UNIVERSIDAD CATÓLICA LUIS AMIGÓ

Secretaría General

Oficina de Comunicaciones y Relaciones Públicas

Coordinación de Habeas Data

MANUAL DE POLÍTICAS Y PROCEDIMIENTOS EN PROTECCIÓN DE DATOS PERSONALES

2023

Contenido

OBJETO

El presente manual tiene el propósito de definir los lineamientos para la implementación, monitoreo, sostenimiento y mejora continua del Programa de Protección de Datos Personales de la Universidad Católica Luis Amigó.

ALCANCE

La Universidad Católica Luis Amigó, identificada con NIT: 890.985.189-9, con domicilio principal en la ciudad de Medellín en la dirección Transversal 51ª 67B-90 y sus sedes ubicadas en las ciudades de: Bogotá Avenida Suba. N° 128A - 51, Manizales Carrera 22 N° 67A - 49, Apartadó Calle 74 No. 97 – 95 Zona Sur - Barrio La Navarra y Montería Calle 64 No6-108. Barrio los Alcázares, en adelante denominada como “La Universidad”, en el rol de responsable o encargada del tratamiento de los datos personales, está comprometida con el adecuado tratamiento de los datos de sus empleados, los estudiantes, los egresados, los clientes, los proveedores y los terceros. Por lo tanto, en el presente documento se articulan los procedimientos y actividades que involucran el tratamiento de los datos personales, los cuales están alineados con las normas y directrices que lo regulan.

MARCO NORMATIVO

Con el propósito de dar un adecuado tratamiento a los datos personales, La Universidad ha identificado el siguiente marco normativo que articula las disposiciones de protección de los datos personales, su confidencialidad y los derechos de los titulares:

- Constitución Política de 1991: En su artículo 15 la Constitución establece lo siguiente: “(…) Todas las personas tienen derecho a su intimidad personal y familiar y a su buen nombre, y el Estado debe respetarlos y hacerlos respetar. De igual modo, tienen derecho a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bancos de datos y en archivos de entidades públicas y privadas. En la recolección, tratamiento y circulación de datos se respetarán la libertad y demás garantías consagradas en la Constitución (…)”.
- Ley 1581 de 2012: Por la cual se dictan las disposiciones generales para la protección de datos personales.
- Decreto Único 1074 de 2015: Por medio del cual se expide el Decreto Único Reglamentario del Sector Comercio, Industria y Turismo.

- Circular Externa 005 de 2017 de la Superintendencia de Industria y Comercio: Por la cual se fijan estándares de un nivel adecuado de protección en el país receptor de la información personal.
- Guía de la Superintendencia de Industria y Comercio para la implementación del Principio de Responsabilidad Demostrada (Accountability).
- Política de tratamiento de datos de la Universidad.
- En general, para la aplicación e interpretación del presente manual, cuando fuere procedente, se aplicarán las demás normas que regulen o complementen lo concerniente a la protección de datos personales.

PRINCIPIOS APLICABLES AL TRATAMIENTO DE DATOS

La Universidad está comprometida con el adecuado tratamiento de los datos personales, por lo cual, en todas las actividades que tengan manejo de datos personales, se deberá garantizar la aplicación de los siguientes principios, los cuales se encuentran alineados con los establecidos en el artículo 4 de la Ley 1581 de 2012:

- **Legalidad:** En todo el proceso de tratamiento de los datos personales, desde el momento de su captura, almacenamiento y eliminación, se debe cumplir con las disposiciones normativas, empleando los datos para fines que estén bajo la ley y a las disposiciones reglamentarias que la desarrollen.
- **Finalidad:** Todos los datos personales que sean capturados en el desarrollo del ejercicio de las funciones educativas y administrativas que tiene la Universidad, deben atender a finalidades específicas de acuerdo con el tratamiento que se le dará al dato. Las finalidades del tratamiento deben ser informadas a los titulares con el propósito que éstos conozcan las actividades que desarrollará la Universidad con los datos personales que está entregando.
- **Libertad:** La recolección, almacenamiento y tratamiento de los datos personales sólo puede realizarse con la autorización previa y expresa del titular, quien debe ser informado sobre el tratamiento que se les dará a sus datos personales. La divulgación o socialización de los datos personales sin la previa autorización, o sin una disposición legal que lo habilite, está prohibido.
- **Veracidad o calidad:** La Universidad debe promover que los datos personales que estarán sujetos a tratamiento deben ser veraces, exactos, completos y actualizados, pues de lo contrario pueden llevar a inducir a errores en la ejecución de tratamiento para el cual fueron capturados.

- **Transparencia:** Cualquier titular de información podrá tener acceso, en cualquier momento, a la información sobre sus datos personales tratados por la Universidad.
- **Acceso y circulación restringida:** El tratamiento de los datos personales sólo podrá ser realizado por aquellos que el titular haya efectivamente autorizado, o por las personas habilitadas por las disposiciones legales vigentes.
- **Seguridad:** Toda la información asociada a los datos personales objeto de tratamiento por parte de la Universidad, deberán protegerse bajo estándares de seguridad adecuados, implementando medidas operativas, técnicas y humanas que eviten su pérdida, adulteración o acceso no autorizado.
- **Confidencialidad:** La Universidad deberá garantizar la reserva de la información y datos personales que no estén bajo la categoría de datos públicos, por lo cual, todas las personas que tengan acceso al tratamiento de los datos personales deberán promover prácticas de manejo de datos que eviten su exposición o suministro a terceros no autorizados.

Dirección del Responsable

Identificación del Tratamiento de Datos Personales: Para los efectos de la presente política se tendrán como datos de identificación del responsable de la Universidad Católica Luis Amigó en cabeza de su rector:

✓ DIRECCIÓN: Transversal 51ª 67B90. Sede principal Medellín
✓ TELÉFONO: (604)4487666
✓ **http://www.ucatolicaluisamigo.educ.o**

La Universidad Católica Luis Amigó para el cumplimiento de sus actividades misionales y administrativas podrá recolectar, eliminar, actualizar, modificar, utilizar, almacenar, transferir y en general realizar diversas operaciones con los Datos Personales. Estos datos, deberán ser utilizados para la finalidad que se señalan en nuestra política de tratamiento de datos personales que se encuentra en nuestro sitio web http://www.ucatolicaluisamigo.educ.o, así mismo los encargados o terceros que tengan acceso a estos datos por el ejercicio de sus funciones o en cumplimiento de las obligaciones de un contrato, mantendrán el tratamiento dentro de las mismas finalidades, atendiendo de forma estricta los deberes de seguridad y confidencialidad ordenados por la Ley 1581 de 2012 y demás normas que la complementan y regulan.

