ACUERDO No. 019
(26 de Abril de 2016)

Por el cual se adopta la Política de Protección de Datos Personales en la Fundación Universitaria del Área Andina.

El Consejo Superior de la Fundación Universitaria del Área Andina, en uso de sus atribuciones legales y estatutarias, en especial de la contenida en el literal e) del artículo 37 del Estatuto General, y

CONSIDERANDO

Que se hace necesario adoptar la política de protección de datos personales en cumplimiento de lo dispuesto en la Ley Estatutaria 1581 del 17 de octubre de 2012, reglamentada por el Decreto 1377 del 27 de junio de 2013 y en la Circular Externa No. 02 del 3 de noviembre de 2015, expedida por la Superintendencia de Industria y Comercio,

Que dicha política fue puesta en consideración del Consejo Superior para su aprobación, en sesión del 26 de abril de 2016, en la cual fue aprobada por unanimidad.

Con fundamento en lo anterior, el Consejo Superior

ACUERDA:

Artículo Primero. Adoptar la Política de Protección de Datos Personales en la Fundación Universitaria, la cual estará estructurada de la siguiente manera:

1. Base legal y ámbito de aplicación:

La política de tratamiento de la Información se desarrolla en cumplimiento de los artículos 15 y 20 de la Constitución Política; de los artículos 17 literal k) y 18 literal f) de la Ley Estatutaria 1581 de 2012, por la cual se dictan disposiciones generales para la Protección de Datos Personales (en adelante LEPD); y del artículo 13 del Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley anterior.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento.

2. Definiciones establecidas en el artículo 3 de la LEPD y el artículo 3 del Decreto 1377 de 2013:

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Datos sensibles:** Se entiende por datos sensible aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las convicciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.
- **Encargado del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el tratamiento de datos personales por cuenta del responsable del tratamiento.
- **Responsable del tratamiento:** Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, decida sobre la base de datos y/o el tratamiento de los datos.
- **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.
- **Aviso de privacidad:** Comunicación verbal o escrita generada por el responsable, dirigida al Titular para el tratamiento de sus datos personales, mediante la cual se le informa acerca de la existencia de las políticas de tratamiento de información que le serán aplicables, la forma de acceder a las mismas y las finalidades del tratamiento que se pretende dar a los datos personales.
- **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.

3. Autorización de la política de tratamiento:

De acuerdo al artículo 9 de la LEPD, para el tratamiento de datos personales se requiere la autorización previa e informada del Titular. Mediante la aceptación de la presente política, todo Titular que facilite información relativa a sus datos personales está consintiendo el tratamiento de sus datos por parte de la Fundación Universitaria del Área Andina en los términos y condiciones recogidos en la misma.

No será necesaria la autorización del Titular cuando se trate de:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

4. Responsable del tratamiento

El responsable del tratamiento de las bases de datos objeto de esta política es La Fundación Universitaria del Área Andina, cuyos datos de contacto son los siguientes:

- Dirección: Calle 71 # 13 - 21- Bogotá DC
- Correo electrónico: protecciondedatos@areandina.edu.co
- Teléfono: (571) 7 42 19 47

5. Principios de la protección de datos

El artículo 4 de la LEPD establece unos principios para el tratamiento de datos personales que se han de aplicar, de manera armónica e integral, en el desarrollo, interpretación y aplicación de la Ley. Los principios legales de la protección de datos son los siguientes:

- **Principio de legalidad:** El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la LEPD, el Decreto 1377 de 2013 y en las demás disposiciones que la desarrollen.
- **Principio de finalidad:** El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.
- **Principio de libertad:** El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e

informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la LEPD:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.

- **Principio de veracidad o calidad:** La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.
- **Principio de transparencia:** En el tratamiento debe garantizarse el derecho del Titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:
  - El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
  - El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
  - Los derechos que le asisten como Titular.
  - La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.
- **Principio de acceso y circulación restringida:** El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la LEPD y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.
- **Principio de seguridad:** La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el Manual Interno de Seguridad, de obligado cumplimiento para todo usuario y personal de la Institución. Cualquier modificación de las normas y

medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

- **Principio de confidencialidad:** Todas las personas que intervengan en el tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento, pudiendo solo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la LEPD y en los términos de la misma.

