CONSEJO DIRECTIVO

ACUERDO No. 100

(21 de diciembre de 2018)

POR MEDIO DEL CUAL SE APRUEBA Y EXPIDE LA POLITICA DE SEGURIDAD DE LA INFORMACION PERSONAL DE LA ESCUELA LATINOAMERICANA DE INGENIEROS, TECNÓLOGOS Y EMPRESARIOS - ELITE.

El Consejo Directivo de la Escuela Latinoamericana de Ingenieros, Tecnólogos y Empresarios - ELITE, en uso de sus atribuciones legales y estatutarias, y

CONSIDERANDO:

Que la Escuela Latinoamericana de Ingenieros, Tecnólogos y Empresarios – ELITE es una Institución de Educación Superior privada sin ánimo de lucro de utilidad común y con carácter académico de Institución Universitaria.

Que mediante Resolución Número 4787 del 8 de mayo de 2012, el Ministerio de Educación Nacional reconoció a la Escuela Latinoamericana de Ingenieros, Tecnólogos y Empresarios - ELITE, la correspondiente personería jurídica para poder ofrecer programas de educación superior.

Que la Constitución Política, en su Artículo 69, consagra la autonomía universitaria, permitiendo que las Instituciones de Educación Superior (IES) puedan darse sus directivas y regirse por sus propios estatutos, de acuerdo con la ley.

Que mediante la Ley 30 de 1992, el Congreso de la Republica, desarrollo el derecho constitucional de la autonomía universitaria, estableciendo los parámetros de la misma para las instituciones de educación superior.

Que el artículo 29 de la citada ley, establece que "La autonomía de las instituciones universitarias, o, escuelas tecnológicas y de las instituciones técnicas profesionales estará determinada por su campo de acción y de acuerdo con la presente Ley en los siguientes aspectos: a) Darse y modificar sus estatutos…"

Que de acuerdo con lo dispuesto en el numeral 3) del artículo 26 del Estatuto Orgánico de la Institución, es función del Consejo Directivo dirigir el desarrollo de las políticas académicas, administrativas y los objetivos de la Institución.

Que de conformidad con los artículos 15 y 20 de la Constitución Política, los cuales fueron desarrollados mediante la ley 1581 de 2012, *"Por la cual se dictan disposiciones generales para la Protección de Datos Personales"* y el Decreto 1377 de 2013, se estableció la obligación y el deber de los administradores de información de personas naturales de atender los preceptos asociados a la protección, manejo y suministro de la misma.

Que de acuerdo con lo anterior, cuando el titular de información personal presta su consentimiento para que estos formen parte de una base de datos de una organización u empresa, pública o privada, ésta se hace responsable del tratamiento de estos datos y adquiere una serie de obligaciones, como son la de tratar dichos datos con seguridad y cautela, velar por su integridad y aparecer como órgano a quien el titular puede dirigirse para el seguimiento de la información y el control de la misma, pudiendo ejercitar los derechos de consultas y reclamos.

Que si bien la responsabilidad del tratamiento de los datos recae en la Institución, sus competencias se materializan en las funciones que corresponden a su personal, por ende el personal de la organización u empresa responsable del tratamiento con acceso, directo o indirecto, a bases de datos que contienen datos personales debe conocer la normativa de protección de datos, la política de protección de datos institucional y los procesos o procedimiento derivados.

Que de conformidad con lo expuesto anteriormente, se estima conveniente aprobar y expedir la política de seguridad de la información personal de la Institución.

En mérito de lo expuesto,

ACUERDA

Artículo Primero: Aprobar y expedir la política de seguridad de la información personal de la Escuela Latinoamericana de Ingenieros, Tecnólogos y Empresarios - ELITE, la cual estará conformada por el siguiente articulado:

CAPITULO I
DEL MANEJO DE INFORMACIÓN PERSONAL.