PROPÓSITOS DE LA POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

a. Facilitar el acceso de niños, niñas y adolescentes al sistema educativo y garantizar su permanencia.
b. Cuidar la intimidad personal, familiar y el su buen nombre a sus titulares de datos personales.
c. Proteger la privacidad e intimidad de sus titulares en el tratamiento de sus datos.
d. Garantizar la custodia adecuada y segura de los datos de los titulares en la Universidad Católica Luis Amigó.

FINALIDAD DEL TRATAMIENTO DE DATOS

El tratamiento de los datos personales de las personas vinculadas con la Universidad Católica Luis Amigó por relaciones académicas, culturales, comerciales, laborales de investigación, informativos o de otra índole tendrán las siguientes finalidades:

a) Envío de información relacionada con actividades desarrolladas por la Universidad Católica Luis Amigó, noticias, oferta de bienes y servicios.
b) Desarrollar la visión y principios filosóficos conforme a sus Estatutos.
c) Cumplir con la normatividad vigente en Colombia para las Instituciones de Educación Superior, en ejercicio de las funciones de inspección y vigilancia o para el logro de los cometidos de calidad como la obtención de Registros Calificados, acreditación de programas, acreditación institucional, certificación del sistema de calidad, acreditación internacional, entre otras.
d) Cumplir las normas aplicables a proveedores, contratistas, dependientes, que impliquen una comunicación o solicitud de información, dentro del marco del derecho común como pueden ser: las normas tributarias, comerciales, laborales, de seguridad social, entre otras.
e) Realizar encuestas de satisfacción o de expectativas de servicio que llegare a ofertar la Universidad Católica Luis Amigó.
f) Mantener un contacto permanente con las personas que han tenido algún tipo de vinculación con la Universidad Católica Luis Amigó que pueda generar algún interés.
g) Informar sobre situaciones que requieran información oportuna para lograr un propósito, entre otros.
h) Fomentar y desarrollar labores de corte investigativo, académico y docente en todos los campos.
i) La información recolectada por medios de grabación y biométricos se utilizará con fines de seguridad de las personas, los bienes e instalaciones y generar la trazabilidad de sus procesos académicos y administrativos, pudiendo ser

empleada también como medio de prueba idóneo en cualquier evento litigioso ante cualquier autoridad judicial y administrativa.

De igual manera, y en sentido general, los titulares autorizan a la Universidad Católica Luis Amigó el tratamiento de sus datos personales para ejecutar y cumplir los contratos, acuerdos y convenios destinados a la prestación de servicios y al giro ordinario de los negocios de la institución. Los datos suministrados por estudiantes, colaboradores, prestadores, socios y demás usuarios de la Universidad Católica Luis Amigó, podrán ser compartidos con otras empresas para fines comerciales o contractuales, salvo revocatoria expresa del titular de los datos, previa certificación por parte de dichas empresas del cumplimiento de las normas relativas al Tratamientos de Datos Personales y la suscripción de un acuerdo para compartir y tratar bases de datos personales.

POLÍTICAS INSTITUCIONALES PARA EL TRATAMIENTO DE DATOS EN LA UNIVERSIDAD CATÓLICA LUIS AMIGÓ

DIRECTRICES GENERALES

Se establecen las siguientes directrices generales en el tratamiento de datos personales que son de obligatorio cumplimiento en la institución y para los terceros Encargados implicados en el tratamiento:

a. Cumplir con toda la normatividad legal vigente colombiana que dicte disposiciones para la protección de datos personales.

b. Los Servidores Amigonianos deben proceder en todo momento bajo los procedimientos y lineamiento de la política de tratamiento de datos, siempre con una actitud proactiva que tenga como base las siguientes actividades.

- Eliminar los datos personales que hayamos recabado, una vez dejen de ser necesarios para la finalidad para la que fueron recogidos.
- Los datos deben ser determinados, es decir, que solo se debe recoger los datos que necesitamos en función de su finalidad.
- El fin para el que se recogen los datos deben ser libres, previos, expresos, inequívocos y ser conocido por el interesado.
- Su recogida y tratamiento debe estar legitimado.

DIRECTRICES ESPECÍFICAS

Se establecen las siguientes directrices específicas en el tratamiento de datos personales que son de obligatorio cumplimiento en la institución y para los terceros Encargados implicados en el tratamiento:

a. El Dato Personal sometido a tratamiento deberá ser veraz, completo, exacto, actualizado, comprobable y comprensible. La universidad mantendrá la información bajo estas características siempre y cuando el titular informe oportunamente sus novedades.

b. Los Datos Personales solo serán tratados por aquellos funcionarios que cuenten con el permiso correspondiente para ello, o quienes dentro de sus funciones tengan a cargo la realización de tales actividades o por los Encargados.

c. Todo dato del cual no se tenga autorización para su tratamiento por parte del titular se considera ilegal tenerlo y por tanto se deberá eliminar de las bases de datos institucionales, dejando el acta correspondiente de su eliminación.

d. La Universidad Católica Luis Amigó autoriza expresamente a los guardianes de datos de la institución para que a través de ellos fluya la información y sean ellos los garantes del adecuado tratamiento del ciclo de vida del dato RAUCS. Con ellos se hace la respectiva trazabilidad del dato.

e. Todas las autorizaciones tanto de titular como de terceras personas autorizadas por titular deben estar en repositorio digital en la Oficina de Administración de Documentos, sin excepción alguna todas deben estar disponibles para ser consultadas a solicitud del titular o de autoridad competente.

f. Todo Dato Personal que no sea Dato Público se tratará por La Universidad Católica Luis Amigó como confidencial, aun cuando la relación contractual o el vínculo entre el Titular del Dato Personal y La Universidad Católica Luis Amigó haya finalizado. A la terminación de dicho vínculo, tales Datos Personales deben continuar siendo Tratados de acuerdo con lo dispuesto por las tablas de retención documental de la institución manejados por la Oficina de Administración de Documentos y demás normas que rigen el tema en lo relacionado con el Ministerio de Educación Nacional y los temas fiscales.

g. Cada área de La Universidad Católica Luis Amigó debe evaluar la pertinencia de anonimizar los actos administrativos y/o documentos de carácter público que contengan datos personales, para su publicación o circulación.