6. Categorías especiales de datos

6.1. Datos sensibles

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

Según el artículo 6 de la LEPD, se prohíbe el tratamiento de datos sensibles, excepto cuando:

- El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de La Fundación, ONG, asociación o cualquier otro organismo sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical, siempre que se refieran exclusivamente a sus miembros o a las personas que mantengan contactos regulares por razón de su finalidad. En estos eventos, los datos no se podrán suministrar a terceros sin la autorización del Titular.
- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

6.2. Derechos de los niños, niñas y adolescentes

El tratamiento de datos personales de niños, niñas y adolescentes está prohibido, excepto cuando se trate de datos de naturaleza pública, y cuando dicho tratamiento cumpla con los siguientes requisitos:

- Que responda y respete el interés superior de los niños, niñas y adolescentes.
- Que se asegure el respeto de sus derechos fundamentales

Cumplidos los anteriores requisitos, el representante legal del niño, niña o adolescente otorgará la autorización previo ejercicio del menor a su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

Es tarea del Estado y las entidades educativas de todo tipo proveer información y capacitar a los representantes legales y tutores sobre los eventuales riesgos a los que se enfrentan los niños, niñas y adolescentes respecto del tratamiento indebido de sus datos personales, y proveer de conocimiento acerca del uso responsable y seguro por parte de niños, niñas y adolescentes de sus datos personales, su derecho a la privacidad y protección de su información personal y la de los demás.

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1377 de 2013. En todo caso, en el tratamiento se asegurará el respeto a los derechos prevalentes de los niños, niñas y adolescentes.

Los derechos de acceso, corrección, supresión, revocación o reclamo por infracción sobre los datos de los niños, niñas y adolescentes se ejercerán por las personas que estén facultadas para representarlos.

7. Funciones y obligaciones

7.1. Responsable del tratamiento

Las obligaciones en materia de seguridad de los datos de La Fundación Universitaria del Área Andina, son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en el Manual Interno de Seguridad.
- Difundir el referido documento entre el personal afectado.
- Mantener el Manual Interno de Seguridad actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la Institución, el contenido de la información de las bases de datos, o como consecuencia de los controles periódicos realizados. De igual

modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.

- Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos en el Manual Interno de Seguridad.
- Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.
- Autorizar, salvo delegación expresa a usuarios autorizados e identificados en el Manual Interno de Seguridad, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel; y el uso de módems y las descargas de datos.
- Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.
- Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.
- Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas, al menos cada tres meses.
- Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos cada dos años.

7.2. Responsables de seguridad

La Fundación Universitaria del Área Andina, designa como responsables de seguridad de las bases de datos a:

Bases de datos sensibles:

- Director Nacional de Servicio al Estudiante,
- Director Nacional de Gestión y Desarrollo Humano,
- Director del Centro Médico y Director de la Clínica de Optometría.
- Director Nacional de Medio Universitario

Bases de datos privadas:

- Dirección Nacional Administrativo

Los responsables de seguridad tienen las siguientes funciones:

- Coordinar y controlar la implementación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión del Manual Interno de Seguridad.
- Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe mensual sobre dicho control.
- Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en el Manual Interno de Seguridad.

- Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.
- Comprobar, al menos cada tres meses, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización del Manual Interno de Seguridad y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.
- Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales.

7.3. Usuarios

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de La Fundación Universitaria del Área Andina, deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.
La Fundación Universitaria del Área Andina, cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben, en su caso, los usuarios de sistemas de identificación sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos.

Las funciones y obligaciones del personal de La Fundación Universitaria del Área Andina, se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la Institución y, específicamente, por el contenido del Manual. La lista de usuarios y perfiles con acceso a los recursos protegidos están recogidos en el Manual Interno de Seguridad. Con carácter general, cuando un usuario trate documentos o soportes que contiene datos personales tiene el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en el Manual por parte del personal al servicio de La Fundación Universitaria del Área Andina, es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y la Institución.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de La Fundación Universitaria del Área Andina, son las siguientes:

- **Deber de secreto:** Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados; en cumplimiento de este deber, los usuarios de la empresa u organización no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.