ARTICULO 1. AMBITO DE APLICACIÓN: La presente política tiene como alcance permitir a todas las personas naturales que suministren información personal a la Institución conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los archivos o bases de datos institucionales en atención a las disposiciones constitucionales, legales y reglamentarias aplicables, en virtud de ello es aplicable a todos los colaboradores y dependencias de la Institución a nivel nacional sin distingo alguno en razón de cargo, denominación del mismo o funciones desarrolladas.

Adicionalmente, esta Política es aplicable a terceros que tengan relación como destinatarios de la información personal contenida en los archivos o bases de datos de la Institución, para ello se dispondrán los instrumentos jurídicos del caso, los cuales en todos los casos deberán atender a la normatividad vigente que le sea aplicable.

PARAGRAFO: Todos los usuarios de la información personal a la que refiere esta política están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los datos y están sujetos al deber de confidencialidad, incluso después de finalizada su relación laboral o

profesional con la Institución , esto incluye la obligación perentoria de suscribir acuerdo de confidencialidad conforme el artículo 4 literal h) de la Ley 1581 de 2012 o la norma que le derogue, modifique o adicione.

ARTICULO 2: DEFINICIONES: Para todos los efectos institucionales y en concordancia con las disposiciones del artículo 3 de la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 se tendrán como definiciones las siguientes:

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

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

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

d. **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.

e. **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial 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.

f. **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, para fines de esta Política la Institución y los colaboradores designados para el efecto.

g. **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, para el caso de esta política puede corresponder

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

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

j. **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.

k. **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.

l. **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.

ARTICULO 3: PRINCIPIOS RECTORES, REQUISTOS Y EXCEPCIONES: Para todos los efectos institucionales y en concordancia con las disposiciones del artículo 3 de la Ley 1581 de

2012 y su Decreto Reglamentario 1377 de 2013 se tendrán como principios de protección de datos los siguientes:

a. **Principio de legalidad:** El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la Constitución Política, la Ley 1581 de 2012, el Decreto 1377 de 2013 y las demás disposiciones que la desarrollen, modifiquen o deroguen.

b. **Principio de finalidad:** El tratamiento debe obedecer a una finalidad legítima, la cual debe ser informada al Titular.

c. **Principio de libertad (excepciones):** 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:

   1. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

   2. Datos de naturaleza pública.

   3. Casos de urgencia médica o sanitaria.

   4. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

   5. Datos relacionados con el Registro Civil de las personas.

d. **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.

e. **Principio de transparencia (requisitos de consentimiento):** 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:

1. El tratamiento al cual será sometidos sus datos y la finalidad del mismo.

2. 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.

3. Los derechos que le asisten como Titular.

4 La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

m. **Principio de acceso y circulación restringida**: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, por ello, 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.

n. **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.

o. **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 los términos legales, reglamentarias o institucionales predicables.

ARTÍCULO 4: CATEGORIAS ESPECIALES DE DATOS: Teniendo la especial condición de la Institución, la multiplicidad de bases de datos y archivos de la misma, así como la sensibilidad de gran parte de la información materia de tratamiento, se establecen las siguientes categorías especiales de datos:

a. 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.

Es excepción para el tratamiento de datos sensibles la configuración de una de las siguientes circunstancias:

1. 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.

2. Cuando 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.

3. Cuando el tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de una 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.

4. Cuando el tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

5. Cuando 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.

b. Datos de 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:

1. Que responda y respete el interés superior de los niños, niñas y adolescentes.
2. 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.

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 en la ley, las normas reglamentarias y esta Política. En todo caso, 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 adolescentes se ejercerán por las personas que estén facultadas para representarlos.

ARTÍCULO 5: DISPOSICIONES INSTITUCIONALES: Para efectos de dar claridad respecto de las funciones y obligaciones de los responsables de tratamiento, de seguridad o usuarios respecto con los archivos y bases de datos donde se consigna información personal, y de cara a dicha información se establece lo siguiente:

A. RESPONSABLES DE TRATAMIENTO: Contarán con las siguientes obligaciones:

1. Coordinar e implementar las medidas de seguridad contenidas en la normatividad institucional.

2. Difundir la normatividad asociada a protección de datos ante el personal afectado.

3. Procurar la actualización de la normatividad siempre que se produzcan cambios relevantes en los sistemas de información institucionales, el sistema de tratamiento, 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.

4. Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos, esto desde la consideración institucional entendida como persona jurídica.

5. Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.

6. Autorizar 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 cuando a ello hubiera lugar.

7. Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.

8. Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.

9. Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas, al menos cada tres meses.

10. 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.

11. Delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.

B. **RESPONSABLES DE SEGURIDAD:** Contarán con las siguientes obligaciones: La Institución designa al secretario General de la Institución o quien hiciere sus veces (a la fecha de expedición de este acuerdo Dr. Alvaro Leandro Barreto Sandoval) como responsable de seguridad de las bases de datos de carácter sensibles como para las bases de datos Automatizadas y no Automatizadas, este responsable de seguridad tiene las siguientes funciones:

1. Coordinar y controlar la implementación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión de la normatividad existente en materia de información personal.

2. 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.

3. Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados.

4. 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.

5. 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 de procedimientos y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.

6. Definir el proyecto de auditoría, interna o externa, al menos cada dos años.

7. Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento.

8. Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales

C. 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 Institución deben actuar de conformidad a las funciones y obligaciones recogidas en el presente apartado.

1. Suscribir el acuerdo de confidencialidad institucional al igual que los formatos que la Institución disponga.

2. Guardar el deber de secreto y confidencialidad respecto de sistemas de información, bases de datos y las informaciones en ella contenidos. Este deber 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.

3. Cuando se traten documentos o soportes que contienen datos personales custodiar los mismos, así como de vigilar y controlar que personas no autorizadas no puedan tener acceso a ellos.

ARTÍCULO 6: FUNCIONES DE CONTROL Y AUTOIRIZACIONES DELEGADAS: Son funciones de control y autorizaciones delegadas asociadas a las medidas de seguridad las siguientes:

1. Acceder a las bases de datos con la solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.

2. No revelar información a terceras personas ni a usuarios no autorizados.

3. Observar las normas de seguridad y trabajar para mejorarlas.

4. No realizar acciones que supongan un peligro para la seguridad de la información.

5. No sacar información de las instalaciones de la organización sin la debida autorización.

6. Usar los recursos y materiales de trabajo en razón 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.

7. Usar impresoras, escáneres u otros dispositivos de copia procediendo a la recogida inmediata de las copias, evitando dejar éstas en las bandejas de los mismos.

8. Notificar las incidencias presentadas, esto quiere decir que 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 pérdida 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 entre otros eventos.

9. Custodiar los soportes utilizados, esto **o**bliga 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.

10. Usar de manera responsable su propia 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

11. Tener presente que el envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades.

12. Salvaguarda y proteger las contraseñas proporcionadas a los usuarios teniéndose de presente que 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.

13. Realizar copia de seguridad de toda la información de bases de datos personales.

14. Gestionar los archivos físicos garantizando que los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad aplicables.

CAPITULO II.
DISPOSICIONES ASOCIADAS A LA SEGURIDAD DE LA INFORMACIÓN.

ARTÍCULO 7: ALCANCE: Esta capitulo recoge las medidas técnicas, humanas y administrativas necesarias para otorgar seguridad a los registros de personas naturales con el fin de impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento, de acuerdo con el principio de seguridad recogido en la normatividad que regula esta materia.

En virtud de lo anterior, este capítulo aplica a las bases de datos objeto de responsabilidad de la Institución así como a los sistemas de información, soportes y equipos empleados en el tratamiento de los datos, que deban ser protegidos de acuerdo con la normativa aplicable, a las personas que participan en el tratamiento y a las infraestructuras donde se ubican dichas bases de datos.