h. Las políticas establecidas por la Universidad Católica Luis Amigó respecto al tratamiento de Datos Personales podrán ser modificadas en cualquier momento. Toda modificación se realizará con apego a la normatividad legal vigente, y las mismas entrarán en vigencia y tendrán efectos desde su publicación a través de los mecanismos dispuestos por la Universidad Católica Luis Amigó para que los titulares conozcan la política de tratamiento de la información y los cambios que se produzcan en ella.

i. La Universidad Católica Luis Amigó será más rigurosa en la aplicación de las políticas de tratamiento de la información cuando se trate del uso de datos

personales de los niños, niñas y adolescentes asegurando la protección de sus derechos fundamentales.

j. Cuando se recolecten datos sensibles se deberá solicitar una autorización especial donde se especifique que por tratarse de datos sensibles no está obligado a autorizar el tratamiento de datos. Esta categoría de datos requiere por parte de la universidad una mayor protección en medidas de seguridad para evitar una fuga o hurto de los mismos.

k. La Universidad Católica Luis Amigó podrá intercambiar información de Datos Personales con autoridades gubernamentales o públicas tales como autoridades administrativas, de impuestos, organismos de investigación y autoridades judiciales, cuando la soliciten en ejercicio de sus funciones.

l. Cuando finalice alguna de las labores de tratamiento de Datos Personales por los Servidores, contratistas o Encargados del tratamiento, y aún después de finalizado su vínculo o relación contractual con la Universidad Católica Luis Amigó, éstos están obligados a mantener la reserva de la información de acuerdo con la normatividad vigente en la materia.

m. El incumplimiento de las políticas de privacidad y de tratamiento de datos personales de la universidad, acarreará la imposición de sanciones correspondientes contempladas en el reglamento interno de trabajo y normas que rigen la Ley 1581 de 2012, las sanciones podrán ser de tipo personal de encontrarse omisión en el cumplimiento de políticas de Habeas Data de la institución o de la Ley.

n. Los servidores, funcionarios y contratistas que tengan archivos y bases de datos pertenecientes al ámbito personal o doméstico en equipos de cómputo de la entidad, deberán mantener dicha información en una carpeta identificable e inequívoca, como de uso personal.

o. La Universidad Católica Luis Amigó no realizará transferencia de información relacionada con Datos Personales a entidades o países que no cuenten con los niveles adecuados de protección de datos, de acuerdo con los estándares que estén fijados en la Superintendencia de Industria y Comercio.

p. En la universidad se entiende que la clave de acceso a los sistemas es de carácter privado, por lo tanto, no se puede compartir la misma y debe ser protegida y custodiada por el dueño de la misma.

q. En la universidad únicamente se permitirá el uso de software autorizado que haya sido adquirido legalmente por la Institución o que teniendo licencia libre tenga permiso de uso.

r. Los guardianes de datos personales son los responsables de establecer los lineamientos de seguridad que se deben aplicar y velar por su cumplimiento con el fin de resguardar la información a su cargo.

s. Es responsabilidad de todos los funcionarios y contratistas de la Universidad Católica Luis Amigó reportar al Departamento de Infraestructura y Desarrollo Tecnológico, los incidentes de seguridad tanto informáticos, como de dato personal. Para activar la ruta de la contención y atención inmediata.

t. Custodiar adecuadamente la información de datos personales alojadas en el equipo de cómputo y periféricos asignados. No transportar datos de titulares en memorias o discos extraíbles sin implementar las medidas necesarias para evitar el acceso, pérdida o consulta no autorizada.

w. Ante una desconexión total o parcial del empleado de la Universidad Católica Luis Amigó se podrá tener acceso al correo corporativo que es de carácter privado sin falta de autorización alguna. Al ser una herramienta de la empresa, esta es la dueña y responsable de todo lo que desde ella se dice. Esto siempre que se refiera a los mensajes enviados desde el correo corporativo (en horario laboral). Y los que se transmitan a través de cuentas privadas, pero operadas desde el ordenador del trabajo.

SEGURIDAD DE LOS DATOS PERSONALES

La Universidad Católica Luis Amigó no responderá en ningún caso y bajo ninguna circunstancia, por los ataques o incidentes contra la seguridad de sus sistemas de información; o por cualquier exposición o acceso no autorizado, fraudulento o ilícito y que pueda afectar la confidencialidad, integridad o autenticidad de la información publicada o asociada con los contenidos y servicios que se ofrecen.

La Universidad Católica Luis Amigó, en estricta aplicación del Principio de Seguridad en el Tratamiento de Datos Personales, proporcionará las medidas técnicas humanas y administrativas que sean necesarias para otorgar seguridad a los registros minimizando el riesgo de su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, fallas técnicas. La obligación y responsabilidad de la Universidad Católica Luis Amigó se limita a disponer de los medios adecuados para este fin.

DISPOSICIONES GENERALES PARA LA OBTENCIÓN DE LA AUTORIZACIÓN

Toda captura, recolección, uso y almacenamiento de datos personales que realice la Universidad en el desarrollo de sus actividades, y de aquellas finalidades dispuestas en la Política de Protección de Datos Personales, requiere de los titulares un consentimiento libre, previo, expreso, inequívoco e informado. Al efecto, la Universidad ha puesto a disposición de los titulares la

autorización para el tratamiento de sus datos personales en los diversos escenarios en los cuales realiza la captura del dato, tanto de manera física como digital, a través de coberturas en modelos de autorizaciones o avisos de privacidad en donde se informa al titular sobre la captura de sus datos personales, el tratamiento al cual serán sometidos incluyendo las finalidades, sus derechos, los canales de ejercicio de sus derechos y la información relacionada sobre la Política de Protección de Datos Personales. En todos los casos la obtención de la autorización se realizará bajo las diferentes modalidades que establece la ley, teniendo en cuenta la naturaleza de cada uno de los canales de captura de la información, y el modo en que la misma es obtenida, es decir, si es a través de un canal escrito, uno verbal o mediante una conducta inequívoca.

1. Es importante tener en consideración que en todos los casos la Universidad debe custodiar las autorizaciones obtenidas para el tratamiento de los datos personales, dado que ésta hace parte de las pruebas exigidas por la Superintendencia de Industria y Comercio. Así las cosas, se deberán guardar los formatos en repositorio digital en la Oficina de Administración de Documentos. Se deben conservar tanto las autorizaciones de llamadas, formularios web, autorizaciones a terceros con el fin de hacer trazabilidad a la debida autorización. La retención documental de las autorizaciones estará alineada con las Tablas de Retención Documental de la Universidad de acuerdo con el tipo de documento que las contiene o a las cuales están asociadas.

