MANUAL DEL SISTEMA DE SEGURIDAD Y GESTIÓN DEL RIESGO DE DATOS PERSONALES Y BASES DE DATOS

1. PRESENTACIÓN

La CORPORACIÓN UNIVERSITARIA U DE COLOMBIA, en adelante la CORPORACIÓN o U DE COLOMBIA, reconoce la protección de los datos personales como un derecho fundamental de las personas y como un componente esencial de la gestión institucional.

En desarrollo de la Política de Tratamiento de Datos Personales y Manejo de Información Biométrica adoptada mediante el Acuerdo CS-155 de 2026, se establece el presente Manual del Sistema de Seguridad y Gestión del Riesgo de Datos Personales y Bases de Datos, como instrumento operativo para prevenir, identificar, gestionar y mitigar los riesgos asociados al tratamiento de información personal.

El presente Manual sustituye la versión 1 del M-PDP 001 de septiembre de 2018 y desarrolla los procedimientos y controles institucionales requeridos para garantizar la seguridad, confidencialidad, integridad, disponibilidad, trazabilidad y tratamiento adecuado de los datos personales.

La elaboración de este Manual responde igualmente a la obligación del responsable del tratamiento de adoptar políticas, procedimientos y mecanismos internos que permitan demostrar el cumplimiento de las obligaciones derivadas del régimen de protección de datos personales.

2. OBJETO

Establecer los lineamientos, responsabilidades, procedimientos y controles administrativos, físicos, técnicos, tecnológicos y humanos que deberá aplicar la CORPORACIÓN para garantizar la adecuada protección de los datos personales y de las bases de datos bajo su responsabilidad o custodia.

El Manual tiene como objetivos específicos:

a) Prevenir accesos, usos, consultas, modificaciones, pérdidas, alteraciones o divulgaciones no autorizadas.
b) Establecer mecanismos para gestionar los riesgos relacionados con el tratamiento de datos personales.
c) Garantizar el ejercicio de los derechos de los titulares.
d) Regular la gestión de autorizaciones, consultas, reclamos e incidentes.
e) Establecer controles especiales para datos sensibles, biométricos y datos de niños, niñas y adolescentes.
f) Regular el tratamiento mediante videovigilancia, aplicaciones, cookies y tecnologías de seguimiento.
g) Establecer controles sobre proveedores y encargados del tratamiento.
h) Regular las transferencias y transmisiones nacionales e internacionales de datos.
i) Establecer reglas de conservación, archivo, supresión y anonimización.
j) Generar evidencia suficiente para demostrar el cumplimiento institucional del régimen de protección de datos personales.

3. ALCANCE

El presente Manual es de obligatorio cumplimiento para todos los procesos, dependencias, órganos, empleados, profesores, contratistas, proveedores, estudiantes, practicantes y demás personas que, en desarrollo de sus funciones o relaciones con la CORPORACIÓN, intervengan en cualquier operación de tratamiento de datos personales.

Se aplica a toda información contenida en medios físicos, digitales, tecnológicos, audiovisuales o biométricos, independientemente del sistema, aplicación, plataforma, dispositivo o medio utilizado para su tratamiento.

El Manual comprende, entre otras, las siguientes categorías de información:

a) Información de aspirantes.
b) Información de estudiantes.
c) Información académica.
d) Información de egresados.
e) Información de profesores.
f) Información de empleados y colaboradores.
g) Información de contratistas y proveedores.

h) Información de visitantes y acompañantes.
i) Información de bienestar institucional.
j) Información relacionada con procesos disciplinarios.
k) Información financiera, crediticia y de cartera, cuando corresponda.
l) Información de salud o cualquier otra información sensible sometida a tratamiento institucional.
m) Información biométrica.
n) Imágenes obtenidas mediante sistemas de videovigilancia.
o) Fotografías y registros audiovisuales.
p) Información obtenida mediante páginas web, aplicaciones móviles, formularios y sistemas tecnológicos.
q) Información contenida en archivos documentales y digitales.

4. MARCO NORMATIVO

El Sistema se desarrollará de conformidad con:

- Constitución Política de Colombia, especialmente los artículos 15 y 20.
- Ley 1581 de 2012.
- Ley 1266 de 2008, cuando resulte aplicable.
- Ley 1098 de 2006, en materia de protección de niños, niñas y adolescentes.
- Ley 594 de 2000, Ley General de Archivos.
- Decreto 1074 de 2015 y sus modificaciones.
- Decreto 1075 de 2015, en lo relacionado con la prestación del servicio de educación superior y las obligaciones institucionales aplicables.
- Decreto 1330 de 2019 y las normas que lo modifiquen, adicionen o sustituyan.
- Instrucciones, circulares, conceptos y guías expedidos por la Superintendencia de Industria y Comercio.
- Demás disposiciones legales, reglamentarias y jurisprudenciales aplicables.
- Acuerdo CS-155 de 2026, por medio del cual la CORPORACIÓN actualizó y adoptó su Política de Tratamiento de Datos Personales y Manejo de Información Biométrica.

