cuenta su madurez, autonomía y capacidad para entender el asunto.

Parágrafo 2. FUNDES, en su condición de entidad educativa, cumplirá el deber legal de proveer información y capacitar a los representantes legales y a los propios menores de edad sobre los eventuales riesgos del tratamiento indebido de sus datos personales en entornos digitales, y sobre el uso responsable y seguro de su información personal y la de los demás. Para ello, incluirá módulos específicos en los procesos de inducción y en las actividades de formación continua dirigidas tanto a estudiantes como a padres de familia y acudientes.

Parágrafo 3. Los estudiantes menores de dieciocho (18) años que accedan a plataformas institucionales en la nube tendrán una experiencia restringida en ciertos servicios, conforme a los Términos de Servicio del proveedor de la plataforma y a las disposiciones del artículo 36 del presente Estatuto. La Administración TIC identificará y configurará adecuadamente las cuentas de estos usuarios en la consola administrativa de la plataforma. El consentimiento parental previo, libre, expreso e informado para el acceso a servicios adicionales de la plataforma será recogido al momento de la matrícula mediante la firma del acudiente en el contrato correspondiente, y será reconfirmado anualmente por FUNDES ante el proveedor, conforme al artículo 36, parágrafo 3.

Parágrafo 4. El representante legal podrá revocar en cualquier momento la autorización para el tratamiento de datos del menor, mediante solicitud escrita dirigida al Oficial de Protección de Datos en los canales previstos en el artículo

18 del presente Estatuto, sin perjuicio de que la revocación pueda limitar el acceso del estudiante a determinados servicios institucionales, lo cual será informado previamente al representante legal.

Parágrafo 5. Queda expresamente prohibido el uso de datos personales de estudiantes menores de edad para fines de perfilamiento comercial, publicidad dirigida o cualquier finalidad ajena a la relación educativa. Los datos de menores no podrán ser compartidos con terceros ajenos a la prestación del servicio educativo, salvo requerimiento legal o judicial. FUNDES extremará las medidas de seguridad sobre las bases de datos que contengan información de menores, conforme a los estándares más exigentes previstos en el presente Estatuto y en la normativa vigente.

Capítulo 3. Datos biométricos, imagen y voz

ARTÍCULO 15. ***Recolección y uso de datos biométricos.*** FUNDES podrá recolectar datos biométricos —tales como huella dactilar, registro facial u otros similares— de los miembros de su comunidad educativa para las siguientes finalidades específicas:

1. Control de acceso físico a las instalaciones de la sede.
2. Control de jornada laboral del personal vinculado.
3. Autenticación de identidad para el acceso a entornos digitales, plataformas educativas y evaluaciones en línea, cuando la naturaleza de la actividad lo justifique.

Dada su naturaleza de datos sensibles, la recolección de datos biométricos requiere autorización explícita, previa e informada del titular, quien será notificado de: la finalidad específica del tratamiento, el período de retención, las medidas de seguridad adoptadas y el carácter facultativo de la respuesta.

Parágrafo 1. Los datos biométricos serán almacenados con cifrado y controles de acceso reforzados, segregados de las demás bases de datos personales. El acceso a estos datos estará restringido al personal estrictamente necesario para la administración del sistema de control de acceso.

Parágrafo 2. Los datos biométricos se conservarán únicamente durante la vigencia de la vinculación del titular con FUNDES. Terminada dicha vinculación, serán eliminados de forma segura dentro de los treinta (30) días hábiles siguientes, salvo que exista obligación legal de conservación.

ARTÍCULO 16. ***Recolección y uso de imagen y voz.*** FUNDES podrá captar, almacenar y utilizar la imagen (fotografía y video) y la voz de los miembros de su comunidad educativa para las siguientes finalidades:

1. Carnetización e identificación institucional.
2. Registros de seguridad mediante circuito cerrado de televisión (CCTV) y sistemas de videovigilancia en áreas comunes de la sede.
3. Registro y documentación de actividades académicas, eventos institucionales, ceremonias de grado y actividades de extensión.
4. Elaboración de material de promoción y difusión institucional, incluyendo publicaciones en redes sociales oficiales, página web, vallas, material impreso y demás medios de comunicación.
5. Grabación de las sesiones de clase con mediación virtual, conforme a la modalidad vigente, orientada a garantizar la calidad académica, la disponibilidad del material para repaso y la trazabilidad del proceso formativo.

La autorización para el uso de imagen y voz se recogerá de forma específica, diferenciándola del consentimiento general para tratamiento de datos personales. Cuando la imagen o voz se destine a fines de promoción o publicidad, el titular será informado de los medios de difusión previstos.

Parágrafo 1. El sistema de videovigilancia (CCTV) de FUNDES constituye un tratamiento de datos personales biométricos sujeto a la Ley 1581 de 2012 y a la Guía de la Superintendencia de Industria y Comercio sobre protección de datos en sistemas de videovigilancia. FUNDES ha evaluado que la videovigilancia es necesaria y proporcional para la finalidad de seguridad de personas y bienes en sus instalaciones, y que no existen medios menos intrusivos igualmente eficaces. Las cámaras se ubicarán exclusivamente en áreas comunes (accesos, corredores, zonas de circulación, parqueaderos, biblioteca y áreas de servicios), quedando expresamente prohibida su instalación en baños, vestidores, consultorios de bienestar universitario o cualquier espacio donde se afecte la intimidad personal. Todas las áreas monitoreadas contarán con señalización visible que incluya, como mínimo: el símbolo de videovigilancia, la identificación de FUNDES como responsable del tratamiento, la finalidad del sistema (seguridad) y los canales de contacto para ejercer derechos de *habeas data*. Las grabaciones de videovigilancia se conservarán por un periodo máximo de treinta (30) días calendario, salvo que exista investigación disciplinaria, administrativa, judicial o requerimiento legal en curso que justifique una conservación mayor. Vencido el periodo de retención, las grabaciones serán eliminadas de forma segura. El acceso a las grabaciones estará restringido al personal de seguridad autorizado, a la Administración TIC, y se suministrará a las autoridades competentes cuando medie requerimiento legal o judicial. La Administración TIC implementará controles de acceso, cifrado en tránsito y en reposo, y registros de auditoría sobre las consultas realizadas a las grabaciones.

Parágrafo 2. Las clases impartidas a través de plataformas de videoconferencia o entornos virtuales de aprendizaje constituyen actividades académicas institucionales en las que la captación de imagen y voz es inherente al proceso pedagógico. FUNDES adopta como política institucional la grabación de las sesiones sincrónicas de clase virtual, con las siguientes finalidades exclusivamente académicas: garantizar la disponibilidad del material de clase para repaso por los estudiantes, asegurar la trazabilidad del proceso formativo, facilitar la evaluación de la calidad docente y respaldar documentalmente las actividades académicas ante eventuales reclamaciones.

Parágrafo 3. La grabación de las sesiones sincrónicas podrá operar bajo una de las siguientes modalidades, según lo determine la Rectoría mediante circular o acto administrativo interno:

1. Modalidad automática: la plataforma LMS graba por defecto todas las sesiones sincrónicas sin requerir activación manual por parte del docente. En esta modalidad, la responsabilidad sobre el tratamiento de los datos de imagen y voz captados recae en FUNDES como responsable del tratamiento, y no en el docente individual. El deber de informar al estudiante se cumple mediante: (i) la cláusula de autorización de tratamiento de datos incluida en el formulario de matrícula; (ii) la mención expresa en el acuerdo pedagógico o *syllabus* de cada curso con componente virtual; y (iii) el indicador visible de grabación activa que la plataforma muestra durante la sesión. No se requiere que el docente anuncie la grabación al inicio de cada sesión, pero se recomienda que en la primera clase del semestre recuerde a los estudiantes la existencia de esta política.
2. Modalidad delegada: la funcionalidad de grabación automática se encuentra desactivada y cada docente decide cuándo grabar, activándola manualmente desde la plataforma. En esta modalidad, el docente

Aprobada según Resolución 1495 del Ministerio de Educación Nacional, reformada según Resolución 5607 de Julio 12 de 2011 / Código ante el ICFES 2741 – NIT. 809.008.799-7
(8)2485862 - 2488787 Carrera 7 No. 10 - 37 733520 / Espinal - Tolima - COL
3202254010 www.fundes.edu.co fundes@fundes.edu.co

que active la grabación deberá informar a los participantes al inicio de la sesión que la clase será grabada, indicando la finalidad académica. La responsabilidad del tratamiento continúa siendo de FUNDES como titular de la plataforma, pero el docente asume el deber de diligencia en la activación y en el aviso oportuno a los participantes.

