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

Universidad del
Rosario

Bogotá D.C., abril de 2019

Contenido

Capítulo I. Disposiciones generales

Manual interno de políticas y procedimientos

El presente *Manual interno de políticas y procedimientos para el tratamiento de datos personales* fue diseñado con el fin de garantizar el adecuado cumplimiento de lo estipulado en la legislación colombiana actual, y tiene la finalidad de regular el tratamiento de los datos personales 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.

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 y 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, contratistas, proveedores, acreedores, etc., dentro del marco de sus actividades diarias tanto en el interior de la organización 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 comerciales.

Objetivos

- 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.

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:** conjunto organizado de datos personales que sea objeto de tratamiento.
- **Conducta inequívoca:** comportamiento que permite concluir de forma razonable que el titular de datos personales otorgó la autorización para el tratamiento de sus datos.
- **Consulta**: proceso mediante el cual el titular de datos personales puede solicitar a La Universidad información acerca de sus datos personales que reposan en las bases de datos.
- **Dato personal:** cualquier información vinculada o que pueda asociarse a una o a varias personas naturales determinadas o determinables.
- **Dato público:** dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión o su oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Dato sensible:** dato que afecta la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como los que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, o a organizaciones sociales o de derechos humanos, o que promueva intereses de cualquier partido político o garanticen los derechos y las garantías de partidos políticos de oposición, así como los datos relativos a la salud y a la vida sexual, y los datos biométricos.
- **Dato semiprivado:** dato que no tiene naturaleza íntima, ni reservada ni pública, y cuyo conocimiento o divulgación pueden interesar no solo a su titular, sino a cierto sector o grupo de personas o a la sociedad en general.
- **Dato privado:** dato que, por su naturaleza íntima o reservada, solo es relevante para el titular.
- **Encargado del tratamiento:** persona natural o jurídica, pública o privada que, por sí misma o en asocio a otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
- **Finalidad:** definición de para qué van a ser utilizados los datos que se están recolectando.
- **Reclamo**: proceso mediante el cual los titulares de los datos personales, podrán solicitar a La Universidad la actualización, la rectificación, la supresión parcial o total de la información, la prueba de la autorización o la revocatoria de esta.
- **Responsable del tratamiento:** persona natural o jurídica, pública o privada que, por sí misma o en asocio a otros, decide sobre la base de datos o el tratamiento de los datos.
- **Titular**: persona natural que actúa por sí misma o en nombre legal de otros (por ejemplo, menores de edad) cuyos datos personales sean objeto de tratamiento.
- **Tratamiento:** operación o conjunto de operaciones sobre datos personales, tales como recolección, almacenamiento, uso, circulación o supresión.
- **Transferencia de datos:** transferencia que tiene lugar cuando el responsable o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que, a su vez, es responsable del tratamiento y se encuentra dentro o fuera del país.
- **Transmisión:** tratamiento de datos personales que implica la comunicación de estos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

Capítulo III. Principios para el tratamiento de datos personales

La Universidad aplicará los siguientes principios específicos, 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 en materia de tratamiento de datos: La Universidad busca garantizar el cumplimiento del Régimen Normativo de Protección de Datos Personales estableciendo obligaciones para sus funcionarios, sus proveedores, sus estudiantes, sus 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.

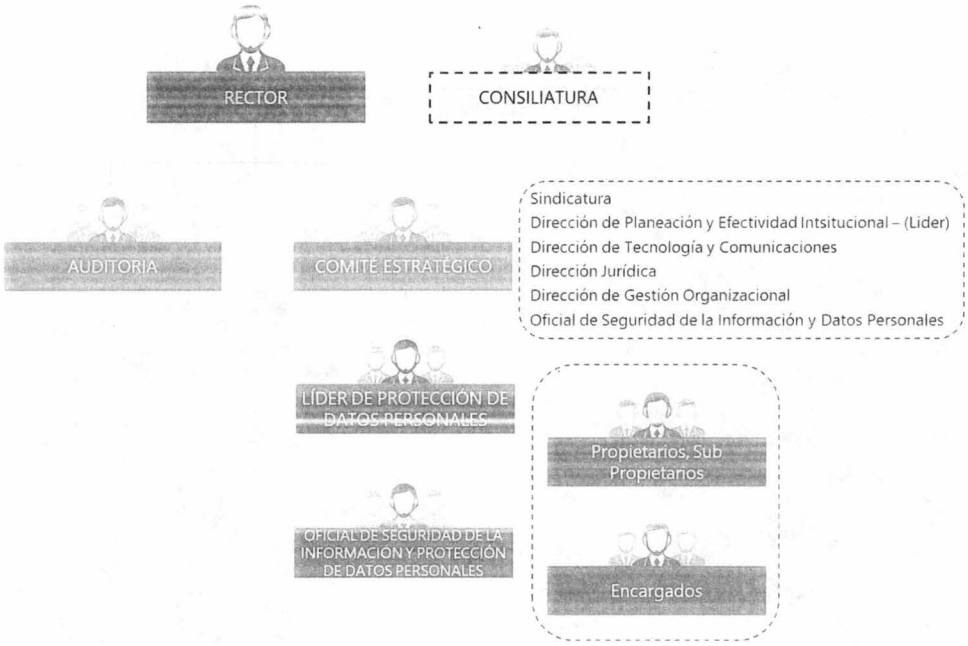
Principio de acceso y circulación restringida: La Universidad ha dispuesto controles de acceso a la información personal contenida en las bases de datos. También ha dispuesto internamente mecanismos para que sus funcionarios puedan tener acceso solo a la información que de acuerdo con su cargo deban 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 funcionarios, 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, inventario de las bases de datos, 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



Responsabilidades de los roles del Sistema de Aseguramiento de Calidad y Tratamiento de Datos Personales

Comité Estratégico en Protección de Datos Personales

Autoridad central en la Universidad del Rosario en materia de protección de datos personales, 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 Protección de Datos personales está integrado por:

Integrantes:

Síndico
Director de Planeación y Efectividad Institucional
Director de Gestión Organizacional
Director de Tecnología Informática y Comunicaciones
Director jurídico

Responsabilidades

Fases	Responsabilidades
Planeación	• Aprobar la Política de Tratamiento de Datos Personales y el *Manual interno de políticas y procedimientos* y, posteriormente, los cambios sustanciales que puedan llegar a presentarse. • Aprobar el presupuesto en pro de las mejoras al Sistema de Aseguramiento de Calidad y Tratamiento de Datos Personales. • Aprobar el plan de trabajo anual en 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 una 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.

