LINEAMIENTOS PARA LA GESTIÓN DEL PROGRAMA INTEGRAL PARA LA PROTECCIÓN DE DATOS PERSONALES

ELABORADO POR: ANDRÉS VÉLEZ,

JEFE DE SEGURIDAD INFORMÁTICA, OFICIAL DE PROTECCIÓN DE DATOS PERSONALES

APROBADO POR: COMITÉ INSTITUCIONAL DE PROTECCIÓN DE DATOS PERSONALES

SEPTIEMBRE DE 2024

Tabla de contenido

1. Alcance

A continuación, se establecen los lineamientos relacionados con la gestión de datos personales de la Fundación Universidad del Norte. Estas disposiciones son obligatorias para todas las dependencias académicas y administrativas que traten con datos e información personal, en aras de dar cumplimiento a la normativa vigente específicamente la Ley estatutaria 1581 de 2012, como base fundamental para el desarrollo de las actividades de tratamiento de datos personales, Decreto único reglamentario 1074 de 2015 y la Guía de principio de responsabilidad demostrada.

Dados los diferentes proyectos y convenios internacionales en los que participa la Universidad, se dará cumplimiento al Reglamento General de Protección de Datos (RGPD) (Reglamento (EU) 2016/679), cuando aplique.

Los objetivos de estos lineamientos son:

- Cumplir la legislación vigente de Protección de Datos Personales en todas las actividades que impliquen una forma de tratamiento de datos personales.
- Almacenar los datos personales recolectados por la Universidad, en condiciones de seguridad informática adecuadas, consolidadas en bases de datos que se encuentran bajo la responsabilidad de la Universidad.
- Tratar los datos personales de acuerdo con la Política de Tratamiento de datos de la Universidad, y para las finalidades por las cuales fueron autorizadas por su titular.
- Garantizar que las áreas que tienen a cargo la custodia y tratamiento bases de datos personales, conozcan sus deberes y obligaciones con relación a la protección y manejo de dichos datos.

En general, el presente documento tiene como objeto brindar información clara y suficiente relacionada al Tratamiento de Datos Personales, la cual es requerida por las diferentes partes interesadas, adicionalmente se contemplan directrices de cumplimiento para sus trabajadores, proveedores y terceros que tengan una relación vinculante con la Universidad.

2. Definiciones

Las definiciones relacionadas en este numeral se encuentran establecidas en la normatividad actual vigente, ley 1581 de 2012, decreto único reglamentario 1074 de 2015 y la Guía de principio de responsabilidad demostrada.

Aviso de privacidad: Comunicación verbal o escrita generada por el Responsable dirigida al Titular para el Tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de Tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del Tratamiento que se pretenden dar a los datos personales.

Base de datos: Conjunto organizado de datos personales que sea objeto de tratamiento.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

Registro Nacional de Bases de Datos: Es el directorio público de las bases de datos sujetas a tratamiento que operan en el país. El registro será administrado por la Superintendencia de Industria y Comercio y será de libre consulta para los ciudadanos.

Responsable del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el Tratamiento de los datos.

Superintendencia de Industria y Comercio: También conocida como SIC por sus siglas, es el organismo designado por la Ley general de protección de datos personales, para velar por el cumplimiento de la legislación en materia de datos personales a través de la Delegatura para la Protección de Datos Personales, y las demás funciones asignadas a través del artículo 21 de la Ley 1581 de 2012.

Titular: Persona natural cuyos datos personales sean objeto de tratamiento.

Transferencia de datos: Tiene lugar cuando el Responsable y/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.

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

Recolección: obtención inicial de los datos personales que suministra el titular a la institución.

Almacenamiento: alude al reposo y conservación de la información personal correspondiente a una base de datos determinada.

Uso: es el empleo de la información personal almacenada en una base de datos para la consecución de una finalidad, que fue informada en la recolección.

Circulación: se refiere al tránsito de la información personal almacenada en una base de datos sea de forma interna o externa.

Supresión: consiste en la eliminación de los datos contenidos en una base de datos determinada, una vez concluya la finalidad del tratamiento.

Autorización: Consentimiento previo, expreso e informado del Titular para llevar a cabo el Tratamiento de datos personales.

Confidencialidad: Elemento de seguridad de la información que permite establecer quienes y bajo qué circunstancias se puede acceder a la misma.

Dato personal: Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.

Dato Público: Es el 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 u 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 Semiprivado: Es aquella información que no es de naturaleza íntima, reservada ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como es el caso de los datos financieros, crediticios o actividades comerciales

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

Derecho de Los Niños, Niñas y Adolescentes: En el Tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes. Sólo podrán tratarse aquellos datos que sean de naturaleza pública.

Gestión de incidentes de seguridad de la información: Procesos para detectar, reportar, evaluar, responder, tratar y aprender de los incidentes de seguridad de la información.