Parágrafo 4. A la fecha de expedición del presente Estatuto, FUNDES opera bajo la modalidad automática de grabación. El cambio de modalidad no requiere reforma del presente Estatuto, sino únicamente comunicación formal de la Rectoría a la comunidad educativa, con una antelación mínima de treinta (30) días calendario al inicio del semestre académico en que entre a regir la nueva modalidad.

Parágrafo 5. El estudiante matriculado en programas o asignaturas con componente virtual acepta, al momento de la matrícula, que las sesiones de clase podrán ser grabadas bajo cualquiera de las modalidades previstas en este artículo, como condición inherente al servicio educativo. FUNDES informará de esta política de manera expresa en la cláusula de autorización de tratamiento de datos.

Parágrafo 6. Las grabaciones de clases virtuales se conservarán en la plataforma institucional durante el semestre académico en curso y hasta treinta (30) días hábiles después de la finalización del periodo de calificaciones y reclamaciones del respectivo curso. Vencido este plazo, serán eliminadas, salvo que exista requerimiento académico, administrativo, disciplinario o legal que justifique una conservación mayor. El acceso a las grabaciones estará restringido a los estudiantes matriculados en el curso, al docente titular y al personal académico y administrativo autorizado.

Parágrafo 7. Se prohíbe a los estudiantes y a cualquier participante la grabación, captura de pantalla, descarga o redistribución no autorizada de las sesiones de clase virtual, ya que ello vulnera los derechos de imagen, voz y propiedad intelectual del docente y de los demás participantes. La infracción de esta prohibición constituye falta disciplinaria.

Parágrafo 8. El uso de herramientas de inteligencia artificial para transcripción automatizada, resumen, traducción, análisis o cualquier otro procesamiento de las grabaciones de clases virtuales se regirá por lo dispuesto en la Política de Buen Uso de Inteligencia Artificial de FUNDES (Resolución Rectoral No. 352 de 2025) y su Manual de Seguridad Técnica (Documento Complementario IV). Queda prohibido subir grabaciones institucionales a plataformas de IA públicas no autorizadas por la Institución.

Capítulo 4. Derechos y procedimientos

ARTÍCULO 17. ***Derechos de los titulares.*** En cumplimiento de la legislación vigente, el titular de datos personales podrá:

1. Conocer, actualizar y rectificar sus datos personales, incluyendo los biométricos y de imagen.
2. Solicitar prueba de la autorización otorgada.
3. Ser informado sobre el uso dado a sus datos personales.
4. Presentar quejas ante la autoridad de protección de datos por infracciones a la normativa.
5. Revocar la autorización o solicitar la supresión del dato cuando no se respeten los principios, derechos y garantías legales y constitucionales.
6. Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

7. Oponerse al tratamiento de sus datos cuando exista una razón legítima y fundada.
8. Solicitar la eliminación de sus datos biométricos al terminar su vinculación con FUNDES.

ARTÍCULO 18. ***Canales de atención y procedimientos.*** Para el ejercicio de los derechos contemplados en el artículo anterior, el titular podrá dirigirse a FUNDES a través de los siguientes canales:

Canal	Datos de Contacto
Correo electrónico	datos.personales@fundes.edu.co
Dirección física	Carrera 7 No. 10-37, El Espinal, Tolima

Las consultas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo. Los reclamos se atenderán en un máximo de quince (15) días hábiles. Cuando no fuere posible atender la solicitud dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la nueva fecha de respuesta, sin superar los plazos máximos legales.

Capítulo 5. Transferencia y transmisión de datos

ARTÍCULO 19. ***Transferencia y transmisión internacional de datos.*** Cuando FUNDES utilice plataformas, servicios en la nube o proveedores tecnológicos ubicados fuera de Colombia, garantizará que la transferencia o transmisión de datos personales se realice conforme a la normativa vigente. Para ello, suscribirá contratos de transmisión de datos con los encargados que contengan como mínimo: las finalidades autorizadas, las obligaciones de seguridad, las restricciones de uso, y las condiciones de devolución o eliminación de los datos. A la fecha de expedición del presente Estatuto, FUNDES utiliza Google Workspace para Educación como plataforma principal de correo electrónico, almacenamiento en la nube y herramientas colaborativas, cuyos servidores se encuentran ubicados en centros de datos de Google LLC en Estados Unidos y otras jurisdicciones. El uso de esta plataforma implica una transmisión internacional de datos personales amparada por los Términos de Servicio de Google Workspace para Educación, los cuales incluyen cláusulas contractuales conformes con los estándares internacionales de protección de datos. FUNDES informará a los titulares, a través de la cláusula de autorización en los instrumentos contractuales, sobre la existencia de esta transmisión internacional.

Parágrafo. FUNDES verificará que el país de destino ofrezca niveles adecuados de protección conforme a la declaración de la autoridad competente, o que se cuente con autorización del titular o con alguna de las causales de excepción legal. Los datos biométricos no serán objeto de transferencia internacional salvo autorización explícita del titular y justificación documentada de necesidad.

ARTÍCULO 20. ***Integración con instrumentos contractuales.*** Los contratos de trabajo, de prestación de servicios, los formularios de matrícula y los convenios con terceros que impliquen tratamiento de datos personales contendrán cláusulas específicas de autorización diferenciada que cubran, según la naturaleza de la relación, las siguientes categorías:

1. Datos personales y de contacto para gestión de la relación académica, laboral o contractual.
2. Datos biométricos para control de acceso y jornada laboral.
3. Imagen y voz para carnetización, registros de seguridad y material de promoción institucional.
4. Monitoreo y auditoría digital de herramientas institucionales con fines de seguridad y cumplimiento.
5. Tratamiento de datos para sistemas de inteligencia artificial con fines de mejora educativa e investigación.
6. Consulta de inhabilidades, antecedentes y verificación académica y laboral, cuando aplique.
7. Datos de salud y núcleo familiar para salud ocupacional y seguridad social.

Parágrafo. El titular declarará que la información proporcionada es veraz y se obligará a reportar cualquier cambio en sus datos personales dentro de los cinco (5) días siguientes a la novedad. FUNDES garantizará los derechos de acceso, rectificación y supresión conforme a la ley vigente.

TÍTULO IV – USO ACEPTABLE DE RECURSOS TIC

ARTÍCULO 21. ***Principio de responsabilidad individual sobre los recursos asignados.*** Toda persona a quien FUNDES asigne un recurso tecnológico —cuenta de correo electrónico, usuario en plataformas académicas (Q10, LMS), acceso a biblioteca digital, almacenamiento en la nube, aplicaciones institucionales o cualquier otro servicio digital— es la única responsable de su correcto uso, custodia y protección. Este principio se materializa en las siguientes obligaciones inderogables:

1. Las credenciales de acceso (usuario y contraseña) son personales, secretas e intransferibles. Su titular no podrá compartirlas, prestarlas, publicarlas, anotarlas en lugares visibles o accesibles a terceros, ni permitir que otra persona las utilice bajo ninguna circunstancia.
2. Todo acto realizado desde una cuenta o sesión asignada se presume ejecutado por su titular. Esta presunción solo podrá ser desvirtuada mediante evidencia técnica verificable que acredite el acceso no autorizado por un tercero, previa denuncia oportuna del incidente.
3. El titular debe cerrar la sesión de sus cuentas institucionales cada vez que finalice su uso, especialmente en equipos compartidos, laboratorios de cómputo, salas de profesores y dispositivos de terceros. Dejar una sesión abierta equivale a dejar la puerta de su responsabilidad abierta.
4. Cuando se utilicen equipos institucionales (computadores de escritorio, portátiles, tabletas), el usuario debe bloquear la pantalla al ausentarse temporalmente y apagar el equipo o cerrar sesión al retirarse del puesto de trabajo o del área de estudio.
5. El usuario no deberá almacenar sus contraseñas en navegadores web de equipos compartidos, ni utilizar la opción de «recordar contraseña» en dispositivos que no sean de su uso personal exclusivo.
6. El titular tiene la obligación de reportar de manera inmediata a la Administración TIC cualquier sospecha de que sus credenciales han sido comprometidas, su cuenta ha sido utilizada sin autorización o su equipo ha sido objeto de acceso indebido.
7. En caso de pérdida, hurto o extravío de un dispositivo en el que se encuentren sesiones activas de cuentas institucionales, el titular deberá solicitar de inmediato el bloqueo de sus accesos a la Administración TIC.