Fases	Responsabilidades
	• 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 Aseguramiento de Calidad y Tratamiento de Datos Personales.
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, el Comité Operativo en Protección de Datos Personales y los resultados en la gestión de riesgos, en pro de la mejora continua del Sistema de Aseguramiento de Calidad y Tratamiento de Datos Personales.

Líder de protección de datos personales

Rol bajo la responsabilidad del 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 de la 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	• Tener reuniones mensuales con el oficial de seguridad de la información 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 Aseguramiento de Calidad y Tratamiento de Datos Personales.
Ajustes	• Tomar decisiones en materia de protección de datos personales cuando el oficial de seguridad de la información no pueda solucionar algún caso de protección de datos personales.

Oficial de seguridad de la información y datos personales

Rol bajo la responsabilidad del oficial de seguridad de la información y datos personales dentro de La Universidad, y cuya responsabilidad consiste en estructurar, diseñar y gestionar el Sistema de Aseguramiento de Calidad y Tratamiento de Datos Personales, para así permitirle a La Universidad cumplir las normas en la materia, generar lineamientos y establecer los controles pertinentes a mitigar riesgos en protección de datos personales, hacer evaluación permanente al programa y adoptar mejoras continuas en pro de la estabilidad de este.

Responsabilidades

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	• Generar lineamientos para evaluar los riesgos en protección de datos personales en los procesos donde se recolecten, se almacenen, se usen, circulen y se supriman datos personales.

Fases	Responsabilidades
	• Presentar semestralmente al Comité Estratégico en Protección de Datos Personales informe acerca de los resultados del Sistema de Aseguramiento de Calidad y Tratamiento de Datos Personales. • Presentar anualmente al Comité Estratégico en Protección de Datos Personales el informe general y consolidado frente al cumplimiento en materia de protección de datos personales. • Servir de enlace y coordinar con las demás áreas de La Universidad para asegurar una gestión transversal del Sistema de Aseguramiento de Calidad y Tratamiento de Datos Personales. • Evaluar continuamente la normativa colombiana en materia de protección de datos personales y seguridad de la información. • Promover una cultura de protección de datos dentro de la organización. • Mantener actualizada la documentación del proceso de gestión de datos personales, incluyendo políticas, procedimientos y formatos. • Controlar los cambios a la documentación, incluyendo políticas, procedimientos y formatos. • Mantener un inventario actualizado de las bases de datos personales en poder de La Universidad, y clasificarlas según su tipo. • 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. • Redactar y validar los contenidos de los contratos de transmisión internacional de datos que se suscriban con encargados no residentes en Colombia. • Gestionar la respuesta a las consultas y los reclamos presentados por los titulares, con base en los procedimientos internos de atención de consultas y reclamos en materia de protección de datos personales. • Hacer un entrenamiento general en protección de datos para todos los empleados de la Universidad. • Hacer el entrenamiento necesario a los nuevos empleados; en especial, a quienes, por las responsabilidades del cargo, tengan acceso a datos personales gestionados por La Universidad. • Reportar a la Superintendencia de Industria y Comercio 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. • Hacer evaluaciones de riesgos en protección de datos personales. • Apoyar a los propietarios y a los sub-propietarios de bases de datos personales y al equipo de colaboradores con las responsabilidades diarias para cumplir 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 Aseguramiento de Calidad y Tratamiento de Datos Personales. • Coordinar las reuniones del Comité Estratégico en Protección de Datos Personales.
Verificación	• Hacer autoevaluación sobre el cumplimiento del plan de trabajo anual en protección de datos personales.

Fases	Responsabilidades
	• Hacer autoevaluación al cumplimiento de las responsabilidades de los propietarios y los sub-propietarios de bases de datos personales (PDP). • Hacer monitoreo al cumplimiento de las responsabilidades de los encargados del tratamiento de datos personales. • Diseñar, en conjunto con los propietarios 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 Aseguramiento de Calidad y Tratamiento de Datos Personales, 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 y el Comité de Protección de Datos Personales.

Propietario de base 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	• Elaborar el plan de trabajo anual en materia de protección de datos personales (dentro del plan de trabajo de los propietarios estará la formación en protección de datos personales, la cual podría ser planificada en conjunto con el oficial de seguridad de la información y datos personales, así como programar la actualización de datos personales de los titulares y planificar la atención a auditorías internas o externas). • Elaborar el presupuesto requerido para ejecutar el plan de trabajo anual en protección de datos personales (podrá necesitar recursos, además de los necesarios para cumplir el plan de trabajo, para la adecuación de formatos físicos o automatizados en los cuales se recolecten datos personales, para el almacenamiento de las autorizaciones, etc.).
Ejecución	• Garantizar la recolección de la autorización de tratamiento de datos personales del titular la autorización. • 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 el formato de autorización, la Política de Tratamiento de Datos Personales y la autorización realizada por el titular. • 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. • Suprimir los datos personales de los titulares siguiendo los lineamientos definidos en el *Manual interno de políticas y procedimientos* para tal fin. • 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 SARI. • Evaluar los riesgos del proceso en materia de protección de datos personales.

Fases	Responsabilidades
	• 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. • Presentar informes mensuales al oficial de seguridad de la información y datos personales con las solicitudes hechas sobre el uso de base de datos personales o usuarios dados de baja. • Promover una cultura de protección de datos personales con el equipo de colaboradores y los demás empleados de la universidad. • 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 tengan claros sus roles y sus responsabilidades, así como su contribución para el logro de los objetivos del Sistema de Aseguramiento de Calidad y Tratamiento de Datos Personales de la Universidad y las consecuencias de su incumplimiento.
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 Aseguramiento de Calidad y Tratamiento de Datos Personales. • Generar lineamientos para incorporar las oportunidades de mejora y monitorear su implementación. • Hacer los ajustes requeridos al plan anual de trabajo, con base en los resultados de la autoevaluación realizada a este.