La normativa señalada deberá entenderse en su versión vigente y cualquier modificación, adición o sustitución será incorporada al Sistema cuando resulte aplicable.

5. PRINCIPIOS DEL SISTEMA

Todas las actividades de tratamiento deberán observar los siguientes principios:

5.1. Legalidad. El tratamiento deberá desarrollarse conforme a la Constitución, la ley y demás disposiciones aplicables.

5.2. Finalidad. Los datos solo podrán ser tratados para finalidades legítimas, específicas y previamente informadas al titular.

5.3. Libertad. El tratamiento requerirá autorización previa, expresa e informada del titular, salvo las excepciones legales.

5.4. Veracidad o calidad. La información deberá ser veraz, completa, exacta, actualizada, comprobable y comprensible.

5.5. Transparencia. El titular tendrá derecho a conocer la existencia de información que le concierna y el tratamiento realizado sobre ella.

5.6. Acceso y circulación restringida. El acceso a los datos deberá limitarse a las personas autorizadas y a las finalidades legalmente permitidas.

5.7. Seguridad. La CORPORACIÓN implementará las medidas técnicas, administrativas, humanas y físicas necesarias para evitar pérdida, adulteración, acceso o tratamiento no autorizado.

5.8. Confidencialidad. Toda persona que intervenga en el tratamiento deberá mantener la reserva y confidencialidad de la información.

5.9. Temporalidad. Los datos serán conservados únicamente durante el tiempo necesario para cumplir la finalidad o durante el plazo establecido por una obligación legal o institucional.

6. PRINCIPIO DE RESPONSABILIDAD DEMOSTRADA

La CORPORACIÓN adoptará un enfoque preventivo y documentado orientado a demostrar el cumplimiento efectivo de la normativa de protección de datos.

Para tal efecto deberá conservar evidencia, entre otros aspectos, de:

a) Políticas y procedimientos vigentes.
b) Inventario de bases de datos y tratamientos.
c) Autorizaciones de los titulares.
d) Avisos de privacidad.
e) Contratos con encargados del tratamiento.
f) Acuerdos de confidencialidad.
g) Gestión de consultas y reclamos.
h) Gestión de incidentes.
i) Análisis de riesgos.
j) Análisis de impacto a la privacidad, cuando corresponda.
k) Capacitación del personal.
l) Actualización del RNBD, cuando legal o institucionalmente corresponda.
m) Procesos de supresión y anonimización.
n) Controles de acceso y seguridad.
o) Auditorías, revisiones y acciones de mejora.

La documentación deberá permitir acreditar qué medidas fueron adoptadas, quién fue responsable, cuándo fueron implementadas y cuál fue su resultado.

7. ESTRUCTURA DE RESPONSABILIDADES

7.1. Representante Legal. Corresponde al Representante Legal:

a) Velar por el cumplimiento institucional de la política.
b) Adoptar las decisiones administrativas necesarias para la protección de los datos.
c) Designar al Oficial de Protección de Datos Personales.
d) Conocer los informes de cumplimiento.
e) Impulsar las medidas correctivas y preventivas que resulten necesarias.
f) Ejercer las demás funciones previstas en la Política y en la legislación.

7.2. Oficial de Protección de Datos Personales – DPO. El DPO será designado por acto administrativo del Representante Legal.

Le corresponderá:

a) Coordinar la implementación de la Política y del presente Manual.
b) Verificar su actualización.
c) Coordinar la atención de consultas y reclamos.
d) Servir de enlace con la SIC.
e) Verificar el cumplimiento del RNBD cuando corresponda.
f) Coordinar el tratamiento especial de datos sensibles y biométricos.
g) Participar en la valoración de riesgos y análisis de impacto.
h) Realizar seguimiento a incidentes de seguridad.
i) Presentar informes periódicos al Representante Legal.
j) Promover actividades de capacitación y sensibilización.
k) Recomendar acciones correctivas y preventivas.
l) Mantener actualizado el sistema documental de protección de datos.

7.3. Oficina o área de Sistemas. Deberá implementar y mantener las medidas técnicas y tecnológicas necesarias para la seguridad de la información y apoyar la gestión de incidentes, accesos, respaldos, recuperación y protección de los sistemas.

7.4. Secretaría General. Apoyará la aplicación institucional de la Política, especialmente en lo relacionado con actos administrativos, procedimientos de atención de titulares, requerimientos de autoridades y gestión documental.

7.5. Líderes de procesos. Cada responsable de proceso deberá identificar las bases de datos utilizadas, las finalidades del tratamiento, los usuarios autorizados y los riesgos asociados.

7.6. Empleados y profesores. Deberán:

a) Utilizar la información exclusivamente para el cumplimiento de sus funciones.
b) Mantener la reserva.
c) Proteger credenciales y mecanismos de acceso.
d) Evitar la extracción o almacenamiento no autorizado.
e) Reportar inmediatamente cualquier incidente.
f) Cumplir las instrucciones del responsable y del DPO.

7.7. Contratistas y proveedores. Deberán cumplir la Política, el presente Manual, las obligaciones contractuales y las disposiciones legales aplicables cuando tengan acceso o traten datos personales por cuenta de la CORPORACIÓN.

