RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

POR LA CUAL SE ACTUALIZA EL MANUAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES DE LA UNIVERSIDAD AUTÓNOMA DE OCCIDENTE

El RECTOR de la **UNIVERSIDAD AUTÓNOMA DE OCCIDENTE** en uso de las facultades que le confieren los estatutos de la Institución, y

CONSIDERANDO:

PRIMERO: Que la Universidad mediante resolución de Consejo Superior No. 686 de diciembre de 2021 actualizó la Política de Tratamiento y Protección de Datos Personales en la Universidad.

SEGUNDO: Que de conformidad con lo establecido por la Ley 1581 de 2012 y el Decreto Reglamentario 1377 de 2013 la Universidad debe adoptar un manual interno de procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.

TERCERO: Que la Universidad ha establecido alianzas estratégicas que le permitirán ampliar su cobertura en la oferta de programas y servicios académicos, lo que implica ampliar las finalidades en el tratamiento de los datos personales bajo su responsabilidad para dar alcance al desarrollo de dichas alianzas.

CUARTO: Que las actividades de evaluación y revisión continúa establecidas dentro del Programa Integral de Gestión de Datos Personales de la Universidad, permiten la identificación y ejecución de mejoras a las políticas, procedimientos y controles establecidos para el tratamiento de los datos personales conforme a la normatividad vigente.

QUINTO: Que de conformidad con el literal k del artículo 33 de los estatutos de la institución es función del Rector, expedir los manuales de procedimientos administrativos.

RESUELVE:

ARTÍCULO ÚNICO: Actualizar el Manual de Tratamiento y Protección de Datos Personales de la Universidad Autónoma de Occidente incluido en el siguiente articulado:

MANUAL DE TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

ARTÍCULO 1°: Objetivo

El objetivo del presente manual es definir los lineamientos que regulan y posibilitan la implementación y puesta en marcha del Programa Integral de Gestión de datos Personales de la Universidad Autónoma de Occidente, en adelante la Universidad, con el propósito de garantizar el tratamiento de datos personales de los miembros de la comunidad universitaria y vinculados, bajo las medidas adecuadas de protección y gestión de los riesgos asociados a ellos.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

ARTÍCULO 2°: Alcance

Los lineamientos establecidos en el presente manual aplican a todas las áreas y dependencias de la Universidad, en tanto actúen como responsables y encargados del tratamiento de datos personales y/o tengan acceso a ellos en el desarrollo de las actividades propias de la Universidad.

ARTÍCULO 3°: Términos y Definiciones

Autorización: Consentimiento previo, expreso e informado emitido por el titular, para llevar a cabo actividades propias del tratamiento de datos personales.

Aviso de Privacidad: Comunicación verbal o escrita emitida por el responsable del tratamiento y dirigida al titular, 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 pretende dar a los datos personales.

Base de Datos: Conjunto organizado de datos personales que puede ser objeto de tratamiento.

Base de Datos Automatizada: Conjunto de datos personales, gestionados a través de una solución tecnológica (Motor de bases de datos, hoja de cálculo, etc.)

Base de Datos Manual: conjunto de datos consolidados en soportes físicos (documentos físicos, expedientes, etc.)

Causahabiente: Persona natural o jurídica que adquiere el derecho de otra por cesión o transmisión mediante una figura jurídica.

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

Dato Personal Privado: Aquellos que por su naturaleza intima o reservada sólo son relevantes para el titular de la misma.

Dato Personal Semiprivado: Es el dato que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su titular sino a cierto sector o grupo de personas.

Dato Biométrico: Datos que describen características físicas que son únicas en cada persona, por lo cual permiten comprobar su identidad de manera única. Dentro de ellos se encuentra la huella dactilar, el iris ocular, rasgos faciales, la voz, etc.

Datos Sensibles: 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

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

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.

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.

Encargado de 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.

Habeas Data (Derecho a la autodeterminación informática): Derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos.

Privacidad de la Información: Característica de la información que tiene como objetivo garantizar la reserva o no divulgación de la misma y constituye un derecho de todo individuo.

Protección de Datos Personales: Conjunto de mecanismos a través de los cuales se garantiza a toda persona el derecho a la autodeterminación informática.

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

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

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

Transferencia: La 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 los mismos 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.

ARTÍCULO 4°: Políticas Generales:

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

Política General de Privacidad de la Información. La UNIVERSIDAD consciente de la importancia del tratamiento transparente, correcto y adecuado que debe darse a la información personal contenida en las bases de datos que administra, y con el propósito de salvaguardar el derecho fundamental a la autodeterminación informática (Habeas Data), garantizar la libre participación de los titulares de la información en los procesos de suministro, captación y actualización de la información, obteniendo, siempre, la autorización previa, expresa e informada para tales fines. En todo caso, LA UNIVERSIDAD se abstendrá de ceder, vender o compartir los datos personales recolectados, sin la expresa autorización de sus titulares, salvo en aquellos casos en que la ley expresamente así lo señale.

Política General de Protección de Datos Personales. La UNIVERSIDAD en su doble condición de responsable y encargado del tratamiento de datos personales de empleados, contratistas, proveedores, instituciones aliadas y destinatarios de información general, adoptará las medidas y conducentes a garantizar el pleno ejercicio de los derechos relacionados con la recolección tratamiento y circulación de datos personales. Para ello, La UNIVERSIDAD declara expresamente que el tratamiento de los datos personales se hará de conformidad con lo establecido por la Ley 1581 de 2012, el Decreto Reglamentario 1377 de 2013 y las normas que los complementen, adicionen y/o reformen, y siempre en armonía con las actividades propias de La UNIVERSIDAD y que faciliten el normal desarrollo del objeto social de la entidad.