3. Roles y Responsabilidades

3.1 Comité de Protección de datos personales

Según Resolución Rectoral No. 10 de enero 31 de 2022, "Por la cual se amplía el Comité de Protección de Datos Personales", el Comité de Protección de Datos Personales tendrá la función de la aprobación del programa integral de gestión de datos personales y realizará seguimiento a su implementación. Cada representante tendrá la obligación de velar por comunicar a sus dependencias, las directrices y recomendaciones del comité, para garantizar la protección de los datos personales tratados en sus áreas, en cumplimiento de la normativa legal.
Corresponde al presidente del Comité y/o al Jefe de Seguridad Informática convocar a las sesiones del Comité las cuales podrán ser presenciales o virtuales.

El Comité de Protección de Datos Personales, estará conformado de la siguiente manera:

- El Director de la Dirección de Tecnología Informática y de Comunicaciones, quien lo presidirá;
- El Director de la Oficina Jurídica;
- El Director de Comunicaciones y Mercadeo;
- El Director de Admisiones,
- Un delegado de la Auditoría;
- Un representante de la academia;
- Un representante del área de Investigaciones
- Un representante del área de Extensión.
- Dos (2) decanos.

3.2 Oficina Jurídica

Es responsabilidad de la Oficina Jurídica:

- Desarrollar y mantener actualizada la política de Protección de Datos, así como también los avisos de privacidad.
- Notificar al oficial de protección de datos personales sobre contratos y/o convenios que impliquen transmisión y o transferencia de datos personales.
- En conjunto con el oficial de protección de datos personales, resolver dudas e inquietudes y determinar cómo proceder referente al tratamiento de datos personales en situaciones particulares.

3.3 Oficial de Protección de Datos Personales

Las funciones del Oficial de Protección de datos son las siguientes:

- Cumplir con la gestión del RNBD (Registro Nacional de Base de Datos) y la gestión de reclamos y consultas de los titulares.
- Actualizar el Registro de Tratamiento de datos personales, según el RGPD.
- Recabar información para determinar las actividades de Tratamiento.
- Analizar y comprobar la conformidad con la normativa de las actividades de Tratamiento.
- Coordinar la definición e implementación de los controles del Programa Integral de Gestión de Datos Personales.
- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
- Impulsar una cultura de protección de Datos personales en poder de la organización y su debida clasificación según su naturaleza.
- Obtener las declaraciones de conformidad de la Superintendencia de Industria y Comercio cuando sea requerido.
- Obtener la certificación de las Normas Corporativas Vinculantes por parte de la Superintendencia de Industria y Comercio cuando sea requerido.
- Revisar los contenidos de los contratos de transferencias nacionales o internacionales de Datos personales que se suscriban con otros responsables del Tratamiento.
- Revisar los contenidos de los contratos de transmisión nacional o internacional de Datos personales que se suscriban con Encargados del Tratamiento.
- Realizar un entrenamiento general en protección de Datos personales para todos los empleados de la compañía.
- Velar por la implementación de planes de auditoría interna para verificar cumplimiento de sus políticas de Tratamiento de información personal.
- Acompañar y asistir a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio.
- Realizar seguimiento al Programa Integral de Gestión de Datos Personales.
- En conjunto con la Oficina Jurídica, resolver dudas e inquietudes y determinar cómo proceder referente al tratamiento de datos personales en situaciones particulares.
- Escalar a los líderes de proceso o responsables de tratamiento de bases de datos las consultas y reclamos de los titulares para su adecuada gestión.

Estas funciones no son excluyentes de las establecidas mediante Resolución Rectoral.

3.4 Líderes de Proceso/Directores de Proyectos

Es responsabilidad de los líderes de proceso o directores de proyectos:

- Informar al Oficial de Tratamiento de Datos Personales, los cambios que deban reportarse según las bases de datos que han sido definidas a su cargo.
- Gestionar los reclamos y consultas de los titulares que el oficial de protección de datos personales escale.
- Reportar posibles riesgos que expongan los datos personales.
- Cumplir con los deberes de confidencialidad, estricto cumplimiento de la política y finalidades autorizadas por los titulares, así como lo definido en este documento.

4. Lineamientos

4.1 Recolección

Para la recolección de la información y de la autorización del tratamiento debe realizarse según la siguiente información:

Medio: Físico o Digital:
Entrega de los datos: Directamente del titular o a través de un tercero (fuentes abiertas, información pública, fuentes autorizadas por ley, tercero con relación contractual).
La recolección debe hacerse:
-A través de la herramienta CRM y sus herramientas de automatización integradas para recolectar datos de poblaciones de prospectos, estudiantes y egresados para la gestión de contactos e información comercial.
- A través de formularios web dispuestos por Marketplace. Estos formularios deben contener aviso de privacidad y el check de autorización.
- A través de formularios web dispuestos por sistemas de colaboración como Formularios de Office365, Zoom; sistemas de gestión de eventos como Eventbrite; sistemas de gestión de encuestas como Qualtrics; para datos de otra población. Estos formularios deben contener aviso de privacidad y el check de autorización. Los funcionarios que recolecten datos personales a través de estas herramientas deben diligenciar el formato de recolección de datos para aplicaciones externas y en conjunto con los datos recolectados (Se debe descargar el reporte que genera la herramienta), deben ser enviados al correo basededatos@uninorte.edu.co en un plazo máximo de 10 días para el almacenamiento de su autorización.
-A través de formularios físicos que deben ser digitalizados realizando la solicitud, en un plazo máximo de 10 días, al correo digitalizacion@uninorte.edu.co . Estos formatos deben contener el aviso de privacidad y la autorización debe llevar la firma de la persona. Un formato físico podrá ser utilizado para recoger los datos de una o varias personas.
-A través de Llamadas. El Centro de Contacto de la Dirección de Tecnología Informática y Comunicaciones es la única oficina en la institución que cuenta con la infraestructura necesaria para grabar las llamadas y por ende registrar las evidencias de consentimiento