Subpropietario de bases de datos personales

Son los líderes de los procesos o las áreas que recolectan, almacenan, usan, circulan y suprimen datos personales y siguen los lineamientos dados por el propietario de bases de datos personales.

Responsabilidades

Fases	Responsabilidades
Planeación	• Elaborar el plan de trabajo anual en materia de protección de datos personales (dentro del plan de trabajo de los propietarios estará la formación en protección de datos personales, la cual podría ser planificada en conjunto con el oficial de seguridad de la información y datos personales, así como programar la actualización de datos personales de los titulares y planificar la atención a auditorías internas o externas).
Ejecución	• Garantizar la recolección de la autorización de tratamiento de datos personales del titular la autorización. • Garantizar la conservación de la autorización para el tratamiento de datos personales suministrada por el titular.

Fases	Responsabilidades
	• Garantizar el uso de los datos personales, según las finalidades descritas en el formato de autorización, la Política de Tratamiento de Datos Personales y la autorización hecha por el titular. • Informar previamente a la recolección de datos personales al oficial de seguridad de la información y datos personales la inclusión en el inventario de bases de datos personales, las nuevas fuentes de recolección y almacenamiento de datos requeridos para el proceso o el área de la cual es responsable, así como la necesidad de circulación externa de datos personales a terceros. • Suprimir los datos personales de los titulares, siguiendo los lineamientos definidos en el *Manual interno de políticas y procedimientos* para tal fin. • 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 SARI. • 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. • Presentar informes mensuales al oficial de seguridad de la información y datos personales con las solicitudes realizadas de uso de base de datos personales o usuarios dados de baja. • Promover una cultura en protección de datos personales con el equipo de colaboradores y los demás empleados de la universidad. • Reportar al oficial de seguridad de la información y datos personales cuando conozca una consulta o un 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 considera que se deben implementar en la gestión de los datos personales. • Asegurar que todos los colaboradores tengan claros sus roles y sus responsabilidades, así como su contribución para el logro de los objetivos del Sistema de Aseguramiento de Calidad y Tratamiento de Datos Personales de la Universidad y las consecuencias de su incumplimiento.
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 Aseguramiento de Calidad y Tratamiento de Datos Personales. • Generar lineamientos para incorporar las oportunidades de mejora y monitorear su implementación. • Hacer los ajustes requeridos al plan anual de trabajo, con base en los resultados de la autoevaluación realizada a este.

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 propietario o los subpropietarios, en su calidad de responsable.

Fases	Responsabilidades
Ejecución	• Tener una política de tratamiento de datos personales. • Garantizar la recolección de la autorización de tratamiento de datos personales del titular de la autorización. • Implementar medidas de seguridad apropiadas para conservar la confidencialidad 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 propietario cualquier comunicación relativa a los datos personales. • Informar al propietario 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. • Garantizar que cuenta con adecuadas medidas de seguridad técnicas, físicas o digitales en el tratamiento de los datos personales. • Hacer oportunamente la actualización, la rectificación o la supresión de los datos tal como lo indiquen el propietario o el subpropietario. • Actualizar o rectificar la información reportada por el propietario o el subpropietario. • Garantizar que los datos personales sean tratados según la finalidad establecida por el propietario o el subpropietario. • Cumplir en todo momento las instrucciones dadas por el propietario o el subpropietario. • Hacer firmar acuerdos de confidencialidad a los contratistas o los trabajadores que, en razón o con ocasión de las labores que prestan, traten datos personales. • Informar inmediatamente cualquier incidente o vulneración que se presenten con los datos personales entregados por el propietario o el subpropietario. • Abstenerse de permitir el acceso a los datos personales entregados por el propietario o los subpropietarios, 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 propietarios o los subpropietarios, 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 propietario o el subpropietario.
Verificación	• Hacer autoevaluación permanente al cumplimiento de las responsabilidades adquiridas, con especial atención a las solicitudes hechas por el propietario o el subpropietario 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 hechos por el titular o el 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	Pasos	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 numeral 6.3. **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 al correo:* habeasdata@urosario.edu.co *como medida proactiva.* **Canales habilitados** **1.** Ingresando la solicitud en la opción "solicitudes" 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.	Titular, tercero autorizado Representante Legal
2	Notificación al titular o al tercero	Según el canal habilitado por La Universidad para radicar la solicitud, se genera una notificación de la siguiente forma: **1.** Opción "solicitudes" de la página *web*: automáticamente, se genera una notificación al usuario sobre el ingreso de la solicitud.	Oficial de seguridad de la información y datos personales

ID	Pasos	Descripción de la actividad	Responsable
		2. Correo electrónico habeasdata@urosario.edu.co y buzón físico: el oficial envía una respuesta al usuario sobre el ingreso de la solicitud, a través del correo registrado.	
3	Validación de la solicitud	Recibida la solicitud, se la 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. 3. Información financiera, académica, laboral. El término máximo para atender la consulta será de *diez días hábiles*, contados a partir del día siguiente a la fecha de su recibo. **Si es reclamo**: la descripción de cada tipo de reclamo se encuentra descrito en la política de tratamiento de datos personales, numeral 6.1.1. Los tipos de reclamos son: 1. Actualización. 2. Rectificación. 3. Supresión de la información. 4. Inclusión de información 5. Revocatoria de la autorización. El término máximo para atender el reclamo será de *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 informarán 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.*	Oficial de seguridad de la información y datos personales
4	Análisis de la solicitud	Se debe analizar si es el titular, un tercero o representante legal quien está generando la solicitud, según lo descrito en la Política de Tratamiento de Datos Personales en el numeral 3.10 y numeral 3.11, donde se define a quiénes se les puede entregar información: **A quiénes se les puede entregar información:** 1. A los titulares o a sus representantes legales. 2. A las entidades públicas o administrativas, en ejercicio de sus funciones legales o por orden judicial. 3. A los terceros autorizados por el titular o por la ley. 4. Los derechos de los niños y los adolescentes se ejercerán por las personas que estén facultadas para representarlos.	Oficial de seguridad de la información y datos personales