- **Funciones de control y autorizaciones delegadas**: El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.
- **Obligaciones relacionadas con las medidas de seguridad implantadas:**
  - Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
  - No revelar información a terceras personas ni a usuarios no autorizados.
  - Observar las normas de seguridad y trabajar para mejorarlas.
  - No realizar acciones que supongan un peligro para la seguridad de la información.
  - No sacar información de las instalaciones de la organización sin la debida autorización.
- **Uso de recursos y materiales de trabajo:** Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse al responsable de seguridad correspondiente que podrá autorizarla y, en su caso, registrarla.
- **Uso de impresoras, escáneres y otros dispositivos de copia:** Cuando se utilicen este tipo de dispositivos debe procederse a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.
- **Obligación de notificar incidencias:** Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento al responsable de seguridad que corresponda, quien se encargará de su gestión y resolución. Algunos ejemplos de incidencias son: la caída del sistema de seguridad informática que permita el acceso a los datos personales a personas no autorizadas, el intento no autorizado de la salida de un documento o soporte, la pérfida de datos o la destrucción total o parcial de soportes, el cambio de ubicación física de bases de datos, el conocimiento por terceras personas de contraseñas, la modificación de datos por personal no autorizado, etc.
- **Deber de custodia de los soportes utilizados:** Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos deben identificar el tipo de información que contienen mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.
- **Responsabilidad sobre los terminales de trabajo y portátiles:** Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción
- **Uso limitado de Internet y correo electrónico:** El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la Institución.

- **Salvaguarda y protección de contraseñas:** Las contraseñas proporcionadas a los usuarios son personales e intransferibles, por lo que se prohíbe su divulgación o comunicación a personas no autorizadas. Cuando el usuario accede por primera vez con la contraseña asignada es necesario que la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.
- **Copias de respaldo y recuperación de datos:** Debe realizarse copia de seguridad de toda la información de bases de datos personales de la Institución.
- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en el Manual de Políticas y Procedimiento y en el Manual Interno de Seguridad.

8. Tratamiento y finalidades de las bases de datos

La Fundación Universitaria del Área Andina, en el desarrollo de su objeto social, lleva a cabo el tratamiento de datos personales relativos a personas naturales que están contenidos y son tratados en bases de datos destinadas a finalidades legítimas, cumpliendo con la Constitución y la Ley.

La siguiente tabla (Tabla I) presenta las distintas bases de datos que manejan la Institución y las finalidades asignadas a cada una de ellas.

Tabla I. Bases de datos y finalidades

Base de datos	Finalidad
Estudiantes.	Reportes internos y externos a otras organizaciones gubernamentales, entre otras. Validación y certificación de estudios a entidades externas. Contacto a estudiantes para procesos internos académico – administrativos; para hacer seguimiento y realizar acciones afirmativas así como hacer seguimiento a las mismas. Para ofrecimiento de servicios de la Institución, entre otros.
Empleados.	✓ Dirección, gestión y desarrollo de los procesos de gestión humana a nivel nacional. ✓ Procesos de vinculación de personal y relaciones laborales. ✓ Procesos de formación y desarrollo de los colaboradores. ✓ Procesos de selección de personal. ✓ Bienestar y calidad de vida, seguridad y salud en el trabajo. ✓ Proceso de pago de nómina y compensación y beneficios de los colaboradores. ✓ Elaboración de informes. ✓ Proceso de contratación de colaboradores, afiliaciones a la seguridad social y presentación de informes. ✓ Procesos relacionados con seguridad y salud en el trabajo y