8. INVENTARIO DE BASES DE DATOS Y ACTIVIDADES DE TRATAMIENTO

La CORPORACIÓN deberá mantener un inventario actualizado de sus bases de datos y actividades de tratamiento.

Para cada base deberá identificarse, como mínimo:

a) Nombre.
b) Proceso responsable.
c) Finalidad.
d) Tipo de titulares.
e) Categorías de datos.
f) Existencia de datos sensibles.
g) Existencia de datos biométricos.
h) Existencia de datos de menores.
i) Medio de almacenamiento.
j) Ubicación.
k) Personas con acceso.
l) Encargados.
m) Transferencias o transmisiones.
n) Plazo de conservación.
o) Medidas de seguridad.
p) Registro ante RNBD, cuando corresponda.

El inventario deberá revisarse al menos una vez al año y cada vez que exista un cambio sustancial en el tratamiento.

9. AUTORIZACIÓN DEL TITULAR

Antes de recolectar datos personales, la CORPORACIÓN deberá informar al titular y obtener la autorización cuando esta sea legalmente exigible.

La autorización deberá identificar claramente:

a) El responsable.
b) La finalidad.

c) Los datos objeto de tratamiento.
d) Los derechos del titular.
e) Los mecanismos para ejercerlos.
f) Los canales institucionales.
g) La posibilidad de tratamiento por encargados, cuando corresponda.

La autorización podrá constar en medios físicos o electrónicos y deberá conservarse de forma que pueda ser consultada y acreditada posteriormente.

10. DATOS SENSIBLES

El tratamiento de datos sensibles se realizará únicamente cuando exista una habilitación legal suficiente.

Cuando se requiera autorización, esta deberá ser expresa, previa e informada.

La CORPORACIÓN aplicará medidas reforzadas de seguridad a este tipo de información y restringirá su acceso al personal que estrictamente lo requiera.

Se consideran, entre otros, datos sensibles aquellos relacionados con salud, datos biométricos, vida sexual, convicciones religiosas o filosóficas, pertenencia sindical y demás categorías legalmente definidas.

11. DATOS BIOMÉTRICOS

Los datos biométricos serán tratados únicamente para finalidades previamente definidas y autorizadas, de acuerdo con la Política institucional.

Antes de iniciar el tratamiento deberá:

a) Informarse al titular que se trata de información sensible.
b) Informarse la finalidad específica.
c) Informarse el carácter facultativo del suministro cuando corresponda.
d) Definirse un mecanismo alterno cuando la persona se niegue al tratamiento biométrico.
e) Restringirse el acceso al personal autorizado.
f) Implementarse mecanismos de seguridad apropiados.
g) Mantener separación entre la identificación del titular y las plantillas o vectores biométricos cuando técnicamente sea posible.
h) Aplicarse cifrado en reposo y tránsito cuando corresponda.
i) Impedir el uso de la información biométrica para finalidades diferentes.

j) Elaborarse y conservarse el análisis de impacto a la privacidad cuando sea requerido.

El análisis de impacto deberá considerar necesidad, proporcionalidad, riesgos para los titulares, alternativas menos invasivas y medidas de mitigación.

12. PRIVACIDAD DESDE EL DISEÑO Y POR DEFECTO

Todo proyecto, aplicación, plataforma, servicio, sistema o proceso nuevo que implique tratamiento de datos personales deberá incorporar criterios de protección de datos desde su fase de diseño.

Antes de su implementación deberá evaluarse, según su nivel de riesgo:

a) Qué datos serán recolectados.
b) Por qué son necesarios.
c) Qué finalidad tendrán.
d) Quién tendrá acceso.
e) Cuánto tiempo serán conservados.
f) Con quién serán compartidos.
g) Si existirán transferencias o transmisiones internacionales.
h) Si se utilizarán datos sensibles o biométricos.
i) Qué riesgos podrían presentarse.
j) Qué medidas de seguridad serán implementadas.

El DPO deberá ser consultado cuando el tratamiento pueda generar riesgos relevantes para los derechos de los titulares.

13. TRATAMIENTO DE DATOS DE NIÑOS, NIÑAS Y ADOLESCENTES

Cuando la CORPORACIÓN trate datos de niños, niñas y adolescentes deberá observar el interés superior del menor y las disposiciones especiales aplicables.

Se deberá evaluar:

a) La necesidad del tratamiento.
b) La finalidad.
c) La proporcionalidad.
d) La naturaleza de la información.
e) La participación del representante legal cuando corresponda.
f) El derecho del menor a ser escuchado conforme a su edad, madurez y autonomía.

El tratamiento de datos sensibles o biométricos de adolescentes deberá estar sometido a las condiciones especiales previstas en la Política institucional y en la legislación aplicable.

14. VIDEOVIGILANCIA

La utilización de sistemas de videovigilancia constituye tratamiento de datos personales.

Las zonas vigiladas deberán contar con avisos visibles y permanentes que informen:

a) La existencia del sistema.
b) La finalidad.
c) La identificación del responsable.
d) El canal para ejercer los derechos del titular.