ID	Pasos	Descripción de la actividad	Responsable
		5. La solicitud de información personal del estudiante mayor de edad, relativa a las gestiones académicas o financieras, y, en general, las concernientes a los datos que son propiedad del titular, se debe entregar únicamente al estudiante titular o a los expresamente autorizados por el titular. 6. La solicitud de información personal del estudiante menor de edad relativa a las gestiones académicas, financieras, y, en general, las concernientes a los datos que son propiedad del titular por ley se puede entregar a sus representantes legales	
5	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, y se verifica que cumpla con los parámetros definidos por la ley y por La Universidad en la Política de Tratamiento de Datos Personales numeral 6.2.4, para la acreditación del titular del dato. **Información que debe acreditar el titular:** **1.** Adjuntar imagen o foto del documento de identificación. **2.** Dado el caso podrá acreditar presentación personal mostrando el documento de identificación ante la oficina del oficial de seguridad de la información y datos personales. **3.** Adjuntar los soportes que quiere hacer valer. **Información que debe acreditar terceros:** **1.** Adjuntar imagen o foto del documento de identificación. **2.** Adjuntar imagen o foto del documento de identificación del titular de la información. **3.** Carta de autorización del titular, con reconocimiento de firma, en caso de que sea un tercero actuando en representación del titular o autenticada. **4.** Adjuntar los soportes que quiere hacer valer. **Información que debe acreditar un Representante legal:** **1.** Adjuntar imagen o foto del documento de identificación. **2.** Adjuntar imagen o foto del documento de identificación del titular de la información. **3.** Registro civil de Nacimiento del menor de edad **4.** Documento que acredite la patria potestad. **5.** Adjuntar los soportes que quiere 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 *tres días hábiles* siguientes al recibo de la solicitud, a fin de que aporte la documentación faltante o cualquier otra aclaración que sea necesaria para la ejecución de la consulta.	Oficial de seguridad de la información y datos personales

ID	Pasos	Descripción de la actividad	Responsable
6	Búsqueda de información	El oficial de seguridad de la información y datos personales envía la consulta o reclamo a: 1. Propietarios y subpropietarios; estos, a su vez, a los encargados de la base de datos que afecta ese dato, para la gestión pertinente. 2. Notifica a otras áreas de La Universidad cuando la consulta así lo amerite. Los propietarios, los subpropietarios y los encargados *(por notificación de los subpropietarios)* 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 dos días hábiles siguientes*, contados a partir de la recepción del requerimiento. Si el propietario, subpropietario y los encargados de la base de datos (por notificación de los subpropietarios) no han podido dar respuesta en el tiempo establecido, deberán enviar justificación al oficial, quien informará al titular el plazo de dos días hábiles más para poder dar respuesta. Si es reclamo, se debe: • Dejar claro que es un "reclamo en trámite" y el motivo de este, en un término no mayor de dos días hábiles. • 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 Propietarios y subpropietarios, y estos, a su vez, a los encargados de la base de datos
7	Alertas	El oficial de seguridad de la información y datos personales generará alertas periódicas, a través de llamada o correo, a los propietarios de las bases de datos, sobre los tiempos de respuesta, y dichos tiempos en ningún caso podrán ser superiores a ocho días hábiles siguientes a la recepción del reclamo.	Oficial de seguridad de la información y datos personales
8	RECLAMO: Actualización y/o Rectificación	Si la solicitud fue catalogada como reclamo de actualización, rectificación y/o inclusion, el propietario, subpropietarios y encargados de la base de datos (por notificación de los subpropietarios) 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 término no mayor de *dos días hábiles* posteriores a haber recibido el reclamo por parte del titular.	Oficial de seguridad de la información y datos personales Propietarios y subpropietarios, y estos, a su vez, a los encargados de la base de datos

ID	Pasos	Descripción de la actividad	Responsable
		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 rectificar (por ejemplo: cambio de nombres o apellidos, cambio de teléfono, cambio de dirección u otros). 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 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 propietario o a los subpropietarios, y estos, a su vez, a los encargados de la base de datos, cuando se presenta un "reclamo en trámite" y el motivo de este, en un término no mayor de *dos días hábiles*; dicho dato no podrá usarse bajo ninguna circunstancia sino hasta que el reclamo sea decidido. e. El propietario, los subpropietarios y los encargados de la base de datos (por notificación de los subpropietarios) actualizan o rectifican los datos según la solicitud descrita por el titular en el reclamo. f. El propietario, los subpropietarios y los encargados de la base de datos (por notificación de los subpropietarios) deben remitir al oficial de seguridad de la información y datos personales la prueba de dicha acción, del antes y el después de la actualización o la rectificación.	
9	RECLAMO: Supresión	El propietario, subpropietarios y los encargados de la base de datos (por notificación de los subpropietarios) 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 de *dos días hábiles* posteriores a haber recibido el reclamo por parte del 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.	Oficial de Seguridad de la Información y Datos Personales Propietarios y subpropietarios, y estos, a su vez, a los encargados de la base de datos

ID	Pasos	Descripción de la actividad	Responsable
		c. Una vez recibido el reclamo completo, el oficial de seguridad de la información y datos personales enviará un correo a el propietario o al subpropietario, y estos, a su vez, a los encargados de la base de datos, avisando que dicho dato presenta un "reclamo en trámite" y el motivo de este, en un término no mayor de dos días hábiles, 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 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. En caso de no ser posible una supresión, reemplazará los datos personales con otros valores no relacionados con los datos originales, pero manteniendo coherentes los datos (lo cual consiste en suprimir datos que permitan identificar al titular) y sustituirá los datos de origen por datos del mismo formato. Se define de la siguiente forma: 1. **Correo**: Sustituir por: supresiondato@habeasdata.com 2. **Celular o número telefónico**: 0000000000 3. **Nombre o Apellidos**: Supresión dato f. Cuando haya dudas sobre la procedencia de la supresión del dato, deberá informar al 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 los datos personales la prueba de dicha acción, del antes y el después de la sustitución o la supresión.	
10	RECLAMO: Revocatoria	El propietario, subpropietarios y los encargados de la base de datos (por notificación de los subpropietarios) 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. 1. 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 propietario, subpropietarios y los encargados de la base de datos (por notificación de los subpropietarios) deberán remitir al	Oficial de seguridad de la información y datos personales Propietarios y subpropietarios, y estos, a su vez, a los encargados de la base de datos