CONTENIDO DE LOS AVISOS DE PRIVACIDAD

De acuerdo con las disposiciones normativas, los avisos de privacidad mediante los cuales se obtiene la autorización de los titulares deben tener los siguientes elementos:

a) Nombre o razón social y datos de contacto del responsable del tratamiento

b) El Tratamiento al cual serán sometidos los datos y la finalidad del mismo.

c) Los derechos que le asisten al titular.

d) Los mecanismos dispuestos por el responsable para que el titular conozca la política de Tratamiento de la información.

e) En todos los casos, debe informar al Titular cómo acceder o consultar la política de Tratamiento de información.

AUTORIZACIÓN EN FORMATOS

Los modelos de autorización de tratamiento de datos personales pueden ser tramitados a través de formatos web o documentos físicos teniendo como base los formatos previamente elaborados por la Universidad que se ubican en la Intranet institucional.

Autorización en Formatos Web

Las áreas que, en el ejercicio de sus funciones, o debido a que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formularios web, deberán tener en cuenta los siguientes aspectos necesarios para su captura:

a) Solicitar sólo aquellos datos personales necesarios conforme con la finalidad del tratamiento.

b) Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento por parte del titular.

c) El envío de la información a través del formulario, deberá estar condicionado a la previa aceptación de la autorización de tratamiento del dato.

d) Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos personales.

e) Validar que la plataforma que soporta el formulario web tenga la capacidad técnica, operativa y de seguridad para almacenar las autorizaciones, y poder tener la trazabilidad en ellas. Se deberá incluir fecha en la que se obtuvo la autorización.

Autorización en formatos físicos

Las áreas que lleven a cabo iniciativas que impliquen la recolección de datos personales a través de formularios físicos, deberán tener en cuenta los siguientes aspectos:

a) Solicitar sólo aquellos datos personales necesarios conforme con la finalidad de la captura.

b) Relacionar en el formato, un aviso de privacidad que incorpore la autorización del tratamiento de los datos.

c) Para que la Universidad pueda realizar el tratamiento de los datos capturados en el formulario, el titular debe dar la autorización. En el evento en que el titular no haya autorizado, deberá ser analizado de manera independiente siempre teniendo en cuenta las excepciones de interés vital, interés legítimo e interés público.

d) Validar que en el aviso de privacidad se encuentren todas las finalidades de tratamiento asociadas a la captura de los datos solicitados.

e) Garantizar la custodia de los formularios con sus respectivas autorizaciones.

Autorización en la toma de imagen (video y fotografías)

Autorización para eventos

Con el propósito de cumplir con las disposiciones legales para el tratamiento de datos privados como la imagen, la Universidad ha dispuesto de avisos de privacidad en la entrada de los auditorios. Sin perjuicio de ello, el área promotora del evento deberá velar por el adecuado cumplimiento de las directrices establecidas sobre protección de datos personales, por lo cual, al inicio de cada presentación se deberá incorporar una diapositiva informativa sobre la captura de la imagen y las finalidades de tratamiento.

Autorización para actividades particulares

Dentro de las actividades que realiza la Universidad, están aquellas en las cuales participan terceros de quienes se puede capturar la imagen por video o fotografía. El área a cargo del tratamiento de los datos gestionará la autorización del titular para el uso de su imagen, garantizando su custodia. Es importante mencionar que la imagen de los empleados y los estudiantes no requieren de una autorización adicional, ya que la Universidad cuenta con la cobertura en los contratos y en el formulario de registro académico, respectivamente. Por último, en cada caso se deberá realizar el análisis sobre la imagen que custodiará la Universidad, dado que, si la misma tiene implicaciones sobre derechos de autor, se deberá contar adicionalmente con el consentimiento del autor para hacer uso de ella.

Custodia de la autorización

Cada área de la Universidad que realice un tratamiento activo de datos personales debe garantizar la custodia y almacenamiento de la autorización para el tratamiento de los datos. Así mismo, se deberán poner a disposición de la Superintendencia de Industria y Comercio o del Oficial de Protección de Datos en el evento en que éstos lo requieran. Se deben tener todas las autorizaciones en el repositorio digital de la Universidad que reposa en la Oficina de Administración de Documentos.

Gobierno en la protección de datos personales

La Universidad dentro de su programa de protección de datos personales ha estructurado unos roles para el desarrollo, verificación y control del programa el cual está constituido por:

a) **Oficial de Protección de Datos Personales:** Es la persona encargada de liderar el programa de protección de datos personales en la Universidad a través de: i) la planeación, ejecución y seguimiento de los elementos que hacen parte

del programa; ii) asesorar y sensibilizar a los empleados de la Universidad en relación con el programa y las principales obligaciones en su ejecución y desarrollo; iii) emitir conceptos y dar respuesta a las inquietudes y requerimientos sobre protección de datos personales a nivel interno y externo, así como asesorar sobre los asuntos relacionados con el manejo de información personal; iv) realizar el seguimiento de las normas sobre protección de datos personales y realizar las adecuaciones pertinentes al programa para procurar su cumplimiento; v) hacer seguimiento a la correcta implementación del programa en la Universidad y vi) gestionar y liderar el proceso de actualización de bases de datos ante el Registro Nacional de Bases de Datos y realizar los reportes legales que los entes de control soliciten.

b) **Guardianes de datos personales:** Son las personas encargadas de las bases de datos identificadas y reportadas antes el Registro Nacional de Bases de Datos, quienes tienen el deber de reportar actualizaciones o cambios sustanciales en la información de la base de datos que deba ser reportada ante la Superintendencia de Industria y Comercio. Adicionalmente, están encargadas de informar sobre cambios en el tratamiento de datos personales, o puntos de captura adicionales que requieran coberturas.

