1. PROPÓSITO

Este documento contiene reglas establecidas por la Universidad de Santander para el tratamiento de información, con el fin de garantizar la confidencialidad y cumplir regulaciones y leyes aplicables a la institución.

2. ALCANCE

Aplica a todas las actividades académico-administrativas de la Universidad relacionadas con el tratamiento de información, desde su captura o elaboración hasta su eliminación o conservación total, en los campus de Bucaramanga, Cúcuta, Valledupar y programas de extensión.

3. CONDICIONES GENERALES

a. Se deben cumplir los lineamientos institucionales relacionados con la reserva de la información, confidencialidad, protección de datos personales, organización y conservación de documentos:

   - Contratos
   - Acuerdos de confidencialidad
   - REG-PI-001-UDES Política de tratamiento de datos personales
   - GED-IN-002-UDES Organización de archivos de gestión y transferencias documentales
   - GED-IN-005-UDES Organización de archivo central y disposición final de los documentos
   - SEI-PR-003-UDES Respaldo y restauración de la información

b. Todos los líderes y colaboradores de la Universidad al realizar las actividades propias de su cargo, asumirán las responsabilidades y las obligaciones que se tienen en el manejo adecuado de la información personal, desde su recolección, almacenamiento, uso, circulación y hasta su disposición final.

c. La Universidad de Santander solicitará al Titular de los datos solamente la información necesaria para los trámites que surtan de la relación académica o administrativa con esta, y únicamente recogerá datos sensibles para salvaguardar un interés vital del Titular previa su autorización (Ley 1581 de 2012).

d. Los datos personales a los que se tiene acceso, así como la información confidencial y sensible de personas naturales y jurídicas, deben ser utilizados solamente para propósitos requeridos o aspectos de ley.

e. La modificación o anulación de datos contenidos en bases de datos o documentos se debe realizar de acuerdo a los procedimientos establecidos en cada proceso/subproceso/centro de trabajo por el personal autorizado. Los permisos de acceso de los usuarios son concedidos por los procesos de Gestión TIC o encargados de las aplicaciones informáticas de acuerdo a los perfiles establecidos, los cuales serán previamente definidos por los líderes de los procesos donde se requiera el uso de información personal.

f. Los datos personales recolectados por un proceso/subproceso/centro de trabajo puede ser utilizado por otro de la Universidad siempre que se trate de un uso estimado por el tipo de servicios que la Institución ofrece y para finalidad contemplada dentro de la Política de Tratamiento de Datos Personales.

g. Durante la ejecución de las actividades, todo documento, carpeta y otros medios de almacenamientos que contienen información sensible, restringida o confidencial debe ser ubicada en áreas protegidas, nunca deben ser ubicados en lugares expuestos a personal no autorizado (interno o externo).

h. Al finalizar el procesamiento de la información o el día laboral, las unidades de conservación (físicas o electrónicas) que la contengan deben ser guardadas en áreas seguras dispuestas para tal fin.

i. El almacenamiento y destrucción de información digital y física se realiza siguiendo los lineamientos del instructivo de Organización de archivos de gestión y transferencias documentales y el Instructivo de Organización de archivo central y disposición final de los documentos en áreas restringidas y medios controlados por los procesos/subprocesos/centros de trabajo o contratación externa según aplique.

j. El respaldo de la información se realiza siguiendo lineamientos del subproceso de Seguridad Informática SEI-PR-003-UDES Respaldo y restauración de la información.

k. Las faltas de cumplimiento de este protocolo pueden tener como resultado acciones disciplinarias conforme a políticas y procedimientos vigentes de la Universidad.

4. DEFINICIONES

Autorización: es el consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales, por parte de la universidad.

Copia de seguridad (backup): es la copia total o parcial de información importante del disco duro, CD, bases de datos u otro medio de almacenamiento.

Dato personal: es cualquier tipo información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables

a) **Dato público**: es el dato que no sea semiprivado, privado o sensible. Se consideran datos públicos, los datos relativos al estado civil de las personas, a su profesión u oficio, a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, en registros públicos, documentos públicos, y sentencias judiciales.

b) **Datos sensibles:** es dato sensible aquel que afecta la intimidad del titular, o cuyo uso indebido puede generar su discriminación, tales como: que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos, entre otros.

Incidencia: cualquier anomalía que afecte o pudiera afectar la seguridad de las bases de datos o información contenida en las mismas.

Respaldo: es la copia de información a un medio del cual se pueda recuperar y restaurar la información original.

Restauración: volver a poner algo en estado inicial.

Titular: es la persona natural cuyos datos personales sean objeto de tratamiento, por parte de la universidad.