Parágrafo. El incumplimiento de las obligaciones previstas en el presente artículo no exime al titular de las consecuencias académicas, administrativas, disciplinarias o legales derivadas de las acciones ejecutadas desde su cuenta. FUNDES no asume responsabilidad por los daños que se deriven de la negligencia del usuario en la protección de sus credenciales y sesiones.

Capítulo 1. Correo electrónico institucional

ARTÍCULO 22. ***Naturaleza y asignación de la cuenta.*** La cuenta de correo electrónico institucional es un recurso intransferible asignado a personas, dependencias, proyectos o eventos oficiales. FUNDES opera dos dominios institucionales: @fundes.edu.co, asignado a docentes, personal administrativo, contratistas y dependencias institucionales; y @estufundes.edu.co, asignado a estudiantes. Toda persona vinculada a los estamentos de FUNDES tiene derecho a una cuenta en el dominio que le corresponda, cuya asignación y administración corresponde al área de Administración TIC. Ambos dominios tienen el carácter de medio de comunicación oficial y las disposiciones del presente Estatuto les son igualmente aplicables.

Parágrafo 1. El correo electrónico institucional constituye el medio de comunicación oficial de FUNDES para todos los efectos académicos, administrativos y disciplinarios, de conformidad con lo dispuesto en el artículo 81 del Reglamento Estudiantil vigente y en las cláusulas pertinentes de los contratos de matrícula y vinculación laboral. Los mensajes enviados al correo institucional del destinatario generan presunción de conocimiento a partir de su entrega en la bandeja de entrada, sin perjuicio de las reglas especiales de notificación personal que la ley o el Reglamento Estudiantil exijan para actos administrativos sancionatorios. Cada miembro de la comunidad educativa tiene el deber de consultar su correo institucional de manera regular y diligente.

Parágrafo 2. Las comunicaciones académicas, avisos, citaciones y demás actos institucionales enviados a través del correo electrónico institucional o de las plataformas oficiales habilitadas por FUNDES (Q10, LMS, Google Grupos) tienen plena validez institucional. El estudiante, docente o funcionario que alegue no haber recibido una comunicación oficial deberá demostrar que existió una falla técnica verificable en la plataforma, sin que pueda invocar como eximente la falta de consulta de su correo o su desconocimiento de las herramientas institucionales.

ARTÍCULO 23. ***Uso permitido del correo.*** El correo institucional será utilizado exclusivamente para fines académicos, de investigación, de gestión administrativa o de extensión propios de la misión de FUNDES. Todo mensaje enviado desde una cuenta institucional a listas de correo o grupos de discusión deberá incluir el siguiente texto al pie: «Las opiniones expresadas en este mensaje son estrictamente personales y no constituyen una posición oficial de la Institución.»

ARTÍCULO 24. ***Límites técnicos y reglas de uso del correo electrónico.*** El correo electrónico institucional opera sobre la plataforma de servicios en la nube contratada por FUNDES para los dominios @fundes.edu.co y @estufundes.edu.co (a la fecha de expedición, Google Workspace para Educación, o la que la Institución adopte en su reemplazo). Los límites técnicos del servicio de correo se rigen por las condiciones vigentes de la plataforma contratada y por las políticas complementarias que defina la Administración TIC. Se establecen las siguientes reglas institucionales, aplicables con independencia de la plataforma:

1. Tamaño de mensajes: el tamaño máximo de envío y recepción por mensaje será el que defina la plataforma vigente. Cuando un archivo adjunto supere el límite de la plataforma, el usuario deberá

utilizar los servicios de almacenamiento en la nube institucional (Drive o equivalente) para compartirlo mediante enlace.

2. Destinatarios y envíos masivos: como política institucional, los envíos dirigidos a más de cien (100) destinatarios simultáneos deberán canalizarse a través de los grupos de distribución oficiales o de la Administración TIC (*PostMaster/WebMaster*), conforme al artículo 8 del presente Estatuto, para garantizar la trazabilidad, evitar la saturación de buzones y prevenir la clasificación como *spam*. Se recomienda el uso de enlaces compartidos en lugar de archivos adjuntos pesados en envíos a listas de distribución.
3. Límites diarios de envío: la plataforma establece límites diarios de mensajes enviados por usuario, cuya superación genera la suspensión temporal automática de la capacidad de envío sin afectar la recepción. La Administración TIC informará a la comunidad los límites vigentes.
4. Tipos de archivo bloqueados: la plataforma bloquea automáticamente ciertos tipos de archivos considerados de riesgo (archivos ejecutables y similares). Los usuarios que necesiten compartir estos archivos deberán utilizar los servicios de almacenamiento en la nube con los controles de acceso correspondientes.

Parágrafo 1. El almacenamiento del correo electrónico institucional forma parte del espacio asignado por la plataforma al dominio de FUNDES. No se establece una política general de eliminación automática de mensajes por antigüedad. La Administración TIC podrá definir políticas de retención, archivado y gestión del almacenamiento conforme a las necesidades de gestión documental y a la disponibilidad del espacio, las cuales serán comunicadas previamente a la comunidad educativa. Se recomienda a los usuarios mantener buenas prácticas de gestión de su buzón: organizar mensajes mediante etiquetas, eliminar periódicamente correos innecesarios, vaciar la papelera con regularidad y utilizar el almacenamiento en la nube en lugar de adjuntos.

Parágrafo 2. La migración de la plataforma de correo electrónico o de servicios en la nube no requiere reforma del presente Estatuto. La Administración TIC, con aprobación de la Rectoría, comunicará a la comunidad educativa los nuevos parámetros técnicos y las instrucciones de transición con la debida antelación.

ARTÍCULO 25. ***Desactivación de cuentas.*** Las cuentas de correo se desactivarán: (i) treinta (30) días hábiles después de terminar la vinculación del titular; (ii) cuando la dependencia o proyecto deje de existir; (iii) cuando la cuenta permanezca inactiva un (1) semestre académico; o (iv) como medida disciplinaria.

Capítulo 2. Acceso a internet y redes

ARTÍCULO 26. ***Principios del acceso a internet.*** FUNDES provee acceso a Internet como herramienta de apoyo a la docencia, la investigación, la gestión administrativa y la extensión. Los usuarios utilizarán este recurso de manera responsable, ética y conforme a la legislación vigente.

ARTÍCULO 27. ***Conductas prohibidas en el uso de internet y redes.*** Queda expresamente prohibido:

1. Realizar *phishing, spoofing*, inundación de *pings*, ataques DDoS o cualquier forma de interrupción de la red.
2. Acceder sin autorización a servidores, cuentas, datos o aplicaciones ajenos.

3. Capturar tráfico de red, falsificar información de enrutamiento o manipular cabeceras de correo.
4. Distribuir, almacenar o facilitar el acceso a material pornográfico, ilegal, difamatorio o que promueva la violencia.
5. Introducir virus, *worms, ransomware* u otro *software* malicioso.
6. Enviar *spam*, cadenas, mensajes piramidales o publicidad no autorizada.
7. Utilizar la cuenta institucional para fines comerciales personales, suscripción a redes sociales personales o listas comerciales.
8. Enviar contenidos de proselitismo político o comercial, cadenas, mensajes anecdóticos, motivacionales o de cualquier otra índole ajena a la misión institucional desde cuentas oficiales. Las comunicaciones de formación cristiana y pastoral institucional, propias de la identidad católica de FUNDES, no se consideran contenido ajeno a la misión y podrán ser difundidas por los canales oficiales autorizados.
9. Revelar la clave de acceso o permitir el uso de la cuenta por terceros.
10. Cualquier forma de acoso, intimidación, difamación o actividad hostil a través de medios electrónicos.
11. Enviar correos desde direcciones no asignadas por la Institución o suplantar la identidad de otro usuario.

Capítulo 3. Plataformas educativas y herramientas digitales

ARTÍCULO 28. ***Sistemas de gestión de aprendizaje (LMS).*** El acceso a las plataformas educativas institucionales —incluyendo Q10, aulas virtuales y sistemas de biblioteca digital— es personal e intransferible. En aplicación del principio consagrado en el artículo 21, el titular de cada cuenta es el único responsable de la custodia de sus credenciales y de toda acción realizada bajo su usuario, incluyendo la entrega de trabajos, la presentación de evaluaciones, las participaciones en foros, las calificaciones y cualquier interacción registrada en la plataforma.