ID	Pasos	Descripción de la actividad	Responsable
		oficial de seguridad de la información y datos personales la prueba de dicha acción, de la revocatoria de la autorización. 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.	
11	Respuesta interna	**Consulta**: en caso de que se imposibilite dar respuesta en los tiempos establecidos anteriormente, el oficial 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 deberá informar al titular el día de vencimiento del primer término, así como las dificultades que se presentaron, e informar que se dará respuesta en los *ocho días hábiles* siguientes al vencimiento del primer término. El propietario, subpropietarios y los encargados de la base de datos (por notificación de los subpropietarios) deben 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 propietario, los subpropietarios y los encargados de la base de datos (por notificación de los subpropietarios), el oficial de seguridad de la información y datos personales deberán elevar el caso al jefe inmediato o, en su defecto, al Comité Estratégico en Protección de Datos Personales.	Propietarios y subpropietarios, y estos, a su vez, a los encargados de la base de datos
12	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
13	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, su almacenamiento, su uso, su circulación y su disposición final.

1. Procedimiento para la recolección de datos personales

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 la prueba de la autorización otorgada por parte del titular, para su posterior consulta.

2. 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:

Forma de almacenamiento de la información

ARCHIVO PROPIO INTERNO Y EXTERNO

Políticas de Gestión Documental

SERVIDOR EXTERNO PROPIO O A CARGO DE UN TERCERO

Contrato de Transmisión de Datos Personales

COMPUTADOR PERSONAL O SERVIDOR PROPIO

Políticas de Seguridad Informatica

3. 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 de Tratamiento de Datos Personales, debe informar, 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 propietario, un subpropietario 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 propietario, el subpropietario o el encargado de la base de datos dicha información, puesto que los datos pudieron ser modificados.
d. Los funcionarios 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.

4. 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 propietario de la base de datos quien sea responsable de la base de datos (ANEXO II Propietarios y Subpropietarios de bases de datos personales) y describir:
    a. Los datos personales que necesita.
    b. La finalidad del uso de los datos personales.
    c. Indicar qué tipo de objetivo, proceso o norma debe cumplir el área para la finalidad ya descrita.
    d. Indicar 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.
    e. La fecha en que se realizaría dicha actividad.
    f. La fecha de eliminación de la base de datos personales al finalizar la actividad, y la prueba de dicha eliminación.

El propietario de la base de datos deberá evaluar el requerimiento teniendo en cuenta los siguientes aspectos:

a. Evaluar si la solicitud es pertinente a los propósitos que se persiguen.
b. Evaluar los efectos que se podrían generar en caso de no facilitar la información.
c. Si el efecto es el incumplimiento normativo o el incumplimiento de un compromiso institucional, se debe facilitar la información.

d. Identificar si para los propósitos que se facilita y se requiere la información, esta se podrá suprimir, para no identificar al titular del dato.
e. Informarle al jefe de área que solicita la información que a esta no se le pueden dar usos diferentes de los relacionados en la Política de Tratamiento de Dato Personal, y que solo será para el propósito perseguido.
f. Si considera que no está fundada su solicitud, no suministrará la base de datos o la información personal.
g. Informar al correo electrónico suministrado las razones por las cuales no se puede suministrar dicha información personal.
h. Informar a la Oficial de Seguridad de la Información y Datos Personales a través del correo habeasdata@urosario.edu.co el consolidado de solicitudes que reciba de los usuarios.

En caso de discrepancias, tanto el jefe de área que solicita la información como el jefe de área que la suministrará 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 contrato de transmisión de datos personales.
Transmisión internacional	Realizar contrato de transmisión de datos personales.
Transferencia nacional	Realizar contrato de transferencia de datos personales.
Transferencia internacional	Realizar contrato de transferencia internacional 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, mostrar el poder o la autorización para la entrega de la información.
Tercero	Aportar la autorización autenticada que suministró el titular para entregar dicha información.
Autoridad judicial	Orden judicial.
Autoridad administrativa	Disposición legal o acto administrativo.

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.

5. 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 Departamento de Tecnología, y este dará los lineamientos correspondientes. No obstante, al momento de establecer o revisar las reglas para la disposición final de la información, el propietario de la base de datos, junto con el profesional del 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.

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

Objetivo

Establecer el contenido de la autorización para el tratamiento de datos personales según los datos por recolectar por parte de los titulares con los cuales La Universidad tenga relación.

1. 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 la debe poder consultar con posterioridad. Dicha autorización debe contener, como mínimo:

a. Información sobre el uso que tendrán los datos recolectados.
b. Finalidades de su tratamiento.
c. Derechos que tiene como titular del dato.
d. Datos del responsable del tratamiento (identificación, dirección física o electrónica).
e. Ubicación 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 la política de tratamiento o en el botón Enviar, se 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 a La Universidad.
c. Cuando se hace una llamada telefónica La Universidad, 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.

2. 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. Informarle al titular el tratamiento que se dará a sus datos personales.
b. Informarle sobre las finalidades de su tratamiento.
c. Los derechos que le asisten como titular del dato.
d. Informar al titular que, por tratarse de datos sensibles, no está obligado a autorizar su tratamiento.
e. Informar cuáles son los datos que serán objeto de tratamiento son sensibles, y la finalidad del tratamiento.
f. 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.
g. Datos del responsable del tratamiento (identificación, dirección física o electrónica).

h. Ubicación, para consultar la Política de Tratamiento de Datos Personales.

3. 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 12 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.

4 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.