El acceso a las grabaciones deberá estar restringido al personal autorizado.

Las imágenes serán utilizadas únicamente para las finalidades institucionales autorizadas.

Como regla general, las imágenes se conservarán por el plazo establecido en la Política institucional, sin perjuicio de su conservación cuando constituyan evidencia para investigaciones administrativas, disciplinarias o procesos judiciales.

Cuando una grabación sea objeto de una solicitud de conservación por una investigación o proceso, deberá aplicarse una medida de preservación que impida su eliminación durante el tiempo necesario.

15. FOTOGRAFÍAS Y REGISTROS AUDIOVISUALES

Los registros fotográficos, audiovisuales o de imagen realizados en eventos institucionales deberán contar con la autorización que corresponda.

La utilización de la imagen deberá respetar:

a) La finalidad informada.
b) La autorización otorgada.
c) Los derechos del titular.
d) Los derechos de autor y demás derechos asociados.

No podrá publicarse material cuyo uso no haya sido autorizado cuando dicha autorización sea exigible.

16. COOKIES Y TECNOLOGÍAS DE SEGUIMIENTO

Las páginas web y aplicaciones institucionales podrán utilizar cookies y tecnologías similares con finalidades funcionales, analíticas o de personalización.

Para las cookies no esenciales deberá obtenerse consentimiento previo mediante mecanismos claros y verificables.

La CORPORACIÓN deberá contar con una Política de Cookies que indique:

a) Tipo de cookie.
b) Finalidad.
c) Duración.
d) Terceros involucrados.
e) Mecanismos para aceptar, administrar o rechazar su utilización.

17. CONTROL DE ACCESO A LA INFORMACIÓN

El acceso a las bases de datos se asignará según las funciones y necesidades de cada usuario.

Se deberán implementar:

a) Usuarios individuales.
b) Contraseñas seguras.
c) Control de privilegios.
d) Restricción por roles.
e) Desactivación o modificación de accesos cuando termine o cambie una relación laboral o contractual.
f) Registro de accesos cuando técnicamente sea posible.
g) Prohibición de compartir credenciales.
h) Revisión periódica de permisos.

Las cuentas de usuarios desvinculados deberán ser desactivadas oportunamente.

18. SEGURIDAD FÍSICA

Los archivos físicos que contengan datos personales deberán mantenerse en lugares con condiciones adecuadas de seguridad.

Se deberán implementar, de acuerdo con el nivel de riesgo:

a) Control de acceso físico.
b) Mecanismos de custodia.
c) Protección contra pérdida, daño o sustracción.
d) Organización documental.
e) Restricción de acceso a archivos sensibles.
f) Destrucción segura de documentos cuando proceda.

No deberán dejarse documentos con información personal en lugares de acceso público o sin control.

19. SEGURIDAD DIGITAL Y TECNOLÓGICA

La CORPORACIÓN deberá implementar medidas de seguridad acordes con el riesgo, incluyendo cuando corresponda:

a) Copias de seguridad.
b) Sistemas de autenticación.
c) Control de acceso.
d) Cifrado.
e) Protección frente a malware.
f) Actualización de sistemas.
g) Gestión de vulnerabilidades.
h) Registro de eventos.
i) Recuperación ante fallas.
j) Protección de dispositivos institucionales.
k) Gestión de usuarios privilegiados.
l) Eliminación segura de información.

Los datos personales no deberán almacenarse en dispositivos, servicios o medios no autorizados por la CORPORACIÓN.

20. TRABAJO REMOTO Y USO DE DISPOSITIVOS

Cuando un empleado, profesor o contratista trate datos personales fuera de las instalaciones institucionales deberá:

a) Utilizar los medios autorizados.
b) Evitar redes inseguras cuando ello represente un riesgo.
c) Mantener protegidos los dispositivos.
d) No permitir acceso de terceros.

e) Evitar el almacenamiento local innecesario.
f) Reportar pérdida, robo o acceso no autorizado.
g) Cumplir las medidas de seguridad establecidas por la CORPORACIÓN.

21. GESTIÓN DE INCIDENTES DE SEGURIDAD

Se considera incidente, entre otros, cualquier evento que produzca o pueda producir:

a) Pérdida.
b) Sustracción.
c) Acceso no autorizado.
d) Divulgación no autorizada.
e) Alteración.
f) Destrucción.
g) Exposición.
h) Uso indebido.
i) Interrupción o indisponibilidad de información personal.
j) Toda persona que tenga conocimiento de un incidente deberá reportarlo inmediatamente al responsable del proceso y al DPO o al canal institucional definido.
k) El reporte deberá incluir, cuando sea posible:
l) Fecha y hora.
m) Persona que reporta.
n) Sistema o base de datos afectada.
o) Descripción del incidente.
p) Información comprometida.
q) Titulares potencialmente afectados.
r) Medidas adoptadas.
s) Evidencias disponibles.