que se entreguen por este canal.
- A través de otros medios aprobados por DTIC o por el comité de protección de datos personales.

No son válidos otros medios distintos a los mencionados anteriormente, por ejemplo, chats personales como WhatsApp.

Todas las bases de datos personales deben estar centralizadas y controladas por el área de DTICS, ningún funcionario, contratista, proveedor, podrá conservar bajo su administración y manejo, bases de datos personales que no gocen de los estándares de seguridad informática institucionales.

4.2 Autorización

Para realizar el tratamiento de datos personales, de manera previa e informada se deberá solicitar al titular de la información la autorización respectiva. En la autorización se deberá explicar cuál es la finalidad del tratamiento y que destinación se le van a dar a los datos, así como los derechos que tiene el titular frente a su información. Cualquier uso de los datos que esté por fuera de la autorización dada, se constituirá en una violación al derecho de habeas data de la persona natural.

La autorización puede ser escrita, verbal o incluso incluir conductas inequívocas (Evitarla en la medida de lo posible) del titular de la información, que permitan concluir que el propietario otorgó la autorización respectiva. En cualquiera de los casos mencionados se deberá contar con la prueba de la autorización previa, expresa e informada del titular de la información.

No se requerirá autorización de datos personales en los siguientes eventos:

- Una entidad pública o administrativa requiera la información, siempre que esté en cumplimiento de sus funciones legales o por decisión judicial. Así mismo en la comunicación remitida a la Universidad, la autoridad deberá justificar las funciones o la providencia judicial en la que se ampara. En este evento se recomienda revisar con la oficina jurídica, si la entrega de datos se adecua a la citada causal antes de realizar cualquier acción.
- Datos de naturaleza pública, tales como documentos públicos, sentencias judiciales debidamente ejecutoriadas, los relativos al estado civil de las personas, información relativa a la profesión u oficio, a la calidad de comerciante o de servidor público.
- Casos de urgencia médica o sanitaria.
- Datos relacionados con el Registro Civil de las Personas.
- Conducta inequívoca al ingresar al campus.
- Cuando se recolecte información personal no sensible de contactos que ya tienen un vínculo con la institución (estudiantes, egresados, exestudiantes, empleados) y

que no hayan revocado su autorización de tratamiento.

- Cuando un titular solicite información a alguna dependencia de la Universidad, por ejemplo, información sobre programas académicos, eventos, becas, créditos, etc., no se requiere contar con el consentimiento expreso o autorización de tratamiento de datos personales, para dar respuesta puntual a la solicitud realizada. Se entiende que se trata de una conducta inequívoca por medio de la cual el titular conoce y autoriza la finalidad de tratamiento de su información, la cual se limita a dar respuesta a su inquietud o solicitud de información.

Las dependencias que utilizan la plataforma CRM deben ingresar en la vista de la persona y registrar en el campo “Ubicación Evidencia de Autorización” de la pestaña “Seguimiento” dónde reposa la evidencia de la autorización de tratamiento.

4.3 Almacenamiento

Las autorizaciones de tratamiento de datos personales deben ser almacenadas en:

- Plataforma CRM y sus herramientas integradas (Salesforce) para la gestión de contactos e información comercial. Toda dependencia académica o administrativa que se encuentre habilitada para hacer uso de este sistema debe realizar la gestión de datos e información personal exclusivamente con este sistema.
- Sistema de Gestión Documental AZDigital, para información recolectada a través de medios físicos y se debe solicitar su digitalización realizando la solicitud, en un plazo máximo de 10 días, al correo digitalizacion@uninorte.edu.co. .
- Sistema desarrollado por Dirección de Tecnología Informática y Comunicaciones donde se debe subir la información obtenida de los formatos de recolección de datos para aplicaciones externas y en conjunto con los datos recolectados (Se debe descargar el reporte que genera la herramienta), los cuales deben ser enviados por los funcionarios al correo basededatos@uninorte.edu.co en un plazo máximo de 10 días para el almacenamiento de su autorización.
- Sistema de grabación de llamadas institucional operado por Dirección de Tecnología Informática y Comunicaciones.

Los datos personales deben ser almacenados en:

- Sistema de Información Banner y sus sistemas integrados.
- Plataforma CRM y sus herramientas integradas (Salesforce) para la gestión de contactos e información comercial. Toda dependencia académica o administrativa que se encuentre habilitada para hacer uso de este sistema debe realizar la gestión de datos e información personal exclusivamente con este sistema.
- Sistemas de Gestión de eventos e inscripción a cursos de extensión e idiomas (Marketplace).
- Turpial y otros sistemas aprobados por Dirección de Tecnología Informática y

Comunicaciones.