5. 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 se ingresa a las instalaciones de La Universidad, se entiende que el titular otorga su autorización para la gestión de imagen a través de las cámaras de seguridad.
b. Cuando se envían datos personales a un correo electrónico de La Universidad.
c. Cuando se envía la hoja de vida para un proceso de selección.

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.
Envío de datos personales al correo electrónico institucional.	a. Cuando el titular envíe su información personal a un correo no autorizado para el envío de dicha información, se le deberá responder al titular informándole los canales habilitados. b. Cuando el correo electrónico sea a un correo autorizado, se le deberá remitir el aviso de privacidad de La Universidad, y solicitar confirmación de recibido, o a través del confirmado del correo electrónico quedará como una confirmación.
Relación contractual.	La Universidad revisará si es previsible la solicitud de los datos que formalicen la relación contractual sin la autorización, dentro del marco de la relación que tiene con el titular.

6. 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 durante 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 relación con el tercero, deberá solicitarle la política de tratamiento de datos personales con la que cuenta.
c. 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 encuentra autorizado para solicitar dicha información.
d. Si un tercero quiere consultar las calificaciones de un estudiante o un 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:
    1. Al estudiante, en ejercicio de su derecho de acceso y consulta.
    2. A un tercero, previa obtención de la autorización del estudiante, donde sea manifestada la finalidad de uso de dicha información.

7. 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 funcionario 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.

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

Los propietarios de las bases de datos 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 propietario 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 propietario, con apoyo del oficial de seguridad de la información y datos personales, así como del Comité Estratégico de Protección de Datos Personales, 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 propietarios, los subpropietarios 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 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.
- Todos los propietarios, los subpropietarios y los usuarios de la información personal que, con ocasión de la actividad que desempeñen en La Universidad, estén a cargo de recibir las autorizaciones tienen la obligación de conservarlas siguiendo los parámetros que se establecen en el presente procedimiento.
- El propietario, el subpropietario o el encargado de las bases de datos son los responsables de coordinar 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
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:

ID	Actividad	Descripción de la actividad
		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 tratamiento al cual serán sometidos sus datos personales y la finalidad de ello. b. 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. c. Los derechos que le asisten como titular. d. Los canales habilitados por La Universidad para ejercer el derecho de *Hábeas data*. e. La autorización para el tratamiento de datos personales deber ser diligenciada por parte del titular de la información; y en caso de ser menor de edad, por quien ejerza la patria potestad o la calidad de representante legal. Cuando el titular autoriza el tratamiento, el responsable de la recolección debe conservar la autorización por parte del titular, para su posterior consulta.
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 propietario, el subpropietario o el encargado deberán 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.

Instrucciones dirigidas a los propietarios, los subpropietarios o los encargados del tratamiento del formato físico

Cuando el propietario, los subpropietarios o el encargado reciban por parte de La Universidad el formato físico con la autorización firmada por parte del titular, el propietario, los subpropietarios 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 propietario, el subpropietarios o el encargado procederán a devolver dicho formato al Área de Gestión Organizacional, 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; es decir, enero de 2018, febrero de 2018, etc.
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.
d. Se verificará el Excel, para complementarlo con los datos que requiere La Universidad.

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.
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 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.

1. 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.

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

De acuerdo con los resultados generados por el análisis que haga el funcionario, 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.

3. 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 funcionario 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.

4. 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.

4.1. 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.

5. 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.

6. 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.

7. 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.

8. 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.

9. 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.

ANEXOS

Anexo 1

1. Ejemplos de autorizaciones para tratamiento de datos personales

Ejemplo autorización expresa:

La autorización expresa de datos personales deberá contener los siguientes elementos:

Título

Autorización para el tratamiento de datos personales

1. Identificación del responsable y finalidad del uso de los datos

Responsable

Texto Ejemplo: Autoriza el tratamiento de sus datos personales a **la Universidad del Rosario** para las siguientes Finalidades: inscripción a estudiantes de posgrado, seguimiento a personas inscritas, reportes ante el Ministerio de Educación de personas inscritas, asignación de fechas de entrevistas, promoción de programas, desarrollo de entrevistas a inscritos para determinar si son o no admitidos a los programas.

2. Tratamiento de datos personales

Texto ejemplo: las comunicaciones derivadas de las anteriores finalidades se podrán realizar a través de medios análogos, físicos y electrónicos y cualquier otro conocido o por conocer, por parte de la Universidad del Rosario y por parte de la entidad con quien La Universidad tenga convenio para ejecutar las actividades descritas en las finalidades. La información personal que nos suministra se utilizará solo para los fines autorizados por usted, y se encuentra bajo nuestra custodia, y eventualmente en custodia con la entidad con la cual La Universidad tiene convenio para ejecutar este tipo de actividades, contando con todas las medidas de seguridad físicas, técnicas y administrativas para evitar su pérdida, su adulteración o su uso fraudulento o no adecuado.

3. Derechos del titular y canales habilitados para ejercer el derecho de *hábeas data*

Derechos

Usted tiene derecho a conocer, actualizar y corregir sus datos personales; también podrá solicitar la supresión o revocar la autorización otorgada para su tratamiento.

Canales habilitados

En caso de un reclamo o una consulta relativa a sus datos personales, puede hacerlo ingresando la petición en la opción "solicitudes" de la página *web* de La Universidad, remitiendo la solicitud al correo electrónico habeasdata@urosario.edu.co o dejando su petición 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. a 7:00 p. m., y los sábados, de 8:00 a. m. a 1:00 p. m.

4. Indicación de la consulta de la política

Si quiere más información sobre el tratamiento de sus datos personales, consulte nuestra Política de Tratamiento de Datos personales en www.urosario.edu.co

Nombre: _____

Firma: _____

Identificación: _____

Fecha: _____

Evidencia de la autorización por parte del titular

Ejemplo de autorización expresa reforzada:

La autorización expresa reforzada de datos personales deberá contener los siguientes elementos:

Título

Autorización para el tratamiento de datos personales

1. Identificación del responsable y finalidad del uso de los datos

Responsable

Texto ejemplo: autorizo el tratamiento de mis datos personales a **la Universidad del Rosario** para las finalidades relativas a la prestación de servicios médicos, como pueden ser: consulta externa de medicina general, medicina del deporte, psiguiatría, psicología, nutrición, atención de enfermería y programación de citas.