Política General de Acceso a la Información, Consultas, Quejas y Reclamos. La UNIVERSIDAD en su doble condición de responsable y encargado del tratamiento de datos personales de estudiantes, aspirantes, egresados, empleados, contratistas, proveedores, instituciones aliadas y destinatarios de información general, adoptará las medidas y procedimientos adecuados para salvaguardar y garantizar el ejercicio que tiene el titular de la información a conocer, actualizar, rectificar, suprimir datos y revocar la autorización para el tratamiento de la información.

ARTÍCULO 5°: Derechos de los Titulares

Es responsabilidad de la Universidad Autónoma de Occidente, garantizar los derechos que la ley de protección de datos confiere a los titulares de los datos que trata.

Los titulares tienen derecho a:

a) Conocer, actualizar y rectificar sus datos personales frente a los responsables del tratamiento o encargados del tratamiento. Este derecho se podrá ejercer, entre otros frente a datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
b) Solicitar prueba de la autorización otorgada al responsable del tratamiento salvo cuando expresamente se exceptúe como requisito para el tratamiento, de conformidad con lo previsto en el artículo 10 de la ley 1581 de 2012.
c) Ser informado por el responsable del tratamiento o el encargado del tratamiento, previa solicitud, respecto del uso que le ha dado a sus datos personales.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

d) Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la ley y las demás normas que la modifiquen, adicionen o complementen.
e) Revocar la autorización y/o solicitar la supresión del dato cuando en el tratamiento no se respeten los principios, derechos y garantías constitucionales y legales. La revocatoria y/o supresión procederá cuando la Superintendencia de Industria y Comercio haya determinado que en el tratamiento el responsable o encargado han incurrido en conductas contrarias a la ley y a la constitución.
f) Acceder en forma gratuita a sus datos personales que hayan sido objeto de tratamiento.

ARTÍCULO 6°: Deberes de la Universidad como responsable y encargada del tratamiento de datos personales

La UNIVERSIDAD como responsable del tratamiento de datos personales, está obligada a:

1. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
2. Solicitar y conservar, en las condiciones previstas en la ley, copia de la respectiva autorización otorgada por el titular.
3. Informar debidamente al titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
5. Garantizar que la información que se suministre al encargado del tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
6. Actualizar la información, comunicando de forma oportuna al encargado del tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
7. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al encargado del tratamiento.
8. Suministrar al encargado del tratamiento, según el caso, únicamente datos cuyo tratamiento esté previamente autorizado de conformidad con lo previsto en la ley.
9. Exigir al encargado del tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del titular.
10. Tramitar las consultas y reclamos formulados en los términos señalados en la ley.
11. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.
12. Informar al encargado del tratamiento cuando determinada información se encuentra en discusión por parte del titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
13. Informar a solicitud del titular sobre el uso dado a sus datos personales.
14. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
15. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

Así mismo, La UNIVERSIDAD como encargada del tratamiento de datos personales, está obligada a:

1. Garantizar al titular, en todo tiempo, el pleno y efectivo ejercicio del derecho a la autodeterminación informática.
2. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
3. Realizar oportunamente la actualización, rectificación o supresión de los datos en los términos que señala la ley.
4. Actualizar la información reportada por los responsables del tratamiento dentro de los diez (10) días hábiles contados a partir de su recibo.
5. Tramitar las consultas y los reclamos formulados por los titulares en los términos señalados en la ley.
6. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y, en especial, para la atención de consultas y reclamos por parte de los titulares.
7. Registrar en la base de datos la leyenda "reclamo en trámite" en la forma en que se regula en la Ley.
8. Insertar en la base de datos la leyenda "información en discusión judicial" una vez notificado por parte de la autoridad competente sobre procesos judiciales relacionados con la calidad del dato personal.
9. Abstenerse de circular información que esté siendo controvertida por el titular y cuyo bloqueo haya sido ordenado por la Superintendencia de Industria y Comercio.
10. Permitir el acceso a la información únicamente a las personas que pueden tener acceso a ella.
11. Informar a la Superintendencia de Industria y Comercio cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los titulares.
12. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

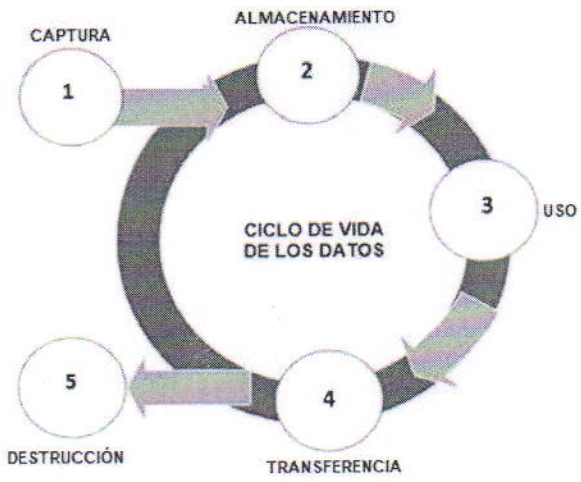
ARTÍCULO 7°: Tratamiento y Protección de Datos Personales en la Universidad

7.1. Ciclo de Vida de los datos

Entiéndase por ciclo de vida del dato, el conjunto de procesos a través de los cuales se captura, almacena, usa, transfiere y destruye datos personales contenidos en bases de datos. El tratamiento y protección de los datos personales, comprenderá los procesos y controles a que serán sometidos los datos personales durante todo su ciclo de vida.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021



7.1.1. Captura de Datos Personales

Conjunto de procesos a través de los cuales la Universidad en el desarrollo de sus actividades misionales recoge datos personales de terceros a través de medios físicos y/o electrónicos previa autorización del titular cuando corresponda.