- Sistemas de colaboración como Formularios de Office365, Zoom; sistemas de gestión de eventos como Eventbrite; sistemas de gestión de encuestas como Qualtrics. Los funcionarios que recolecten datos personales a través de estas herramientas deben diligenciar el formato de recolección de datos para aplicaciones externas y enviarlo, junto con los datos recolectados (Se debe descargar el reporte que genera la herramienta), al correo basededatos@uninorte.edu.co en un plazo máximo de 10 días para el almacenamiento de su autorización.

Dirección de Tecnología Informática garantizará que en cada uno de los sistemas anteriormente mencionados existan mecanismos para almacenar la información de manera segura.

Es responsabilidad de cada área garantizar que no compartan o circule la información a personas no autorizadas.

4.4 Uso y Circulación

La información que deba circular a través de cada una de las áreas de la Institución y que corresponde a estudiantes, funcionarios administrativos, docentes y terceros en general se podrá hacer de la siguiente manera:

- Circulación interna: Los datos personales solo serán tratados por el personal debidamente autorizado, y, en el caso de los datos sensibles, deberá garantizarse estrictos niveles de confidencialidad. Para esto se hace se hace uso de la Herramienta de colaboración corporativa y herramienta CRM.
- Circulación externa: Corresponde al tratamiento de datos personales que deba realizar un agente externo a la institución.
    - Debe evitarse si:
        - En la autorización dada por el titular de la información, no se incluyó la posibilidad de entregar a terceras entidades, dentro o fuera de Colombia, su información.
        - El tercero está en un país que no proporciona los niveles adecuados de protección de datos, conforme con los estándares fijados por la Superintendencia de Industria y Comercio.
        - El tercero no cumple con los estándares de seguridad mínimos establecidos por la Dirección de Tecnología e Informática de la Universidad del Norte.
        - La entrega de datos a terceros no está amparada en un contrato o convenio.
    - Puede darse de dos formas:
        - Transmisión (Entre la universidad y un encargado): Debe suscribirse un contrato de transmisión de datos que regule el acceso a los datos

por parte del tercero ya sea en línea (Accesos a sistemas directamente) o fuera de línea.

- Transferencia (Entre la universidad y un responsable): Se debe evitar esta figura solicitando a los titulares de los datos entregar la información directamente al otro responsable. En caso de que sea estrictamente necesario debe suscribirse un contrato de transferencia de datos.

No son válidos para realizar la circulación y uso de los datos, otros medios distintos a los mencionados anteriormente, por ejemplo, chats personales como WhatsApp.

Para el caso de gestión de cobranza y de mercadeo se debe cumplir con lo estipulado en la Ley 2300 de 2023, en cuanto a los horarios (de acuerdo con la hora legal colombiana) y medios de contacto.

En todo caso la entrega de datos personales a terceras entidades y la recepción de datos personales de parte de otra entidad deberá ser avalado por el Comité de Datos Personales, así como las condiciones de esta entrega.
En estos casos deberá asegurarse la inclusión en el contrato con los terceros, de la cláusula de responsabilidad conforme a los lineamientos de la política de gestión de encargados del tratamiento, con la finalidad de que el tratamiento se realice bajo los lineamientos legales vigentes.
Lo anterior, garantizará el respeto de los derechos de los titulares, los que son armónicos con las disposiciones establecidas en la política de tratamiento de datos personales.

4.4.1 Datos Sensibles

En la recolección de información sensible, es decir, aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos; se debe tener presente que el titular no está obligado a autorizar su tratamiento, y así se debe indicar en los textos de autorización de tratamiento de datos personales, por tanto ninguna actividad podrá condicionarse a que el titular suministre datos personales sensibles.

Las áreas que recolectan datos sensibles deben evitar compartir dicha información con otras áreas, salvo solicitud expresa y aprobada por el oficial de protección de datos personales.

4.4.2 Menores de edad

El tratamiento de información de menores de edad está proscrito por la Ley, y requiere obligatoriamente de la autorización de sus representantes legales o cuando contando con dicho aval, el uso del dato pone al menor en circunstancia de vulnerabilidad, de tal manera que sus derechos fundamentales, así como su intimidad y seguridad se ven afectados.
El tratamiento de datos personales está permitido excepcionalmente, con autorización del tutor legal de menor, cuando: - La finalidad del tratamiento responda al interés superior de los niños, niñas y adolescentes • Se asegure el respeto de sus derechos fundamentales de los niños, niñas y adolescentes. • De acuerdo con la madurez del niño, niña o adolescente se tenga en cuenta su opinión. • Se cumpla con los requisitos previstos en la Ley 1581 de 2012 para el tratamiento de datos personales.