2. Tratamiento de datos personales:

Informar datos sensibles objeto de tratamiento

Texto ejemplo: entiendo y autorizo el tratamiento de mis datos personales; entre ellos, datos personales privados y sensibles, como datos relativos a salud y a situación política o judicial, que puedo suministrar durante el transcurso de la asesoría que el consultorio me esté prestando.

Carácter facultativo de datos sensibles y de menores

Texto ejemplo: en caso de ser representante legal del menor de edad, autorizo el tratamiento de sus datos personales, y, en general, de la información personal que tenga que suministrar del menor o menores de edad. Entiendo, y se me ha informado, el carácter facultativo de las respuestas a las preguntas que versen sobre datos de niños y adolescentes.

Tratamiento de datos personales

Texto ejemplo: las comunicaciones derivadas de las anteriores finalidades se podrán realizar a través de medios análogos, físicos y electrónicos y cualquier otro conocido o por conocer, por parte de la Universidad del Rosario y por parte de la entidad con quien La Universidad tenga convenio para ejecutar las actividades descritas en las finalidades.

La información personal que nos suministra se utilizará solo para los fines autorizados por usted, y se encuentra bajo nuestra custodia, y eventualmente, en custodia con la entidad con la cual La Universidad tiene convenio para ejecutar este tipo de actividades, contando con todas las medidas de seguridad físicas, técnicas y administrativas para evitar su pérdida, su adulteración o su uso fraudulento o no adecuado. En caso de que la custodia y el almacenamiento sean hechos por una entidad con la que se tenga relación contractual, usted autoriza la transmisión de sus datos personales, incluyendo los datos personales sensibles a un tercer país, que cuenta con los estándares de seguridad en la protección de datos personales fijados por la Superintendencia de Industria y Comercio.

3. Derechos del titular y canales habilitados para ejercer el derecho de *hábeas data*

Derechos

Usted tiene derecho a conocer, actualizar y corregir sus datos personales; también podrá solicitar la supresión o revocar la autorización otorgada para su tratamiento.

Canales habilitados

En caso de un reclamo o una consulta relativa a sus datos personales, puede hacerla ingresando la petición en la opción "solicitudes" de la página *web* de La Universidad, remitiendo la solicitud al correo electrónico habeasdata@urosario.edu.co o dejando su petición 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. a 7:00 p. m., y los sábados de 8:00 a. m. a 1:00 p. m.

4. Indicación de la consulta de la política

Si quiere más información sobre el tratamiento de sus datos personales, consulte la Política de Tratamiento de Datos personales en www.urosario.edu.co

Nombre: _____

Firma: _____

Identificación: _____

Fecha: _____

Evidencia de la autorización por parte del titular

Ejemplo de autorización uso de imagen en eventos

Autorización para el tratamiento de datos personales

1. Identificación del responsable y finalidad del uso de los datos

Responsable

Autorizo el tratamiento de mis datos personales a **la Universidad del Rosario**, en adelante, La Universidad, para las siguientes finalidades

a. Autorizo a LA UNIVERSIDAD a captar o fijar por medio de fotografía o cualquier otro medio audiovisual mi imagen, mi voz, mis opiniones, mis declaraciones, mis comentarios o mis reacciones en cualquier producto, formato, medio o plataforma vinculados directa o indirectamente con el objeto de LA UNIVERSIDAD, y a divulgar o difundir total o parcialmente dicha información.

b. Autorizo expresamente a LA UNIVERSIDAD a utilizar mi imagen individual o en grupo en actividades dentro y fuera de la comunidad académica, siempre y cuando dichas actividades tengan una connotación académica o comercial para el desarrollo del objeto social de LA UNIVERSIDAD en las áreas de investigación, docencia, extensión o cualquier otra forma de utilización que considere conveniente.

c. La utilización de mi imagen deberá, en todo caso, ser realizada por LA UNIVERSIDAD dentro del marco del respeto de los derechos fundamentales y del artículo 14 de la Constitución Política de Colombia.

d. Autorizo a LA UNIVERSIDAD a la divulgación de mi imagen sin restricciones ni límites en el tiempo o geográficos, así como sin limitación para su reproducción o su difusión en cualquier medio conocido o por conocer, siempre y cuando se realice bajo los supuestos establecidos en el presente documento. En virtud de esa autorización, mi imagen podrá ser exhibida en el territorio colombiano y en el extranjero, y, en general, podrá ser utilizada a través de cualquier medio directo o indirecto, electrónico o virtual, o por cualquier otro medio conocido o por conocer.

e. Manifiesto que por la utilización de mi imagen no recibiré ningún tipo de remuneración, y, por tanto, la autorización de esta se concede a título gratuito.

f. Autorizo a LA UNIVERSIDAD a reproducir, transformar, comunicar públicamente y distribuir mi imagen en el formato que ella establezca.

g. En caso de presentarse cualquier reclamación o acción judicial o extrajudicial por parte de un tercero en cuanto a los derechos sobre mi imagen, asumiré toda responsabilidad y saldré en defensa y saneamiento de los derechos aquí otorgados; para todos los efectos, LA UNIVERSIDAD actuará como un tercero de buena fe.

h. Declaro que, a mi leal saber y entender, no se requiere el consentimiento de ninguna otra persona para permitirle a LA UNIVERSIDAD el uso de mi imagen, y que tal uso no viola ni infringe mis derechos personales, ni derechos de terceros ni de ningún otro tipo.

2. Tratamiento de datos personales

Si bien la información suministrada por usted se encuentra bajo nuestra custodia, ella puede estar almacenada en nuestros servidores o en los servidores de la entidad con los cuales La Universidad tiene convenio para almacenamiento de información, contando con todas las medidas de seguridad físicas, técnicas y administrativas para evitar su pérdida, su adulteración y su uso fraudulento o no adecuado. Por lo anterior, usted autoriza la transmisión de sus datos personales, incluyendo los datos personales sensibles a un tercer país, que cuenta con los estándares de seguridad en la protección de datos personales fijados por la Superintendencia de Industria y Comercio.