Parágrafo. FUNDES no se responsabiliza por el uso indebido derivado de la negligencia en la protección de las credenciales. Si un tercero accede a la cuenta del titular por descuido de éste y ejecuta acciones académicas (entrega de trabajos, participación en evaluaciones, modificación de información), dichas acciones se imputarán al titular de la cuenta, salvo que éste acredite haber reportado oportunamente el incidente.

Parágrafo. El uso de herramientas de inteligencia artificial integradas en las plataformas LMS o conectadas a ellas (tales como asistentes de IA, generadores de contenido, correctores automatizados o funcionalidades de aprendizaje adaptativo) se regirá adicionalmente por la Política de Buen Uso de Inteligencia Artificial (Resolución Rectoral No. 352 de 2025). La Administración TIC, en coordinación con la Vicerrectoría Académica, determinará cuáles herramientas de IA están habilitadas en el entorno LMS institucional.

ARTÍCULO 29. ***Herramientas ofimáticas y almacenamiento en la nube***

El uso de herramientas ofimáticas y de almacenamiento en la nube provistas por FUNDES es exclusivo para fines institucionales. La selección y configuración del cliente de correo es responsabilidad del usuario, dentro de los parámetros de seguridad definidos por la Administración TIC. La Institución ofrece servicios de agenda y contactos, pero el respaldo (*backup*) de la información personal es responsabilidad exclusiva del usuario.

ARTÍCULO 30. ***Clases con mediación virtual y activación de cámara.*** La educación con mediación virtual o híbrida que ofrece FUNDES se fundamenta en la interacción pedagógica activa entre docente y estudiantes, lo cual exige la

Aprobada según Resolución 1495 del Ministerio de Educación Nacional, reformada según Resolución 5607 de Julio 12 de 2011 / Código ante el ICFES 2741 – NIT. 809.008.799-7
(8)2485862 - 2488787 Carrera 7 No. 10 - 37 733520 / Espinal - Tolima - COL
3202254010 www.fundes.edu.co fundes@fundes.edu.co

participación visible y verificable de los participantes. En ese contexto, la activación de la cámara durante las sesiones sincrónicas de clase virtual constituye un requerimiento pedagógico legítimo y no una medida de vigilancia, fundamentado en las siguientes consideraciones:

1. La verificación de la identidad del estudiante conectado, como garantía de la integridad académica y el principio de evaluación personalísima.
2. La interacción visual como componente esencial de la comunicación pedagógica, que permite al docente percibir la comprensión, la atención y la participación efectiva del estudiante.
3. La construcción de comunidad de aprendizaje, que requiere presencia social activa de los participantes.
4. El registro y la evaluación de la participación académica, como criterio formativo y sumativo conforme al acuerdo pedagógico.

Parágrafo 1. Cada docente, en ejercicio de su autonomía de cátedra y conforme al acuerdo pedagógico del curso, podrá establecer la activación de cámara como requisito de participación en las sesiones sincrónicas virtuales. Esta exigencia deberá ser comunicada de manera expresa en el programa del curso o *syllabus* desde el inicio del semestre académico. FUNDES respalda institucionalmente al docente que establezca dicho requisito como parte de su estrategia pedagógica.

Parágrafo 2. El estudiante matriculado en programas o asignaturas con componente virtual acepta, al momento de la matrícula, que la activación de cámara podrá ser requerida como condición de participación académica. La negativa injustificada y reiterada a activar la cámara, cuando sea requerida por el docente, podrá ser considerada como inasistencia o falta de participación, con las consecuencias académicas previstas en el Reglamento Estudiantil.

Parágrafo 3. Cuando un estudiante acredite circunstancias excepcionales documentadas que le impidan de manera razonable activar la cámara —tales como limitaciones técnicas verificables de conectividad, condiciones de salud debidamente certificadas o situaciones de vulnerabilidad que comprometan su seguridad— podrá solicitar al docente una alternativa de participación. El docente evaluará la solicitud y, de considerarla procedente, acordará con el estudiante un mecanismo alternativo que preserve los objetivos pedagógicos del curso. La Vicerrectoría Académica dirimirá los desacuerdos que surjan entre docente y estudiante en esta materia.

Parágrafo 4. El cumplimiento del deber de informar sobre la grabación de las sesiones se regirá por la modalidad vigente conforme al artículo 16 del presente Estatuto. Cuando opere la modalidad automática, el aviso institucional en la matrícula, el *syllabus* y el indicador de la plataforma satisfacen dicho deber. Cuando opere la modalidad delegada, el docente que active la grabación deberá adicionalmente informar a los participantes al inicio de la sesión correspondiente.

Parágrafo 5. La activación de cámara requerida por el docente y la política institucional de grabación son complementarias y coherentes entre sí, con independencia de la modalidad de grabación vigente. La sesión grabada constituye evidencia académica verificable de la participación efectiva del estudiante y del desarrollo de las actividades formativas. Una sesión en la que no sea posible verificar la presencia real de los participantes pierde gran parte de su valor como respaldo académico y probatorio, razón por la cual la exigencia de cámara activa resulta pedagógicamente necesaria y normativamente proporcional.

Capítulo 4. Uso de redes sociales externas

ARTÍCULO 31. ***Redes sociales institucionales.*** Las cuentas oficiales de FUNDES en redes sociales son administradas exclusivamente por las personas designadas por la Rectoría o la Vicerrectoría Administrativa. Ningún miembro de la comunidad educativa podrá crear cuentas, páginas o grupos en redes sociales que utilicen el nombre, el escudo, el logo o cualquier signo distintivo de FUNDES sin autorización previa de la Rectoría.

ARTÍCULO 32. ***Conducta en redes sociales personales.*** FUNDES respeta la libertad de expresión de los miembros de su comunidad educativa en sus redes sociales personales. Sin embargo, cuando en dichos espacios se haga referencia directa o indirecta a la Institución, sus directivos, docentes, estudiantes o personal, el usuario deberá:

1. Abstenerse de utilizar la cuenta de correo institucional (@fundes.edu.co o @estufundes.edu.co) para registrarse en redes sociales personales.
2. Actuar con responsabilidad, evitando publicaciones que puedan afectar la honra, el buen nombre o la imagen de FUNDES o de cualquier miembro de la comunidad educativa.
3. No divulgar información institucional confidencial, datos personales de terceros o contenido protegido por derechos de autor a través de redes sociales personales.
4. Dejar claro que las opiniones expresadas son personales y no representan la posición oficial de la Institución.

Parágrafo 1. El incumplimiento de estas disposiciones que cause perjuicio a FUNDES o a terceros podrá dar lugar a las acciones disciplinarias y legales correspondientes.

Parágrafo 2. Cuando las publicaciones realizadas en redes sociales personales configuren conductas tipificadas como faltas en el Reglamento Estudiantil, el Reglamento Profesoral o el Reglamento Interno de Trabajo —tales como difamación, injuria, acoso, ciberacoso, divulgación no autorizada de datos personales de miembros de la comunidad educativa, o publicaciones que afecten gravemente la convivencia o el normal desarrollo de las actividades institucionales—, se aplicarán los procedimientos disciplinarios previstos en el reglamento correspondiente según la calidad del infractor (estudiante, docente o funcionario), con pleno respeto del debido proceso y del derecho de defensa. Lo anterior no constituye censura previa ni restricción a la libertad de expresión constitucionalmente protegida, sino el ejercicio legítimo de la potestad disciplinaria institucional frente a conductas que exceden los límites del discurso protegido, conforme a la jurisprudencia de la Corte Constitucional en la materia. FUNDES podrá, adicionalmente, ejercer las acciones civiles o penales a que hubiere lugar cuando la conducta configure injuria, calumnia u otros delitos tipificados en la legislación penal colombiana.

Capítulo 5. Canales de comunicación institucional preferentes

ARTÍCULO 33. ***Preferencia por canales institucionales.*** FUNDES dispone de herramientas institucionales versátiles que garantizan la interacción entre docentes, estudiantes y personal administrativo de manera ágil, segura y verificable. En consecuencia, la comunicación oficial relacionada con actividades académicas, administrativas y de gestión institucional deberá canalizarse preferentemente a través de los medios provistos por FUNDES, entre los cuales se encuentran:

1. Plataforma académica Q10: módulos de cursos, tablero de anuncios, chat integrado y funcionalidades de seguimiento.
2. Correo electrónico institucional (@fundes.edu.co y @estufundes.edu.co) y sus herramientas asociadas: Google Chat, Google Grupos, etiquetas y carpetas del correo.
3. Aulas virtuales y plataformas LMS institucionales.
4. Los demás medios que la Institución habilite oficialmente.