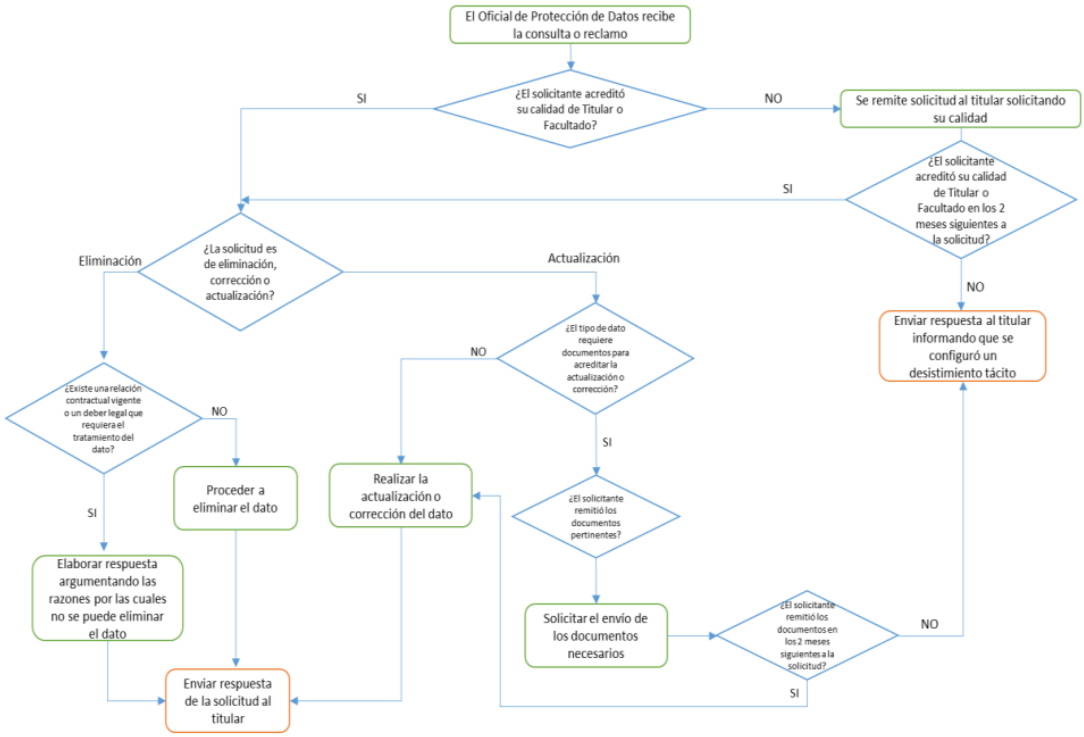
c) **Comité de Habeas Data:** Está encargado de realizar el seguimiento a los principales temas del programa de protección de datos personales en la Universidad. Es el escenario de control en donde se revisan, discuten, validan y aprueban directrices enfocadas a implementar, consolidar y mejorar las actividades que hacen parte del programa de protección de datos personales. Se reúne para tratar casos muy específicos.

PROCEDIMIENTO DE ATENCIÓN DE CONSULTAS Y RECLAMOS

El procedimiento de consultas y reclamos se ejecutará de acuerdo con los términos incluidos en la ley y acogidos por la Política de Protección de Datos Personales de la Universidad Católica Luis Amigó. Las solicitudes que pueden ser catalogadas como consultas o reclamos pueden llegar por los canales habilitados de protección de datos, los cuales son correo: protecciondedatos@amigo.edu.co, o ser recibidas por cualquier persona vinculada a la Universidad habiendo cumplido con el diligenciamiento del formato “acceder a derechos” establecido para tal fin.

En este último caso, es necesario que la solicitud sea remitida al canal de protección de datos personales para que el Oficial de Protección de Datos Personales pueda hacer seguimiento a su trámite y su respectivo cierre.

A continuación, se presenta el esquema de trámite de consultas y reclamos:



Los tiempos de respuesta de las consultas serán de diez (10) días hábiles desde la fecha de recibo, y de los reclamos serán de quince (15) días hábiles desde su recibo. En aquellos eventos en los cuales el Oficial de Protección de Datos Personales evidencie que la solicitud del titular no puede ser tramitada debido a que la Universidad debe contar con la información asociada a los datos personales del titular, o porque se encuentra en sistemas de información tecnológicos que requieren de un concepto técnico, podrá integrar una mesa de trabajo entre la Dirección Jurídica, la Jefatura de Tecnologías de la Información, según corresponda, a efectos de contar con un concepto jurídico y técnico integral para dar efectiva respuesta al titular sobre el trámite y cumplimiento de su solicitud.

ACREDITACIÓN DEL PRINCIPIO DE LA RESPONSABILIDAD DEMOSTRADA (“ACCOUNTABILITY”) Y EL RELACIONAMIENTO CON TERCEROS

Para llevar a cabo un adecuado tratamiento de los datos personales, el Oficial de Protección de Datos Personales deberá validar los siguientes elementos de manera periódica:

a) Revisión de las actividades que generan algún tipo de tratamiento de los datos personales.
b) Validación de los puntos de captura de información personal, identificando el tipo de información que se recolecta y sus finalidades.
c) Inventario y actualización de las bases de datos identificadas.
d) Seguimiento al cumplimiento de las medidas de seguridad de las bases de datos y repositorios de información que se encuentren en el inventario.
e) Identificación de terceros que realizarán el tratamiento de datos personales.

Los elementos antes relacionados son la base para la determinación de incorporación de coberturas jurídicas y técnicas en la Universidad, para que se pueda llevar a cabo un adecuado tratamiento de los datos personales en cumplimiento de las disposiciones legales y reglamentarias.

Adicionalmente, como parte de un análisis integral, la Universidad procurará mantener relaciones con terceros que reflejen un compromiso por la protección de los datos personales y la operación que ellos implican. Al efecto, en los contratos que la Universidad suscriba se incorporarán cláusulas de protección de datos personales, y adicionalmente, se podrá solicitar a los terceros en el desarrollo del vínculo comercial o contractual, información que permita validar el cumplimiento de las directrices contenidas en la Política de Protección de Datos Personales de la Universidad, así como aquellas directrices legales y reglamentarias, cuando se estime necesario.

Los terceros que realicen un tratamiento de datos personales de los cuales la Universidad es responsable, deberán acreditar el cumplimiento de los requisitos del régimen de protección de datos personales, aportando: i) la política de protección de datos personales; ii) información sobre los canales habilitados para el trámite de consultas y reclamos y iii) el cumplimiento sobre el registro de las bases de datos ante el Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio.

Sin perjuicio de lo anterior, la Universidad podrá realizar verificaciones aleatorias en el desarrollo del vínculo comercial o contractual para validar que se esté efectivamente cumpliendo con las disposiciones de protección de datos, por lo cual se podrá solicitar evidencias o soportes del cumplimiento. En todos los casos, la Universidad podrá incluir cláusulas en los contratos referidas al cumplimiento de las disposiciones sobre protección de datos personales.

En el evento en el cual la Universidad evidencie un incumplimiento de las disposiciones sobre protección de datos por parte del tercero, puede sugerir que se lleve a cabo un acuerdo para su cumplimiento; en el caso en que éste no cumpla, podrá promover la terminación de la relación contractual o comercial vigente.