	bienestar de colaboradores. ✓ Procesos de formación y desarrollo. ✓ Procesos de formación de las personas. ✓ Elaboración de certificaciones. ✓ Entre otras actividades necesarias en desarrollo de las relaciones laborales con la Institución. ✓ Para ofrecimiento de servicios de la Institución, entre otros.
Salud.	✓ Identificación del usuario, agendamiento de citas, transcripción de incapacidades, entre otros. Diligenciamiento de la historia clínica. ✓ Prestación de servicios o acompañamientos en salud entre otros. ✓ Para ofrecimiento de servicios de la Institución, entre otros.
Egresados.	✓ Para seguimiento y realización de acciones afirmativas, para realizar contactos y ofrecer actividades académicas y de integración, ✓ Para fidelizar al personal egresado. ✓ Para actualización de información de la Institución. ✓ Para atender requerimientos de terceros de información acerca del egresado. ✓ Para ofrecimiento de servicios de la Institución, entre otros.
Becas.	✓ Contacto de estudiantes. ✓ Remisión de información acerca de los beneficios. ✓ Contacto a los beneficiarios para ceremonia de entrega del beneficio en eventos. ✓ Seguimiento y contacto de los beneficiarios entre otros. ✓ Para ofrecimiento de servicios de la Institución, entre otros.
Proveedores.	✓ Para cotización de bienes y servicios. ✓ Para adquisición de bienes y servicios. ✓ Para solicitud de soporte derivado de la adquisición de bienes o prestación de servicios. ✓ Para ofrecimiento de servicios de la Institución, entre otros.
Cartera.	✓ Tramitar créditos estudiantiles. ✓ Consulta de personas dentro del trámite de créditos. ✓ Reportar información financiera y de comportamiento crediticio a centrales de riesgo. ✓ Cumplimiento de disposiciones legales contenidas en la Ley de Habeas Data y demás normas concordantes. ✓ Para seguimiento y control dentro del desarrollo de contrato de mutuo de dinero y otras relaciones que surjan entre el deudor y la Institución entre otras necesidades. ✓ Para ofrecimiento de servicios de la Institución, entre otros.
Centro de atención universitaria.	✓ Para la orientación de todas las personas que requieran apoyo dentro de la Institución. ✓ Para ofrecimiento de servicios de la Institución, entre otras

	actividades.
Comunicaciones.	✓ Para enviar comunicados a la Comunidad Universitaria y medios de comunicación. ✓ Para ofrecimiento de servicios de la Institución, entre otras actividades.

9. Derechos de los Titulares

De acuerdo con el artículo 8 de la LEPD y a los artículos 21 y 22 del Decreto 1377 de 2013, los Titulares de los datos pueden ejercer una serie de derechos en relación al tratamiento de sus datos personales. Estos derechos podrán ejercerse por las siguientes personas.

1. Por el Titular, quién deberá acreditar su identidad en forma suficiente por los distintos medios que le ponga a disposición el responsable.
2. Por sus causahabientes, quienes deberán acreditar tal calidad.
3. Por el representante y/o apoderado del Titular, previa acreditación de la representación o apoderamiento.
4. Por estipulación a favor de otro y para otro.

Los derechos de los niños, niñas o adolescentes se ejercerán por las personas que estén facultadas para representarlos.

Los derechos del Titular son los siguientes:

- **Derecho de acceso o consulta:** Se trata del derecho del Titular a ser informado por el responsable del tratamiento, previa solicitud, respecto al origen, uso y finalidad que le han dado a sus datos personales.
- **Derechos de quejas y reclamos**. La Ley distingue cuatro tipos de reclamos:
  - **Reclamo de corrección:** el derecho del Titular a que se actualicen, rectifiquen o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
  - **Reclamo de supresión:** el derecho del Titular a que se supriman los datos que resulten inadecuados, excesivos o que no respeten los principios, derechos y garantías constitucionales y legales.
  - **Reclamo de revocación:** el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.
  - **Reclamo de infracción:** el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.
- **Derecho a 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 LEPD.
- **Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones:** el Titular o causahabiente solo podrá elevar esta queja una vez

haya agotado el trámite de consulta o reclamo ante el responsable del tratamiento o encargado del tratamiento.

10. Atención a los Titulares de datos

Fernando Laverde Morales con C. C. No. 94. 260. 476 de Bogotá como representante legal de la Fundación Universitaria del Área Andina o quien haga sus veces, será el encargado de la atención de peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos. Teléfono: 7 42 19 47. Correo electrónico: protecciondedatos@areandina.edu.co.

11. Procedimientos para ejercer los derechos del Titular

11.1. Derecho de acceso o consulta

Según el artículo 21 del Decreto 1377 de 2013, el Titular podrá consultar de forma gratuita sus datos personales en dos casos:

1. Al menos una vez cada mes calendario.
2. Cada vez que existan modificaciones sustanciales de las políticas de tratamiento de la información que motiven nuevas consultas.

Para consultas cuya periodicidad sea mayor a una por cada mes calendario, la Fundación Universitaria del Área Andina, solamente podrá cobrar al Titular los gastos de envío, reproducción y, en su caso, certificación de documentos. Los costos de reproducción no podrán ser mayores a los costos de recuperación del material correspondiente. Para tal efecto, el responsable deberá demostrar a la Superintendencia de Industria y Comercio, cuando ésta así lo requiera, el soporte de dichos gastos.

El Titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a La Fundación Universitaria del Área Andina, enviado, mediante correo electrónico a protecciondedatos@areandina.edu.co, indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a Calle 71 # 13 - 21- Bogotá DC. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Petición en que se concreta la solicitud de acceso o consulta.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada, cuando corresponda.

El Titular podrá elegir una de las siguientes formas de consulta de la base de datos para recibir la información solicitada:

- Visualización en pantalla.

- Por escrito, con copia o fotocopia remitida por correo certificado o no.
- Telecopia.
- Correo electrónico u otro medio electrónico.
- Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por la Fundación Universitaria del Área Andina.

Una vez recibida la solicitud, la Fundación Universitaria del Área Andina, resolverá la petición de consulta en un plazo máximo de diez (10) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento del primer término. Estos plazos están fijados en el artículo 14 de la LEPD.

Una vez agotado el trámite de consulta, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

11.2. Derechos de quejas y reclamos

El Titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido a la Fundación Universitaria del Área Andina, enviado, mediante correo electrónico a protecciondedatos@areandina.edu.co, indicando en el Asunto "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a Calle 71 # 13 - 21- Bogotá DC. La solicitud deberá contener los siguientes datos:

- Nombre y apellidos del Titular.
- Fotocopia de la Cédula de Ciudadanía del Titular y, en su caso, de la persona que lo representa, así como del documento acreditativo de tal representación.
- Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o inflación.
- Dirección para notificaciones, fecha y firma del solicitante.
- Documentos acreditativos de la petición formulada que se quieran hacer valer, cuando corresponda.

Si el reclamo resulta incompleto, se requerirá al interesado dentro de los cinco (5) días siguientes a la recepción del reclamo para que subsane las fallas. Transcurridos dos (2) meses desde la fecha del requerimiento, sin que el solicitante presente la información requerida, se entenderá que ha desistido del reclamo.

Una vez recibido el reclamo completo, se incluirá en la base de datos una leyenda que diga "reclamo en trámite" y el motivo del mismo, en un término no mayor a dos (2) días hábiles. Dicha leyenda deberá mantenerse hasta que el reclamo sea decidido.

La Fundación Universitaria del Área Andina, resolverá la petición de consulta en un plazo máximo de quince (15) días hábiles contados a partir de la fecha de recibo de la misma. Cuando no fuere posible atender al reclamo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Una vez agotado el trámite de reclamo, el Titular o causahabiente podrá elevar queja ante la Superintendencia de Industria y Comercio.

12. Medidas de seguridad

La Fundación Universitaria del Área Andina, con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la LEPD, ha implementado medidas técnicas, humanas y administrativas necesarias para garantizar la seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Por otra parte, La Fundación Universitaria del Área Andina, mediante la suscripción de los correspondientes contratos de transmisión, ha requerido a los encargados del tratamiento con los que trabaje la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales.

A continuación se exponen las medidas de seguridad implantadas por La Fundación Universitaria del Área Andina, que están recogidas y desarrolladas en su Manual Interno de Seguridad.

Tabla II. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) y bases de datos (automatizadas, no automatizadas)

Gestión de documentos y soportes	Control de acceso	Incidencias	Personal	Manual Interno de Seguridad
1. Medidas que eviten el acceso indebido o la recuperación de los datos que han sido descartados, borrados o destruidos. 2. Acceso restringido al lugar donde se almacenan los datos. 3. Autorización del responsable para la salida de documentos o	1. Acceso de usuarios limitado a los datos necesarios para el desarrollo de sus funciones. 2. Lista actualizada de usuarios y accesos autorizados. 3. Mecanismos para evitar el acceso a datos con derechos	1. Registro de incidencias: tipo de incidencia, momento en que se ha producido, emisor de la notificación, receptor de la notificación, efectos y medidas correctoras. 2. Procedimiento	1. Definición de las funciones y obligaciones de los usuarios con acceso a los datos 2. Definición de las funciones de control y autorizaciones delegadas por el responsable del tratamiento. 3. Divulgación entre	1. Elaboración e implementación del Manual de obligado cumplimiento para el personal. 2. Contenido mínimo: ámbito de aplicación, medidas y procedimientos de seguridad, funciones y obligaciones del personal, descripción de las bases de datos, procedimiento ante incidencias, procedimiento de copias y recuperación de

soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes.	distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado	de notificación y gestión de incidencias.	el personal de las normas y de las consecuencias del incumplimiento de las mismas	datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