3. Derechos del titular y canales habilitados para ejercer el derecho de *hábeas data*

Usted tiene derecho a conocer, actualizar y corregir sus datos personales; también podrá solicitar la supresión o revocar la autorización otorgada para su tratamiento. En caso de un reclamo o una consulta relativa a sus datos personales, puede hacerla ingresando la petición en la opción "solicitudes" de la página *web* de La Universidad, remitiendo la solicitud al correo electrónico habeasdata@urosario.edu.co o dejando su petición 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. a 7:00 p. m., y los sábados de 8:00 a. m. a 1:00 p. m.

4. Indicación de la consulta de la política

Si quiere más información sobre el tratamiento de sus datos personales, consulte nuestra Política de Tratamiento de Datos personales en www.urosario.edu.co/politica

Nombre: _____

Firma: _____

Identificación: _____

Fecha: _____

Evidencia de la autorización por parte del titular

Aviso de privacidad
Universidad del Rosario

La Universidad del Rosario, como responsable del tratamiento de datos personales, le informa, por medio del presente aviso, las finalidades del tratamiento de los datos personales: gestión administrativa, académica y cultural de la comunidad universitaria, conforme a su vinculación con La Universidad —en especial, de estudiantes prospectos, inscritos, admitidos, y estudiantes activos e inactivos; envío de comunicaciones físicas y electrónicas con el fin de brindar información de la oferta académica y de actividades curriculares y extracurriculares organizadas por La Universidad; gestión de beneficios para los egresados, a través de alianzas, convenios y descuentos en productos y servicios en salud, turismo, deporte, recreación, servicios profesionales y publicaciones, contratación y gestión de nómina de personal, creación y actualización de proveedores; garantizar la seguridad de los bienes y las personas que se encuentran en las instalaciones de La Universidad, a través de actividades de videovigilancia, prestación de servicios de salud y consulta médica general, y trámite a la solicitud de consultas y reclamos.

Cuando se trate de datos personales de menores de edad, la Universidad del Rosario respeta los derechos prevalentes en el tratamiento de los datos personales, así como el aseguramiento por el interés superior de los niños, y los adolescentes. Por lo anterior, es obligación de La Universidad informarle que no está obligado a entregar la información del menor, pues se trata de un proceso voluntario.

En el tratamiento de los datos personales que recoge La Universidad, es nuestro deber informarle que son facultativas las preguntas relativas a datos personales sensibles.

Los tipos de tratamiento de la información personal por parte de La Universidad se establecen en: recolección, uso, circulación restringida, almacenamiento y disposición final. Para conocer los detalles puede, consultarlos en la Política de Tratamiento de Datos Personales.

Usted tiene derecho a conocer, actualizar y corregir sus datos personales; también podrá solicitar la supresión o revocar la autorización otorgada para su tratamiento. En caso de un reclamo o una consulta relativos a sus datos personales, puede hacerlos ingresando la petición en la opción "solicitudes" de la página *web* de La Universidad remitiendo la solicitud al correo electrónico habeasdata@urosario.edu.co, o dejando su petición 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. a 7:00 p. m., y los sábados de 8:00 a. m. a 1:00 p. m.

Si quiere más información sobre el tratamiento de sus datos personales, consulte nuestra Política de Tratamiento de Datos personales en www.urosario.edu.co.

Autorización a través de llamada telefónica

Condición: el responsable de la captura de los datos personales debe realizar la llamada desde una línea que grabe.

Guion:

Le informamos que esta llamada está siendo grabada para garantizar la efectiva prestación del servicio. "Para poder continuar, ¿Usted autoriza el tratamiento de sus datos personales a la Universidad del Rosario, conforme a nuestra Política de Tratamiento de Datos Personales, ubicada en el home de nuestra página web www.urosario.edu.co para el suministro, el contacto y el envío de información referente a su actividad académica, de bienestar o financiera en La Universidad?

- Si la respuesta es afirmativa: se procede a capturar los datos personales y registrarlos en la herramienta de CRM requerida para el proceso.
- ***Si la respuesta es negativa:*** *No se pueden capturar los datos personales; solo se brinda información y se le indica que no es posible enviarle información pues no autorizó el tratamiento de los datos.*

ANEXO II

Propietarios y subpropietarios de bases de datos personales

A continuación se relacionan los propietarios por cada base de datos personales pertenecientes a La Universidad:

N°	Base de datos	Propietario	Subpropietarios
1	Consultorio Jurídico	Director, Consultorio Jurídico	Psicólogo estudiantil
			Profesional de práctica jurídica
			coordinador área conciliación
2	Contratistas	Jefe de contratación y nómina	
3	Educación Continua	Gerente de Educación Continua	Coordinador Mercadeo Educon
4	Egresados	Director de Desarrollo y Egresados	Asistente de sistemas e información
5	empleados	Jefe de Contratación y Nómina	
		Jefe de Atracción, Selección y Formación	
		Coordinador de Seguridad y Salud en el Trabajo	
6	Estudiantes	Director de Registro y Control Académico	Jefe de Deportes
			Director de Formación y Desarrollo
			Jefe de servicios
			Director de estudiantes
			Directores de programa
			Director de Comunicaciones Estratégicas
7	Estudiantes prospectos	Director de Marketing y Comunicaciones	Coordinación inforosario
			Jefe de Promoción y Divulgación
			Coordinador de relacionamiento con colegios
8	Historias clínicas	Coordinador de Servicio Médico	
9	Inscritos y admitidos	Coordinador de Admisiones	
10	PQR	Jefe de servicios	
		Oficial seguridad de información y datos personales	
11	Profesores	Profesional de Gestión y Liderazgo	
12	Proveedores, acreedores y otros	Jefe de compras y suministros	Profesional de compras y suministros
			Directora de contabilidad
13	Videovigilancia	Jefe de seguridad y servicios generales	