INICIATIVAS QUE IMPLICAN EL TRATAMIENTO DE DATOS PERSONALES Y ANÁLISIS DE IMPACTO DE PRIVACIDAD

La Universidad reconoce la importancia de proteger los datos personales de todos los titulares, es por esto que cualquier tipo de iniciativa que implique el tratamiento de datos personales deberá ser objeto de análisis de manera previa, a efectos de validar el alcance de las coberturas que deben tenerse en cuenta para el desarrollo de la misma.

El análisis de impacto de la privacidad permite validar el cumplimiento de las disposiciones legales y reglamentarias en el ejercicio de la captura y tratamiento de los datos personales en relación con el entorno universitario y los titulares de información.

Trámite de solicitudes de conceptos o análisis de impacto de privacidad
Los tramites sobre solicitud de conceptos, análisis de impacto de privacidad o coberturas particulares de autorizaciones, serán tramitadas por el Oficial de Protección de Datos Personales a través del correo: protecciondedatos@amigo.edu.co.

PROGRAMA DE SENSIBILIZACIÓN Y CAPACITACIÓN

Para la Universidad es muy importante tener actualizados a los empleados administrativos y profesores sobre las disposiciones y reglamentación relacionada con la protección de los datos personales. Al efecto, la Universidad incorporó dentro de su programa de inducción los principales conceptos, lineamientos y disposiciones prácticas sobre el tratamiento de los datos personales, el cual será complementada con la capacitación liderada por el área de Gestión Humana a través del curso virtual en Habeas Data que es de obligatorio cumplimiento.

Adicionalmente, durante cada año se llevan a cabo capacitaciones a los guardianes de datos que permita comprender y aprehender las directrices sobre manejo de información y medias de seguridad de acuerdo con el desarrollo de la operación de cada área de la Universidad.

VERIFICACIÓN DEL CUMPLIMIENTO DE LAS DISPOSICIONES SOBRE DATOS PERSONALES

El Oficial de Protección de Datos Personales podrá, en cualquier momento, adelantar auditorías de supervisión de cumplimiento de las disposiciones sobre protección de datos personales, con el propósito de garantizar el adecuado cumplimiento y desarrollo del programa en la Universidad. Como resultado de las revisiones pueden levantarse planes de acción para cerrar las brechas encontradas.

Además, con el fin de mejorar el cumplimiento y las buenas prácticas en la gestión de los datos se ha creado el cargo de guardián de datos a nivel país constituido por 58 empleados, a continuación, se listan sus responsabilidades.

1. Identificar las bases de datos existentes en su área específica y garantizar el correcto manejo de las mismas, ajustadas a las finalidades determinadas en la Política de Tratamiento de Datos.
2. Garantizar la Seguridad de la Información de acuerdo con la clasificación y niveles de acceso definidos por el Oficial de Tratamiento de Datos al interior de su Unidad.
3. Gestionar el acompañamiento necesario a los ejercicios de sensibilización permanente al interior de su área en el manejo de datos personales.
4. Vigilar en su área correspondiente el cumplimiento de las Políticas de Tratamiento de Datos Personales.
5. Realizar las gestiones correspondientes para el diligenciamiento y resolución de las solicitudes que en materia de Tratamientos de Datos Personales presenten los titulares y cuyo adelantamiento corresponda a su área, en coordinación permanente con el Oficial de Tratamiento de Datos.
6. Vigilar el cumplimiento estricto, desde su propia área, de los términos de procedimiento dispuestos en las Políticas de Tratamiento de Datos Personales para la resolución de consulta y reclamos, con la coayuvancia del Oficial de Tratamiento de Datos.
7. Reportar al Oficial de Tratamiento de Datos los incidentes de seguridad que se presenten al interior de su área y que afecten las bases de datos a su disposición.
8. Llevar el registro de los reclamos realizados por los titulares de datos del área respectiva, asegurar su resolución y guardar las evidencias correspondientes ante cualquier reclamación futura o supervisión por parte del ente de vigilancia.
9. Capacitarse permanentemente en materia de protección de datos, en las jornadas que para ello establezca la Institución.
10. Presentar informe sobre el tratamiento de datos de su área en los términos que lo requiera el Oficial de Datos para efectos de control en todos los niveles de la Institución.
11. Las demás que se asignen en razón de sus responsabilidades dentro de los reglamentos, políticas, procedimientos internos de la Institución y la normatividad vigente.

PROCEDIMIENTO DE TRATAMIENTO DE LAS PQRSF DE HABEAS DATA

ACTIVIDAD	PROCEDIMIENTO	RESPONSABLE
Recepción PQRS - tratamiento de datos	Toda solicitud del titular del dato para corregir, actualizar, suprimir sus datos personales o para revocar la autorización en los casos establecidos en la ley 1581 de 2012, que ingrese por cualquiera de los medios de atención con los que cuanta la Universidad Católica Luis Amigó, se direccionará al correo: protecciondedatos@amigo.edu.co O se entregará personalmente diligenciando el formato para acceder a derechos, adjuntando la copia de documento de identidad. Canales disponibles en la institución para solicitar el tratamiento de datos personales: Correo electrónico; línea telefónica; buzones físicos; página web; oficinas de atención a usuario. Si la solicitud está incompleta, debe contactarse al titular en un plazo no mayor a 5 días hábiles a través de correo electrónico; e indicar el procedimiento que debe seguir, para hacer efectiva la solicitud, y se registrara en la base de datos con la observación “reclamo incompleto”.	Agentes del centro de contacto Oficial de tratamiento de datos
Verificación y registro (reclamo completo y en trámite)	Si la solicitud está completa, el Oficial de tratamiento de datos realiza la creación de la petición, se clasifica y se identifica el archivo con la leyenda “reclamo en trámite” teniendo en cuenta los tiempos establecidos para la respuesta según el Título V de la	Oficial de tratamiento de datos

	Ley 1581 de 2012 se procede a su escalonamiento.	
Direccionamiento Actuación requerida	El Oficial de tratamiento de datos redirecciona vía correo electrónico la comunicación a cada uno de los 58 guardianes de datos de la institución a nivel país para que efectúen la búsqueda de los datos y realicen el tratamiento requerido por el titular. Estos a su vez en un plazo no mayor a tres días hábiles deberán contestar el correo sea que hayan realizado tratamiento o no, además deberán marcar las bases de datos con la leyenda en color rojo "reclamo en trámite"	Guardianes de datos Unidades encargadas
Concepto Jurídico	Si la causa del PQRSF es un "DERECHO VULNERADO", se debe direccionar al proceso de radicación, para su tratamiento, revisión, solución su respuesta debe ser radicada.	Unidad requerida Radicación
Notificación	Notificar al titular de la solución de su PQRSF a través del correo: protecciondedatos@amigo.edu.co	Oficial de tratamiento de datos

AVISO DE PRIVACIDAD

La **Universidad Católica Luis Amigó** como responsable o encargado del tratamiento de los datos personales obtenidos de sus usuarios, proveedores, contratistas, clientes y en general de todas las personas que hayan facilitado o que en el futuro faciliten sus datos personales, en cumplimiento de la Ley 1581 de 2012 y las demás normas que la reglamenten o complementen, reglamenten o modifiquen, informa al **TITULAR** de los datos personales que le asisten los siguientes derechos:

- Conocer, actualizar y rectificar sus datos personales.
- Solicitar prueba de la autorización otorgada.
- Conocer el uso que le ha dado a sus datos personales.
- Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la normatividad.
- Revocar la autorización y/o solicitar la supresión del dato.