Se debe EVITAR hacer uso de imágenes de menores de edad cuando: (i) Se exhibe a los menores siendo víctimas o victimarios de hechos punibles (ii) el uso de la fotografía pone al menor en una circunstancia de vulnerabilidad, de tal manera que sus derechos fundamentales, así como su intimidad y seguridad puedan ser afectados con el uso de la foto y (iii) El uso de la fotografía no sea estrictamente necesario para la finalidad que se persigue.

Conforme con el artículo 44 de la Constitución Política de Colombia, los derechos de los niños prevalecen sobre los derechos de los demás, lo que significa que su bienestar prima sobre cualquier interés administrativo, académico o científico.

Los sistemas y procesos deben estar en la capacidad de solicitar los datos del tutor legal, en caso de niños, niñas y adolescentes menores a 18 años. Para los casos de suministrar información sobre el acceso al servicio educativo de la Universidad, es viable la autorización por parte del mayor de 12 años, sin la autorización previa del tutor legal, por tratarse de un interés superior como lo es el acceso a la educación.

4.4.3 Campañas masivas

Los siguientes son los lineamientos que deben cumplirse en la realización de las campañas o envíos masivos de mensajes de promoción o mercadeo:

- Las campañas de mercadeo o promoción deberán ser realizadas solamente con titulares de los cuales se tenga su consentimiento expreso o autorización de tratamiento. Para el caso de los estudiantes, egresados o funcionarios, este consentimiento se obtiene en el momento de su vinculación con la institución.
- Todas las campañas masivas realizadas vía correo electrónico deberán contar con una opción de “darse de baja” o “unsusbcribe”, de tal manera que los titulares puedan solicitar que no se les envíe información de ese tipo. Cabe aclarar que una solicitud de “darse de baja” de una lista de distribución aplica para una cuenta de correo y no para la persona (una persona puede tener varias cuentas de correo y la

solicitud de “darse de baja” de la lista de distribución aplica para la cuenta de correo en la que recibió el mensaje correspondiente a la campaña y no para todas sus cuentas de correo). En ningún caso puede entenderse una solicitud de “darse de baja” como una revocatoria de autorización de tratamiento, la cual debería realizarse usando el procedimiento descrito en la Política de privacidad de datos personales que se encuentra publicada en el sitio web institucional. Sin embargo, es importante tener presente que, si una persona revoca la autorización de tratamiento o no la entrega y si su solicitud es procedente, no podrá ser objetivo en ninguna campaña de mercadeo o promoción. La plataforma CRM provee todas las funcionalidades para realizar campañas de envío de correos electrónicos en forma masiva de información, promoción de programas, invitación a ferias o eventos. En ese sentido, deberán seguirse los pasos de creación de listas de público objetivo, definición de campañas, asociación de listas de público objetivo a campañas y el uso de la herramienta dispuesta para el envío y seguimiento de correos masivos. El detalle de cómo realizar estas tareas se encuentra descrito en el manual de usuario del sistema.

- Los mensajes SMS podrán ser enviados únicamente a titulares que hayan manifestado un interés por un evento o tema en particular. No podrán enviarse mensajes SMS de manera masiva.

4.4.4 Uso de Imágenes

Las fotografías o videos a través de los cuales se fija la cara de una persona u otras partes del cuerpo que hacen identificable al titular, se entiende como recolección de dato biométrico. En el caso de actividades académicas, de investigación o extensión se entiende que los mismos no tienen una finalidad doméstica y en consecuencia es indispensable que se obtenga la autorización por escrito del titular, entendiendo que el dato biométrico es un dato sensible.

Si la fotografía o filmación incluye a personas que pueden ser identificadas o individualizadas, el responsable de la fotografía deberá solicitar autorización para usar la imagen, en especial si se está en un espacio privado o en un salón de clases, un laboratorio, baño y en general en cualquier espacio donde existe una mayor expectativa de privacidad, así el mismo no sea privado.

En el caso de las fotografías o filmaciones, con fines académicos o científicos, de una cirugía o de un paciente que presenta una patología médica, requieren de la autorización del médico tratante, cirujano o entidad responsable del equipo médico correspondiente, quienes a su vez deben garantizar que el paciente haya dado su autorización para esta fijación.

En los eventos públicos o privados, se debe comunicar al público e informar mediante aviso de privacidad que la actividad va a ser fotografiada, grabada, transmitida y puesta a

disposición en los canales y redes sociales institucionales, por lo que es posible que su asistencia al evento quede fijada en la grabación. Así mismo, mencionar que esta grabación hará parte de los archivos institucionales, los cuales pueden ser usados para creación de contenido institucional, tales como folletos, videos, libros, etc. Este anuncio al público debe quedar grabado o filmado como evidencia y consulta posterior.

4.4.5 Charlas, simposios, congresos

Se debe verificar con el organizador del evento, si el conferencista ha aceptado la grabación de su intervención o no. En caso de que el organizador indique que el invitado ha aceptado esta grabación, el responsable del evento deberá solicitarle de manera previa al inicio de la actividad, la autorización de tratamiento de datos personales.

