MANUAL INTERNO DE POLÍTICAS Y PROCEDIMIENTOS PARA EL TRATAMIENTO DE DATOS PERSONALES

Universidad del Rosario

LEY 1581 DE 2012

Versión 2.0 – Julio de 2023

Bogotá D. C.

Contenido

Capítulo I. Disposiciones generales

Objetivo General

El presente *Manual interno de políticas y procedimientos para el tratamiento de los datos personales* está diseñado con el fin de asegurar el cumplimiento de lo estipulado en la legislación actual acerca de la protección de los datos personales, y tiene la finalidad de regular el tratamiento de los datos que hace La Universidad con el fin de garantizar y proteger los derechos de los titulares, considerando lo dispuesto en el numeral k) del artículo 17 de la Ley 1581 de 2012.

Objetivos específicos

- Determinar criterios, procedimientos y requisitos necesarios para el cumplimiento de la ley enmarcada dentro de la protección de datos personales.

- Establecer reglas para la recolección, el almacenamiento, el uso, la circulación y la supresión o la disposición final de la información personal.

Alcance

El presente manual tiene como propósito establecer criterios, procedimientos y requisitos para el tratamiento de datos personales que reposan en las bases de datos, archivos físicos y digitales del Colegio Mayor de Nuestra Señora del Rosario (en adelante, La Universidad). Estas directrices deben ser cumplidas y acatadas por toda la comunidad rosarista, dentro del marco de sus actividades diarias tanto en el interior de la Universidad como en las relaciones que se tengan con terceros.

El presente manual se articula con la Política de Tratamiento de Datos Personales de La Universidad, es de obligatorio cumplimiento y debe ser aplicado en todos los procesos y los procedimientos actuales y futuros que La Universidad incorpore en el ejercicio de sus actividades estratégicas, tácticas y operativas.

Capítulo II. Definiciones

Para el desarrollo y la implementación de este manual, La Universidad adopta las definiciones establecidas en la Ley 1581 de 2012 y el capítulo I del Decreto 1377 de 2013, para una comprensión adecuada:

Autorización: Consentimiento previo, expreso e informado del titular para llevar a cabo el tratamiento de datos personales.
Base de datos personales: Conjunto organizado de datos personales que sea objeto de tratamiento.
Consentimiento del titular: Es una manifestación de la voluntad, informada, libre e inequívoca, a través de la cual el titular de los datos de carácter personal acepta que un tercero utilice su información.
Consultas: Los titulares o sus causahabientes podrán consultar la información personal del titular que repose en cualquier base de datos, sea esta del sector público o privado. El responsable o encargado del tratamiento deberá suministrar a estos, toda la información contenida en el registro individual o que esté vinculada con la identificación del titular.
Dato Personal: Se refiere a cualquier información asociada a una persona natural (identificada o identificable), relativa tanto a su identidad (nombre y apellidos, domicilio, filiación, etc.) como a su existencia y ocupaciones (estudios, trabajo, enfermedades, etc.).

- Dato Público: Es el dato calificado como tal por la Constitución o la Ley y todos aquellos que no sean semiprivados o privados, de conformidad con la ley colombiana. Son públicos, entre otros, los datos contenidos en documentos públicos, gacetas y boletines judiciales, sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva y los relativos al estado civil de las personas.
- Dato Semiprivado: Es semiprivado el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como el dato financiero y crediticio de actividad comercial o de servicios.
- Dato Privado: Es el dato que por su naturaleza íntima o reservada sólo es relevante para el titular.
- Datos Sensible: Para los propósitos de la presente política, se entiende por dato sensible todo aquel que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos 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.

Encargado del tratamiento: Es quien gestiona y/o manipula los datos de carácter personal a nombre del responsable, pero no decide cómo, ni con qué fin. Su trabajo es operativo y se hace con base a las indicaciones e instrucciones del responsable del tratamiento.
Habeas Data: Es el derecho que tiene todo titular de información de conocer, actualizar, rectificar u oponerse a la información concerniente a sus datos personales.
Protección de datos de carácter personal: Es un derecho fundamental que tienen todas las personas naturales. Busca la protección de su intimidad y privacidad frente a una posible vulneración por el tratamiento indebido de datos personales capturados por un tercero.
Reclamo: El titular o sus causahabientes que consideren que la información contenida en una base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley o en la presente política, podrán presentar un reclamo ante el responsable del tratamiento o el encargado del tratamiento.
Responsable del tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos personales.
Tratamiento: Cualquier operación o procedimientos físicos o automatizados que permita captar, registrar, reproducir, conservar, organizar, modificar, transmitir los datos de carácter personal.
Titular de los datos personales: Es la persona natural cuyos datos personales son objeto de tratamiento por parte de un tercero.

Capítulo III. Principios para el tratamiento de datos personales

La Universidad aplicará los siguientes principios rectores, que se establecen a continuación, los cuales constituyen las directrices para seguir en la recolección, el almacenamiento, el uso, la circulación y la disposición final de los datos personales:

Principio de legalidad: La Universidad busca garantizar el cumplimiento del Régimen Normativo de Protección de Datos Personales estableciendo obligaciones para sus colaboradores, estudiantes, profesores y las demás personas vinculadas a la institución.

Principio de finalidad: el tratamiento de datos personales que hace La Universidad está sometido y atiende a una finalidad legítima, la cual es informada al respectivo titular de los datos personales en el momento de la recolección de su información.

Principio de libertad: el tratamiento de datos personales solo puede efectuarse con el consentimiento previo, expreso e informado del titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento.

Principio de veracidad o calidad: La Universidad internamente ha dispuesto mecanismos de actualización de la información personal, con el fin de que esta sea veraz, completa, exacta y actualizada.

Principio de transparencia: en cumplimiento de este principio, La Universidad garantiza el derecho del titular a obtener de esta, en cualquier momento y sin restricciones, información acerca de la existencia de cualquier tipo de información o dato personal que sea de su interés o su titularidad.

Principio de acceso y circulación restringida: La Universidad ha dispuesto controles de acceso a la información personal contenida en las bases de datos. También ha dispuesto internamente mecanismos para que sus colaboradores puedan tener acceso solo a la información que de acuerdo con su cargo deban conocer. También ha establecido acuerdos de confidencialidad y contratos de transmisión de datos personales con encargados de la información, para brindar todas las garantías que permitan proteger la información personal.

Principio de seguridad: La Universidad ha establecido diferentes tipos de medidas tecnológicas, físicas y administrativas para evitar cualquier tipo de tratamiento no autorizado de los datos personales por parte de terceros que no se encuentren facultados para acceder a dicha información.

Principio de confidencialidad: todas y cada una de las personas que interactúen en el tratamiento de datos personales realizado por La Universidad, y que administren, manejen, actualicen o tengan acceso a la información personal, comercial, contable, técnica, comercial o de cualquier otro tipo que se encuentre en bases de datos o que sea suministrada en la ejecución y el ejercicio de sus funciones se comprometen a conservarla y mantenerla de manera estrictamente confidencial y a no revelarla a terceros. La Universidad garantiza este principio contando con medidas preventivas legales y técnicas con sus colaboradores, sus proveedores y las demás personas que tengan acceso a información de cualquier tipo, para evitar su divulgación o su obtención sin autorización del titular del dato.

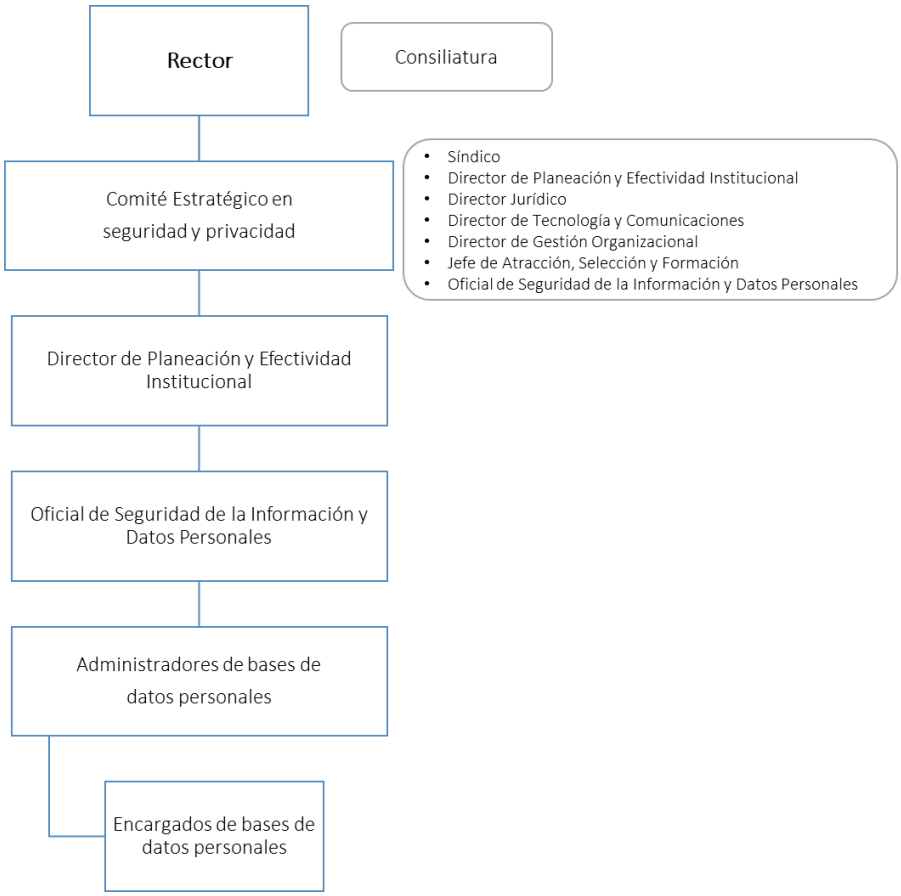
Principio de responsabilidad demostrada: La Universidad está en capacidad de demostrar ante la Superintendencia de Industria y Comercio que ha implementado las obligaciones exigidas por la legislación colombiana en protección de datos personales atendiendo a su naturaleza jurídica, los servicios que ofrece a la comunidad académica y al público en general, estableciendo políticas, procedimientos, manuales, estructura de gobierno, identificación de los riesgos asociados al manejo de datos y, en general, el cumplimiento de las obligaciones establecidas en la ley.