- Acceder a sus datos personales y en general todos los derechos consignados en el artículo 8 de la Ley 1581 de 2012.

La **Universidad Católica Luis Amigó** notifica al **TITULAR** que ha establecido el siguiente canal, para que estos derechos puedan ser ejercidos en el correo electrónico: protecciondedatos@amigo.edu.co

Todas las consultas y reclamos pueden ser enviadas a este correo electrónico, en donde se adoptarán mecanismos de prueba de la radicación y trámite de los mismos. Los datos personales recolectados al inicio, durante, después de la relación comercial, laboral, de servicios, contractual y/o personal serán almacenados, usados, suprimidos, procesados, compilados, transferidos, sometidos a circulación, actualizados, dispuestos conforme a la Ley 1581 de 2012, su decreto reglamentario y Política de Tratamiento de Datos Personales de la Universidad Católica Luis Amigó.

La Política de Tratamiento de Datos Personales de la Universidad Católica Luis Amigó se encuentra disponible para su consulta en la página web http:// www.ucatolicaluisamigo.edu.co tratara los datos sensibles bajo estrictos estándares de seguridad y confidencialidad. Para este fin, se han implementado medidas administrativas, técnicas y jurídicas, de obligatorio cumplimiento para los involucrados.

La Universidad Católica Luis Amigó se permite informar, que el TITULAR tiene la libre facultad de no autorizar el tratamiento de sus datos sensibles. La Universidad Católica Luis Amigó como Institución de Educación Superior es una institución sin ánimo de lucro, con Personería Jurídica otorgada mediante Resolución MEN, pone a conocimiento del TITULAR, para todos los efectos legales sus datos de contacto:

- Número de identificación tributaria: 890.985.189-9
- Domicilio principal: transversal 51ª No. 67B-90
- Correo electrónico: protecciondedatos@amigo.edu.co
- Teléfono de contacto: (604) 448 76 66

Por lo anterior, otorgo mi consentimiento a la Universidad Católica Luis Amigó de forma voluntaria, previa, explicita, informada e inequívoca para tratar mi información personal para el cumplimiento del objeto de la prestación de servicios educativos y académicos, finalidades laborales, comerciales, investigativos, formativas o científicas e informativas de acuerdo con la Política de Tratamiento de Datos Personales y por tanto, me comprometo a leer la política mencionada. Igualmente, autorizo a la Universidad Católica Luis Amigó a modificar o actualizar la política con el fin de atender reformas legislativas, dando aviso previo por medio de correo electrónico.

BASES DE DATOS REGISTRADAS Y RESPONSABILIDAD DE SU CUSTODIA

Número de base de datos	Categoría de datos	Unidad responsable	Recomendaciones de uso y de tratamiento
1	Sensible	Bienestar U atención psicológica	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.
2	Sensible	Bienestar U asesoría psicológica	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.
3	Sensible	Conducta de entrada Gimnasio	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.
4	Semiprivada	Lab. psicología listados de asistencia	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
5	Semiprivada	Inscripción torneos internos	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
6	Sensible	Perfiles Psicológicos	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.
7	Categoría Especial	Vacaciones recreativas - recreando	El guardián de datos de esta información debe realizar esfuerzos adicionales en seguridad y en privacidad con el fin de custodiar de manera superior los datos de esta categoría. Esto implica entre otras cosas mayores niveles de seguridad en su almacenamiento y circulación.
8	Categoría Especial	Apartado Mercadeo	El guardián de datos de esta información debe realizar esfuerzos adicionales en seguridad y en privacidad con el fin de custodiar de manera superior los datos de esta categoría. Esto implica entre otras cosas mayores niveles de seguridad en su almacenamiento y circulación.

9	Semiprivada	CRM Monitor	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
10	Semiprivada	Regionalización Cali	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
11	Semiprivada	Asistentes eventos de extensión	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
12	Sensible	Usuarios externos Consultorio Jurídico	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.
13	Categoría Especial	Mercadeo Registro Nacional Bachilleres	El guardián de datos de esta información debe realizar esfuerzos adicionales en seguridad y en privacidad con el fin de custodiar de manera superior los datos de esta categoría. Esto implica entre otras cosas mayores niveles de seguridad en su almacenamiento y circulación.
14	Semiprivada	Mercadeo Interesados postgrados	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
15	Semiprivada	ESDEGAN	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
16	Semiprivada	Estudiantes Activos Admisiones y Registro Académico	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
17	Semiprivada	Graduados	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
18	Semiprivada	Portal Institucional, Web Master	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.

19	Semiprivada	Bienestar Virtual, Web Master	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
20	Semiprivada	RADIUS, Web Master	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
21	Semiprivada	Soporte técnico, Web Master	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
22	Semiprivada	Revistas institucionales Fondo Editorial	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
23	Pública	Terceros DATOS PUBLICOS	Por su naturaleza no requiere autorización y el nivel de seguridad es mínimo, no requiere comportamientos especiales de seguridad, ni de privacidad.
24	Pública	Proveedores (Contabilidad)	Por su naturaleza no requiere autorización y el nivel de seguridad es mínimo, no requiere comportamientos especiales de seguridad, ni de privacidad.
25	Semiprivada	Usuarios de préstamo Biblioteca	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
26	Semiprivada	Relaciones Laborales	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
27	Semiprivada	Tiquetes aéreos	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
28	Categoría Especial	Mercadeo extensión IMOLKO	El guardián de datos de esta información debe realizar esfuerzos adicionales en seguridad y en privacidad con el fin de custodiar de manera superior los datos de esta categoría. Esto implica entre otras cosas mayores niveles de seguridad en su almacenamiento y circulación.
29	Semiprivada	Visitantes Torniquetes	Se debe en todo momento garantizar la adecuada circulación y disposición final, con