Si el invitado es una figura pública, se recomienda que en la invitación se le manifieste que: (i) Su participación va a ser grabada, transmitida y puesta a disposición en los canales y redes sociales institucionales. (ii) Su imagen va a ser usada para la publicidad del evento y que su participación será retratada para efecto de los archivos institucionales. (iii) Que los archivos institucionales pueden ser usados para creación del contenido institucional, tales como folletos, videos, libros, documentales, etc (iv) Que el invitado se hace plenamente responsable de las declaraciones o comentarios que realice durante la actividad y en consecuencia su participación no representa la opinión de la Universidad del Norte. Así mismo se debe indicar que en caso de no estar de acuerdo, el invitado debe manifestar tal decisión al organizador del evento.

4.4.5 Datos anónimos

Se entiende que el dato es anónimo, cuando desde su recolección, análisis o correlación de los datos no se tendrá información a través de la cual una persona sea identificada o identificable. En estos casos se podrá prescindir de la autorización respectiva.

De manera ilustrativa, se presentan los siguientes ejemplos a través de los cuales se observa cuando no se está frente a datos anónimos:

- El proceso de recolección incluye la grabación del sujeto y sus respuestas.
- Se incluye una descripción física de la persona, que hace que el titular de la información sea identificable.
- Se describe el ambiente de trabajo, de estudio o características del lugar de residencia, que hace que el titular de la información sea identificable.
- Se incluye información de los representantes legales de menores de edad, así no se indique el nombre del menor.

Se deberá anonimizar completamente los datos en el marco de actividades académicas, para entrega a terceras entidades en virtud de una relación contractual o información de

menores de edad, especialmente si son datos sensibles.

4.5. Supresión

La supresión de los datos personales es una exigencia de la Ley para los datos sobre los cuales no se cuenta con una finalidad legítima para permanecer almacenados al interior de la entidad.
Cuando se eliminen documentos físicos o electrónicos de datos personales, se deberá efectuar un procedimiento que asegure:

- Que la eliminación sea autorizada por el área que custodia la información.
- Que sea apropiada e irreversible.
- Que sea documentada y confidencial.

Lo anterior, solo se puede realizar si las series documentales han perdido valor y utilidad administrativa. Cuando el titular tenga una relación contractual o una vinculación académica vigente, no procederá la solicitud de supresión, ni cuando las normas aplicables exijan la conservación; caso de la información contable y del sistema general de seguridad social.
Cuando se realice la supresión de datos personales de las bases de datos, deberá dejarse constancia de ello a través de un acta o documento equivalente.

4.6 Sensibilización y entrenamiento para el tratamiento adecuado de los datos personales.

Para el desarrollo seguro de las actividades institucionales, los funcionarios, contratistas y terceros vinculados con la Universidad, deben de recibir la sensibilización; es decir, las orientaciones necesarias para la implementación de la Ley de Protección de Datos Personales. El Oficial de Tratamiento de Datos Personales debe genera los procesos de Sensibilización y Entrenamiento, así como evaluar de manera periódica la pertinencia de los contenidos establecidos. Los puntos establecidos para determinar y mejorar los contenidos de sensibilización y entrenamiento serán:

Los cambios de la normatividad lega establecida en el marco de la regulación para el tratamiento de datos personales.
Las políticas, procedimientos y controles establecidos en el marco de la implementación del Plan Integral de Tratamiento de datos personales. Sera responsabilidad todos los funcionarios participar en las diferentes capacitaciones.

4.7 Gestión de encargados del tratamiento

La Universidad realizara procesos de encargo de datos personales a terceros con quienes tenga una relación operativa o contractual para la prestación de servicios necesarios para su funcionamiento administrativo o de conformidad con sus actividades académicas, de investigación y extensión. En ese sentido, se adoptarán las medidas necesarias para que las entidades y las personas que las representan y que tengan acceso a datos personales cumplan con la Política de Tratamiento de Datos de la Universidad y con los principios de protección de datos personales y obligaciones establecidas en la Ley. Conforme a lo definido en el ARTÍCULO 2.2.2.25.5.2. del decreto único 1074 de 2015 se define que para la **contratación de encargados deberá establecerse un contrato de transmisión de datos personales**, el contrato que suscriba el Responsable con los encargados para el tratamiento de datos personales bajo su control y responsabilidad señalará los alcances del tratamiento, las actividades que el encargado realizará por cuenta del responsable para el tratamiento de los datos personales y las obligaciones del Encargado para con el titular y el Responsable.

La Universidad establecerá en sus contratos con encargados, los procesos de encargo del tratamiento en dicho contrato. El Encargado se comprometerá a dar aplicación a las obligaciones del responsable bajo la política de Tratamiento de la información fijada por este y a realizar el Tratamiento de datos de acuerdo con la finalidad que los Titulares hayan autorizado y con las leyes aplicables. Además de las obligaciones que impongan las normas aplicables dentro del citado contrato, deberán incluirse las siguientes obligaciones en cabeza del respectivo encargado: 1. Dar Tratamiento, a nombre del responsable, a los datos personales conforme a los principios que los tutelan. 2. Salvaguardar la seguridad de las bases de datos en los que se contengan datos personales encargados, con iguales o mejores estándares de seguridad. 3. Guardar confidencialidad respecto del tratamiento de los datos personales.