Capítulo IV. Estructura administrativa para el cumplimiento de la Política de Tratamiento de Datos Personales

1. Gobierno

En cumplimiento de las disposiciones legales en materia de protección de datos personales, por medio del presenta manual, se establece el Gobierno del Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información definido al interior de La Universidad y que se encuentra compuesto por los siguientes roles y/o áreas: Comité Estratégico en Seguridad y Privacidad de los Datos Personales y la Información, Director

de Planeación y Efectividad Institucional, Oficial de Seguridad de la Información y Datos Personales, Administradores de Bases de Datos Personales, Encargados de Bases de Datos Personales.



Este Sistema de Gestión velará por el cumplimiento del régimen legal de protección de datos personales al interior de La Universidad.

2. Roles y Responsabilidades del Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información

A continuación, se mencionan las responsabilidades de cada uno de los miembros del Gobierno en Protección de Datos Personales de la Universidad:

Comité Estratégico en Seguridad y Privacidad de los Datos Personales y la Información

Autoridad central en la Universidad en materia de protección de datos personales y seguridad de la información, responsable de tomar decisiones sobre la protección de los datos de los titulares y proteger sus intereses y los de La Universidad. El Comité Estratégico en seguridad y privacidad de los Datos Personales y la información está integrado por:

Integrantes:

- Síndico
- Director de Planeación y Efectividad Institucional

- Director de Gestión Organizacional
- Director de Tecnología Informática y Comunicaciones
- Director Jurídico
- Jefe de Selección, Atracción y Formación
- Oficial de Seguridad de la Información y Datos Personales

Responsabilidades del Comité Estratégico en Seguridad y Privacidad de los Datos Personales y la Información

Fases	Responsabilidades
Planeación	• Aprobar la Política de Tratamiento de Datos Personales, la Política de Seguridad de la Información, Ciberseguridad y Protección de la Privacidad y los manuales que adopten políticas y procedimientos para el cumplimento de las mismas y, posteriormente los cambios sustanciales que puedan llegar a presentarse. • Aprobar el presupuesto en pro de las mejoras al Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información. • Realizar seguimiento al plan de trabajo anual en materia de protección de datos personales.
Ejecución	• Generar lineamientos en pro de cumplir con la normativa colombiana e internacional en materia de protección de datos personales. • Generar cultura organizacional para la protección de datos personales.
Verificación	• Solicitar al Oficial de Seguridad de la Información y Datos Personales, al menos una vez al año, un informe del cumplimiento de la Universidad en materia de protección de datos personales. • Presentar, al menos una vez al año, un informe general frente al cumplimiento en materia de protección de datos personales a la Consiliatura. • Asistir a las reuniones semestrales con el fin de monitorear el efectivo cumplimiento del Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información. • Asistir a los comités extraordinarios en caso de que se lleguen a presentar.
Ajustes	• Generar acciones de intervención, control, revisión, implementación y toma de decisiones con las áreas de La Universidad relacionadas con la protección de datos personales, cuando sea necesario. • Generar lineamientos basados en los informes presentados por los entes de control internos y externos, los resultados en la gestión de riesgos, en pro de la mejora continua del Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información.

Líder de protección de datos personales

Rol que ejerce el Director de Planeación y Efectividad Institucional, cuyo fin es apoyar las responsabilidades del Oficial de Seguridad de la Información y Datos Personales.

Fases	Responsabilidades
Planeación	• Elaborar el plan de trabajo anual en materia de protección de datos personales en compañía del Oficial de Seguridad de la Información y Datos Personales. • Elaborar el presupuesto requerido para ejecutar el plan de trabajo anual en protección de datos personales.
Ejecución	• Ser el representante de La Universidad en materia de protección de datos personales ante otros actores.
Verificación	• Realizar reuniones periódicas con el Oficial de Seguridad de la Información y Datos Personales, con el fin de validar el cumplimiento del plan de trabajo.

	• Asistir a las reuniones semestrales con el fin de monitorear el efectivo cumplimiento del Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información.
Ajustes	• Garantizar la continuidad de la operación en materia de protección de datos personales frente a ausencias laborales programadas y no programadas.

Oficial de Seguridad de la Información y Datos Personales

Rol bajo la responsabilidad del Director de Planeación y Efectividad Institucional dentro de La Universidad, y cuya responsabilidad consiste en estructurar, diseñar y liderar el Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información, para así permitirle a La Universidad cumplir las normas en la materia, generar lineamientos e identificar los controles pertinentes para mitigar riesgos en protección de datos personales, hacer evaluación al programa y adoptar mejoras continuas en pro de la estabilidad de este.

Fases	Responsabilidades
Planeación	• Elaborar el plan de trabajo anual en materia de protección de datos personales. • Elaborar el presupuesto requerido para ejecutar el plan de trabajo anual en protección de datos personales.
Ejecución	• Identificar, analizar y evaluar los riesgos en materia de protección de datos personales, incorporando elementos de seguridad de la información a la metodología de gestión de riesgos (SARI) de la Universidad. • Presentar anualmente al Comité Estratégico en Seguridad y Privacidad de los Datos Personales y la Información el informe general y consolidado frente al cumplimiento en materia de protección de datos personales. • Actuar como enlace y coordinar con las demás áreas de la Universidad, para asegurar una gestión transversal del Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información. • Tener conocimiento acerca de la normativa colombiana en materia de protección de datos personales. • Promover una cultura de protección de datos dentro de la Universidad. • Realizar actualizaciones a la documentación del proceso de gestión de datos personales, incluyendo políticas, procedimientos y formatos. • Mantener un inventario actualizado de las bases de datos personales en poder de La Universidad. • Registrar las bases de datos de la Universidad en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la Superintendencia de Industria y Comercio. • Obtener las declaraciones de conformidad de la Superintendencia de Industria y Comercio, cuando así sea requerido. • Validar los contenidos de los contratos o anexos de transmisión de datos generados por la Dirección Jurídica que se suscriban con encargados. • Gestionar las respuestas a las consultas y reclamos presentados por los titulares, con base en los procedimientos internos de atención de consultas y reclamos en materia de protección de datos personales. • Coordinar con la Dirección de Gestión Humana la inducción necesaria a los nuevos empleados y a los miembros de la Comunidad Rosarista, acerca de la concientización en materia de protección de datos personales; en especial, a quienes, por las responsabilidades del cargo, tengan acceso a datos personales gestionados por la Universidad. • Evaluar y decidir el reporte a la Superintendencia de Industria y Comercio acerca de los incidentes de seguridad de la información que involucren datos personales.

	• Acompañar y asistir a la Universidad en la atención a las visitas y los requerimientos que haga la Superintendencia de Industria y Comercio. • Apoyar a los administradores de bases de datos personales con aquellas dudas que surjan en materia de protección de datos personales y frente al cumplimento de la Política de Tratamiento de Datos Personales. • Participar en los proyectos que desarrolle la Universidad en los cuales se involucren datos personales generando lineamientos respecto al tratamiento de los datos. • Definir los roles, las responsabilidades, la cadena de rendición de cuentas y la estructura organizacional para el Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información. • Liderar las reuniones del Comité Estratégico en Seguridad y Privacidad de los Datos Personales y la Información.
Verificación	• Hacer autoevaluación sobre el cumplimiento del plan de trabajo anual en protección de datos personales. • Diseñar, en conjunto con la Dirección de Gestión Organizacional, los Administradores de Bases de Datos Personales, los planes de mitigación a riesgos, acorde con los resultados de las evaluaciones de riesgos.
Ajustes	• Evaluar la pertinencia de las diferentes oportunidades de mejora recibidas de los entes de control interno y externo frente al Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información, así como generar lineamientos para incorporarlas y monitorear su implementación. • Hacer los ajustes requeridos al plan anual de trabajo, con base en la retroalimentación generada por el Comité Estratégico en Seguridad y Privacidad de los Datos Personales y la Información.

Administradores de Bases de Datos Personales

Son los líderes de los procesos o las áreas que recolectan, almacenan, usan, circulan y suprimen datos personales y deciden sobre la finalidad de la base de datos personales y el tratamiento de estos.

Responsabilidades

Fases	Responsabilidades
Planeación	• Definir o identificar acciones en caso de requerirse, para establecer controles que fortalezcan o aporten a la seguridad y privacidad de los datos personales de la base de datos personales que administra. • Definir el presupuesto en caso de requerirse, para generar controles que aporten a la seguridad y privacidad de los datos personales de la base de datos personales que administra.
Ejecución	• Garantizar la recolección de la autorización de tratamiento de datos personales del titular. • Garantizar la continuidad de las responsabilidades en materia de protección de datos personales frente a ausencias laborales programadas y no programadas. • Garantizar la conservación de la autorización para el tratamiento de datos personales suministrada por el titular. • Garantizar el uso de los datos personales, según las finalidades descritas en, la Política de Tratamiento de Datos Personales, la autorización realizada por el titular y el Manual Interno. • Informar previamente al Oficial de Seguridad de la Información y Datos Personales la inclusión en el inventario de bases de datos personales, así como las nuevas fuentes de recolección y almacenamiento de datos requeridos para el proceso o área de la cual es responsable, así como la necesidad de circulación externa de datos personales a terceros.