22. PROCEDIMIENTO DE ATENCIÓN DE INCIDENTES

El tratamiento de un incidente comprenderá las siguientes etapas:

22.1. Detección. Identificación del evento.

22.2. Registro. Documentación formal del incidente.

22.3. Contención. Implementación de medidas inmediatas para evitar su propagación.

22.4. Evaluación. Determinación de la naturaleza, alcance y nivel de riesgo.

22.5. Mitigación. Aplicación de medidas para reducir el impacto.

22.6. Recuperación. Restablecimiento de la operación y seguridad.

22.7. Reporte. Cuando corresponda, se efectuará el reporte ante la Superintendencia de Industria y Comercio dentro del término legal aplicable.

22.8. Cierre. Se documentará la causa, las medidas adoptadas, las responsabilidades determinadas y las acciones de mejora.

23. CONSERVACIÓN DE EVIDENCIAS DE INCIDENTES

Las evidencias relacionadas con incidentes deberán conservarse de forma segura para garantizar:

a) Integridad.
b) Autenticidad.
c) Trazabilidad.
d) Disponibilidad.
e) Confidencialidad.

Cuando las evidencias sean relevantes para investigaciones disciplinarias, judiciales o administrativas, se conservarán durante el tiempo requerido.

24. CONSULTAS DE LOS TITULARES

Las consultas podrán presentarse por los siguientes canales institucionales:

Correo electrónico: comunicaciones@udecolombia.edu.co Canal físico: Calle 56 # 41-147, Medellín, Antioquia. Canal web: mesa de ayuda.

El solicitante deberá acreditar su identidad o legitimación cuando corresponda.

Las consultas deberán atenderse dentro de los diez (10) días hábiles siguientes a su recepción.

Cuando no sea posible responder dentro de dicho término, se informará al titular antes de su vencimiento la razón de la demora y la fecha de respuesta, sin que esta pueda superar cinco (5) días hábiles adicionales.

La respuesta deberá corresponder a la información efectivamente existente y bajo custodia institucional.

25. RECLAMOS DE ACTUALIZACIÓN, RECTIFICACIÓN O SUPRESIÓN

Los titulares, sus representantes o causahabientes podrán presentar reclamos cuando consideren que la información:

a. Es incorrecta.
b. Está incompleta.
c. Debe ser actualizada.
d. Está siendo utilizada para una finalidad no autorizada.
e. Debe ser suprimida cuando jurídicamente proceda.
f. El reclamo deberá contener:
g. Identificación del titular.
h. Descripción de los hechos.
i. Petición concreta.
j. Documentos o pruebas disponibles.
k. Datos de contacto.

Cuando el receptor no sea competente, deberá trasladar el reclamo al área competente e informar al interesado.

Una vez recibido el reclamo completo, deberá registrarse la expresión **“reclamo en trámite”** y el motivo correspondiente.

La respuesta se emitirá dentro de los quince (15) días hábiles siguientes a la recepción del reclamo.

Cuando exista imposibilidad de responder dentro de dicho término, se informarán los motivos de la demora y la fecha de respuesta, que no podrá superar ocho (8) días hábiles adicionales.

26. SUBSANACIÓN

Cuando el reclamo esté incompleto, confuso o resulte insuficiente para su trámite, se solicitará al interesado que lo complete dentro del plazo institucional aplicable.

Cuando transcurra el término legal sin que se atienda el requerimiento de subsanación, se aplicarán las consecuencias jurídicas previstas en la normativa.

27. REGISTRO Y TRAZABILIDAD DE SOLICITUDES

La CORPORACIÓN conservará registro de:

a) Fecha de recepción.
b) Identificación del solicitante.
c) Tipo de solicitud.
d) Área responsable.
e) Fecha de traslado.
f) Fecha de respuesta.
g) Contenido de la respuesta.
h) Evidencia de envío.
i) Actuaciones adicionales.

Este registro deberá permitir verificar el cumplimiento de los términos legales.

28. SUMINISTRO DE INFORMACIÓN A TERCEROS

La información personal solo podrá suministrarse cuando exista fundamento legal o autorización del titular.

Podrá suministrarse, según corresponda:

a) Al titular.
b) A sus causahabientes.
c) A sus representantes legales.
d) A entidades públicas o administrativas en ejercicio de sus funciones legales.
e) Por orden judicial.
f) A terceros expresamente autorizados.

Las solicitudes deberán someterse a verificación previa de identidad, legitimación, competencia y fundamento jurídico.

29. SOLICITUDES DE AUTORIDADES

Las solicitudes formuladas por autoridades deberán ser recibidas, registradas y remitidas al área competente.

La CORPORACIÓN deberá verificar:

a) Identidad de la autoridad.
b) Competencia.
c) Fundamento jurídico.
d) Alcance de la solicitud.
e) Información requerida.

Solo se suministrará la información estrictamente necesaria y permitida. Las respuestas deberán conservarse como soporte de cumplimiento.

30. ENCARGADOS DEL TRATAMIENTO

Todo tercero que trate datos personales por cuenta de la CORPORACIÓN deberá ser identificado como encargado cuando jurídicamente corresponda.