Todo medio de recolección de datos personales que se emplee deberá ser autorizado por el Oficial de Protección de Datos de la Universidad con el propósito de verificar que el mismo se ajusta a la normatividad establecida para el efecto.

Todo medio de recolección físico que se genere en las dependencias deberá ser publicado de manera formal en el Portal Administrativo y se deberá gestionar a través de la Oficina de Planeación de la Universidad.

Para la elaboración de medios de recolección digitales usando la solución de formularios de Google, los colaboradores deberán seguir las recomendaciones de configuración establecidas con el objetivo de salvaguardar la integridad y privacidad de la información, las cuales pueden ser consultadas accediendo a los medios establecidos por la institución para el efecto.

Para los formularios de inscripción a eventos institucionales en los cuales se capturen datos personales, se debe incluir la autorización para el tratamiento de datos personales establecida para el efecto. Para eventos que impliquen finalidades distintas descritas en la autorización se deberá solicitar la autorización al Oficial de Protección de Datos.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

Ningún colaborador de la Universidad está autorizado para realizar por cuenta propia y para finalidades no institucionales, captura de datos personales.

7.1.1.1 Características de los Datos Personales

Un dato es considerado como personal cuándo:

1. Permite Identificar de manera única e inequívoca a una persona natural o jurídica.
2. Al relacionar dos o más datos es posible determinar la identidad de una persona natural o jurídica.
3. Los datos personales pueden ser de cualquier tipo incluyendo videos, fotografías, datos biométricos, numéricos, textos, etc.

7.1.1.2 Finalidades

La Universidad ha establecido como finalidades para la recolección y tratamiento de datos personales de terceros, las siguientes:

1. Garantizar a los usuarios el ejercicio pleno del derecho a la educación.
2. Contactar al interesado a través de cualquier medio, incluidos los electrónicos, a fin de proporcionarle información relacionada con las acciones formativas y servicios de enseñanza de la Universidad. Esta información incluirá ofertas, descuentos, becas, información comercial e información general de la Universidad.
3. Facilitar el proceso de pre-inscripción en la acción formativa que el interesado en cada caso seleccione.
4. Enviar publicidad relacionada con las preferencias del interesado a partir de sus hábitos de navegación (cookies dirigidas o de publicidad).
5. Adelantar los trámites necesarios para la formalización de la matrícula, con inclusión del alta en las diferentes plataformas online que fueran necesarias. La base legal radica en que el tratamiento es necesario para la ejecución de un contrato en el que el interesado es parte o para la aplicación a petición de este de medidas precontractuales.
6. Gestionar adecuadamente la actividad académica relacionada con la formación en la que el interesado se matricule.
7. Prestación de asistencia personalizada en el uso de las plataformas virtuales a través de los diferentes medios de contacto que haya facilitado a la Universidad tales como mensajes SMS, WhatsApp, emails, o llamadas telefónicas.
8. Fines de control y seguridad y el cumplimiento normativo de las obligaciones de LA UNIVERSIDAD.
9. Realización de encuestas de satisfacción y estudios de mercado.
10. Envío de información relacionada con los diferentes procesos de inscripción, selección y admisión a programas académicos de la universidad.
11. Cumplir las regulaciones aplicables a las entidades de educación superior privadas en Colombia.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

12. Adelantar la promoción y publicidad de actividades, productos y servicios académicos que ofrece la Universidad.
13. Establecer contacto con egresados para efectos de promoción y divulgación de actividades y eventos de interés institucional.
14. La adquisición de bienes y/o servicios para el normal desarrollo de las actividades institucionales orientadas a la prestación adecuada de los servicios de educación.
15. Desarrollar actividades legales, parafiscales, administrativas, y/o académicas relacionadas con la gestión de aspirantes, estudiantes, empleados, ex empleados, proveedores y contratistas.
16. Desarrollar actividades encaminadas a propender por el bienestar de la comunidad universitaria.
17. Para fines estadísticos, científicos o históricos.
18. Dar cumplimiento a obligaciones contraídas con los Titulares de los Datos Personales en el desarrollo de la relación que existe(a) entre el Titular de los Datos Personales y la Universidad.
19. Transmisión nacional e internacional de datos en los casos que se requiera, bajo los parámetros establecidos por la Ley.
20. Las demás finalidades que determine la Universidad en su calidad de Responsable del Tratamiento de Datos Personales con el fin de dar cumplimiento a las obligaciones legales y a sus políticas internas y que sean comunicados a los Titulares en el momento de la recolección de los Datos Personales, y en todo caso de acuerdo con la ley.

Es responsabilidad del encargado o líder de dependencia en la cual se genere un nuevo medio de recolección de datos personales, verificar que la finalidad con la que se genera el nuevo medio de recolección corresponda a las definidas por la Universidad para el efecto. En caso de requerirse recolección de información con finalidades no autorizadas, se deberá informar al Oficial de Protección de Datos acerca de la necesidad puntual, quien analizará la solicitud en asocio con la Oficina de Asesoría Jurídica.