Parágrafo 1. FUNDES no prohíbe el uso de aplicaciones de mensajería externa como WhatsApp, Telegram u otras similares para la comunicación entre docentes y estudiantes. Sin embargo, la Institución hace una recomendación enfática en contra de su uso como canal habitual para la gestión académica, por las siguientes razones de orden jurídico y práctico:

1. La información compartida por canales externos queda fuera del control y la oficialidad institucional, lo que dificulta la sustentación de pruebas ante reclamaciones académicas o disciplinarias.
2. El uso de grupos de mensajería puede propiciar situaciones de acoso laboral, incumplimiento de las políticas de desconexión laboral y vulneración de derechos de *habeas data* de los participantes.
3. Los audios, capturas de pantalla y mensajes de *chats* externos son fácilmente manipulables y adulterables, incluso con herramientas de inteligencia artificial, lo que compromete su valor probatorio.
4. Quien crea y sostiene un grupo de mensajería externa con estudiantes asume la responsabilidad sobre el tratamiento de los datos personales (números telefónicos, imágenes de perfil, estados) allí involucrados, frente a lo cual FUNDES no tiene incidencia ni responsabilidad.

Parágrafo 2. Los docentes, funcionarios administrativos y contratistas que opten por utilizar canales de mensajería externa para comunicarse con estudiantes o con otros miembros de la comunidad lo hacen bajo su exclusiva responsabilidad, renunciando expresamente a invocar las políticas de desconexión laboral respecto de las interacciones sostenidas por dichos medios, y asumiendo el compromiso de garantizar los derechos de *habeas data* y consentimiento de los involucrados.

Parágrafo 3. A la hora de las reclamaciones académicas, resulta significativamente más viable sustentar pruebas desde las plataformas institucionales que desde chats personales externos. FUNDES insta a los docentes y funcionarios a no renunciar a su bienestar, a la protección de su intimidad y a su vida personal y familiar.

Capítulo 6. Netiqueta y comunicación digital

ARTÍCULO 34. ***Normas de convivencia en comunicaciones digitales.*** Los usuarios de los recursos TIC de FUNDES observarán las siguientes normas de convivencia digital:

1. Evitar el uso sostenido de letras mayúsculas, ya que en el entorno digital equivale a gritar.
2. Mantener un tono respetuoso, profesional y coherente con la misión institucional.
3. No enviar correos a personas que hayan solicitado no recibirlos.
4. Utilizar el esquema de dirección electrónica oculta (CCO) al crear listas de correo, para proteger la privacidad de los destinatarios.
5. Ser cuidadoso al abrir archivos adjuntos o enlaces de remitentes desconocidos o sospechosos.

ARTÍCULO 35. ***Dispositivos personales y móviles (BYOD).*** Los miembros de la comunidad educativa podrán utilizar dispositivos personales —computadores portátiles, tabletas y teléfonos inteligentes— para acceder a los recursos TIC institucionales (correo, plataformas académicas, almacenamiento en la nube y demás servicios), bajo las siguientes condiciones:

1. Mantener el sistema operativo del dispositivo actualizado a la última versión estable disponible.
2. Contar con un método de bloqueo de pantalla activo (PIN, patrón, huella o reconocimiento facial) en todo dispositivo móvil que acceda a cuentas institucionales.
3. Activar el cifrado del dispositivo cuando el sistema operativo lo permita.
4. No instalar aplicaciones de origen desconocido o no verificado que puedan comprometer la seguridad del dispositivo y, por extensión, de las cuentas institucionales.
5. No conectarse a redes Wi-Fi públicas o no seguras para acceder a información institucional confidencial; en caso de necesidad, utilizar conexión VPN o datos móviles.
6. No utilizar dispositivos con *jailbreak* (iOS) o *root* (Android) para acceder a recursos institucionales, por cuanto estas modificaciones eliminan las barreras de seguridad del sistema operativo.

Parágrafo 1. Cuando la Administración TIC lo determine, los dispositivos móviles que accedan a cuentas institucionales podrán ser registrados en el sistema de gestión de dispositivos móviles (MDM) de la plataforma. El registro permite a la Administración TIC aplicar políticas de seguridad básicas (requisitos de contraseña, cifrado, borrado remoto de la cuenta institucional) sin acceder a los datos personales del usuario. El usuario será informado antes del registro y la inscripción será condición de acceso desde el dispositivo.

Parágrafo 2. En caso de pérdida, hurto o extravío de un dispositivo móvil en el que se encuentren sesiones activas de cuentas institucionales, el titular deberá notificarlo de manera inmediata a la Administración TIC para que proceda al cierre remoto de las sesiones activas y, si el MDM está habilitado, al borrado remoto de los datos institucionales del dispositivo. La demora en el reporte no exime al titular de las consecuencias derivadas del acceso no autorizado a su cuenta.

Parágrafo 3. FUNDES no accederá ni interferirá con los datos personales, aplicaciones, fotografías ni contenido privado almacenado en los dispositivos personales de los usuarios. Las medidas de seguridad aplicadas a través del MDM se limitarán exclusivamente a la protección del entorno institucional (perfil de trabajo), con pleno respeto a la privacidad del entorno personal del dispositivo.

Capítulo 7. Cumplimiento de condiciones de la plataforma tecnológica

ARTÍCULO 36. ***Obligaciones derivadas de los Términos de Servicio de la plataforma.*** FUNDES contrata servicios de plataforma tecnológica (correo, almacenamiento, videoconferencia, herramientas colaborativas y demás) con proveedores cuyas condiciones de servicio imponen obligaciones tanto a la Institución como a los usuarios finales. Todo miembro de la comunidad educativa que utilice los servicios institucionales se obliga a cumplir las condiciones de uso aceptable establecidas por el proveedor, en cuanto sean compatibles con la legislación colombiana y con el presente Estatuto.

Parágrafo 1. La Administración TIC está obligada a identificar y configurar adecuadamente las cuentas de los usuarios menores de dieciocho (18) años en la plataforma, conforme a los requerimientos del proveedor y a la

legislación vigente de protección de datos de menores. Los menores de edad tendrán una experiencia restringida en ciertos servicios de la plataforma (contenido explícito filtrado, acceso limitado a servicios adicionales, restricciones en herramientas de inteligencia artificial y creación de contenido público). La habilitación de servicios adicionales para menores requerirá la verificación del consentimiento parental obtenido por FUNDES, conforme a lo previsto en el artículo 14 del presente Estatuto.

Parágrafo 2. Cuando el proveedor de la plataforma modifique sus Términos de Servicio, políticas de privacidad, restricciones por edad o condiciones de uso de servicios adicionales, la Administración TIC evaluará el impacto de los cambios, informará a la comunidad educativa y adoptará las medidas de cumplimiento necesarias, sin que ello requiera reforma del presente Estatuto.

Parágrafo 3. FUNDES confirmará anualmente ante el proveedor de la plataforma el cumplimiento de las obligaciones relativas al consentimiento parental, la designación de edad de los usuarios y la revisión de acceso a servicios adicionales, conforme al calendario y procedimiento definidos por el proveedor.

Capítulo 8. Buenas prácticas de ciberseguridad para la comunidad educativa

ARTÍCULO 37. ***Recomendaciones de seguridad digital.*** FUNDES promueve las siguientes buenas prácticas de ciberseguridad, las cuales complementan las obligaciones formales establecidas en el presente Estatuto y constituyen un estándar mínimo de conducta responsable para todos los miembros de la comunidad educativa:

En materia de contraseñas y autenticación:

1. Activar la verificación en dos pasos (2FA) en la cuenta institucional. Esta funcionalidad añade una capa adicional de seguridad que impide el acceso a la cuenta incluso si la contraseña es comprometida. La Administración TIC podrá hacerla obligatoria.
2. Utilizar contraseñas de al menos doce (12) caracteres que combinen letras mayúsculas y minúsculas, números y símbolos especiales. Evitar contraseñas basadas en datos personales (fecha de nacimiento, número de documento, nombre de familiares).
3. No reutilizar la misma contraseña en múltiples servicios. Si se necesita gestionar varias contraseñas, utilizar un gestor de contraseñas confiable.
4. Cambiar la contraseña de inmediato si se sospecha que pudo haber sido comprometida, y reportarlo a la Administración TIC.