	• Mantener comunicación constante con el encargado de la base de datos personales en especial cuando se reciba alguna consulta o reclamo que afecte la base de datos que administra e informar al Oficial de Seguridad de la Información y Datos Personales frente a algún cambio sustancial. • Desarrollar las actividades descritas y asignadas a este rol en el procedimiento interno de atención de consultas y reclamos en materia de protección de datos personales. • Reportar los incidentes en seguridad de la información a través de los medios estipulados en el Sistema de Administración del Riesgo Integrado (SARI). • Identificar y evaluar los riesgos del proceso en materia de protección de datos personales. • Diseñar e implementar los planes de mitigación de riesgos en compañía del Oficial de Seguridad de la Información y Datos Personales, acorde con los resultados de las evaluaciones de riesgos. • Implementar medidas de seguridad apropiadas para conservar la confidencialidad de la información de los titulares. • Promover una cultura de protección de datos personales con el equipo de colaboradores y los demás empleados de su área. • Reportar al Oficial de Seguridad de la Información y Datos Personales cuando conozca una consulta o reclamo en protección de datos personales. • Informar al Oficial de Seguridad de la Información y Datos Personales cuando esté en negociación con un futuro proveedor al cual La Universidad deba entregar bases de datos o información confidencial. • Informar al Oficial de Seguridad de la Información y Datos Personales las mejoras que considere que se deben implementar en la gestión de los datos personales. • Asegurar que todos los colaboradores bajo su cargo tengan claros sus roles y responsabilidades, así como su contribución para el logro de los objetivos del Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información de la Universidad y las consecuencias de su incumplimiento. • Participar y/o recibir las auditorías en materia de protección de datos personales en caso de presentarse.
Verificación	• Hacer autoevaluación permanente al cumplimiento de las responsabilidades adquiridas, con especial atención a la recolección de la autorización para el tratamiento de datos personales y la conservación de esta.
Ajustes	• Evaluar la pertinencia de las diferentes oportunidades de mejora recibidas de los entes de control internos y externos frente al Sistema de Gestión de Seguridad y Privacidad de los Datos Personales y la Información. • Generar lineamientos para incorporar las oportunidades de mejora y monitorear su implementación.

Encargado de bases de datos personales

Es un tercero, ajeno a la universidad, y quien hace el tratamiento de datos personales bajo instrucciones y por cuenta del responsable (Administradores de Bases de Datos Personales).

Fases	Responsabilidades
Ejecución	• Contar con una política de tratamiento de datos personales. • Garantizar la recolección de la autorización de tratamiento de datos personales del titular de la autorización bajo los lineamientos proporcionados por el Administrador de Bases de Datos Personales de la Universidad. • Implementar medidas de seguridad apropiadas para conservar la confidencialidad, integridad y disponibilidad de la información de los titulares.

	• Prestar la mayor diligencia debida en la ejecución de su labor respecto a la protección y la seguridad del dato personal, en bases de datos tanto digitales como físicas. • Informar inmediatamente al Administrador de Bases de Datos Personales de la Universidad cualquier comunicación relativa a los datos personales. • Informar al Administrador de Bases de Datos Personales de la Universidad cualquier reclamo o consulta que reciba por parte del titular de los datos personales, en un término máximo de un día hábil posterior a la fecha de recibo. • Adoptar un manual interno de políticas y procedimientos para salvaguardar la seguridad de los datos personales entregados por la Universidad. • Firmar un acuerdo de transmisión de datos personales donde se enmarquen las responsabilidades frente al tratamiento de los mismos. • Garantizar que cuenta con adecuadas medidas de seguridad técnicas, físicas o administrativas para el tratamiento de los datos personales. • Hacer oportunamente la actualización, rectificación o supresión de los datos tal como lo indique el Administrador de Bases de Datos Personales. • Garantizar que los datos personales sean tratados según la finalidad establecida por el Administrador de Bases de Datos Personales de la Universidad. • Cumplir en todo momento las instrucciones dadas por el Administrador de Bases de Datos Personales de la Universidad. • Tener acuerdos de confidencialidad con los contratistas o los trabajadores que, en razón o con ocasión de las labores que prestan, traten datos personales. • Informar inmediatamente al Administrador de Bases de Datos Personales de la Universidad cualquier incidente o vulneración que se presenten con los datos personales entregados. • Abstenerse de permitir el acceso a los datos personales entregados por el Administrador de Bases de Datos Personales de la Universidad, aunque así haya sido indicado. En caso de requerimiento judicial o administrativo para revelar total o parcialmente los datos personales de La Universidad, deberá comunicarlo por escrito a los administradores, quienes, junto con el oficial, se encargarán de determinar los lineamientos para el caso en concreto. • Garantizar la destrucción efectiva de la información una vez termine la ejecución del contrato. Por ningún motivo podrá guardar copia alguna de datos personales. • Devolver la totalidad de la información que contenga datos personales según lo dispuesto por el administrador.
Verificación	• Hacer autoevaluación permanente al cumplimiento de las responsabilidades adquiridas, con especial atención a las solicitudes hechas por el Administrador de Bases de Datos Personales de la Universidad en materia de protección de datos personales.

Capítulo V. Procedimientos para ejercer el derecho de hábeas data

Hábeas data: derecho que tienen todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en bases de datos y en archivos de entidades públicas y privadas. En los artículos 14 y 15 de la Ley 1581 de 2012 se exponen los procedimientos para ejercer este derecho a través de consultas o reclamos. A continuación, damos a conocer el procedimiento interno para gestionar el derecho de *hábeas data* (consultas y reclamos).

Procedimiento para la atención de consultas y reclamos

Objetivo

Dar a conocer los pasos que se dan internamente para poder tramitar, de forma oportuna y precisa, las consultas y los reclamos hechos por parte del titular de los datos personales o terceros, con el fin de darle a conocer la información contenida en su registro individual o que esté asociada al titular del dato personal.

Alcance

Inicia con la radicación de la consulta o el reclamo solicitados por el titular o un tercero, y termina con la respuesta oportuna y precisa por parte del Oficial de Seguridad de la Información y Datos Personales, con base en los tiempos y los lineamientos definidos en el artículo 14 y 15 de la Ley 1581 de 2012 en protección de datos personales.

Descripción del procedimiento

ID	Paso	Descripción de la actividad	Responsable
1	Radicación de la solicitud	La solicitud es radicada a través de los canales habilitados por La Universidad para consultas y reclamos descritos en la Política de Tratamiento de Datos Personales en el numeral 10. **Si alguien de la comunidad Rosarista recibe una solicitud de protección de datos personales, debe informar cuáles son los canales habilitados para este trámite y enviar el caso inmediatamente al correo: habeasdata@urosario.edu.co.* **Canales habilitados** 1. Ingresando la solicitud en la opción "solicitudes" en la sección Protección de Datos de la página *web* de La Universidad: www.urosario.edu.co 2. Remitiendo la solicitud al correo electrónico habeasdata@urosario.edu.co 3. Dejando la solicitud en el buzón físico ubicado en el Edificio Santafé (Carrera 6 N° 12 C-13, Bogotá, D. C.), en el horario de atención de lunes a viernes 7:00 a. m.-7:00 p. m., y los sábados, de 8:00 a. m.-1:00 p. m.* ** El Coordinador de Servicio de Casa UR deberá remitir a través de correo electrónico el archivo digital de esta solicitud al Oficial de Seguridad de la Información y Datos Personales.*	Titular Tercero y Coordinador de Servicio de Casa UR
2	Validación de la solicitud	Recibida la solicitud, se debe validar según los términos definidos por la Ley 1581 de 2012 en los artículos 14 y 15, y según como sea catalogada dicha solicitud: **Si es consulta:** Los tipos de consulta son: 1. Acceso a los datos personales. 2. Información acerca del uso de los datos personales. El término máximo para atender la consulta será de *(10) diez días hábiles*, contados a partir de la fecha de recibo de la misma.	Oficial de Seguridad de la Información y Datos Personales

		Si es reclamo: la descripción de cada tipo de reclamo se encuentra descrito en la Política de Tratamiento de Datos Personales, numeral 9. Los tipos de reclamos son: 1. Actualización. 2. Corrección. 3. Supresión. 4. Revocatoria de la autorización. ** La revocatoria de autorización dará lugar cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. Para la misma el titular deberá aportar evidencia de esto.* El término máximo para atender el reclamo será de *(15) quince días hábiles*, contados a partir del día siguiente a la fecha de su recibo. ** Cuando no fuere posible atender la consulta o el reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho días hábiles siguientes al vencimiento del primer término.*	
3	Acreditación del titular o tercero	Tanto para consulta como para reclamo, se solicita la siguiente documentación, a fin de validar que es el titular o un tercero autorizado. Se verifica que cumpla con los parámetros establecidos por la ley y por La Universidad en la Política de Tratamiento de Datos Personales numeral 10, para la acreditación del titular del dato. Información que debe acreditar el titular: a. Solicitud realizada a través de los canales de comunicación habilitados para el ejercicio del derecho de habeas data. b. Adjuntar fotocopia del documento de identificación, en los casos que aplique. c. Adjuntar los soportes que desea hacer valer. Información que debe acreditar un tercero: a. Solicitud realizada a través de canales de comunicación habilitados para el ejercicio del derecho de hábeas data. b. Documento de representación, en caso de que actúe como apoderado. c. Carta de autorización del titular, con reconocimiento de firma, en caso de que sea un tercero actuando en representación del titular. d. Fotocopia del documento de identificación del titular y la persona autorizada. e. Adjuntar los soportes que desea hacer valer. *(*) En todo caso y en cualquier momento, La Universidad podrá solicitar información adicional para dar trámite a la respectiva consulta o reclamo.* En caso de no cumplir con los parámetros, deberá informar al titular dentro de los tiempos estipulados por ley, a fin de que aporte la	Oficial de Seguridad de la Información y Datos Personales