Tratamiento: es cualquier operación o conjunto de operaciones sobre tratamiento de datos personales, tales como la recolección, almacenamiento, uso, actualización, circulación o supresión.

5. DESARROLLO DEL CONTENIDO

5.1 PRÁCTICAS EN LAS ÁREAS DE OFICINA

- Clasifique la información física o electrónica, para implementar medidas de seguridad según se requiera.

- Cada usuario es responsable de asegurar toda unidad de conservación física o electrónica que contenga información sensible o confidencial, en lugar restringido.

- Durante el procesamiento de la información los documentos se conservan en carpetas o similares para no exponerlos en escritorio al público.

- Al finalizar la jornada de trabajo, los documentos deben resguardarse, si se trata de documentos con información sensible o confidencial se asegurarán en archivos con llave o con medidas electrónicas para tal fin.

- Se dispondrá de controles de acceso a las áreas de archivo o almacenamiento de información sensible o confidencial.

- Todos los equipos de cómputo deben estar protegidos con contraseñas de acceso cuando el área de trabajo esté desocupada o desatendida.

- Las contraseñas de los equipos de cómputo o aplicaciones no deben registrarse en notas en el escritorio, en lugar visible o de fácil acceso.

- La documentación impresa que contiene información sensible o confidencial debe ser retirada inmediatamente de los equipos de impresión o escaneo.

- Las impresoras o equipos de reprografía (fotocopiadoras, escáner, fax) deben ser ubicados en áreas donde no se exponga la información sensible o confidencial al público.

- Al realizar procesos de eliminación documental, los documentos con información sensible o confidencial deben destruirse de forma mecánica (destructoras de papel) o manual según aplique.

5.2 PRÁCTICAS PARA TRABAJO EN ÁREAS EXTERNAS

Para el trabajo en casa o en áreas diferentes a las establecidas por la Institución, se debe atender además de las Prácticas en áreas de oficina (numeral 5.1) aplicables, las siguientes recomendaciones para el cuidado de los documentos y protección de la información:

- Aplique los formatos y modelos de documentos establecidos para los trámites institucionales.

- Cumpla los procesos de revisión y aprobación según le haya informado el proceso/subproceso responsable.
- Proteja en todo momento la información institucional que está procesando de forma física o digital.
- Para trabajo remoto, conéctese a la red interna de la Universidad a través de una VPN asignada por el subproceso de Seguridad Informática.
- Si cuenta con una conexión remota, organice y conserve los documentos digitales en Disco D, carpeta del proceso/subproceso, caso contrario, en una carpeta en OneDrive de la cuenta de correo institucional asignada.
- Utilice la cuenta de correo o canales habilitados por la institución para transferir documentos, no realice esta acción a través de servicios de mensajería personal.
- Nunca pierda de vista su equipo de cómputo o dispositivo móvil, si requiere ausentarse cierre sesión y si es el caso resguarde el equipo.
- Proteja los documentos físicos del polvo, la humedad o daños en su estructura por la manipulación.
- Organice y conserve los documentos físicos en carpetas rotuladas según asunto.
- Una vez, retorne o se restablezcan las actividades presenciales en la Universidad, los documentos de conservación deben ser incorporados a los archivos.
- Desarrolle acciones de bioseguridad cuando manipule documentos en soporte papel e incluso elementos de oficina de uso común, atienda las recomendaciones de la Guía de conservación preventiva para documentos de archivo GED-GU-002-UDES.

5.3 CONSULTA DE LA INFORMACIÓN

- La consulta de información se realizará de acuerdo a procedimientos y medios establecidos e informados por los procesos/subprocesos/centros de trabajo de la Universidad.
- El titular de los datos, previamente identificado o mediante un tercero debidamente autorizado tiene derecho al acceso a su información.

- La autorización de terceros sobre acceso a la información, se dará bajo el diligenciamiento de formato institucional o documento autenticado.
- Los encargados o representantes de menores de edad podrán consultar su información en los términos de ley.
- Para las consultas en medios telefónicos, el encargado realizará preguntas relacionadas con la información tratada, que validen la identidad del Titular.
- Los requerimientos de información para atender acciones legales, deben ser solicitadas por las autoridades pertinentes.

5.4 SOLUCIÓN DE CONFLICTOS

Cuando no exista claridad sobre la naturaleza de la información para su uso y tratamiento, si esta corresponde a pública o sensible, Gestión Documental con asesoría de la Oficina Jurídica brindará el concepto pertinente, en un plazo no mayor a 10 días hábiles.