En materia de equipos y sesiones:

1. No dejar equipos encendidos y logueados al retirarse del puesto de trabajo, del laboratorio o del aula. Utilizar el atajo Windows + L (en Windows) o Ctrl + Comando + Q (en Mac) para bloquear la pantalla rápidamente.
2. Configurar el bloqueo automático de pantalla tras un periodo de inactividad no mayor a cinco (5) minutos.
3. Cerrar todas las sesiones institucionales abiertas en navegadores de equipos compartidos antes de retirarse.

4. No guardar contraseñas en los navegadores de equipos que no sean de uso personal exclusivo. Utilizar siempre la navegación privada (incógnito) al acceder a cuentas institucionales desde equipos compartidos o dispositivos de terceros, incluyendo los equipos de salas de juntas, auditorios, aulas con proyector y cualquier otro equipo de uso colectivo.
5. Al realizar presentaciones en salas de juntas, auditorios o aulas con equipos compartidos, tener presente que al iniciar sesión en una cuenta de Google (por ejemplo, para acceder a un archivo en Drive), todo el ecosistema de servicios queda sincronizado (correo, Drive, Chat, Calendar, Fotos). Se recomienda: (i) abrir una ventana de incógnito para la presentación y cerrarla al terminar; (ii) preferir la opción de compartir el archivo mediante enlace público o restringido, sin necesidad de iniciar sesión en el equipo; (iii) en todo caso, cerrar sesión expresamente de la cuenta de Google al finalizar, verificando que no quede sesión activa en ninguna pestaña; y (iv) nunca aceptar la opción «recordar contraseña» ni «mantener sesión iniciada» en estos equipos.

En materia de dispositivos móviles:

1. Activar el bloqueo de pantalla y el cifrado del dispositivo.
2. En caso de pérdida o hurto del dispositivo móvil, reportar de inmediato a la Administración TIC y utilizar las herramientas de localización y borrado remoto del sistema operativo (Encontrar mi dispositivo en Android, Buscar mi iPhone en iOS).
3. No descargar aplicaciones de fuentes no oficiales (*sideloading*) en dispositivos donde se tenga acceso a cuentas institucionales.
4. Mantener las aplicaciones institucionales actualizadas a la última versión disponible.

En materia de correo electrónico y navegación:

1. Desconfiar de correos que soliciten datos personales, contraseñas o información financiera, incluso si aparentan provenir de FUNDES o de entidades conocidas. Verificar siempre la dirección del remitente.
2. No hacer clic en enlaces sospechosos ni descargar archivos adjuntos de remitentes desconocidos. En caso de duda, reportar el mensaje a la Administración TIC antes de abrirlo.
3. Verificar que las páginas web donde se ingresen credenciales muestren el protocolo seguro (https://) y correspondan al dominio oficial.
4. No almacenar información institucional confidencial en servicios de almacenamiento en la nube personales o no autorizados.

En materia de redes y conectividad:

1. Evitar el acceso a cuentas institucionales desde redes Wi-Fi públicas abiertas (cafeterías, aeropuertos, centros comerciales) sin protección VPN.
2. Desactivar el Bluetooth y la conexión automática a redes Wi-Fi cuando no se estén utilizando.
3. No compartir la conexión a internet del dispositivo móvil (*hotspot*) con personas no autorizadas cuando se esté conectado a la red institucional.

En materia de uso de inteligencia artificial:

1. El uso de herramientas de inteligencia artificial se realizará conforme a la Política de Buen Uso de Inteligencia Artificial (Resolución Rectoral No. 352 de 2025) y sus documentos complementarios.
2. No subir datos personales sensibles, información confidencial institucional, grabaciones de clases, trabajos de estudiantes ni documentos internos de FUNDES a plataformas de IA públicas no autorizadas por la Institución.
3. Declarar el uso de IA en trabajos académicos conforme a la Guía de Citación y Atribución de Contenidos Generados con IA (Documento Complementario III de la Res. 352/2025) y a los formatos institucionales establecidos.
4. Asumir la responsabilidad personal por la exactitud, pertinencia y originalidad del contenido generado o asistido por IA que se presente como propio.
5. Cumplir las medidas de seguridad técnica previstas en el Manual de Seguridad Técnica para Uso de IA (Documento Complementario IV de la Res. 352/2025), incluyendo la gestión de credenciales de acceso a herramientas de IA institucionales.

Parágrafo. Las buenas prácticas contenidas en el presente artículo tienen carácter orientativo y formativo. Su incumplimiento no constituye por sí solo una falta disciplinaria, pero la negligencia reiterada en su observancia que derive en un incidente de seguridad podrá ser valorada como agravante en el proceso disciplinario correspondiente.

TÍTULO V – CIBERSEGURIDAD

ARTÍCULO 38. ***Clasificación de la información.*** FUNDES clasificará sus activos de información en los niveles de: pública (libre acceso), interna (uso institucional), confidencial (acceso restringido a personas autorizadas) y reservada (cuya divulgación puede causar daño grave). Cada custodio es responsable de aplicar la clasificación y los controles de seguridad correspondientes.

Parágrafo. El presente Título establece el marco general de ciberseguridad aplicable a toda la infraestructura tecnológica de FUNDES. Las medidas de seguridad técnica específicas para el uso de herramientas de inteligencia artificial se rigen por el Manual de Seguridad Técnica para Uso de IA (Documento Complementario IV de la Resolución Rectoral No. 352 de 2025), el cual complementa las disposiciones aquí contenidas en lo relativo al entorno de IA.

ARTÍCULO 39. ***Gestión de accesos y credenciales.*** Todo acceso a los sistemas de información de FUNDES requiere autenticación individual. En desarrollo del principio de responsabilidad individual consagrado en el artículo 21 del presente Estatuto y sin perjuicio de las obligaciones allí establecidas, los usuarios observarán las siguientes reglas específicas en materia de seguridad de accesos:

1. Cambiar la contraseña inmediatamente al recibir por primera vez las credenciales de acceso a cualquier sistema o plataforma institucional.
2. Utilizar contraseñas robustas conforme a los parámetros técnicos definidos por la Administración TIC, los cuales podrán incluir requisitos de longitud mínima, combinación de caracteres y periodicidad de renovación.
3. No utilizar la misma contraseña institucional para cuentas personales o servicios externos.

4. No compartir, dictar, prestar, escribir en papel visible, almacenar en archivos de texto sin cifrar ni comunicar sus credenciales por ningún medio, incluyendo correo electrónico, mensajería o llamadas telefónicas. Ningún funcionario, docente o administrador de FUNDES solicitará la contraseña de un usuario; cualquier solicitud en ese sentido debe ser reportada como intento de *phishing*.
5. Cerrar sesión de todas las plataformas institucionales (correo, Q10, LMS, biblioteca digital, Drive) al finalizar su uso. En equipos de laboratorios, salas de cómputo y sala de profesores, esta obligación es imperativa e inmediata.
6. Bloquear la pantalla del equipo de cómputo al ausentarse, incluso por periodos breves, mediante el atajo de teclado correspondiente o la configuración de bloqueo automático.
7. No permitir que otra persona utilice su sesión abierta para realizar acciones en su nombre, ni siquiera con fines aparentemente legítimos o por solicitud de un superior.
8. Utilizar autenticación multifactor cuando la Administración TIC la habilite para servicios críticos.

Parágrafo 1. La Administración TIC implementará el principio de mínimo privilegio: cada usuario recibirá únicamente los permisos estrictamente necesarios para el desempeño de sus funciones. Los permisos de acceso serán revisados periódicamente y revocados de manera inmediata al cambiar las funciones del usuario o al terminar su vinculación con FUNDES.

Parágrafo 2. La Administración TIC podrá configurar el cierre automático de sesiones por inactividad en los sistemas institucionales como medida complementaria de seguridad. Esta medida no exime al usuario de su obligación de cerrar sesión manualmente.

Parágrafo 3. Las credenciales de acceso a herramientas institucionales de inteligencia artificial se rigen por las mismas reglas del presente artículo y, adicionalmente, por las medidas específicas previstas en el Manual de Seguridad Técnica para Uso de IA (Documento Complementario IV de la Resolución Rectoral No. 352 de 2025).