		documentación faltante o cualquier otra aclaración que sea necesaria para la ejecución de la consulta.	
4	Búsqueda de información	Envío de la consulta o reclamo presentado por el titular, tercero a: 1. Administrador de Bases de Datos Personales; estos a su vez, a los encargados de la base de datos que afecta ese dato, para la gestión pertinente. 2. Notificar a otras áreas de La Universidad cuando la consulta así lo amerite. Los administradores y encargados de Bases de Datos Personales deberán realizar la búsqueda en bases de datos, bancos de datos o archivos donde se haga tratamiento de datos personales asociados al titular de la información, con el fin de asegurar al titular o al tercero la existencia o no de su información personal en las bases de datos de La Universidad. Estas áreas deberán hacer la búsqueda de la información del titular, en bases de datos tanto magnéticas como físicas, y dar respuesta al requerimiento interno *dentro de los tiempos estipulados por ley*, contados a partir de la recepción del requerimiento. Si el administrador y los encargados de la base de datos no han podido dar respuesta en el tiempo establecido, deberán enviar justificación al Oficial de Seguridad de la Información y Datos Personales, quien informará al titular el plazo de dos días hábiles más para poder dar respuesta. Si es reclamo, se debe: • Dejar claro en el envío de la solicitud que es un “reclamo en trámite" y el motivo de este. • Solicitar el no uso de los datos del presente reclamo hasta que el reclamo sea decidido.	Oficial de Seguridad de la Información y Datos Personales
5	RECLAMO: Actualización Corrección	Si la solicitud fue catalogada como reclamo de actualización y/o corrección, el administrador y encargado de la base de datos personales deben: a. Luego de hacer la búsqueda de información, una vez encontrado el registro con la información del titular no podrá hacerse ningún tipo de tratamiento de datos personales diferente de su almacenamiento en un tiempo no mayor al estipulad por ley. b. En los casos en que haya dudas sobre la actualización de los datos, podrán solicitarle al Oficial de Seguridad de la Información y Datos Personales que se comunique con el titular, para que este indique cuál dato es el que se debe actualizar o corregir. c. Si transcurridos dos meses desde la fecha del reclamo el titular no ha presentado la información requerida, se entenderá que ha desistido del reclamo. El oficial de seguridad de la información y	Oficial de Seguridad de la Información y Datos Personales Administradores, y estos, a su vez, a los encargados de la base de datos

		datos personales cerrará el caso, según sea el canal, e indicará la causa del cierre. d. Una vez recibido el reclamo completo, el Oficial de Seguridad de la Información y Datos Personales enviará un correo a el Administrador, y estos, a su vez, a los Encargados de la base de datos personales, cuando se presenta un “reclamo en trámite" y el motivo de este, en un término no mayor a lo estipulado por ley; dicho dato no podrá usarse bajo ninguna circunstancia sino hasta que el reclamo sea decidido. e. El Administrador y los Encargados de la base de datos personales (por notificación de los administradores) actualizan o rectifican los datos según la solicitud descrita por el titular en el reclamo. f. El Administrador y los Encargados de la base de datos personales (por notificación de los administradores) deben remitir al, Oficial de Seguridad de la Información y Datos Personales la prueba de dicha acción.	
6	RECLAMO: Supresión	El Administrador y los Encargados de la base de datos personales deben: a. Luego de hacer la búsqueda de información, una vez encontrado el registro con la información del titular no podrá hacerse ningún tipo de tratamiento de datos personales de este titular diferente de su almacenamiento, en un término no mayor a lo estipulado por ley luego de haber recibido el reclamo por parte del Oficial de Seguridad de la Información y Datos Personales y/o Titular. a. En los casos en que haya dudas sobre la supresión de dicho dato, podrán solicitarle al Oficial de Seguridad de la Información y Datos Personales que se comunique con el titular, para que indique cuál dato es el que se debe suprimir (por ejemplo: correo, teléfono, dirección u otros). b. Si transcurridos dos meses desde la fecha del reclamo el titular no ha presentado la información requerida, se entenderá que ha desistido del reclamo. El Oficial de Seguridad de la Información y Datos Personales deberá cerrar el caso en el sistema e indicar la causa del cierre. c. Una vez recibido el reclamo completo, el Oficial de Seguridad de la Información y Datos Personales enviará un correo a el Administrador, y estos, a su vez, a los Encargados de la base de datos personales, avisando que dicho dato presenta un “reclamo en trámite" y el motivo de este, en un término no mayor a lo estipulado por ley, y ese dato no podrá usarse bajo ninguna circunstancia hasta que el reclamo sea decidido. d. La solicitud de supresión total de la información no procederá cuando el titular tenga el deber legal o contractual de permanecer en las bases de datos. • Los datos no se pueden borrar en su totalidad, ya que pueden ser requeridos para fines estadísticos y acordes a la actividad	Oficial de Seguridad de la Información y Datos Personales Administradores, y estos, a su vez, a los encargados de la base de datos

		desarrollada por La Universidad, en virtud de su objeto social. Se debe validar con el Oficial de Seguridad de la Información y Datos Personales la viabilidad de la supresión del dato. e. Luego de identificar los datos, se procederá a realizar la técnica de sustitución. Se procederá a reemplazar los datos personales a que haya lugar con otros valores no relacionados con los datos originales, pero manteniendo coherentes los datos (Se define de la siguiente forma: 1. Correo: Sustituir por: supresiondato@habeasdata.com 2. Celular o número telefónico: 0000000000 **En el caso que se presente una supresión frente a los datos de un titular que se identifique está en el sistema de información Salesforce, se debe proceder a realizar la activación y desactivación de los check relacionados al cumplimiento de habeas data.* f. Cuando haya dudas sobre la procedencia de la supresión del dato, deberá informar Oficial de Seguridad de la Información y Datos Personales, y, en conjunto, tomar la decisión de la supresión o no del dato personal. g. Deberá remitir al Oficial de Seguridad de la Información y Datos Personales la prueba de dicha acción.	
7	RECLAMO: Revocatoria	El Administrador y los Encargados de la base de datos personales deben: a. Luego de hacer la búsqueda de información y una vez encontradas las autorizaciones de las cuales el Titular hace el reclamo, se deben analizar las finalidades autorizadas. • Según el sistema de información que contenga la autorización del titular, se procederá a revocar la finalidad que presenta el titular en el reclamo. b. El Administrador y los Encargados de la base de datos personales deben remitir al Oficial de Seguridad de la Información y Datos Personales la prueba de dicha acción. Nota: no podrá hacerse una revocatoria completa de la autorización del tratamiento de datos personales cuando exista obligación legal por parte de La Universidad de conservar los datos del titular.	Oficial de Seguridad de la Información y Datos Personales Administradores, y estos, a su vez, a los encargados de la base de datos
8	Respuesta interna	Consulta: en caso de que se imposibilite dar respuesta en los tiempos establecidos anteriormente, el Oficial de Seguridad de la Información y Datos Personales deberá informar al titular el día de vencimiento del primer término, así como las dificultades que se presentaron, e informar que se le dará respuesta en los *cinco días hábiles* siguientes al vencimiento del primer término. Reclamo: en caso de que se imposibilite dar respuesta en los tiempos establecidos anteriormente, el Oficial de Seguridad de la Información y Datos Personales deberá informar al titular el día de vencimiento del primer término, así como las dificultades que se presentaron, e	Oficial de Seguridad de la Información y Datos Personales Administrador de Base de Datos Personales.

		informar que se dará respuesta en los *ocho días hábiles* siguientes al vencimiento del primer término. El Administrador de la base de datos personales debe enviar la respuesta al Oficial de Seguridad de la Información y Datos Personales y adjuntar la evidencia de la actividad realizada. Si, por el contrario, no se recibe respuesta por parte del Administrador de la Base de Datos Personales, el Oficial de Seguridad de la Información y Datos Personales deberá elevar el caso al jefe inmediato o, en su defecto, al Comité Estratégico en Seguridad y Privacidad de los Datos Personales y la Información.	
9	Respuesta externa	Una vez se haya resuelto la consulta o el reclamo, se enviará comunicado al titular o el tercero, a través del medio dispuesto para tramitar los requerimientos. La respuesta al titular o el tercero es el resultado del trámite interno realizado. **En caso de que no se pueda generar la supresión del dato, se debe generar respuesta al titular informando el motivo de no poder suprimir completamente los datos personales.*	Oficial de Seguridad de la Información y Datos Personales
10	Archivar	Se deben archivar todas las comunicaciones realizadas en la solicitud, para posteriores consultas.	Oficial de Seguridad de la Información y Datos Personales

Capítulo VI. Procedimiento para el tratamiento de datos personales

Objetivo

Establecer directrices para toda la comunidad rosarista en cuanto a las responsabilidades y las obligaciones que se tienen en el manejo adecuado de la información personal, así como en su recolección, almacenamiento, uso, circulación y disposición final.

Procedimiento para la recolección de datos personales

La Universidad realiza la recolección de la información personal, a través de los siguientes medios. Sin limitarse a ellos:

- Aplicativos y Formularios virtuales: Cuando ingresa a los diferentes servicios soportados por sistemas de información y aplicaciones.
- Chat: Cuando se solicita información a través de medios virtuales.
- Llamadas telefónicas: En consulta por vía telefónica se capturan datos personales, incluida la grabación de la llamada.
- Formularios físicos: Cuando acceden a algunos de nuestros servicios por los canales presenciales, se obtienen sus datos personales a través de formularios físicos, encuestas dirigidas a la comunidad académica, entre otros.
- Cámaras de video: Cuando se encuentra en las instalaciones de La Universidad con el propósito de velar por la seguridad de los bienes y las personas.
- Sistemas biométricos: Para algunos servicios, La Universidad ha adoptado sistemas de identificación biométrica.

La Universidad garantiza que, en los instrumentos de recolección de información personal, se solicita la autorización para el tratamiento de datos personales, de manera libre, previa, expresa y en general, cuenta con todos los requisitos establecidos en las disposiciones legales para la protección de datos personales.