5. Anexos

5.1 Modelos de consentimientos y avisos de privacidad

A continuación, se presentan modelos de formatos para obtener el consentimiento de tratamiento y avisos de privacidad para formularios impresos y en formato web. Además, el aviso de privacidad relacionado con el tratamiento de la videovigilancia.

Las áreas pudieran adoptar avisos de privacidad específicos que vayan acorde con el tratamiento de datos personales que realizan o cuando se desee consolidarlos con otros formatos o autorizaciones que se recolectan de los titulares (Consentimientos médicos, investigaciones reguladas por el comité de ética, procesos de financiamiento estudiantil,

etc.), pero en esos casos, deben solicitar a la Oficina Jurídica el apoyo para la redacción de estos.

AVISO DE PRIVACIDAD

Este formulario contiene preguntas personales, sociales y académicas, y con su diligenciamiento, usted acepta el uso y tratamiento que la Fundación Universidad del Norte identificada con NIT 890.101.681-9 con domicilio en la ciudad de Barranquilla, Colombia, Km 5 Antigua Vía a Puerto Colombia, con línea telefónica de contacto 3509509, dará a esta información en consonancia con la Constitución, en la Ley 1581 de 2012, y a las políticas que se pueden consultar en el siguiente link: http://www.uninorte.edu.co/politica-de-privacidad-de-datos, y en especial con la siguiente finalidad: (incluir finalidad del tratamiento).

Como titular de la información a suministrar declara que la misma es totalmente actual, exacta y veraz. Asimismo, reconoce que es el único responsable de la información falsa, inexacta que suministre.

Sus derechos como titular de los datos suministrados, son los previstos en la Constitución y la Ley 1581 de 2012, y especialmente acceder en forma gratuita a los datos proporcionados, solicitar actualización y rectificación de su información, solicitar prueba de la autorización otorgada, revocatoria de la autorización y/o solicitar la supresión del dato (salvo cuando por disposición legal o contractual sea obligatorio conservar la información), presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a la normativa vigente.

Los titulares podrán ejercitar, en cualquier momento, sus derechos derivados o relacionados con la protección de datos personales (habeas data) a través de los medios y procedimiento indicado en la política de protección de datos personales de la Universidad al cual puede acceder en el siguiente link: https://www.uninorte.edu.co/politica-de-privacidad-de-datos.

Así mismo, he sido informado sobre el carácter facultativo que tiene el suministro de información sensible o datos de las niñas, niños y adolescentes. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES PARA ASUNTOS GENERALES DE LA UNIVERSIDAD

Por este medio acepto plenamente y autorizo a la FUNDACIÓN UNIVERSIDAD DEL NORTE a la recolección y tratamiento de los datos personales a través de formularios físicos, electrónicos o por cualquier medio por el cual pueda entregar a la UNIVERSIDAD información personal, para que esta proceda con la incorporación de los datos facilitados en la bases de datos de las cuales es titular y responsable la UNIVERSIDAD, y su tratamiento en los términos estipulados en el presente documento y en las normas vigentes al interior de la UNIVERSIDAD. La finalidad para la recolección, uso y tratamiento de datos personales a que se refiere esta política es la adecuada gestión, administración, mejora de las actividades y distintos servicios de la UNIVERSIDAD, realización de procesos internos, estadísticas, análisis cuantitativo y cualitativo de las actividades, tales como uso del campus o de los servicios ofrecidos por la UNIVERSIDAD, entre otros que resulten de interés para la institución. Igualmente podrá referirse al ofrecimiento de nuevos productos o mejora de los existentes que puedan contribuir con el bienestar académico, administrativo, financiero o de formación, ofrecidos por la UNIVERSIDAD o por terceros relacionados con su objeto. Manifiesto que la información anteriormente entregada a la UNIVERSIDAD es totalmente actual, exacta y veraz y reconozco mi obligación de mantener, en todo momento, actualizados los datos, de forma tal que sean veraces y exactos. En todo caso, reconozco que soy el único responsable de la información falsa o inexacta que realice y de los perjuicios que cause a la UNIVERSIDAD o a terceros, por la información que facilite. Al facilitar datos de carácter personal, acepto igualmente la remisión de información acerca de noticias, cursos, eventos, boletines y productos relacionados con la UNIVERSIDAD. La UNIVERSIDAD hará un uso responsable de la información entregada por los titulares, además de lo consagrado en su política de privacidad de uso y tratamiento de información personal, privacidad y confidencialidad de la información existente en las bases de datos solo suministrará información cuando este lo solicite o autorice expresamente, cuando medie decisión judicial o administrativa o cuando esta información esté prevista en los convenios interinstitucionales suscritos por la UNIVERSIDAD. He sido informado sobre el carácter facultativo que tiene el suministro de información sensible la cual tendrá carácter reservado y acerca de los derechos que me asisten como titular, para conocer, actualizar y solicitar la rectificación o supresión de datos conforme a los procedimientos y políticas de la institución establecidas en:

https://www.uninorte.edu.co/politica-de-privacidad-de-datos. Así mismo, sobre el carácter facultativo que tiene el suministro de información sensible o datos de las niñas, niños y adolescentes. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

La responsabilidad en el tratamiento de la presente información estará a cargo de la Fundación Universidad del Norte, Km.5 Vía Puerto Colombia - Tel. (57) (5) 3509509 - Barranquilla, Colombia.