7.1.1.3 Solicitud de autorización

A excepción de los datos de tipo público la captura de datos personales requiere la autorización previa y expresa de su titular. Si al validar los campos del medio de recolección, el responsable identifica datos personales diferentes a los de carácter público, se deberá adicionar al medio de recolección las finalidades para las cuales son recolectados los datos y la solicitud de autorización del titular para el tratamiento de sus datos personales. Dicha autorización se deberá conservar en medio físico o electrónico en el área o dependencia dueña del medio de captura de datos, y durante el tiempo que se traten los datos recolectados.
El Oficial de Protección de Datos apoyará al responsable del medio de recolección con la definición de la autorización a incluir en el medio.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

7.1.2 Almacenamiento, Transferencia y Destrucción de datos

Todos los colaboradores de la Universidad deberán acatar los lineamientos de seguridad definidos para el almacenamiento, transferencia y/o destrucción de información, en los términos establecidos en la Resolución de Rectoría No. 7526 del 23 de octubre de 2019- Manual institucional para el inventario, la clasificación, etiquetado y manejo de la información para su protección, y atenerse a las políticas de seguridad y privacidad de la información definidas por la Universidad.

ARTÍCULO 8°: Actualización de Datos

Además de los mecanismos establecidos para el ejercicio del derecho a la autodeterminación informática, los titulares podrán actualizar sus datos de manera presencial, diligenciando los formatos correspondientes para tal fin o a través de las campañas de contacto telefónico realice la Universidad con tal fin.

En aplicación del principio de veracidad y calidad de los datos, la Universidad podrá desarrollar campañas de actualización de datos, utilizando diferentes mecanismos, en todo caso, siempre se informará al titular las finalidades del tratamiento, y de ser necesario, se solicitará la autorización respectiva.

Todo mecanismo para la actualización de datos deberá incluir mecanismos de validación que permitan verificar la identidad del titular, ya sea mediante solicitud de documento de identificación, la realización de preguntas aleatorias o cualquier otro medio adecuado a tal fin.

ARTÍCULO 9°: Tratamiento de Datos Personales de Categoría Especial

La categoría especial de Datos Personales, comprende aquellos datos de carácter sensible, relacionados con el origen racial, étnico, orientación política, convicciones religiosas o filosóficas, pertenencia a sindicatos, organizaciones sociales, de derechos humanos o aquellos que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, información relativa a la salud, la vida sexual, datos biométricos, datos derivados de visitas domiciliarias, estudios de seguridad, pruebas psicotécnicas y en general aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar discriminación.

El tratamiento de datos personales de categoría especial deberá someterse a los siguientes lineamientos:

1. Deberá contar con la autorización explícita del titular para el tratamiento de datos personales, salvo en los casos que por ley no sea necesario el otorgamiento de dicha autorización.
2. Se podrán someter a tratamiento datos sensibles sin autorización del titular cuando dicho acto sea necesario para salvaguardar el interés vital del titular y/o aquel se encuentre física o jurídicamente incapacitado para hacerlo.
3. Se podrán someter a tratamiento información personal sin autorización del titular, cuando aquella se refiera a datos necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
4. Se podrán someter a tratamiento información personal sin autorización del titular, cuando

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

aquella tenga una finalidad histórica, estadística o científica. En estos eventos deberá suprimirse la identidad de los titulares.

9.1 Autorización para el tratamiento de datos sensibles

El tratamiento de datos sensibles sólo podrá realizarse con el consentimiento, previo, expreso e informado del titular. En estos eventos los datos personales sometidos a tratamiento, no podrán ser obtenidos y/o divulgados sin previa autorización expresa del titular, salvo mandato legal u orden judicial que releve de dicho consentimiento.

Los mecanismos para obtener el consentimiento para el tratamiento de los datos sensibles, serán definidos por la Universidad dependiendo de las circunstancias y finalidades del caso, y podrá realizarse mediante formularios, llamadas telefónicas, cajas de chequeo, entre otros, de tal forma que pueda acreditarse la efectiva autorización por parte del titular o su representante legal.

Al momento de solicitarse el consentimiento, deberá informarse al titular o su representante legal que, por tratarse de datos sensibles no se encuentra obligado a suministrarlos y autorizar su tratamiento.

La autorización por parte del titular debe ser obtenida a más tardar al momento de su recolección informándole la finalidad específica del tratamiento de los mismos y debe utilizar mecanismos que garanticen su consulta posterior.
La autorización para el tratamiento de datos sensibles debe contener: i) identificación plena del responsable; ii) tipo de dato que se recolectará; iii) finalidad del tratamiento.

9.2 Tratamiento de Información Médica

La captación, grabación, transmisión, almacenamiento, conservación con información médica, diagnósticos e historias clínicas, serán considerados de carácter sensible por lo que deberán ser tratados de acuerdo a los lineamientos establecidos para los datos de tipo confidencial (Ver Resolución de Rectoría No. 7526 del 23 de octubre de 2019-Manual institucional para el inventario, la clasificación, etiquetado y manejo de la información para su protección).

9.3 Tratamiento de Datos Biométricos

La captación, grabación, transmisión, almacenamiento, conservación o reproducción en tiempo real o posterior de un dato biométrico serán considerados de carácter sensible por lo que deberán ser tratados de acuerdo a los lineamientos establecidos para los datos de tipo confidencial (Ver Resolución de Rectoría No. 7526 del 23 de octubre de 2019-Manual institucional para el inventario, la clasificación, etiquetado y manejo de la información para su protección).

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

La captura de datos personales a través de herramientas biométricas solo podrá ser efectuada a través de los mecanismos y dependencias autorizadas para ello en la Universidad, y en todo caso se deberá contar con la autorización del titular.

Cuando las dependencias de la Universidad realicen cubrimiento fotográfico de un evento, dentro o fuera del Campus, ya sea a través de la Dirección de Comunicaciones o con equipos propios del área, debe garantizar el diligenciamiento del formato **DC-1.8-FO04** Autorización uso de imagen para eventos.