6. OBTENCIÓN AUTORIZACIÓN PARA TRATAMIENTO DE DATOS PERSONALES

Toda captura, recolección, uso y almacenamiento de datos personales que realice la Universidad en el desarrollo de sus actividades, en concordancia con las finalidades dispuestas en la Política de Protección de Datos Personales, requiere de los titulares un consentimiento libre, previo, expreso, inequívoco e informado.
Los procesos/subprocesos/centros de trabajo de la Universidad podrán obtener la autorización para el manejo, de datos, mediante diferentes medios, entre ellos el documento físico, electrónico, mensaje de datos, internet, sitios web, o en cualquier otro formato que en todo caso permita la obtención del consentimiento mediante conductas inequívocas, a través de las cuales se concluya sin lugar a dudas que de no haberse surtido la misma por parte del titular o la persona legitimada para ello, los datos no se hubieran almacenado o recolectado en la base de datos, dicha autorización será solicitada por LA UNIVERSIDAD de manera previa al tratamiento de los datos personales.

Por lo anterior, se deberán guardar los formatos físicos en donde existan autorizaciones, el registro de llamadas o de los formularios web en los cuales se da trazabilidad sobre la aceptación del tratamiento.

6.2 Autorización en Formatos

Los modelos de autorización de tratamiento de datos personales pueden ser tramitados a través de formatos web o documentos físicos.

6.2.2 Autorización en formatos físicos

Los procesos/subprocesos/centro de trabajo que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formatos físicos, deben tener en cuenta los siguientes aspectos:

- Solicitar sólo aquellos datos personales necesarios conforme con la finalidad de la captura.
- Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento de los datos.
- Para que la Universidad pueda realizar el tratamiento de los datos capturados en el formulario, el titular debe dar la autorización. Cuando el titular no haya autorizado, deberá ser analizado el evento de manera independiente.
- Garantizar la custodia de los formularios con sus respectivas autorizaciones

6.2.1 Autorización en Formatos Web

Los procesos/subprocesos/centros de trabajo que, en el ejercicio de sus funciones, realicen la recolección de datos personales a través de formularios web, deberán tener en cuenta los siguientes aspectos necesarios para su captura:

- Solicitar sólo aquellos datos personales necesarios conforme con la finalidad del tratamiento.
- Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento por parte del titular.
- El envío de la información a través del formulario, deberá estar condicionado a la previa aceptación de la autorización de tratamiento del dato.
- Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales.
- Gestión TIC debe garantizar que la plataforma que soporta el formulario web tenga la capacidad técnica, operativa y de seguridad para almacenar las autorizaciones y poder tener la trazabilidad en ellas.

6.3 Autorización en la toma de imagen (video y fotografías)

6.3.1 Autorización en eventos

Comunicaciones, los procesos, subprocesos, centros de trabajo o encargados del evento, debe velar por el adecuado cumplimiento de las directrices establecidas sobre protección de datos personales, por lo cual, al inicio de cada presentación incorpora una diapositiva informativa sobre la captura de la imagen y las finalidades de tratamiento.

6.3.2 Autorización para publicación de contenidos

La autorización de uso de imagen para el desarrollo de contenidos en los medios de comunicación institucional, para investigación o promoción, en formato físico o digital, se realiza a través del diligenciamiento del formato COM-FT-002-UDES Autorización de uso de imagen, Comunicaciones, los procesos, subprocesos o centros de trabajo, deben garantizar la custodia de los formularios con sus respectivas autorizaciones.

La imagen de los empleados y los estudiantes no requieren de una autorización adicional, ya que la Universidad dispone lo concerniente a través de clausula en los contratos y en el formulario de inscripción académico, respectivamente.

7. VIDEOVIGILANCIA

La Universidad de Santander utiliza medios de video vigilancia instalados en diferentes sitios internos y externos de sus Campus y sedes, la información recolectada por estos mecanismos se utiliza para fines de seguridad de los bienes, instalaciones y personas que se encuentren en éstas, o como prueba en cualquier tipo de proceso interno, judicial o administrativo, en cumplimiento de las normas legales.

Los Titulares de los datos, deben ser informados de la existencia de los medios de vigilancia a través de la difusión en sitios visibles, de anuncios con alertas. No obstante, ningún dispositivo de video vigilancia se sitúa en lugares que puedan afectar la intimidad de los Titulares.

8. CAPACITACIÓN

La Universidad dentro de su programa de inducción y reinducción, incluye la difusión de conceptos, lineamientos, responsabilidades y disposiciones prácticas sobre el tratamiento de los datos personales y seguridad de la información.