Tabla III. Medidas de seguridad comunes para todo tipo de datos (públicos, semiprivados, privados, sensibles) según el tipo de bases de datos

Bases de datos no automatizadas			Bases de datos automatizadas	
Archivo	**Almacenamiento de documentos**	**Custodia de documentos**	**Identificación y autenticación**	**Telecomunicaciones**
1. Archivo de documentación siguiendo procedimientos que garanticen una correcta conservación, localización y consulta y ejercicio de los derechos de los Titulares.	1. Dispositivos de almacenamiento con mecanismos que impidan el acceso a personas no autorizadas.	1. Deber de diligencia y custodia de la persona a cargo de documentos durante la revisión o tramitación de los mismos.	1. Identificación personalizada de usuarios para acceder a los sistemas de información y verificación de su autorización. 2. Mecanismos de identificación y autenticación; Contraseñas: asignación, caducidad y almacenamiento cifrado.	1. Acceso a datos mediante redes seguras.

Tabla IV. Medidas de seguridad para datos privados según el tipo de bases de datos

Bases de datos automatizadas y no automatizadas			Bases de datos automatizadas			
Auditoría	**Responsable de seguridad**	**Manual Interno de Seguridad**	**Gestión de documentos y soportes**	**Control de acceso**	**Identificación y autenticación**	**Incidencias**
1. Auditoría ordinaria (interna o externa) cada dos meses. 2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de	1. Designación de uno o varios responsable de seguridad. 2. Designación de uno o varios encargados	1. Controles periódicos de cumplimiento	1. Registro de entrada y salida de documentos y soportes: fecha, emisor y receptor, número, tipo de información, forma de	1. Control de acceso al lugar o lugares donde se ubican los sistemas de información.	1. Mecanismo que limite el número de intentos reiterados de acceso no autorizados.	1. Registro de los procedimientos de recuperación de los datos, persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable

información. 3. Informe de detección de deficiencias y propuesta de correcciones. 4. Análisis y conclusiones del responsable de seguridad y del responsable del tratamiento. 5. Conservación del Informe a disposición de la autoridad.	del control y la coordinación de las medidas del Manual Interno de Seguridad. 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.		envío, responsable de la recepción o entrega.			del tratamiento para la ejecución de los procedimientos de recuperación.

Tabla V. Medidas de seguridad para datos sensibles según el tipo de bases de datos

Bases de datos no automatizadas				**Bases de datos automatizadas**		
Control de acceso	**Almacenamiento de documentos**	**Copia o reproducción**	**Traslado de documentación**	**Gestión de documentos y soportes**	**Control de acceso**	**Telecomunicaciones**
1. Acceso solo para personal autorizado. 2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados.	1. Archivadores, armarios u otros ubicados en áreas de acceso protegidas con llaves u otras medidas.	1. Solo por usuarios autorizados. 2. Destrucción que impida el acceso o recuperación de los datos.	1. Medidas que impidan el acceso o manipulación de documentos.	1. Sistema de etiquetado o confidencial. 2. Cifrado de datos. 3. Cifrado de dispositivos portátiles cuando salgan fuera.	1. Registro de accesos: usuario, hora, base de datos a la que accede, tipo de acceso, registro al que accede. 2. Control del registro de accesos por el responsable de seguridad.	1. Transmisión de datos mediante redes electrónicas cifradas.

					Informe mensual. 3. Conservación de los datos: 2 años.	

13. Transferencia de datos a otros países

De acuerdo con el Título VIII de la LEPD, se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos. Se entiende que un país ofrece un nivel adecuado de protección de datos cuando cumpla con los estándares fijados por la Superintendencia de Industria y Comercio sobre la materia, los cuales en ningún caso podrán ser inferiores a los que la presente ley exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

- Información respecto de la cual el Titular haya otorgado su autorización expresa e inequívoca para la transferencia.
- Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del Titular por razones de salud o higiene pública.
- Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
- Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
- Transferencias necesarias para la ejecución de un contrato entre el Titular y el responsable del tratamiento, o para la ejecución de medidas precontractuales siempre y cuando se cuente con la autorización del Titular.
- Transferencias legalmente exigidas para la salvaguardia del interés público, o para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

En los casos no contemplados como excepción, corresponderá a la Superintendencia de Industria y Comercio proferir la declaración de conformidad relativa a la transferencia internacional de datos personales. El Superintendente está facultado para requerir información y adelantar las diligencias tendentes a establecer el cumplimiento de los presupuestos que requiere la viabilidad de la operación.