Si el cubrimiento fotográfico lo realiza la Dirección de Comunicaciones, dicha dependencia solo entregará las fotos al solicitante, cuando se haga entrega del formato diligenciado por los asistentes del evento.

En los eventos en los que se realicen grabaciones en video y transmisiones en vivo, a través de redes sociales o UAO Play, debe proyectarse una imagen en la que se anuncie a los asistentes, sobre la transmisión, para que aquellas personas que no deseen ser grabadas, se ubiquen en una zona que será definida por los organizadores del evento, y a la cual no tenga acceso la cámara.

El tratamiento de datos personales en sistemas de Video Vigilancia se realizará siguiendo los lineamientos para captura y tratamiento de datos en sistemas de video vigilancia establecidos por la Superintendencia de Industria y Comercio.

9.4 Tratamiento de datos de niños, niñas y adolescentes

El Tratamiento de datos personales privados de niños, niñas y adolescentes está prohibido. La Universidad tratará datos personales privados de niños, niñas y adolescentes, siempre bajo los requisitos establecidos por la ley y garantizando el derecho de los menores a ser escuchados teniendo en cuenta su grado de madurez, solo en los siguientes eventos

1. Cuando se trate de un interés superior.
2. Cuando se requiera proteger sus derechos fundamentales.
3. Cuando se obtenga autorización previa de sus padres y/o representantes legales.

El representante legal del niño, niña o adolescente es el único autorizado para permitir el tratamiento de datos personales del menor de edad.

Utilización de imágenes de menores de edad: En las campañas publicitarias que se utilicen imágenes de menores de edad, será necesario contar con el consentimiento previo y explícito de sus padres y/o representante legal para lo cual se deberá diligenciar el documento de autorización respectivo.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

ARTÍCULO 10°: Mecanismos de Comunicación.

El Oficial de Protección de Datos generará las comunicaciones necesarias para dar a conocer eventos importantes, avance y estado del Programa Integral de Gestión de Datos.
Las comunicaciones dirigidas a la comunidad universitaria e interesados se realizarán a través de la Dirección de Comunicaciones de la Universidad, usando los mecanismos habituales establecidos tanto impresos como digitales.

10.1 Presentación de Informes

El Oficial de Protección de Datos será el responsable de la presentación de informes, a autoridades institucionales o entidades de control y titulares del dato, que den cuenta de las actuaciones frente a eventuales violaciones de privacidad de la información de titulares. Así mismo informará periódicamente a la alta dirección de la Universidad sobre el estado del Programa Integral de Gestión de datos Personales.

A continuación, se presenta la descripción de los informes periódicos dirigidos a la alta dirección de la Universidad:

Informe o Reporte	Descripción	Frecuencia de entrega	Usuario
Informe de Estado del Programa Integral de Gestión de Datos Personales	Informe sobre el estado, novedades y avances del Programa Integral de Gestión de datos personales de la Universidad.	Semestral	Rector, Vicerrectores, Director de Tecnologías de Información, Contraloría.
Informe de gestión de incidentes que involucran datos personales	Informe de los incidentes presentados en el semestre y la gestión realizada sobre el particular.	Semestral	Rector, Vicerrectores, Director de Tecnologías de Información, Contraloría.

10.2 Comunicaciones Externas.

Las modificaciones a la Política de Tratamiento y Protección de Datos, será informada a través de los medios de comunicación masiva establecidos por la Universidad.

En el evento de presentarse situaciones de eventual violación de la privacidad de la información, el Oficial de Protección de Datos, realizará las gestiones respectivas al interior de la Universidad, siguiendo el Manual para la gestión de incidentes de seguridad y privacidad de la información-**DVT-3.2-MU6**. Una vez concluida la indagación, reportará a los titulares afectados (estudiantes, profesores, colaboradores, contratistas y proveedores), el resultado, y, si es del caso las consecuencias asociadas y las acciones a adoptar para disminuir el daño potencial y prevenir futuros incidentes similares.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

El Oficial de Protección de Datos reportará en los términos de ley, ante la Superintendencia de Industria y Comercio los incidentes que se presentaren sobre violaciones al régimen de datos personales de los titulares de la información. El reporte debe ser realizado a través del aplicativo RNBD dispuesto por la SIC https://rnbd.sic.gov.co/sisi/login.

ARTÍCULO 11°: Inventario de Bases de Datos con Información Personal

El Oficial de Protección de Datos de la Universidad mantendrá un inventario de las bases de datos automatizadas y manuales que contengan datos personales. Así mismo es el responsable de realizar el reporte de las bases de datos en el Registro Nacional de Bases de Datos https://rnbd.sic.gov.co/sisi/login.
El inventario de las bases de datos de la Universidad Autónoma de Occidente reposará en el repositorio http://alfresco.uao.edu.co , bajo la administración de la Dirección de Tecnologías de Información, de manera indefinida, dado que es la fuente para registrar cambios, o nuevas bases de datos en el Registro Nacional de Bases de Datos.

Las bases de datos nuevas, se deberán reportar en el Registro Nacional de Bases de Datos dentro de los dos meses siguientes a su creación.
La actualización del inventario de bases de datos con datos personales, en el Registro Nacional de Bases de Datos deberá ser realizada dentro de los (10) diez primeros días hábiles de cada mes, a partir de la inscripción de la base de datos, cuando se realicen cambios substanciales en la información registrada.

Es responsabilidad de la Unidad de Proyectos y Desarrollo de la Dirección de Tecnologías de Información, informar al Oficial de Protección de Datos, sobre la creación de nuevos sistemas de información que involucren la captura o tratamiento de datos personales, con el fin de incluir las nuevas bases de datos dentro del inventario oficial de bases de datos de la Universidad.