Conforme a lo anterior, la recolección de datos personales debe obedecer a los principios de necesidad y de finalidad; es decir, no se pueden solicitar datos personales que no sean necesarios para el proceso que se requiera adelantar. Su recolección debe limitarse a los datos personales que son pertinentes y adecuados a la finalidad para la cual van a ser recolectados. Ningún colaborador de La Universidad podrá solicitar información personal que no se encuentre relacionada con las finalidades de la recolección, las que, a su vez, La Universidad ha definido en la Política de Tratamiento de Datos Personales.

A continuación, se enuncian los pasos principales para garantizar un adecuado procedimiento al recolectar datos personales:

a. El responsable de la recolección de datos personales debe verificar que el medio que va a utilizar para recolectar información tiene un sistema que permita guardar la evidencia de la autorización otorgada por parte del titular. Si no cuenta con dicho sistema, debe hacer la solicitud al oficial de seguridad de la información y datos personales, quien verificará y direccionará según sea la solicitud.
b. El responsable de la recolección de los datos personales debe asegurarse de informar al titular, sea por vía oral o escrita, o por conducta inequívoca, lo siguiente:
    1. El tratamiento al cual serán sometidos sus datos personales y la finalidad.
    2. Si se deben solicitar datos sensibles, informar que no está obligado a autorizar su tratamiento, e informar de forma previa y explícita cuáles de los datos por recolectar son sensibles y cuál será su tratamiento.
    3. Los derechos que le asisten como titular.
    4. Los canales habilitados por La Universidad para ejercer el derecho de *hábeas data*.
    5. La autorización para el tratamiento de datos personales deber ser diligenciada por parte del titular de la información, en caso de ser menor de edad, por quien ejerza la patria potestad o por su representante legal.
    6. Cuando el titular autoriza el tratamiento, el responsable de la recolección debe conservar prueba de la autorización otorgada por parte del titular, para su posterior consulta.

Procedimiento para el almacenamiento de la información personal

Las formas actuales que La Universidad tiene para el almacenamiento de la información y para el control del cumplimiento de la normativa en protección de datos personales son las siguientes:

Formas de almacenamiento de la información

Procedimiento para el uso de la información personal

Los usos de la información personal que hace La Universidad se encuentran descritos en la Política de Tratamiento de Datos Personales; en caso de que algún área identifique nuevos usos diferentes de los descritos en la Política, debe informar, al Oficial de Seguridad de la Información y Datos Personales a través

del correo de habeasdata@urosario.edu.co el nuevo uso que se quiere hacer y revisar cuáles son los documentos que se deben actualizar.

a. En caso de que un área diferente de la que recolectó inicialmente el dato personal requiera utilizar los datos personales que se han obtenido, ello se podrá hacer siempre y cuando en la autorización se haya informado sobre dicho uso, se encuentre en la Política de Tratamiento de Datos Personales o sea un uso previsible por el tipo de servicios que ofrece La Universidad.
b. Cada área debe garantizar que en las prácticas de reciclaje de documentos físicos no se divulguen información confidencial ni datos personales. Por lo anterior, no se podrán reciclar hojas de vida, ni títulos académicos, ni certificaciones académicas o laborales, ni resultados de exámenes médicos ni ningún documento que contenga información que permita identificar a una persona.
c. En caso de que un administrador o un encargado haya facilitado datos personales o bases de datos a algún área para un fin determinado, el área que solicitó los datos personales no podrá utilizar dicha información para una finalidad diferente de la relacionada en la Política de Tratamiento de Datos Personales; al finalizar la actividad, es deber del área que solicitó la información eliminar la base de datos o los datos personales utilizados evitando el riesgo de desactualización de información o casos en los cuales durante ese tiempo un titular haya presentado algún reclamo. Y si quiere usar nuevamente esa información, deberá solicitarle al administrador o el encargado de la base de datos dicha información, puesto que los datos pudieron ser modificados.
d. Los colaboradores no podrán tomar decisiones que tengan un impacto significativo en la información personal, o que tengan implicaciones legales, con base exclusivamente en la información que arroja el sistema de información, por lo que deberán validar la información a través de otros instrumentos físicos o de manera manual, y, si es necesario, de manera directa por parte del titular del dato, en los casos en que así sea necesario.

Procedimiento para la circulación de la información personal

Las áreas que soliciten la entrega de bases de datos con información personal deberán llevar a cabo el siguiente procedimiento:

1. La solicitud la debe remitir al correo del administrador de la base de datos personales (ANEXO I Administradores de bases de datos personales) y describir:
    a. Los datos personales que necesita.
    b. La finalidad del uso de los datos personales.
    c. Relacionar el responsable de la recepción de la base de datos personal y el correo electrónico para el envío de la información personal o la base de datos.
    d. La fecha en que se realizaría la actividad para la cual se requieren los datos.
    e. El cargo de quien será el administrador de la base de datos entregada. En caso de requerir compartir la base de datos a un tercero, realizar la solicitud del anexo de transmisión de datos a la Dirección Jurídica a través de URLegal.
    f. La fecha de eliminación de la base de datos personales al finalizar la actividad, y la prueba de dicha eliminación.

El Administrador de la Base de Datos Personales deberá evaluar el requerimiento teniendo en cuenta los siguientes aspectos:

a. Evaluar si la solicitud es pertinente a los propósitos que se persiguen.
b. Identificar si para los propósitos que se facilita y se requiere la información, se pueden suprimir los datos de identificación para no identificar al titular del dato.

c. Informar a la persona que solicita la información, que no se le puede dar uso diferente a los relacionados en la Política de Tratamiento de Dato Personal, y que solo será para el propósito perseguido.
d. Si considera que no está fundada su solicitud, no suministrará la base de datos o la información personal.
e. Informar al correo electrónico suministrado las razones por las cuáles no se puede suministrar dicha información personal.

En caso de discrepancias, tanto la persona que solicita la información como el Administrador de Base de Datos Personales podrán solicitar al Oficial de Seguridad de la Información y Datos Personales, a través del correo habeasdata@urosario.edu.co apoyo para resolver dicho asunto.

Las formas actuales que La Universidad tiene para la circulación de la información y el control del cumplimiento de la normativa en protección de datos personales son las siguientes:

Forma de circulación de la información	Control - Cumplimiento de la Ley 1581 de 2012
Transmisión Nacional	Realizar Anexo de transmisión de datos personales.
Transmisión Internacional	Realizar Anexo de transmisión de datos personales.
Transferencia Nacional	Realizar Anexo de transferencia de datos personales.
Transferencia Internacional	Realizar Anexo de transferencia de transferencia de datos, o solicitar declaración de conformidad ante la SIC, si no es un país catalogado como seguro.
Representante Legal	Si es el padre de un estudiante, deberá demostrarlo a través del documento de identidad y registro civil que demuestren el parentesco. Si se trata de un tercero, que actúa en nombre del titular, presentar el poder o la autorización para la entrega de la información.
Tercero	Aportar la autorización que suministró el titular para entregar dicha información.
Autoridad Judicial	Orden judicial.
Autoridad Administrativa	Disposición legal o acto administrativo.
Entre Unidades internas de la Universidad	Realizar correo incluyendo lo descrito en el procedimiento para la circulación de la información personal

Las áreas que, en virtud de los procesos ya preestablecidos por La Universidad deban circular internamente la información en virtud de su actividad habitual, deberán tomar medidas apropiadas para proteger la información.

Procedimiento para la disposición final de la información personal

Las políticas para la disposición final de la información personal en bases de datos físicas son las dispuestas en la Política de Gestión Documental de la Universidad. Para la información personal en bases de datos magnéticas se deberá hacer la solicitud al Dirección de Tecnología y Comunicaciones, y este dará los lineamientos correspondientes. No obstante, al momento de establecer o revisar las reglas para la disposición final de la información, el administrador de la base de datos, junto con el Área de Gestión Documental, deberá observar los principios de finalidad y de temporalidad de la información. Es decir, no se podrán destruir las autorizaciones para

el tratamiento de datos personales, independientemente del formato en que se encuentre, si la información de dicho titular de la información aún se encuentra en uso; así mismo y en relación con la información física que vaya a ser eliminada, se deberán de tener en cuenta, las siguientes recomendaciones:

- Asegúrese de que el lugar que almacena los documentos que pretende eliminar cuenta con medidas de seguridad eficaces frente a posibles intromisiones exteriores.
- Los documentos no deben permanecer al descubierto, en el exterior del edificio, no deben amontonarse en lugares de paso, ni en espacios abiertos accesible a quién no debe conocer esos datos.
- Todo papel u otro soporte físico que contenga datos personales y que vaya a ser arrojado al recipiente de basura, deberá previamente ser destruido de forma que la información no sea reutilizada o legible.
- El papel que se pretenda reciclar no debe contener datos personales, de ser así debe ser destruido, no reconstruido.
- Todo papel u otro soporte físico que contenga datos personales solo podrá ser almacenado y destruido por las personas que estén debidamente autorizadas para ello.

Capítulo VII. Procedimiento de generación de la autorización para el tratamiento de datos personales según sea el caso

Objetivo

Establecer la estructura de la autorización para el tratamiento de datos personales según los datos a recolectar por parte de los administradores de las bases de datos personales o quienes lideran actividades que impliquen captura de datos.

Autorización expresa

La autorización expresa, implica que La Universidad, de manera detallada, le informe al titular el alcance del uso de los datos personales, así como otros requisitos detallados en la ley; así mismo, se le debe poder consultar con posterioridad. Dicha autorización debe contener, como mínimo:

a. El responsable del tratamiento de los datos personales. (Nombre o razón social)
b. Finalidades del tratamiento de los datos.
c. Información sobre el uso que tendrán los datos recolectados.
d. Derechos que le asisten como titular del dato y forma de ejercerlos
e. Medio o mecanismos para consultar la Política de Tratamiento de Datos Personales.