Las transmisiones internacionales de datos personales que se efectúen entre un responsable y un encargado para permitir que el encargado realice el tratamiento por cuenta del responsable, no requerirán ser informadas al Titular ni contar con su consentimiento, siempre que exista un contrato de transmisión de datos personales.

14. Datos de navegación

El sistema de navegación y el software necesario para el funcionamiento de la página web de la Fundación Universitaria del Área Andina recogen algunos datos personales, cuya transmisión se haya implícita en el uso los protocolos de comunicación de Internet.

Por su propia naturaleza, la información recogida podría permitir la identificación de usuarios a través de su asociación con datos de terceros aunque no se obtenga para ese fin. En esta categoría de datos se encuentran, la dirección IP o el nombre de dominio del equipo utilizado por el usuario para acceder a la página web, la dirección URL, la fecha y hora y otros parámetros relativos al sistema operativo del usuario.

Estos datos se utilizan con la finalidad exclusiva de obtener información estadística anónima sobre el uso de la página web o controlar su correcto funcionamiento técnico, y se cancelan inmediatamente después de ser verificados.

15. Cookies o web bugs

Este sitio web no utiliza cookies o web bugs para recabar datos personales del usuario, sino que su utilización se limita a facilitar al usuario el acceso a la página web. El uso de cookies de sesión, no memorizadas de forma permanente en el equipo del usuario y que desaparecen cuando cierra el navegador, únicamente se limitan a recoger información técnica para identificar la sesión con la finalidad de facilitar el acceso seguro y eficiente de la página web. Si no desea permitir el uso de cookies puede rechazarlas o eliminar las ya existentes configurando su navegador, e inhabilitando el código Java Script del navegador en la configuración de seguridad.

16. Vigencia

Las bases de datos responsabilidad de la Fundación Universitaria del Área Andina, serán objeto de tratamiento durante el tiempo que sea razonable y necesario para la finalidad para la cual son recabados los datos. Una vez cumplida la finalidad o finalidades del tratamiento, y sin perjuicio de normas legales que dispongan lo contrario. La Fundación Universitaria del Área Andina, procederá a la supresión de los datos personales en su posesión salvo que exista una obligación legal o contractual que requiera su conservación. Por todo ello, dicha base de datos ha sido creada sin un periodo de vigencia definido.

La presente política de tratamiento permanece vigente desde 26 de abril de 2016.

Anexo I
SOLICITUDES DE ACCESO Y RECLAMOS POR LOS TITULARES

Tabla I. Registro de solicitudes de acceso y de reclamos por parte de los Titulares

Identificación del usuario	
Nombre y apellidos del usuario	
Departamento	
Identificación del solicitante	
Tipo de procedimiento	
Fecha	
Tipo de solicitud	
Nombre y apellidos del solicitante	
C.C./NIT	
Dirección postal	
Municipalidad	
Observaciones	

Anexo II
REGISTRO DE INCIDENCIAS

Tabla II. Modelo de registro de incidencias

Fecha y hora	
Tipo de incidencia	
Descripción	
Efectos	
Medidas correctoras	
Emisor de la notificación	
Receptor de la notificación	
Persona que ejecuta el proceso de recuperación	
Datos restaurados	
Datos grabados manualmente	

Artículo Segundo.- Ordenar la implementación de la política aprobada, para lo cual se expedirán los manuales y procedimientos a los que hubiere lugar para garantizar su correcta aplicación.

Artículo Tercero.- Vigencia. El presente Acuerdo rige a partir de su expedición.

COMUNÍQUESE Y CUMPLASE

Dado en Bogotá D. C. a los veintiséis (26) días del mes de abril de dos mil dieciséis (2016).

AREANDINA
Fundación Universitaria del Área Andina
Rectoría

FERNANDO LAVERDE MORALES
Presidente

AREANDINA
Fundación Universitaria del Área Andina
Secretaría General

MARÍA ANGÉLICA CORTÉS MONTEJO
Secretaria General