ARTÍCULO 40. ***Protección contra software malicioso.*** La Administración TIC ejecutará regularmente soluciones de antivirus y antimalware en los buzones de correo, servidores y equipos institucionales. La periodicidad se ajustará según el nivel de amenazas. La Institución no se responsabiliza por el bloqueo automático de mensajes infectados o identificados como *spam*.

Parágrafo. Los usuarios de equipos institucionales tienen prohibido: (i) desactivar, desinstalar, modificar o eludir las soluciones de antivirus, antimalware, cortafuegos o cualquier otra herramienta de seguridad instalada por la Administración TIC; (ii) instalar *software*, aplicaciones, extensiones de navegador o complementos en equipos institucionales sin autorización previa de la Administración TIC, con independencia de que el *software* cuente o no con licencia; (iii) modificar la configuración de seguridad, de red o de sistema operativo de los equipos institucionales; y (iv) conectar dispositivos de almacenamiento externo (USB, discos portátiles) a equipos institucionales sin verificación previa de la Administración TIC cuando exista sospecha de contenido malicioso. El incumplimiento de estas prohibiciones constituye falta disciplinaria y, cuando genere un incidente de seguridad, podrá ser valorado como agravante.

ARTÍCULO 41. ***Copias de respaldo.*** FUNDES implementará una estrategia de copias de respaldo para sus sistemas críticos que contemple al menos una copia local y una copia en ubicación diferente, con frecuencia acorde al nivel de

criticidad. Se realizarán pruebas periódicas de restauración. El respaldo de archivos personales es responsabilidad exclusiva del usuario.

ARTÍCULO 42. ***Segmentación de red y monitoreo.*** La red institucional será segmentada lógicamente para separar los entornos académico, administrativo, de dispositivos IoT y de invitados. La Administración TIC podrá monitorear el tráfico de red con fines exclusivos de seguridad, desempeño y cumplimiento normativo, con respeto a los derechos fundamentales de los usuarios.

ARTÍCULO 43. ***Auditoría y monitoreo de herramientas institucionales.*** FUNDES se reserva la potestad de realizar auditorías y revisiones sobre el uso de las herramientas y recursos tecnológicos institucionales —incluyendo correo electrónico, almacenamiento en la nube (Drive), plataformas LMS, CRM, sistemas académicos y demás aplicaciones administradas por la Institución— con las siguientes finalidades:

1. Verificar el cumplimiento del presente Estatuto Digital y de las demás políticas institucionales.
2. Detectar y prevenir incidentes de seguridad, accesos no autorizados y usos indebidos de los recursos.
3. Garantizar la integridad y disponibilidad de los sistemas de información.
4. Cumplir obligaciones legales, contractuales o requerimientos de autoridades competentes.
5. Mejorar la calidad de los servicios tecnológicos institucionales.

Parágrafo 1. Las auditorías digitales se realizarán conforme a los principios de proporcionalidad, necesidad y mínima intervención. Los alcances, la periodicidad y los protocolos de las auditorías serán aprobados por la Rectoría. En ningún caso la auditoría se utilizará como instrumento de vigilancia indiscriminada o persecución.

Parágrafo 2. Los miembros de la comunidad educativa autorizan la realización de estas auditorías al aceptar el presente Estatuto o al suscribir los instrumentos contractuales que contengan la cláusula de autorización de monitoreo y auditoría digital. Los recursos TIC institucionales son de propiedad de FUNDES y su uso constituye un privilegio condicionado al cumplimiento de las políticas internas.

Parágrafo 3. Los resultados de las auditorías serán tratados como información confidencial. Su divulgación se limitará al personal autorizado, a la Rectoría, al Oficial de Protección de Datos y, cuando corresponda, a las autoridades competentes.

ARTÍCULO 44. ***Protección del correo con estándares técnicos.*** La Administración TIC implementará mecanismos técnicos de protección del correo electrónico institucional, tales como protocolos de autenticación de remitentes y filtros de contenido malicioso, conforme a los estándares y mejores prácticas de la industria.

TÍTULO VI – RESPUESTA A INCIDENTES Y GESTIÓN DE BRECHAS

ARTÍCULO 45. ***Deber de reporte.*** Todo miembro de la comunidad educativa que identifique o sospeche de un incidente de seguridad, un uso indebido de recursos TIC o una posible vulneración de datos personales, está obligado a reportarlo de inmediato a la Administración TIC o al Oficial de Protección de Datos, según corresponda.

ARTÍCULO 46. ***Plan de respuesta a incidentes.*** FUNDES mantendrá un plan documentado de respuesta a incidentes de seguridad que comprenderá las fases de: preparación (equipo, roles, herramientas); detección y análisis (tipo, alcance, severidad); contención, erradicación y recuperación; y actividades post-incidente (lecciones aprendidas, actualización de controles, comunicaciones).

ARTÍCULO 47. ***Notificación a la autoridad y a los titulares.*** Cuando un incidente de seguridad afecte datos personales, FUNDES notificará a la autoridad competente en protección de datos dentro de los plazos establecidos por la normativa vigente. Asimismo, informará a los titulares afectados cuando el incidente represente un riesgo significativo para sus derechos, indicando la naturaleza del incidente, los datos comprometidos, las medidas adoptadas y las recomendaciones para mitigar posibles efectos adversos.

ARTÍCULO 48. ***Simulacros y mejora continua.*** La Administración TIC coordinará la realización de al menos un simulacro anual de respuesta a incidentes. Los resultados se documentarán y servirán como insumo para la actualización del plan.

TÍTULO VII – USO RESPONSABLE DE INTELIGENCIA ARTIFICIAL

ARTÍCULO 49. ***Uso de inteligencia artificial.*** El uso de herramientas y sistemas de inteligencia artificial en FUNDES se rige por la Política de Buen Uso de Inteligencia Artificial (Resolución Rectoral No. 352 de 2025) y sus documentos complementarios: el Protocolo Operativo del Comité de Ética en IA (Documento Complementario II), la Guía de Citación y Declaración de IA (Documento Complementario III) y el Manual de Seguridad Técnica para Uso de IA (Documento Complementario IV). Dicha normativa regula de manera integral los principios éticos, la clasificación de usos, las reglas de transparencia y atribución, las prohibiciones específicas y las medidas de seguridad técnica aplicables al uso de IA en el ámbito educativo institucional.

Parágrafo. Las infracciones a la Política de Buen Uso de Inteligencia Artificial constituyen falta disciplinaria conforme al régimen previsto en el presente Estatuto. Cuando la conducta configure adicionalmente fraude académico, plagio o suplantación de identidad, se aplicarán las sanciones del Reglamento Estudiantil o del Reglamento Interno de Trabajo, según corresponda.

TÍTULO VIII – PROPIEDAD INTELECTUAL EN ENTORNO DIGITAL

ARTÍCULO 50. ***Software y licenciamiento.*** Se prohíbe la instalación, distribución o uso de *software* sin la licencia correspondiente o sin la autorización de la Administración TIC en equipos y sistemas de FUNDES. Esta prohibición incluye aplicaciones de escritorio, aplicaciones portátiles (que no requieren instalación), extensiones de navegador y herramientas en línea que almacenen o procesen datos institucionales. La Institución mantendrá un inventario actualizado de licencias y de *software* autorizado conforme a las obligaciones legales aplicables.

ARTÍCULO 51. ***Material protegido por derechos de autor.*** Se prohíbe la reproducción, digitalización o distribución no autorizada de obras protegidas por derechos de autor a través de los recursos TIC de FUNDES. Los usos

amparados por las excepciones legales de reproducción con fines educativos se ejercerán dentro de los límites de la legislación vigente.

ARTÍCULO 52. ***Titularidad de obras creadas en contexto institucional.*** La titularidad de los derechos patrimoniales de las obras creadas en el marco de funciones contractuales se regirá por la legislación vigente y los contratos individuales. Los derechos morales permanecerán siempre en cabeza del autor. Los estudiantes son autores exclusivos de sus trabajos de grado, salvo pacto expreso en contrario. FUNDES podrá solicitar licencias de uso para fines académicos, de investigación o de archivo.

ARTÍCULO 53. ***Contenido generado con asistencia de IA.*** Los productos generados con asistencia de IA no gozan automáticamente de protección por derechos de autor, en la medida en que el derecho colombiano exige aporte creativo humano original. La persona que utilice IA como herramienta deberá realizar una contribución creativa sustancial al producto final.