Algunos casos de autorización expresa:

La autorización expresa se debe utilizar en todos los medios de captura de datos personales que administra La Universidad; algunos de estos casos son:

a. Cuando se recogen datos personales a través de un formulario *web*, dando clic en "Autorizo el tratamiento de mis datos personales a la Universidad del Rosario bajo su Política de Tratamiento de Datos Personales", o en el botón Enviar. De esta forma el titular está autorizando de manera expresa el tratamiento de los datos personales.
b. Cuando los titulares diligencian formularios físicos o firman el documento físico, donde se encuentra la autorización para el tratamiento de datos personales, se autoriza de manera expresa el tratamiento de sus datos personales.
c. Cuando se hace una llamada telefónica La Universidad y se almacena la grabación de dicha llamada, con el fin de conservar la autorización para el tratamiento de datos personales.
d. Cuando se recogen datos personales de niños y adolescentes para su tratamiento por parte de La Universidad, con fines de oferta académica.

e. Cuando se recogen datos personales sensibles, caso en el cual se le advierte del carácter facultativo a las preguntas que versen sobre este tipo de información, y de análisis de necesidad de solicitar dicha información y el titular expresamente lo autoriza.

Autorización expresa reforzada

La autorización expresa reforzada se debe adoptar en los casos en que La Universidad solicite datos personales sensibles, o datos personales de niños, niñas y adolescentes.

La autorización expresa reforzada debe contener los siguientes elementos:

a. El responsable del tratamiento de los datos personales. (Nombre o razón social)
b. Finalidades del tratamiento de los datos.
c. Informar al titular que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento
d. Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso.
e. Informar el carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas traten sobre datos sensibles o sobre los datos de niños o adolescentes.
a. Información sobre el uso que tendrán los datos recolectados.
b. Derechos que le asisten como titular del dato y forma de ejercerlos.
c. Medio para consultar la Política de Tratamiento de Datos Personales.

Autorización para el tratamiento de datos personales de niñas, niños y adolescentes

a. En los casos en que se soliciten datos personales a un adolescente menor de edad, con el fin de brindarle información sobre la oferta académica, La Universidad entiende que cuenta con la autorización del menor de edad, en los términos del Concepto 17-10463 de la Superintendencia de Industria y Comercio: “Para el tratamiento de los datos de contacto de los adolescentes por parte de las instituciones educativas y exclusivamente con la finalidad de brindarles información sobre sus programas, es posible que la autorización previa y expresa sea otorgada directamente por el adolescente. - Se entiende que el adolescente ha dado su autorización para el tratamiento de sus datos personales cuando: (i) sea por escrito; (ii) sea oral o (iii) mediante conductas inequívocas, es decir, aquellas que no admiten duda o equivocación, del titular que permitan concluir de forma razonable que otorgó la autorización. El silencio no puede asimilarse a una conducta inequívoca. Cuando se trate de datos personales sensibles la autorización para el tratamiento de tales datos deberá hacerse de manera explícita”.
b. La regla anterior aplica exclusivamente para menores que se encuentren en el rango de edad de 14 a 17 años. Si la edad es inferior al rango establecido, La Universidad deberá obtener la autorización y los datos a través del representante legal.
c. Los datos personales que se soliciten a los menores de edad en calidad de estudiantes activos de La Universidad se encuentran legitimados dentro de los servicios educativos que la institución presta al titular; no obstante, en la autorización del titular al ingresar por primera vez en La Universidad deberá indicar que el titular cuenta con la autorización del representante legal para el uso de la información por parte de La Universidad.

Autorización para el tratamiento de datos personales sensibles

La Universidad debe recolectar los datos personales sensibles en los casos que sean estrictamente necesarios para la efectiva prestación de los servicios académicos y administrativos que sean requeridos.

a. Cuando el titular ha dado la autorización expresa para su tratamiento, salvo si la ley establece que no es necesario otorgar dicha autorización.

b. Cuando el tratamiento sea necesario para proteger intereses vitales del titular, y si este se encuentra física o jurídicamente incapacitado, caso en el cual se le solicitará la autorización al representante legal.
c. Cuando el tratamiento sea efectuado en el curso de actividades legítimas y con las debidas garantías por parte de La Universidad.
d. Cuando el tratamiento se refiera a datos que sean necesarios para el reconocimiento, el ejercicio o la defensa de un derecho en un proceso judicial.
e. Cuando el tratamiento tenga finalidad histórica, estadística o científica. En este caso, La Universidad ha dispuesto las medidas conducentes a la supresión de la identidad de los titulares.

Autorización por conductas inequívocas

La autorización por conductas inequívocas puede darse de diferentes formas, y puede variar según la relación que La Universidad tenga con el titular del dato.

Algunos casos de autorización por conductas inequívocas son:

a. Cuando usted ingresa a las instalaciones de La Universidad está aceptando mediante conductas inequívocas la autorización para el tratamiento de datos personales a La Universidad, no obstante, el aviso de video vigilancia le informa la finalidad de la captura de su imagen.
b. Cuando usted envía información personal a un correo electrónico institucional de La Universidad, autoriza el tratamiento de sus datos personales para el trámite que desea realizar.
c. Cuando se soliciten datos personales que son previsibles producto de una relación contractual vigente con La Universidad.

La Universidad deberá establecer cuáles actividades en las que se soliciten datos personales se consideran conductas inequívocas, y deberá actualizar la Política de Tratamiento de Datos Personales incorporando dicha novedad.

Controles para implementar en la autorización por conductas inequívocas

La Universidad deberá propender por obtener de manera expresa la autorización para el tratamiento de datos personales por parte del titular. Sin perjuicio de lo anterior, los controles que La Universidad deberá tener en cuenta cuando la autorización se genere por conductas inequívocas son los siguientes:

Conducta inequívoca	Control - Cumplimiento de la Ley 1581 de 2012
Ingreso a las instalaciones de la Universidad.	Incorporar en lugares visibles el aviso de videovigilancia.

Autorización suministrada por un tercero

a. En los casos en que La Universidad trate datos personales, suministrados por un tercero, con quien La Universidad tenga convenio, deberá verificar en la etapa de negociación, que en el contrato quede el clausulado de la responsabilidad de solicitud de autorización para el tratamiento de datos personales.
b. En los casos en que un tercero le solicite datos personales a La Universidad, esta deberá solicitarle a dicho tercero, el documento que acredite que se encuentre autorizado para solicitar dicha información.
c. Si un tercero desea consultar las calificaciones de un estudiante o egresado deberá solicitar la autorización del titular del dato, es decir, del estudiante, para su respectiva consulta. Por lo anterior y conforme a lo establecido en el concepto 14-268304 de la Superintendencia de Industria y Comercio, las calificaciones se entregarán: i) Al estudiante, en ejercicio de su derecho de acceso y consulta, ii) Un tercero, previa

obtención de la autorización del estudiante, donde sea manifestada la finalidad de uso de dicha información.

Casos en los cuales NO se requiere autorización

Existen casos en los cuales no es necesario solicitar la autorización del titular del dato en la recolección o la circulación, respectivamente, ya sea porque:

a. Existe una disposición legal que obliga a la solicitud de dicho dato o información personal.
b. Cuando sea el representante legal del menor de edad y solicite dicha información, y responda y respete el interés superior del adolescente.
c. Cuando se trate de datos personales públicos.
d. Cuando la información sea solicitada por una entidad pública o administrativa en ejercicio de sus funciones.
e. Cuando exista una orden judicial.
f. En casos de urgencia médica o sanitaria.
g. Cuando se trate de datos personales relacionados con el registro civil de las personas.
h. Cuando el tratamiento de los datos sea autorizado por la ley, para fines históricos, estadísticos o científicos.

En todo caso, el colaborador encargado de la recolección o la circulación del dato donde no sea obligatoria la autorización para el tratamiento de datos personales, en los casos aquí establecidos, deberá tomar las medidas necesarias para validar que el tercero a quien se le va a suministrar el dato se encuentra plenamente facultado para recibir dicha información, así se trate de una entidad administrativa en ejercicio de sus funciones.

Datos personales recolectados antes de la entrada en vigencia de la Ley 1581 de 2012 y sus decretos reglamentarios

Los Administradores de las Bases de Datos Personales deberán seguir las siguientes reglas con el fin de obtener la autorización para el tratamiento de datos personales de los datos obtenidos antes de la Ley 1581 de 2012 y sus decretos reglamentarios:

a. Para los datos personales recogidos antes del 27 de junio del 2013, se formalizó la autorización del tratamiento de datos personales conforme al aviso que La Universidad publicó, en cumplimiento del artículo 10 del Decreto 1377 de 2013. Por lo anterior, internamente el responsable de la base de datos deberá identificar los titulares a quienes se les solicitaron los datos personales generados antes de esa fecha, y clasificará o identificará dichos datos conforme a este tipo de forma de obtener la autorización.
b. Los datos personales o las bases de datos que se generaron a partir del 28 de junio de 2013 y hasta el día de hoy deberán contar con la autorización expresa del titular para el uso de dicha información, e identificar a los titulares de los datos personales.
c. El responsable de la base de datos personales, con apoyo del Oficial de Seguridad de la Información y Datos Personales, así como del Comité Estratégico en Seguridad y Privacidad de los Datos Personales y la Información, deberá establecer un plan de acción para formalizar los datos personales que aún no tienen autorización, por lo cual podría tomar algunas de las siguientes medidas:
    1. Identificar si dichos datos personales no están dentro de las excepciones según las cuales no es necesaria la autorización para el tratamiento de datos personales.
    2. Suprimir los datos personales, siempre y cuando no haya una disposición que exija su conservación o se incumpla algún compromiso legal.
    3. Solicitar la autorización para el tratamiento de datos personales por cualquier medio, y de modo que se pueda probar con posterioridad que la persona ha suministrado la autorización.

Capítulo VIII. Procedimiento de solicitud y conservación de autorizaciones para el tratamiento de datos personales

Objetivo

Definir los pasos necesarios para la solicitud y la conservación de la autorización por parte de los Administradores de Bases de Datos Personales, quiénes lideren actividades que impliquen captura de datos o los encargados de la información de datos personales de La Universidad, a través de los medios establecidos por esta.