Ningún colaborador de la Universidad está autorizado para generar nuevas bases adicionales a las oficiales, que contengan datos personales, bajo la responsabilidad de la Universidad, así como la extracción y almacenamiento local por largo tiempo, de datos personales contenidos en las bases de datos oficiales.

ARTÍCULO 12°: Aviso de Privacidad y Política de tratamiento y protección de datos.

La Universidad ha definido su política de tratamiento y protección de datos, así como su aviso de privacidad dando cumplimiento a lo establecido por la ley de protección de datos.
El aviso de privacidad se encontrará siempre publicado en la página web de la Universidad, accesible a todos los públicos de interés, y desde el mismo se tendrá acceso a la política.
El aviso de privacidad siempre deberá contener como mínimo los siguientes datos:
1. Nombre o razón social y datos de contacto de la Universidad como responsable de tratamiento.
2. El tratamiento al cual serán sometidos los datos y las finalidades del mismo.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

3. Los derechos de los titulares.
4. Los mecanismos dispuestos por la Universidad para informar a los titulares acerca de la Política de tratamiento y las modificaciones substanciales sobre la misma y el aviso de privacidad.

ARTÍCULO 13°: Gestión de Riesgos Asociados al Tratamiento de Datos.

La gestión de riesgos asociados al tratamiento de datos personales se realizará bajo la metodología prevista por la institución para el efecto.

ARTÍCULO 14°: Mecanismos de Capacitación y Sensibilización

Anualmente el Oficial de Protección de Datos de la Universidad definirá el plan de capacitaciones y sensibilizaciones en seguridad y privacidad de la información a realizar en el transcurso del año.

El plan deberá ser presentado y coordinado con el Departamento de Recursos Humanos, con el objetivo de lograr la alineación con los planes institucionales de capacitación.

Para la definición de la temática a incluir dentro del plan de capacitación y sensibilización se tendrá en cuenta los siguientes aspectos:

1. Resultados de auditorías realizadas al Programa Integral de Gestión de Datos Personales.
2. Resultados de auditorías realizadas por la Contraloría, que involucren aspectos de seguridad y privacidad de la información.
3. Resultado del análisis de los incidentes de Seguridad y Privacidad de la Información.
4. Resultados de evaluaciones de capacitaciones anteriores.
5. Modificaciones a los procedimientos relacionados con el tratamiento y protección de datos personales.
6. Modificaciones a la Ley 1581 de 2012 y sus decretos reglamentarios.

Una vez definido el contenido del plan se deberá identificar cada uno de los públicos objetivo a los cuales se debe dirigir la capacitación o sensibilización y se procederá a definir el contenido de cada temática teniendo en cuenta los diferentes públicos.

Será el Oficial de Protección de Datos quien desarrolle y/o apruebe todo material para el desarrollo de capacitaciones en protección de datos personales y determinará la inclusión de medios de evaluación, que permitan conocer el nivel de entendimiento por parte de los públicos.

Los mecanismos empleados para la realización de las capacitaciones y sensibilizaciones, podrán variar de acuerdo al contenido, la cobertura que se quiera lograr, y el público al cual esté orientada la temática:

- Charlas Presenciales
- Cursos Virtuales
- Medios Impresos
- e Mailing

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

- Protectores de Pantalla y de Escritorio.

Para la definición del plan, el Oficial de Protección de Datos deberá diligenciar el formato Plan de Capacitación Seguridad y Privacidad-**DVT-3.2-FO04**.

Durante el desarrollo de todo curso o charla, se deberá diligenciar el formato de asistencia correspondiente, el cual será custodiado por el Oficial de Protección de Datos de la Universidad.

ARTÍCULO 15°: Atención de Consultas y Reclamos de protección de Datos

Las consultas y reclamos en relación a la protección de datos personales, serán atendidos solo a través de los medios establecidos para tal fin: Correo electrónico datospersonales@uao.edu.co bajo responsabilidad del Oficial de Protección de Datos, o mediante comunicación escrita dirigida a la Secretaria General – Datos personales, calle 25 # 115 – 85 Santiago de Cali.

Los responsables al interior de la Universidad, darán respuesta dentro de los tiempos establecidos siguiendo el procedimiento Atención de consultas y reclamos de protección de datos-**DVT-3.2-PD4.1**.

Las solicitudes que expresen el deseo de los titulares de no ser contactados con fines comerciales (Ofrecimiento de programas, cursos, etc.), implica la marcación de los contactos y sus datos en las bases de datos de contactos de la Universidad, actividad que será ejecutada de por las áreas a quienes corresponde la generación de éste tipo de campañas.

15.1 Tiempos de Respuesta

Las **consultas** serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma, si pasado este tiempo no ha sido posible su atención, se informará al interesado los motivos y fecha en la cual se brindará respuesta, dentro de un tiempo no superior a cinco (05) días hábiles siguientes al vencimiento del primer término.

Los **reclamos** que comprenden corrección, actualización o supresión o cuando se advierta el presunto incumplimiento de la Universidad, frente a los deberes establecidos por las leyes aplicables, serán atendidos en los siguientes términos:

1. Si la información mínima solicitada para el trámite se encuentra incompleta, se solicitará al interesado dentro de los 5 días hábiles siguientes a la recepción del reclamo, completar la información, trascurridos dos meses desde el momento del registro del reclamo sin suministrar la información faltante, se entenderá que el interesado ha desistido del reclamo.
2. El término máximo para atender el reclamo será de quince días hábiles contados a partir del día siguiente a la fecha de su recibo. Si no es posible atender el reclamo dentro de dicho termino, se informará al interesado los motivos y fecha en la cual se brindará respuesta, dentro de un tiempo no superior a los 8 días hábiles siguientes al vencimiento

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

del primer término.