Antes de contratar o autorizar el acceso a información deberán evaluarse:

a) Necesidad del acceso.
b) Finalidad.
c) Categorías de datos.
d) Medidas de seguridad.
e) Confidencialidad.
f) Gestión de incidentes.
g) Conservación.
h) Supresión o devolución.
i) Transferencias o transmisiones.
j) Subcontratación, cuando aplique.

31. CONTRATOS CON ENCARGADOS

Los contratos con encargados deberán establecer, según corresponda:

a) Objeto y alcance del tratamiento.
b) Finalidad.
c) Categorías de datos.
d) Obligaciones del encargado.
e) Medidas de seguridad.
f) Confidencialidad.
g) Gestión de incidentes.
h) Atención de consultas y reclamos.
i) Restricción de subcontratación.
j) Prohibición de utilizar la información para finalidades distintas.
k) Reglas de devolución, supresión o destrucción.
l) Condiciones de transferencia y transmisión.
m) Auditoría o verificación de cumplimiento cuando corresponda.

32. CONFIDENCIALIDAD

Las personas que tengan acceso a datos personales deberán suscribir los instrumentos de confidencialidad definidos por la CORPORACIÓN cuando corresponda.

La obligación de reserva continuará aun después de terminado el vínculo laboral, contractual o institucional, mientras subsista la obligación legal o institucional de confidencialidad.

33. TRANSFERENCIAS Y TRANSMISIONES INTERNACIONALES

Toda transferencia o transmisión internacional deberá ser previamente identificada y evaluada.

La CORPORACIÓN verificará:

a) País de destino.
b) Calidad del receptor.
c) Finalidad.
d) Base jurídica.
e) Nivel de protección aplicable.
f) Existencia de autorización.

g) Contrato de transmisión cuando corresponda.
h) Medidas de seguridad.
i) Condiciones de conservación y devolución.

Las transmisiones internacionales a encargados deberán sujetarse al régimen establecido en el Decreto 1074 de 2015 y demás normas vigentes.

Cuando intervengan servicios en la nube, plataformas SaaS o sistemas administrados desde el exterior, deberán identificarse expresamente las condiciones de tratamiento internacional.

34. INFORMACIÓN EN SERVICIOS DE NUBE Y PLATAFORMAS TECNOLÓGICAS

Antes de contratar o implementar servicios en la nube que involucren datos personales, la CORPORACIÓN deberá evaluar:

a) Ubicación del proveedor.
b) Ubicación de los datos.
c) Tratamiento efectuado.
d) Subencargados.
e) Medidas de seguridad.
f) Cifrado.
g) Respaldos.
h) Procedimiento de eliminación.
i) Retorno o recuperación de la información.
j) Transferencias internacionales.
k) Gestión de incidentes.

La decisión deberá documentarse cuando el nivel de riesgo lo amerite.

35. CONSERVACIÓN Y RETENCIÓN

La información será conservada durante el tiempo necesario para cumplir la finalidad y las obligaciones legales o institucionales aplicables.

La CORPORACIÓN aplicará las Tablas de Retención Documental y las reglas especiales establecidas en la Política CS-155.

Cuando exista una obligación legal de conservación superior, esta prevalecerá sobre cualquier plazo administrativo interno.

36. PLAZOS INSTITUCIONALES DE REFERENCIA

Conforme al Acuerdo CS-155, se aplicarán, entre otros, los siguientes criterios:

a) Datos académicos de estudiantes: conforme a las Tablas de Retención Documental y la normativa aplicable.
b) Datos laborales y de talento humano: diez (10) años contados desde la terminación del vínculo, sin perjuicio de otras obligaciones legales.
c) Datos biométricos: durante la vigencia del vínculo y hasta seis (6) meses después de su terminación, salvo las excepciones previstas.
d) Imágenes de videovigilancia: hasta noventa (90) días calendario, salvo conservación por razones probatorias.
e) Datos de proveedores y contratistas: diez (10) años desde la terminación contractual, sin perjuicio de obligaciones superiores.
f) Datos de aspirantes no admitidos o no vinculados: un (1) año desde la decisión correspondiente, salvo autorización o deber legal de conservación.

37. SUPRESIÓN Y ANONIMIZACIÓN

Cuando concluya la finalidad y no exista obligación legal de conservación, deberá evaluarse la supresión o anonimización.

La supresión deberá realizarse mediante mecanismos que impidan la recuperación no autorizada de la información.

Cuando los datos sean conservados para fines estadísticos, históricos o científicos, deberán aplicarse medidas de anonimización cuando resulte procedente.

La supresión o anonimización deberá dejar evidencia de:

a) Base de datos.
b) Fecha.
c) Responsable.
d) Tipo de información.
e) Método utilizado.
f) Justificación.

38. GESTIÓN DOCUMENTAL

Los documentos que contengan datos personales deberán administrarse conforme a las Tablas de Retención Documental y los procedimientos de archivo institucional.

La clasificación documental deberá considerar el nivel de sensibilidad de la información.

Los documentos físicos que deban destruirse deberán ser eliminados mediante mecanismos seguros.

Los documentos digitales deberán eliminarse de acuerdo con procedimientos técnicos que reduzcan el riesgo de recuperación no autorizada.