Alcance

Inicia con la solicitud de la autorización para el tratamiento de datos personales al titular y termina con la conservación de la autorización en carpeta física o digital, para su posterior consulta.

Políticas

- Todos los formatos físicos, formularios digitales que se encuentren en páginas *web*, aplicaciones móviles, *chat* y *videochat* de La Universidad, así como la recepción de llamadas telefónicas donde se capturen datos personales, deberán contener la autorización para el tratamiento de datos personales.
- Los Administradores de Bases de Datos Personales y quienes lideren actividades que impliquen captura de datos tienen la obligación de solicitar la autorización y conservar la evidencia de la misma siguiendo los parámetros que se establecen en el presente procedimiento.
- El Administrador o encargado de Bases de Datos Personales, coordinaran la aplicación de este procedimiento, y gestionarán las autorizaciones generadas en formularios físicos, digitales y audios para que se encuentren bajo la custodia, la conservación y la disposición final, de acuerdo con los lineamientos o las políticas establecidos en La Universidad o de terceros encargados de datos personales.

Descripción del procedimiento solicitud y conservación autorizaciones

¿Qué es una autorización para el tratamiento de datos personales?

Es el consentimiento que da cualquier persona para que La Universidad, la cual es responsable del tratamiento de la información, pueda utilizar los datos personales del titular. La ley 1581 de 2012 indica que "el consentimiento debe ser previo, expreso e informado"; es decir, que el dueño de la información autorice y sepa para qué y cómo se utilizará dicha información.

Descripción del procedimiento

ID	Actividad	Descripción de la actividad	Responsable
1	Solicitar la autorización	Deberá solicitar al titular la autorización para el tratamiento de los datos personales por parte de La Universidad; esta autorización puede ser: 1. Por escrito. 2. De forma oral. 3. Mediante conducta Inequívoca. La autorización del tratamiento de datos personales que se van a solicitar al titular por parte del responsable de la captura de los datos debe ser:	Administrador de la base de datos personales o Líder de la actividad que implique la captura de datos Encargados bajo las disposiciones entregadas por el administrador de la

		1. **Previa**: es decir, que se debe solicitar la autorización antes de recolectar cualquier dato personal. 2. **Expresa**: es decir, que se pueda evidenciar fácilmente su autorización y que no quede duda de su autorización. 3. **Informada**: es decir, informarle lo siguiente: a. El responsable del tratamiento de los datos personales. (Nombre o razón social) b. Finalidades del tratamiento de los datos. c. Informar al titular que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento d. En caso que aplique: Informar al titular de forma explícita y previa, además de los requisitos generales de la autorización para la recolección de cualquier tipo de dato personal, cuáles de los datos que serán objeto de Tratamiento son sensibles y la finalidad del Tratamiento, así como obtener su consentimiento expreso. e. En caso que aplique: Informar el carácter facultativo de la respuesta a las preguntas que le sean hechas, cuando estas traten sobre datos sensibles o sobre los datos de niños o adolescentes. f. Información sobre el uso que tendrán los datos recolectados. g. Derechos que le asisten como titular del dato y forma de ejercerlos. h. Medio para consultar la Política de Tratamiento de Datos Personales.	base de datos personales.
2	Conservar la autorización	Deberá conservar la prueba de la autorización, de acuerdo con lo estipulado en la Política de Gestión Documental de la Universidad, otorgada por el titular, para su posterior consulta. La disposición final de la autorización para el tratamiento de datos personales se regirá por los tiempos establecidos en las tablas de retención documental de La Universidad, o se procederá a actualizar dichos tiempos en caso de que, por ley o distintos motivos, se requiera ampliar o disminuir el tiempo de retención. El administrador de la base de datos personales deberá verificar la disposición final del expediente tomando en cuenta la tabla de retención; en caso de que sea su destrucción, debe verificar el cumplimiento de la Política de Gestión Documental de La Universidad. No se podrá destruir la autorización si los datos personales del titular aún se encuentran en uso.	Administrador de la base de datos personales Líder de la actividad que implique la captura de datos Encargados bajo las disposiciones entregadas por el administrador de la base de datos.

Instrucciones dirigidas a los administradores o los encargados del tratamiento del formato físico

Cuando el administrador o el encargado reciban por parte de La Universidad el formato físico con la autorización firmada por parte del titular, el administrador o el encargado deberán responder por su administración, su custodia y su conservación durante el tiempo que tengan la información en sus instalaciones.

Una vez cumplidas las condiciones para la devolución de los formatos físicos, el administrador o el encargado a través del administrador procederán a devolver dicho formato al Área de Gestión Documental, a través de la Mesa de Servicios 2030 de La Universidad observando las siguientes reglas:

a. Se deben organizar por paquetes, por mes y año;
b. Se deben archivar en carpeta Yute; la cantidad de documentos (folios) no puede exceder las 200.
c. Cada capeta debe estar codificada y con la descripción de su contenido.

Capítulo IX. Procedimiento para el tratamiento de datos personales sensibles

Objetivo

Establecer las directrices para el tratamiento de datos personales sensibles.

¿Cuáles son los datos personales sensibles?

Los datos personales sensibles son todos los que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación y afectar su dignidad. Algunos datos personales sensibles son: los que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, a organizaciones sociales o de derechos humanos, o que promuevan intereses de cualquier partido político o avalen los derechos y las garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual y los datos biométricos (huella dactilar). Por lo anterior, la ley y las buenas prácticas exigen requisitos adicionales en cuanto a su recolección, sus usos y su conservación respecto a otros tipos de datos personales.

Políticas para la captura y el uso de imágenes

1. En los eventos realizados por La Universidad deberá incorporarse en el registro de asistencia, o en la inscripción a dicho evento, la autorización para el tratamiento de datos personales, incluyendo la imagen del titular en formato de fotografía y video. Para esto debe utilizar las autorizaciones validadas por la Universidad.
2. En caso de que sea imposible obtener la autorización por estos medios, se deberá incorporar un aviso en las instalaciones del evento, o comunicarlo de forma verbal o, a través de pantallas, informar la captura y la divulgación de la imagen para fines de difundir el evento.
3. En los casos en que sea complejo obtener la autorización expresa o por conductas inequívocas del titular del dato, La Universidad deberá capturar las imágenes en planos en los que sea difícil identificar a las personas.
4. La autorización para el uso de imagen debe dejar en claro, de manera clara y expresa, los usos y el tipo de tratamiento que se le dará a la imagen, así como los derechos que tiene el titular del dato.
5. Las imágenes que sean usadas o se capturen para fines comerciales y publicitarios deberán contar con autorización expresa y escrita para el tratamiento de datos personales y derechos de autor.
6. Las imágenes que se divulguen a través de los canales de comunicación que tiene La Universidad habilitados deberán tener autorización para el tratamiento de datos personales y de derechos de autor.

Analizar la necesidad de recolección de datos personales sensibles

El responsable que esté liderando el proceso en el cual debe solicitar datos personales de carácter sensible deberá realizar la siguiente evaluación:

a. Justificar la necesidad y la pertinencia de la solicitud de cada dato personal sensible al proceso que se requiere; es decir, por qué La Universidad requiere solicitar dicho dato personal, y si es proporcional para el propósito que se persigue.

b. Indicar si existe disposición legal que exija su solicitud por parte de La Universidad.
c. En caso de que no sea obligatorio, por alguna disposición legal, la solicitud de dicho dato personal sensible, indicar qué efectos traería para el proceso o para La Universidad no solicitar ese dato personal sensible.
d. Indicar qué efectos tendrían para La Universidad y para el titular la exposición o la divulgación de ese dato personal sensible.

Toma de decisión sobre el tipo de dato personal sensible por recolectar

De acuerdo con los resultados generados por el análisis que haga el colaborador, se deberán tener en cuenta los siguientes criterios:

a. En caso de que exista una disposición legal que exija su recolección, puede proceder con la solicitud del dato personal sensible de forma obligatoria.
b. En caso de que no exista una disposición legal obligatoria, y sin ese dato no se pueda avanzar con el proceso interno que La Universidad necesita cumplir, podrá solicitar dicho dato personal, pero no de forma obligatoria.
c. Si no hay consecuencias legales o administrativas por no obtener ese dato personal sensible, no se lo deberá solicitar.

En la recolección de datos personales sensibles

En la recolección de datos personales de carácter sensible se deben observar las siguientes reglas:

a. Se deben recolectar datos personales sensibles en los casos en que ellos sean estrictamente necesarios para la efectiva prestación de los servicios académicos y administrativos requeridos por la comunidad académica.
b. Cuando los datos sean solicitados en formato físico, deberán señalarse aquellos espacios donde se solicite consignar sobre dichos datos su no obligatoriedad.
c. Cuando los datos personales sean solicitados en formulario digital, el colaborador que haga la solicitud deberá verificar que las casillas sobre preguntas que versen sobre datos sensibles no se encuentren como obligatorias.
d. Cuando los datos personales sensibles se soliciten mediante una llamada telefónica, La Universidad deberá informar el carácter facultativo a las preguntas que versen sobre este tipo de datos, además de conservar el audio con la autorización para el tratamiento de datos personales.
e. En los casos en que por ley sea obligatoria la solicitud de datos personales sensibles, las casillas se deberán diligenciar de manera también obligatoria.

Solicitud de autorización para el tratamiento de datos personales sensibles

En los instrumentos en los que se soliciten datos personales sensibles, se deberán tener en cuenta las siguientes reglas:

a. Se debe incorporar la autorización reforzada para el tratamiento de datos personales.
b. Dicha autorización debe cumplir con el procedimiento para la solicitud y la conservación de autorizaciones.
c. Informar al titular que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento.
d. Informarle dentro de la autorización cuál dato personal es considerado sensible, además de las finalidades de la recolección.
e. Cumplir con las demás disposiciones relacionadas a la autorización de datos sensibles que se cita en el presente manual.