ARTÍCULO 16°: Requisitos para Legitimación del Titular

Es responsabilidad de la Universidad garantizar que, dentro de los procedimientos establecidos para dar respuesta al ejercicio de los derechos de consulta, corrección, actualización o supresión de datos personales, se incluyan mecanismos que permitan determinar que el titular es quien ejerce sus derechos, para lo cual se deberá constatar lo siguiente:

1. Si el ejercicio de derechos es solicitado por un titular, se debe acreditar su identidad en forma suficiente mediante: Confrontación del documento de identificación personal (cédula de ciudadanía, cedula de extranjería, pasaporte, etc.); preguntas de seguridad, comunicación a través de canales que cuenten con login o verificación de usuario a través de accesos controlados, validación de datos de identificación básicos; cuando sea por medios virtuales y/o contacto telefónico.
2. Si el ejercicio lo realiza un causahabiente, se debe verificar tal calidad. Para esto se debe requerir documento que certifique la calidad de causahabiente por sucesión o transmisión de derechos; tales como: registro civil de nacimiento, sentencia y/o poderes debidamente constituidos.
3. En caso de ser un representante y/o apoderado del titular, o por estipulación o a favor de otro o para otro, se debe acreditar la representación o apoderamiento a través de documento debidamente legalizado. Por ejemplo, poder debidamente autenticado o documento privado avalado por un notario o autoridad judicial.
4. Cuando se trate un representante legal de los niños, niñas o adolescentes se debe constatar la calidad mediante registro de nacimiento o documento que acredite la calidad de representante. Por ejemplo, sentencia judicial que determine la custodia en cabeza de un tercero.

ARTÍCULO 17°: Tratamiento de datos personales donde Intervienen Terceros.

17.1 Tratamiento de datos a través de encargados

En el desarrollo de sus actividades misionales, la Universidad podrá suscribir actos o contratos dentro de las cuales se delegue en un tercero la realización de gestiones en su nombre que involucren el tratamiento de datos personales de los cuales la Universidad es responsable. En este evento es responsabilidad de la Universidad, en cabeza del Oficial de Protección de Datos Personales verificar que todo vínculo contractual donde actúe un tercero como encargado del tratamiento de datos personales cumpla los parámetros:

1. Incluir previsiones donde se establezca que los encargados cumplen con las disposiciones colombianas en materia de protección de datos.
2. Que conocen la política de tratamiento y protección de datos de la Universidad y efectúan el tratamiento de datos de conformidad con la misma.
3. Que conocen la Política de Seguridad y Privacidad de la información de la Universidad y efectúa e tratamiento de datos de conformidad con la misma.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

4. Que adelanta al interior de su organización programas de formación en seguridad y protección de datos personales, dirigido a sus colaboradores, en especial a aquellos o que tienen acceso a información de carácter personal.
5. Que autoriza a la Universidad para la realización de auditorías periódicas sobre su sistema de tratamiento y protección de datos.
6. Que garantiza la existencia de acuerdos con sus colaboradores acerca de sus compromisos en el cumplimiento de las normas establecidas sobre tratamiento y protección de datos personales.
7. Que garantiza que el tratamiento de los datos personales, que hace por cuenta de la Universidad se hará exclusivamente de acuerdo a las finalidades señaladas por la Universidad.
8. Que garantiza que reportará a la Universidad los incidentes de seguridad relacionados con la información suministrada por la Universidad, para que el Oficial de Protección de Datos Personales informe al ente de control y los titulares afectados. .

17.2 Tratamiento de datos personales por parte de terceros vinculados

Cuando por virtud de actos o contratos suscritos por la Universidad, terceros vinculados tuvieren acceso a información confidencial y/o personal de la cual la Universidad es responsable, se exigirá al contratista el cumplimiento de las siguientes obligaciones:

1. Definir las medidas de seguridad física, lógica y administrativa para el tratamiento de la información y en general de las actividades a realizar cuando el servicio sea prestado fuera de las instalaciones de la Universidad.
2. Cuando aplique, definir los mecanismos de conexión del proveedor a la infraestructura tecnológica de la Universidad.
3. Establecer cláusulas de confidencialidad con el proveedor, sus empleados y subcontratistas.
4. Definir mecanismos de identificación y autenticación de usuarios, cuando las actividades requieran de un sistema de propiedad del contratista y/o proveedor.

Apoyo del Oficial de Protección de datos en la elaboración de acuerdos con Terceros

En todo acuerdo que involucre tratamiento de datos personales bajo la responsabilidad de la Universidad, el líder de la negociación deberá contactar al Oficial de Protección de Datos con el fin de identificar la naturaleza y volumen de la información que se le encargara al tercero, la actividad de tratamiento a la cual serán sometidos los datos personales y las medidas que garanticen la protección e integridad de la información suministrada.

17.3 Seguimiento y supervisión del contrato

En todo contrato que involucre transmisión, transferencia o tratamiento de datos personales por cuenta de terceros, corresponderá al interventor realizar auditorías y/o revisiones

periódicas al Programa Integral de Gestión de Datos Personales del proveedor con el propósito de verificar el cumplimiento de los términos pactados en materia de seguridad y privacidad de la información, en especial:

1. Los procedimientos de atención de consultas y reclamos.
2. Los procedimientos asociados con el tratamiento de datos personales (actualización, eliminación y/o disposición, entre otros).
3. El aviso de privacidad y/o solicitudes de autorización.
4. Que el proveedor esté utilizando la información personal de acuerdo a las finalidades y parámetros definidos por la Universidad.
5. Que el proveedor haya informado al Oficial de Protección de Datos Personales todo incidente de seguridad del que tenga conocimiento, con el propósito de identificar el plan de acción a implementar por el proveedor que ejecute una actividad de tratamiento de la información.