39. RNBD

La CORPORACIÓN atenderá las obligaciones relacionadas con el Registro Nacional de Bases de Datos de conformidad con la normativa vigente y con sus obligaciones institucionales.

El responsable del seguimiento deberá mantener actualizada la información correspondiente cuando legalmente proceda.

La información deberá revisarse como mínimo:

a) En las actualizaciones obligatorias.
b) Cuando se creen nuevas bases sujetas a registro.
c) Cuando se produzcan cambios sustanciales.
d) Cuando cambien las finalidades.
e) Cuando se modifiquen medidas de seguridad relevantes.
f) Cuando cambien las condiciones de transferencia internacional.

40. DERECHOS DE LOS TITULARES

La CORPORACIÓN garantizará, entre otros, los siguientes derechos:

a) Conocer, actualizar y rectificar los datos.
b) Solicitar prueba de la autorización, cuando sea exigible.
c) Ser informado sobre el uso dado a la información.
d) Presentar quejas ante la autoridad competente.
e) Solicitar la revocatoria de la autorización cuando jurídicamente proceda.
f) Solicitar la supresión en los casos legalmente procedentes.

g) Acceder gratuitamente a los datos personales objeto de tratamiento en los términos de la ley.
h) Ejercer los derechos relacionados con información financiera, crediticia, comercial o de servicios cuando corresponda.

41. TRATAMIENTO DE INFORMACIÓN ACADÉMICA

La información académica de los estudiantes deberá utilizarse exclusivamente para las finalidades institucionales autorizadas o legalmente habilitadas.

Comprende, entre otra:

a) Matrícula.
b) Historia académica.
c) Calificaciones.
d) Asistencia.
e) Procesos de grado.
f) Seguimiento académico.
g) Acompañamiento estudiantil.
h) Permanencia y prevención de la deserción.
i) Bienestar.
j) Reportes ante autoridades.

El acceso deberá restringirse a las personas que lo requieran para el cumplimiento de sus funciones.

42. INFORMACIÓN DE BIENESTAR Y ACOMPAÑAMIENTO

La información obtenida en actividades de bienestar, acompañamiento psicológico, orientación o apoyo institucional deberá recibir especial protección cuando contenga datos sensibles.

Su acceso estará limitado al personal autorizado y se utilizará exclusivamente para las finalidades correspondientes.

Los informes institucionales deberán priorizar, cuando sea posible, información estadística o anonimizada.

43. INFORMACIÓN DE TALENTO HUMANO

La información de empleados y profesores deberá utilizarse para las finalidades relacionadas con:

a) Selección.
b) Vinculación.
c) Nómina.
d) Seguridad social.
e) Evaluación.
f) Capacitación.
g) Gestión administrativa.
h) Obligaciones legales.
i) Seguridad y bienestar.

El acceso deberá limitarse a las dependencias y funcionarios autorizados.

44. DATOS FINANCIEROS, DE CARTERA Y CREDITICIOS

Cuando la CORPORACIÓN trate información financiera, crediticia, comercial o de servicios deberá observar adicionalmente las disposiciones aplicables de la Ley 1266 de 2008 y demás normas vigentes.

Los datos deberán utilizarse exclusivamente para finalidades relacionadas con la gestión autorizada.

45. COMUNICACIONES INSTITUCIONALES

Los datos de contacto podrán utilizarse para el envío de información institucional cuando ello corresponda a las finalidades autorizadas o legalmente habilitadas.

Las comunicaciones deberán respetar los principios de finalidad, transparencia y seguridad.

Los destinatarios deberán disponer de mecanismos adecuados para ejercer sus derechos frente al tratamiento.

46. CAPACITACIÓN Y SENSIBILIZACIÓN

La CORPORACIÓN implementará un programa de capacitación en protección de datos dirigido a las personas que intervengan en el tratamiento.

Como mínimo deberá abordar:

a) Principios de protección de datos.
b) Derechos de los titulares.
c) Autorizaciones.
d) Datos sensibles y biométricos.
e) Tratamiento de información académica.
f) Seguridad de la información.
g) Incidentes.
h) Confidencialidad.
i) Uso adecuado de correo y sistemas.
j) Videovigilancia.
k) Protección de menores.
l) Manejo de información en dispositivos personales o remotos.

Deberán conservarse evidencias de asistencia y contenido impartido.

47. AUDITORÍA Y VERIFICACIÓN

La CORPORACIÓN podrá realizar verificaciones periódicas sobre:

a) Cumplimiento de la Política.
b) Cumplimiento del Manual.
c) Bases de datos.
d) Autorizaciones.
e) Accesos.
f) Proveedores.
g) Incidentes.
h) Consultas y reclamos.
i) RNBD.
j) Conservación.
k) Supresión.
l) Biometría.
m) Videovigilancia.
n) Transferencias internacionales.

Los hallazgos deberán generar acciones correctivas o preventivas cuando corresponda.