Así mismo, los procesos/subprocesos/centros de trabajo podrán solicitar a Gestión Documental y Seguridad Informática, según aplique, capacitaciones específicas para sus grupos de interés, a través de los mecanismos internos establecidos.

9. TRATAMIENTO DE INCIDENTES SEGURIDAD DE LA INFORMACIÓN

Los procesos, subprocesos y centros de trabajo establecerán las medidas de seguridad de carácter preventivo para evitar la pérdida de la información, su adulteración, así como la consulta, uso, circulación o acceso no autorizado o fraudulento.

a. Identificación de incidentes

Los eventos sospechosos o anormales, en los que se observe potencial perdida de reserva o confidencialidad de la información, integridad o disponibilidad de la misma deben ser evaluados para determinar si son o no, un incidente.

b. Reporte

Los potenciales incidentes de seguridad de información deben ser reportados una vez conocido el hecho, al líder de cada proceso, subproceso, centro de trabajo quien a su vez notificará de forma inmediata al Oficial de Protección de Datos Personales a través del correo habeasdata@udes.edu.co

c. Evaluación

El Oficial de Protección de datos, contará con el apoyo del Jefe de Talento Humano, Jefe de Seguridad Informática, Jefe Jurídico para determinar si se trata de un incidente de seguridad de la información.

d. Toma de acción

Si se determina que se presentó incidente de seguridad de la información, se procede con el líder del proceso/subproceso/centro de trabajo correspondiente a:

- Establecer y ejecutar las acciones para contener y revertir el incidente
- Identificar las causas e impacto del mismo y generar las acciones de mejora para mitigar los riesgos
- Comunicar al titular o titulares afectados (si aplica)
- Se debe documentar las actuaciones realizadas en torno del tratamiento del incidente.

e. Notificación ante la SIC

La violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de datos, se reportarán al Registro Nacional de Bases de Datos dentro de los quince (15) días hábiles siguientes al momento en que se detecten y sean puestos en conocimiento del Oficial de Protección de datos personales.

f. Seguimiento

El Oficial de Protección de Datos Personales preparará un análisis anual de los incidentes reportados dirigido a Rector/Representante Legal de la Universidad. Las conclusiones de este informe se utilizarán en la elaboración de campañas de concientización que ayuden a minimizar la probabilidad de incidentes futuros.

CONTROL DE CAMBIOS

VERSIÓN 02	**DESCRIPCIÓN DEL CAMBIO**
FECHA DE APROBACIÓN 28/09/2020 **RESPONSABLE** Esperanza Rojas Rojas Directora de Gestión Documental	En Condiciones Generales (3), se incluye: Literal a. cumplir el procedimiento SEI-PR-003-UDES Literal b. Responsabilidades y obligaciones frente al adecuado manejo de la información Literal e. Tratamiento de modificación o anulación de datos, permisos de acceso a aplicaciones informáticas Literal f. Uso de datos recolectados por otra área de trabajo Literal i. Almacenamiento y destrucción de información. En definiciones se incluye el término Incidencia (4) Se ajusta en Título término Recomendaciones por Prácticas (5.2) En Consulta de información, se incluye consulta de información se realizará de acuerdo a procedimientos y medios establecidos e informados. Se incluye numeral 6. Obtención para tratamiento de datos personales, 7. Video vigilancia, 8. Capacitación, 9. Tratamiento de incidentes seguridad de la información.
VERSIÓN 02	**DESCRIPCIÓN DEL CAMBIO**
FECHA DE APROBACIÓN 26/01/2023 **RESPONSABLE** Equipo de trabajo Campus Bucaramanga-Cúcuta-Valledupar.	En la revisión anual de documentos no presentó cambios. Se ajusta logo institucional, tamaño del logo Icontec, tipología y color en código de certificación. Se ajustan entradas y presentación del control de cambios, según Procedimiento Control de Documentos y Registros.
VERSIÓN 03	**DESCRIPCIÓN DEL CAMBIO**
FECHA DE APROBACIÓN 11/12/2023 **RESPONSABLE** Equipo de trabajo Campus Bucaramanga-Cúcuta-Valledupar.	En numeral 5.1 PRÁCTICAS EN LAS ÁREAS DE OFICINA, se agrega "manual según aplique" En numeral 6.3.2 Autorización para publicación de contenidos se ajusta trazabilidad del formato autorización de uso de imagen, en razón a que cambio el área responsable del mismo. Se actualiza imagen de sello IQNET, conforme al cambio que muestra el manual del uso de la marca de conformidad de la certificación ICONTEC para sistemas de gestión. Se ajustan entradas del control de cambios, según Procedimiento Control de Documentos y Registros.