El interventor informará al Oficial de Protección de Datos Personales, cuando el proveedor no cumpla con las condiciones establecidas para el tratamiento de datos personales.

17.4 Terminación del contrato

Al finalizar el contrato por el vencimiento del plazo contractual o por incumplimiento de las obligaciones del encargado del tratamiento, el supervisor y/o interventor del contrato debe verificar que el proveedor haya realizado en los términos establecidos por la Universidad la devolución o destrucción de la información que se le haya suministrado.

ARTÍCULO 18°: Evaluación y Revisión Continua del Programa Integral de Gestión de Datos Personales.

18.1 Revisión de las Políticas de Protección de datos

Las políticas del programa integral de protección de datos, serán revisadas anualmente, dentro del primer semestre del año, o cuando se presenten cambios normativos de ley, políticas institucionales, cambios en los procesos, oportunidades de mejora identificados que impliquen el ajuste o cambio de las políticas, o inclusión de finalidades no cubiertas por las políticas vigentes.

La revisión incluirá la política de tratamiento y protección de datos, el aviso de privacidad, las políticas generales de tratamiento de la información, y el gobierno de seguridad y privacidad de la información. Dicha revisión será realizada por un equipo conformado por el Oficial de Protección de Datos, la Contraloría, la Oficina de Asesoría Jurídica y la Coordinación de Seguridad Informática.

Los cambios efectuados sobre la política de tratamiento y protección de datos deberán ser presentados al Consejo Superior de la Universidad para su aprobación y publicación.

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP

La programación de revisión, y los resultados de la misma, serán consignados en el formatoDVT-3.2-FO06 Revisión de políticas de seguridad y privacidad..

18.2 Supervisión y Revisión al Programa Integral de Gestión de Datos Personales

A partir de la implementación del programa integral de gestión de datos personales de la Universidad, dentro del segundo semestre del año en curso se realizará una evaluación de acogimiento de las políticas y aplicación de los controles del programa dentro de las dependencias y procesos de la Universidad.

El Oficial de Protección de Datos, definirá el alcance y contenido de la evaluación a realizar. La información será consignada en el formato DVT-3.2-FO05 Plan de auditoria seguridad y privacidad info.

Como resultado de la evaluación, el Oficial de Protección de Datos, en conjunto con los líderes de las dependencias incluidas en el alcance de la evaluación, deberá establecer un plan de acción para cierre de las brechas identificadas.

El plan de Auditoria junto con los soportes y resultado de la evaluación anual, reposará en el repositorio http://alfresco.uao.edu.co , bajo la administración de la Dirección de Tecnologías de Información.

18.3 Evaluación de Controles del Programa Integral de Gestión de Datos Personales

El monitoreo al Programa Integral de Protección de Datos Personales es un proceso continuo, para lo cual la Universidad ha definido las métricas que permitirán tener una visión del desempeño del programa y los controles definidos, dichas métricas serán calculadas de manera periódica, y serán ajustadas de acuerdo a los resultados obtenidos en el tiempo, con el objetivo de ser mejoradas para obtener información ajustada a la realidad de los controles y procesos establecidos. Las métricas se encuentran consignadas en el formato Hoja de Caracterización de Métricas.

Los resultados obtenidos a través de evaluaciones y la medición periódica de las métricas, permitirá identificar oportunidades de mejora del Sistema Integral de Protección de Datos, y a partir de las cuales desarrollar las acciones necesarias que permitan mejorar la seguridad y protección de los datos personales bajo responsabilidad de la Universidad.

Para brindar un mayor conocimiento del tratamiento de datos personales dentro de las actividades específicas de diferentes procesos de la institución, se consultarán los siguientes anexos:

- **Lineamientos para la captura y tratamiento de datos en sistemas de video vigilancia.**

ORIGEN Y APROBACIÓN	Vo.Bo.	
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL	
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR	
Revisado por: DIRECCIÓN JURÍDICA	ODS	
Revisado por: CONTRALORÍA	LPVO	
Aprobado por: RECTORÍA	LHP	

RESOLUCIÓN DE RECTORÍA No. 7749 DEL 15 DE DICIEMBRE DE 2021

- **Lineamientos para la realización de campañas de tele mercadeo y envío de comunicaciones vía correo electrónico.**
- **Tratamiento de datos personales en procesos de selección y contratación laboral, contrato de aprendizaje y convenios para prácticas y/o pasantías.**

ARTÍCULO 19°: La presente resolución deroga las disposiciones que le sean contrarias.

Dada en Santiago de Cali, a los quince (15) días del mes de diciembre del año dos mil veintiuno (2021).

LUIS H. PÉREZ
Rector

ROBERTO NAVARRO SÁNCHEZ
Secretario General

ORIGEN Y APROBACIÓN	Vo.Bo.
Solicitado por: OFICIAL DE PROTECCIÓN DE DATOS	YMCL
Revisado por UNIDAD DE ARCHIVO Y GESTIÓN DOCUMENTAL	ILSR
Revisado por: DIRECCIÓN JURÍDICA	ODS
Revisado por: CONTRALORÍA	LPVO
Aprobado por: RECTORÍA	LHP