48. INDICADORES DE CUMPLIMIENTO

El Sistema podrá ser evaluado mediante indicadores como:

48.1. Autorizaciones

Porcentaje de autorizaciones válidas registradas

Número de autorizaciones verificadas / Número de tratamientos que requieren autorización × 100.

48.2. Atención de consultas

Porcentaje de consultas atendidas dentro del término legal

Número de consultas atendidas oportunamente / Total de consultas recibidas × 100.

48.3. Atención de reclamos

Porcentaje de reclamos atendidos dentro del término legal

Número de reclamos atendidos oportunamente / Total de reclamos recibidos × 100.

48.4. Capacitación

Cobertura de capacitación

Número de personas capacitadas / Número de personas obligadas a capacitarse × 100.

48.5. Gestión de incidentes

Porcentaje de incidentes gestionados conforme al procedimiento

Número de incidentes gestionados conforme al protocolo / Total de incidentes registrados × 100.

48.6. Control de encargados

Porcentaje de encargados con documentación contractual vigente

Número de encargados con contrato y cláusulas de protección de datos / Total de encargados identificados × 100.

48.7. Actualización de bases

Porcentaje de bases de datos revisadas

Número de bases revisadas / Total de bases identificadas × 100.

49. ACCIONES CORRECTIVAS Y PREVENTIVAS

Cuando se identifique un incumplimiento, vulnerabilidad o riesgo, el responsable deberá establecer:

a) Descripción del hallazgo.
b) Causa.
c) Riesgo.
d) Acción correctiva.
e) Acción preventiva.
f) Responsable.
g) Fecha de cumplimiento.
h) Evidencia.
i) Verificación de eficacia.

Las acciones deberán realizarse de manera proporcional al nivel de riesgo.

50. TRATAMIENTO DE INCUMPLIMIENTOS INTERNOS

El incumplimiento del presente Manual podrá generar las consecuencias establecidas en:

a) Reglamentos internos.
b) Contratos.
c) Reglamento estudiantil.
d) Reglamento laboral.
e) Acuerdos de confidencialidad.
f) Normativa disciplinaria institucional.
g) Legislación vigente.

La CORPORACIÓN garantizará el debido proceso cuando corresponda.

51. REVISIÓN DEL MANUAL

El presente Manual deberá revisarse:

a) Por lo menos una vez al año.
b) Cuando se modifique la Política de Protección de Datos.

c) Cuando cambie la legislación.
d) Cuando se incorporen nuevas tecnologías.
e) Cuando se implementen nuevas bases de datos.
f) Cuando se presenten incidentes relevantes.
g) Cuando cambien los riesgos identificados.
h) Cuando la autoridad competente emita nuevas instrucciones.

52. CONTROL DE CAMBIOS

Versión	Fecha	Descripción
1	Septiembre de 2018	Creación del Manual del Sistema de Seguridad y Gestión del Riesgo de Datos Personales y Bases de Datos.
2	Septiembre de 2026	Actualización integral y armonización con el Acuerdo CS-155 de 2026, incorporación de controles sobre datos sensibles y biométricos, videovigilancia, cookies, menores de edad, incidentes, responsabilidad demostrada, DPO, RNBD, conservación, supresión, transferencias y transmisiones internacionales. CS-155 Deroga la CS—139.

53. DOCUMENTOS ASOCIADOS

Hacen parte del Sistema, según corresponda:

1) Política de Tratamiento de Datos Personales y Manejo de Información Biométrica – Acuerdo CS-155 de 2026.
2) Formato de autorización para tratamiento de datos personales.
3) Formato de autorización de datos sensibles.
4) Formato de autorización para tratamiento de datos biométricos.
5) Aviso de privacidad.
6) Avisos de videovigilancia.
7) Política de Cookies.
8) Formato de consulta de datos personales.
9) Formato de reclamo.
10) Formato de reporte de incidentes.

11) Registro de incidentes.
12) Acuerdos de confidencialidad.
13) Contratos de transmisión de datos personales.
14) Contratos de transferencia internacional.
15) Formato de evaluación de proveedores y encargados.
16) Inventario de bases de datos.
17) Registro de tratamientos.
18) Análisis de impacto a la privacidad.
19) Registro de supresión o anonimización.
20) Manual de archivo digital.
21) Manual de archivo documental.
22) Manual y términos de uso de aplicaciones institucionales.
23) Registros de capacitación.
24) Registros de auditoría y seguimiento.

54. DISPOSICIÓN FINAL

El presente Manual constituye el instrumento operativo para la implementación de la Política de Tratamiento de Datos Personales y Manejo de Información Biométrica de la CORPORACIÓN UNIVERSITARIA U DE COLOMBIA.

Todas las dependencias, funcionarios, profesores, contratistas, proveedores y demás personas obligadas deberán conocer, aplicar y cumplir sus disposiciones.

Su aplicación deberá armonizarse permanentemente con la Constitución Política, la Ley 1581 de 2012, el Decreto 1074 de 2015, el régimen aplicable al sector educativo, las instrucciones de la Superintendencia de Industria y Comercio y las demás normas que regulen la protección de datos personales.

PUBLÍQUESE, COMUNÍQUESE Y CÚMPLASE.