			acta de eliminación de datos cuando se amerite.
30	Semiprivada	Visitantes Parqueaderos	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
31	Semiprivada	Mercadeo Contadores públicos. Se le cambia el nombre por: Contadores públicos extensión.	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
32	Semiprivada	Visitantes extranjeros–OCRI	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
33	Semiprivada	Movilidad OCRI (Transmisión con Encargados)	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
34	Semiprivada	Soporte Virtualidad	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
35	Semiprivada	DICOM - ahora se llama Campus Virtual	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
36	Sensible	Consultorio Psicológico	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.
37	Sensible	Consultorio Médico	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales

			a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.
38	Semiprivada	Pares Evaluadores Revistas-Luisa Fernanda Córdoba Quintero, Asistente Editorial	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
39	Semiprivada	Seguros estudiantiles	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
40	Privada	Pago de nómina Bancolombia	Estos datos pueden afectar la intimidad misma de la persona, por lo tanto, el guardián de datos de estas unidades de información debe implementar medidas adicionales de seguridad con el fin de evitar pérdidas y accesos no autorizados a los datos. Es obligación del guardián de datos velar por la integralidad y disponibilidad de los datos.
41	Privada	Pago de nómina Banco Bogotá	Estos datos pueden afectar la intimidad misma de la persona, por lo tanto, el guardián de datos de estas unidades de información debe implementar medidas adicionales de seguridad con el fin de evitar pérdidas y accesos no autorizados a los datos. Es obligación del guardián de datos velar por la integralidad y disponibilidad de los datos.
42	Privada	Pago de nómina Banco Davivienda	Estos datos pueden afectar la intimidad misma de la persona, por lo tanto, el guardián de datos de estas unidades de información debe implementar medidas adicionales de seguridad con el fin de evitar pérdidas y accesos no autorizados a los datos. Es obligación del guardián de datos velar por la integralidad y disponibilidad de los datos.

43	Privada	Pago de nómina Banco AVVILLAS	Estos datos pueden afectar la intimidad misma de la persona, por lo tanto, el guardián de datos de estas unidades de información debe implementar medidas adicionales de seguridad con el fin de evitar pérdidas y accesos no autorizados a los datos. Es obligación del guardián de datos velar por la integralidad y disponibilidad de los datos.
44	Semiprivada	AP Agencias de prácticas	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
45	Pública	Ap Proveedores	Por su naturaleza no requiere autorización y el nivel de seguridad es mínimo, no requiere comportamientos especiales de seguridad, ni de privacidad.
46	Semiprivada	BG Agencias de prácticas	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
47	Pública	BG Proveedores	Por su naturaleza no requiere autorización y el nivel de seguridad es mínimo, no requiere comportamientos especiales de seguridad, ni de privacidad.
48	Semiprivada	BG Visitantes	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
49	Categoría Especial	BG Mercadeo	El guardián de datos de esta información debe realizar esfuerzos adicionales en seguridad y en privacidad con el fin de custodiar de manera superior los datos de esta categoría. Esto implica entre otras cosas mayores niveles de seguridad en su almacenamiento y circulación.
50	Sensible	MAN Asesoría psicológica	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.
51	Sensible	MAN Consultorio Jurídico	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.

52	Semiprivada	MAN Inscritos eventos extensión	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
53	Categoría Especial	MAN Mercadeo	El guardián de datos de esta información debe realizar esfuerzos adicionales en seguridad y en privacidad con el fin de custodiar de manera superior los datos de esta categoría. Esto implica entre otras cosas mayores niveles de seguridad en su almacenamiento y circulación.
54	Semiprivada	MAN secretaria admin presup	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
55	Sensible	MONT Consultorio Jurídico	El guardián de datos de esta unidad debe implementar medidas de seguridad adicionales a las existentes para garantizar el resguardo de la información y evitar perdida, vulneración o acceso no autorizado a los datos.
56	Semiprivada	MONT Extensión	Se debe en todo momento garantizar la adecuada circulación y disposición final, con acta de eliminación de datos cuando se amerite.
57	Categoría Especial	MONT Mercadeo	El guardián de datos de esta información debe realizar esfuerzos adicionales en seguridad y en privacidad con el fin de custodiar de manera superior los datos de esta categoría. Esto implica entre otras cosas mayores niveles de seguridad en su almacenamiento y circulación.
58	Categoría Especial	Video vigilancia - Dato biométrico	El guardián de datos de esta información debe realizar esfuerzos adicionales en seguridad y en privacidad con el fin de custodiar de manera superior los datos de esta categoría. Esto implica entre otras cosas mayores niveles de seguridad en su almacenamiento y circulación.

Recomendaciones finales

Tenga en cuenta además que, en la intranet en el **Sistema de gestión por procesos**, en el link **Documentación de los procesos** encontrará la pestaña de **Tratamiento de datos personales** donde podrá consultar:

- Comunicados
- Política de Seguridad
- Preguntas Frecuentes

- Autorizaciones
- Procedimientos
- Política de tratamiento de datos
- Funciones de los guardianes de datos, comunicado 040
- Manual de tratamiento de datos personales

Recuerde que dentro de sus funciones esta dar cabal cumplimiento a los procedimientos estipulados por la institución en cada una de las actividades del ciclo de vida del dato, por lo tanto, le invitamos a consultar permanentemente los procedimientos que se encuentran en la intranet institucional, además revisar los videos que se encuentran allí para su capacitación permanente.

Protocolo de actuación ante un incidente de seguridad

- La persona que detecta la incidencia, informa de la misma al Departamento de Infraestructura y Desarrollo Tecnológico al correo: jefe.itecnologica@amigo.edu.co ó vía telefónica: (604) 4487666.

  Extensiones: 9561 - 9650

- Recibida la comunicación, el Departamento de Infraestructura y Desarrollo Tecnológico activa el protocolo de incidente de seguridad (informático o de dato personal) recaba todos los datos necesarios para abrir la incidencia, analizado el caso y haciendo la contención inicial adecuada e inmediata.
- Reportará la incidencia en datos personales a la coordinación de datos personales al correo: protecciondedatos@amigo.edu.co siempre y cuando el incidente sea un dato personal.
- La persona implicada debe diligenciar el formato de reporte de incidente de seguridad de dato personal que será el insumo para el reporte ante la SIC.
- Como aspecto final el Departamento de Infraestructura y Desarrollo Tecnológico adoptará las medidas necesarias para evitar que en la institución en el futuro no se vuelva a repetir el incidente.