Casos en los que no es necesaria la autorización para el tratamiento de datos personales sensibles

En los siguientes casos, conforme a las disposiciones legales, no es obligatorio solicitar la autorización para el tratamiento de datos personales sensibles:

a. Cuando la ley establezca que no es necesario otorgar dicha autorización.
b. Cuando el tratamiento sea necesario para proteger intereses vitales del titular, y este se encuentre física o jurídicamente incapacitado, caso en el cual se le solicitará la autorización al representante legal, al apoderado, al tutor u otro.
c. Cuando el tratamiento se refiera a datos necesarios para el reconocimiento, el ejercicio o la defensa de un derecho en un proceso judicial.

En todo caso, en los casos en que no sea necesario solicitar la autorización para el tratamiento de datos personales sensibles, La Universidad deberá, como medida preventiva y en los casos en que sea posible, solicitar la autorización del tratamiento de datos personales.

Limitaciones en los usos de los datos personales sensibles

a. Los usos de los datos personales sensibles deben obedecer estrictamente a las finalidades consignadas en la autorización para el tratamiento de datos personales.
b. En caso de que se evidencie un nuevo uso de los datos personales sensibles recolectados, La Universidad deberá solicitar una nueva autorización para el tratamiento de datos personales.

Circulación de datos personales sensibles

En la circulación de los datos personales sensibles se deben seguir las siguientes reglas:

a. En los casos en que sea necesario comunicar, divulgar o entregar datos personales sensibles, ya sea dentro del marco del desarrollo o la ejecución de una actividad institucional o una investigación a un tercero o a un empleado de La Universidad que, por un tema de coyuntura, deba conocer esos datos, deberá dicha información aplicar mecanismos de supresión de identificación del titular, para que se evite identificar o asociar al titular del dato, a no ser que, por la actividad, sea indispensable la identificación del titular del dato.
b. Establecer en los contratos de transmisión de datos personales las medidas de seguridad que deben aplicar para la custodia y la transferencia de dichos datos personales.

Captura de datos personales biométricos

La identificación de las personas a través de sistemas biométricos deberá seguir las reglas establecidas en la presente política; así mismo, además del análisis que debe hacer el dueño del proceso dentro de La Universidad, establecido en la necesidad de recolección de datos personales sensibles, deberá tener en cuenta los siguientes aspectos:

a. Que el sistema sea adecuado, pertinente y no excesivo, tomando en cuenta para la finalidad que se persigue.
b. Garantizar que la configuración que tiene por defecto el sistema tenga las medidas de seguridad adecuadas que permitan proteger los datos personales.
c. Solicitar autorización para el tratamiento de dichos datos personales.

Requerimientos para solicitar videos capturados a través del CCTV

En caso de que el titular de la información solicite consultar imágenes o videos donde se capture su información, deberá, a su vez, aportar la siguiente información:

a. Indicar los hechos de la solicitud estableciendo fecha y hora.
b. Justificar la necesidad de la solicitud.
c. Aportar los documentos que permitan justificar que el titular es la persona indicada para hacer dicha solicitud y el objetivo de esta.
d. En caso de que el interesado sea un tercero, deberá aportar el documento de autorización para el acceso a esa información por parte del titular del dato.

En todo caso, La Universidad no estará obligada al suministro de dicha información cuando en el video aparezcan personas diferentes del solicitante.

Procedimiento para trámites por solicitud de videos

Para que proceda el trámite, La Universidad:

a. Revisará dicha solicitud y verificará si es procedente revisando que no afecte el derecho a la intimidad, y otros derechos fundamentales de terceras personas diferentes del titular de la información que se encuentren en dichas imágenes o videos, y revisando si el objeto argumentando por el solicitante es legítimo.
b. Verificará que la información aún se encuentre disponible. En caso de que no se encuentre disponible, informará al solicitante.
c. En caso de que afecte derechos fundamentales de terceros, La Universidad verificará internamente si los hechos que describe el titular se generaron, y le informará al titular sobre los hallazgos encontrados.
d. En caso de que no afecte derechos fundamentales de terceros, La Universidad citará al solicitante para que pueda observar el video.
e. En caso de que solicite copia de dicho video y ello afecte derechos de terceros, el solicitante deberá obtener la orden judicial o administrativa correspondiente.

Capítulo X. Deberes de las partes involucradas en el tratamiento de información personal dentro de la Universidad

Deberes de las personas que bajo sus funciones traten datos personales

Todas las personas que bajo sus funciones traten datos personales deberán tener en cuenta las siguientes reglas:

- Cumplir con la Política de Tratamiento de Datos Personales y el Manual Interno de Políticas y Procedimientos.
- Informar a través de los canales habilitados cualquier anomalía sobre el cumplimiento de la presente política de tratamiento de datos personales y el Manual Interno de Políticas y Procedimientos.
- Abstenerse de compartir sus credenciales de acceso (pasaporte virtual) con otras personas.
- Reportar de manera inmediata al correo electrónico habeasdata@urosario.edu.co, en caso que por error humano, tenga conocimiento de datos personales de estudiantes u otros titulares de La Universidad.
- Abstenerse de publicar o divulgar datos personales de estudiantes o colaboradores de La Universidad, como calificaciones, datos de contacto e identificación en redes sociales, páginas web, carteleras, número de celular salvo que tenga autorización expresa para realizar dicha acción.

Deberes de la Universidad

A continuación, se enumeran los deberes que tiene La Universidad para el efectivo tratamiento de datos personales:

a. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data;
b. Solicitar y conservar, copia de la respectiva autorización otorgada por el Titular;
c. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada;
d. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento;
e. Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible;
f. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada;
g. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento;
h. Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en el régimen de protección de datos personales;
i. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular;
j. Tramitar las consultas y reclamos formulados por los titulares;
k. Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo;
l. Informar a solicitud del Titular sobre el uso dado a sus datos;
m. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
n. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.
o. Respetar las condiciones de seguridad y privacidad de la información del titular.

Capitulo XVI. Notificación y Gestión de Incidencias.

El Manual de Usuario del Registro Nacional de Bases de Datos, define como incidente de seguridad de datos personales a la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de datos personales que sean tratados bien sea por el responsable del Tratamiento o por su Encargado.

Frente a un incidente de seguridad de datos personales todo colaborador y/o contratista de la Universidad tiene la obligación de:

- Notificar de manera inmediata al Oficial de Seguridad de la Información y Datos Personales al correo electrónico habeasdata@urosario.edu.co con asunto “incidente de seguridad” el hecho presentado.
- La notificación debe contener:
    - Fecha y hora del incidente.
    - Fecha y hora de conocimiento del incidente.
    - Descripción detallada del incidente presentado.
    - Impactos que puede producir la incidencia.
    - Persona a quien reportó el incidente.

Capitulo XVII. Prohibición General de Compartir Información

Se encuentra estrictamente prohibido transferir o ceder bases de datos o archivos (incluidos los documentos físicos) a terceras personas o entidades fuera de la Universidad o incluso en su interior que no tengan la autorización para el conocimiento de información personal bajo su poder en relación a su actividad laboral o de prestación de servicios. El incumplimiento de lo aquí estipulado será considerado como una falta grave de acuerdo al Reglamente Interno de Trabajo de la Universidad o dependiendo del caso, como una causal de incumplimiento y por ende de terminación unilateral por parte de la Universidad del contrato de prestación de servicios.

Así mismo, por regla general y disposición legal, La Universidad no comparte, transmite, transfiere los datos personales que recolecta a terceros, con quien previamente no haya firmado acuerdo de confidencialidad y anexo de transmisión de datos personales. También, ha dispuesto controles de acceso para el ingreso de sus colaboradores a los sistemas de información de La Universidad, exclusivamente a la información que de acuerdo al rol y/o cargo debe conocer.

ANEXO

Administradores de bases de datos personales

A continuación, se relacionan los administradores por cada base de datos personales registradas ante la Superintendencia de Industria y Comercio por parte de La Universidad:

Base de Datos Personales	Administradores
Acudientes	Gerente Comercial
	Gerente de Marketing
	Coordinador de Admisiones
App's	Jefe de Implementación, Calidad y Operación
	Gestor de Proyectos Académicos Virtuales
	Profesional de Relacionamiento Institucional
	Profesional en Formación Integral
Aspirantes	Gerente Comercial
	Gerente de Marketing
Clientes	Administrador Negocios Institucionales
Consultorio Jurídico	Director Consultorio Jurídico
Contratistas	Jefe de Contratación y Nómina
Educación Continua	Coordinador Mercadeo Educación Continua
	Jefe Comercial Clientes Individuales
Egresados	Director de Extensión y Egresados
	Asistente de Sistemas e Información
Empleados	Jefe de Contratación y Nómina
Estudiantes	Director de Registro y Control Académico
	Jefe de Deportes
	Coordinador de Empleabilidad e Inserción Laboral
	Profesional de Gestión Documental
	Profesional Analítica de Datos
	Coordinador de Participación y Liderazgo
	Coordinador de Movilidad Global
Servicios de Salud y Psicoeducación	Coordinador de Servicio Médico
	Coordinador de Psicología y Calidad de Vida
Inscritos y admitidos	Coordinador de Admisiones
Escuela de Teatro Musical - MISI	Director de Escuela de Niños y Jóvenes
PQR	Profesional Analítica de Datos
	Oficial Seguridad de Información y Datos Personales
Profesores	Jefe Enseñanza Aprendizaje y Trayectoria Profesoral
Proveedores, acreedores, deudores y donantes	Jefe de Compras y Suministros
	Auxiliar de Compras y Suministros
	Director Filantropía
	Asistente Administrativo - Filantropía
Video vigilancia	Jefe de Seguridad y Servicios Generales

Universidad del
Rosario