TÍTULO IX – CONVIVENCIA Y CIUDADANÍA DIGITAL

ARTÍCULO 54. ***Principio de convivencia digital.*** FUNDES promueve una cultura de ciudadanía digital responsable, fundamentada en el respeto mutuo, la integridad, la inclusión, la tolerancia y el uso ético de la tecnología. Todo miembro de la comunidad educativa contribuirá a mantener un entorno digital seguro, respetuoso y propicio para el aprendizaje.

ARTÍCULO 55. ***Prevención del ciberacoso.*** Constituye ciberacoso cualquier conducta reiterada de hostigamiento, intimidación, amenaza, humillación o exclusión ejercida a través de medios electrónicos contra cualquier miembro de la comunidad educativa, sea a través de canales institucionales o externos. FUNDES investigará los reportes y aplicará las medidas disciplinarias y de acompañamiento correspondientes.

ARTÍCULO 56. ***Identidad y huella digital.*** Los usuarios son responsables de la gestión de su identidad digital y de las consecuencias de su huella digital en el entorno académico y profesional. FUNDES fomentará la formación en gestión responsable de la identidad digital como parte de los procesos de inducción.

ARTÍCULO 57. ***Bienestar digital.*** FUNDES promoverá el uso equilibrado y saludable de la tecnología, incorporando en sus programas de bienestar acciones de sensibilización sobre el uso responsable de dispositivos, la gestión del tiempo en entornos digitales, la prevención de conductas adictivas y el respeto al derecho a la desconexión laboral.

TÍTULO X – RÉGIMEN DISCIPLINARIO DIGITAL Y DISPOSICIONES FINALES

Capítulo 1. Clasificación de faltas

ARTÍCULO 58. ***Faltas leves.*** Se consideran faltas leves:

1. El uso ocasional del correo institucional para fines ajenos a la misión de FUNDES, sin causar perjuicio.

2. El incumplimiento de las normas de netiqueta.
3. La omisión del *disclaimer* (descargo de responsabilidad) obligatorio.
4. El descuido en la custodia de credenciales de acceso o el abandono de sesiones abiertas en equipos compartidos, cuando no genere daño efectivo.
5. El uso de canales externos de mensajería para comunicación académica habitual, sin configurar perjuicio a terceros.

ARTÍCULO 59. *Faltas graves.* Se consideran faltas graves:

1. La reincidencia en faltas leves.
2. El préstamo, compartición o divulgación deliberada de credenciales de acceso a terceros, o la utilización de credenciales ajenas.
3. El abandono reiterado de sesiones institucionales abiertas en equipos compartidos que genere riesgo o daño efectivo a la información institucional o de terceros.
4. El uso del correo institucional para fines comerciales personales, proselitistas o de distribución de contenidos prohibidos.
5. La negligencia en el manejo de datos personales que genere riesgo para los titulares.
6. La instalación o uso de *software* sin licencia en equipos institucionales.
7. El uso de IA sin cumplir las reglas de transparencia y atribución.
8. La obstrucción de las auditorías digitales, las investigaciones disciplinarias o los reportes de incidentes.
9. La creación no autorizada de cuentas o grupos en redes sociales utilizando signos distintivos de FUNDES.
10. La divulgación de datos biométricos, de imagen o voz de terceros sin la autorización correspondiente.

ARTÍCULO 60. *Faltas gravísimas.* Se consideran faltas gravísimas:

1. La realización de *hacking*, *phishing*, ataques DDoS u otras conductas tipificadas como delitos informáticos.
2. El acceso no autorizado a datos personales, bases de datos, cuentas o sistemas de información ajenos.
3. La distribución de material pornográfico, ilegal o que promueva la violencia a través de recursos institucionales.
4. La suplantación de identidad, incluyendo la generación de *deepfakes* o contenido sintético engañoso.
5. El fraude académico mediante IA u otros medios tecnológicos.
6. La sustracción, alteración o destrucción dolosa de información institucional.
7. La violación deliberada de las políticas de protección de datos que cause daño a los titulares.
8. La manipulación o adulteración de registros de auditoría digital.

Capítulo 2. Sanciones

ARTÍCULO 61. *Sanciones aplicables.* Las sanciones se aplicarán de manera progresiva y proporcional a la gravedad de la falta, la intencionalidad, la reincidencia y el daño causado:

1. Faltas leves: amonestación escrita y obligación de capacitación sobre uso responsable de TIC.

2. Faltas graves: suspensión temporal del acceso a recursos TIC por uno (1) a seis (6) meses, sin perjuicio de las consecuencias académicas o laborales previstas en los reglamentos.
3. Faltas gravísimas: cancelación definitiva del acceso a recursos TIC, proceso disciplinario conforme al reglamento aplicable, y denuncia ante autoridades competentes cuando la conducta configure delito.

Parágrafo. La aplicación de sanciones se adelantará con pleno respeto del debido proceso, el derecho de defensa y el principio de doble instancia, conforme a los reglamentos institucionales vigentes.

Capítulo 3. Disposiciones finales

ARTÍCULO 62. ***Capacitación y sensibilización.*** FUNDES incluirá en sus programas de inducción y formación continua módulos sobre protección de datos personales, ciberseguridad, uso responsable de TIC, uso ético de la Inteligencia Artificial y manejo de canales institucionales de comunicación. Estos módulos se actualizarán anualmente conforme a la evolución normativa y tecnológica.

ARTÍCULO 63. ***Integración normativa.*** El presente Estatuto Digital se integra al ordenamiento institucional de FUNDES como norma complementaria del Reglamento Estudiantil, el Reglamento Interno de Trabajo, el Manual de Convivencia y los demás instrumentos normativos internos. La Política de Ingreso, Permanencia y Seguridad (Resolución 222-L de 2018) continúa vigente en lo relativo a seguridad física, control de acceso, Tarjeta de Identificación Personal (TIP) y procedimientos de visitantes; el tratamiento de datos personales captados por los sistemas de videovigilancia y de control de ingreso se regirá por lo dispuesto en el presente Estatuto. La aceptación expresa del presente Estatuto será requisito para la matrícula, la vinculación laboral y la suscripción de contratos que impliquen acceso a recursos TIC o tratamiento de datos personales.

ARTÍCULO 64. ***Articulación con cláusulas contractuales.*** Los contratos de trabajo y de prestación de servicios vigentes al momento de la expedición del presente Estatuto se entenderán complementados por éste en todo lo relativo al uso de recursos TIC, protección de datos personales, auditoría digital y uso de inteligencia artificial. Para los nuevos contratos, FUNDES incorporará cláusulas de autorización integral conforme a lo dispuesto en el artículo 20 del presente Estatuto, incluyendo las autorizaciones específicas diferenciadas para: datos personales y de contacto; datos biométricos; imagen y voz; monitoreo y auditoría digital; tratamiento de datos para sistemas de IA; consulta de antecedentes; y datos de salud.

ARTÍCULO 65. ***Revisión y actualización.*** La Rectoría, con el apoyo de la Administración TIC y del Oficial de Protección de Datos, realizará una revisión integral del presente Estatuto al menos una vez al año, o cuando cambios normativos, tecnológicos o institucionales lo hagan necesario. El Rector podrá expedir circulares reglamentarias para la operativización de las disposiciones del presente Estatuto, sin alterar su contenido sustancial.

ARTÍCULO 66. ***Vigencia y derogatoria.*** El presente Estatuto Digital rige a partir de la fecha de su publicación y comunicación, y deroga integralmente la Resolución Rectoral No. 165 del 13 de febrero de 2014 (por la cual se establecieron disposiciones para el uso del correo electrónico institucional, el acceso a internet y normas sobre protección de datos personales), cuyo contenido ha sido integrado, actualizado y ampliado en el presente instrumento normativo. Igualmente, se derogan todas las demás disposiciones internas, circulares, memorandos y actos administrativos que resulten contrarios al presente Estatuto.

Parágrafo. Las autorizaciones de tratamiento de datos personales válidamente otorgadas con anterioridad a la expedición del presente Estatuto mantienen su vigencia para las finalidades originalmente informadas, de conformidad con el artículo 10 del Decreto 1377 de 2013 (compilado en el DUR 1074 de 2015) y el artículo 12, parágrafo 2, del presente Estatuto. FUNDES dispondrá de un plazo de seis (6) meses contados a partir de la publicación del presente Estatuto para adecuar la totalidad de sus instrumentos contractuales, formularios de matrícula y formatos de autorización a las disposiciones aquí contenidas.