AVISO DE PRIVACIDAD (INGRESO AL CAMPUS Y VIDEOVIGILANCIA)

La Fundación Universidad del Norte recolectará, almacenará y utilizará la información suministrada para el ingreso a nuestro campus con la finalidad de mantener la seguridad e integridad de la Institución, y de acuerdo a lo establecido en nuestra Política de Protección de Datos Personales, la cual puede ser consultada en el siguiente link: http://www.uninorte.edu.co/politica-de-privacidad-de-datos. Así mismo, la Universidad implementa sistemas de videovigilancia en su campus y alrededores con la misma finalidad.

Sus derechos como titular de los datos suministrados, son los previstos en la Constitución y la Ley 1581 de 2012, y especialmente acceder en forma gratuita a los datos proporcionados, solicitar actualización y rectificación de su información, solicitar prueba de la autorización otorgada, revocatoria de la autorización y/o solicitar la supresión del dato (salvo cuando por disposición legal o contractual sea obligatorio conservar la información), presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a la normativa vigente.

Los titulares podrán ejercitar, en cualquier momento, sus derechos derivados o relacionados con la protección de datos personales (habeas data) a través de los medios y procedimiento indicado en la política de protección de datos personales de la Universidad al cual puede acceder en el siguiente link: https://www.uninorte.edu.co/politica-de-privacidad-de-datos.

Así mismo, se informa sobre el carácter facultativo que tiene el suministro de información sensible o relacionada con niños, niñas y adolescentes, la cual tendrá carácter reservado. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

AUTORIZACIÓN PARA EL TRATAMIENTO DE DATOS PERSONALES
MODELO TEMAS ESPECÍFICOS

Declaro que he sido informado que la FUNDACIÓN UNIVERSIDAD DEL NORTE es la responsable del tratamiento de los datos personales obtenidos a través del diligenciamiento del presente formulario y que he leído las Políticas de Tratamiento de Datos Personales disponibles en el sitio web https://www.uninorte.edu.co/politica-de-privacidad-de-datos.

La responsabilidad en el tratamiento de la presente información estará a cargo de la Fundación Universidad del Norte, Km.5 Vía Puerto Colombia - Tel. (57) (5) 3509509 - Barranquilla, Colombia.

Manifiesto que la información anteriormente entregada a la UNIVERSIDAD es totalmente actual, exacta y veraz y reconozco mi obligación de mantener, en todo momento, actualizados los datos, de forma tal que sean veraces y exactos. En todo caso, reconozco que soy el único responsable de la información falsa o inexacta que realice y de los perjuicios que cause a la UNIVERSIDAD o a terceros, por la información que facilite. Al facilitar datos de carácter personal, acepto igualmente la remisión de información acerca de noticias, cursos, eventos, boletines y productos relacionados con la UNIVERSIDAD. La UNIVERSIDAD hará un uso responsable de la información entregada por los titulares, además de lo consagrado en su política de privacidad de uso y tratamiento de información personal, privacidad y confidencialidad de la información existente en las bases de datos solo suministrará información cuando este lo solicite o autorice expresamente, cuando medie decisión judicial o administrativa o cuando esta información esté prevista en los convenios interinstitucionales suscritos por la UNIVERSIDAD. He sido informado sobre el carácter facultativo que tiene el suministro de información sensible la cual tendrá carácter reservado y acerca de los derechos que me asisten como titular, para conocer, actualizar y solicitar la rectificación o supresión de datos conforme a los procedimientos y políticas de la institución establecidas en: https://www.uninorte.edu.co/politica-de-privacidad-de-datos. Así mismo, sobre el carácter facultativo que tiene el suministro de información sensible o datos de las niñas, niños y adolescentes. Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición así como los datos relativos a la salud, a la vida sexual y los datos biométricos.

Por ello, consiento y autorizo de manera previa, expresa e inequívoca que mis datos personales sean tratados con sujeción a lo establecido en sus Políticas de Protección de Datos Personales, atendiendo a las finalidades en ellas señaladas, y las siguientes: (incluir finalidad del tratamiento)

Igualmente, queda autorizada la grabación de imágenes o cualquier otro registro que sirvan de soporte y evidencia de los eventos realizados. (incluir esta parte si es pertinente)

Como Titular de información tengo derecho a conocer, actualizar y rectificar mis datos personales, solicitar prueba de la autorización otorgada para su tratamiento, ser informado sobre el uso que se ha dado a los mismos, presentar quejas ante la SIC por infracción a la ley, revocar la autorización y/o solicitar la supresión de mis datos en los casos en que sea procedente y acceder en forma

gratuita a los mismos mediante solicitud por escrito dirigida a la Universidad al correo electrónico: (incluir)

Autorizo
No Autorizo