ARTÍCULO 8: DEFINICIONES: Para todos los efectos institucionales y en concordancia con las disposiciones de la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2.013 se tendrán como definiciones las siguientes:

a. **Acceso autorizado:** Autorización concedida a un usuario para el uso de determinados recursos en dispositivos automatizados, es el resultado de una autentificación correcta, generalmente mediante el ingreso de usuario y contraseña.

b. **Autenticación:** Procedimiento de verificación de la identidad de un usuario.

c. **Contraseña:** Seña secreta que permite el acceso a dispositivos, información o bases de datos antes inaccesibles. Se utiliza en la autentificación de usuarios que permite el acceso autorizado.

d. **Control de acceso:** Mecanismo que permite acceder a dispositivos, información o bases de datos mediante la autentificación.

e. **Copia de respaldo:** Copia de los datos de una base de datos en un soporte que permita su recuperación.

f. **Identificación:** Proceso de reconocimiento de la identidad de los usuarios.

g. **Incidencia:** Cualquier anomalía que afecte o pueda afectar a la seguridad de los datos, constituyendo un riesgo para la confidencialidad, disponibilidad o integridad de las bases de datos o de los datos personales que contienen.

h. **Perfil de usuario:** Grupo de usuarios a los que se da acceso.

i. **Recurso protegido:** Cualquier componente del sistema de información, como bases de datos, programas, soportes o equipos, empleados para el almacenamiento y tratamiento de datos personales.

j. **Responsable de seguridad**: Una o varias personas designadas por el responsable del tratamiento para el control y la coordinación de las medidas de seguridad.

k. **Sistema de información:** Conjunto de bases de datos, programas, soportes y/o equipos empleados para el tratamiento de datos personales.

l. **Soporte:** Material en cuya superficie se registra información o sobre el cual se pueden guardar o recuperar datos, como por ejemplo papel, cinta de video, CD, DVD, disco duro u otros.

m. **Usuario:** Sujeto autorizado para acceder a los datos o recursos, o proceso que accede a los datos o recursos sin identificación de un sujeto.

ARTICULO 9: ACTUALIZACIÓN: Este capítulo debe ser sometido a actualización siempre que se produzcan cambios en los sistemas de información, el sistema de tratamiento, la organización o el contenido de la información de las bases de datos, que puedan afectar a las medidas de seguridad implementadas por la Institución. Así mismo, el manual debe adaptarse en todo momento a la normativa legal en materia de seguridad de datos personales.

ARTICULO 10: MEDIDAS DE SEGURIDAD: Las bases de datos institucionales son accesibles únicamente por las personas designadas por la Institución, los responsables de seguridad señalados en esta norma, se encargarán de gestionar los permisos de acceso a los usuarios, el procedimiento de asignación y distribución que garantiza la confidencialidad, integridad y almacenamiento de las contraseñas, durante su vigencia, así como la periodicidad con la que se cambian.

A continuación, se enumeran y detallan las medidas de seguridad implementadas por la Institución:

1. MEDIDAS DE SEGURIDAD COMUNES:

1.1. Gestión de documentos y soportes

Los documentos y soportes en los que se encuentran las bases de datos se determinan en el inventario de documentos y soportes.

Los encargados de vigilar y controlar que personas no autorizadas no puedan acceder a los documentos y soportes con datos personales son los usuarios autorizados para acceder a estos. Los usuarios autorizados estarán referidos en el presente Capítulo.

Los documentos y soportes deben clasificar los datos según el tipo de información que contienen, ser inventariados y ser accesibles solo por el personal autorizado, salvo que las características de los mismos hagan imposible la identificación referida, en cuyo caso se dejará constancia motivada en el registro de entrada y de salida de documentos.

La identificación de los documentos y soportes que contengan datos personales sensibles debe realizarse utilizando sistemas de etiquetado comprensibles y con significado que permita a los usuarios autorizados identificar su contenido y que dificulten la identificación para el resto de personas.

La salida de documentos y soportes que contengan datos personales fuera de las infraestructuras que están bajo el control del responsable del tratamiento debe ser autorizada por este último. Este precepto también es aplicable a los documentos o soportes anexados y enviados por correo electrónico.

1.2. Control de acceso

El personal de la Institución solamente debe acceder a aquellos datos y recursos necesarios para el desarrollo de sus funciones y sobre los cuales se encuentren autorizados por el responsable del tratamiento.

La Institución se ocupará del almacenamiento de una lista actualizada de usuarios, perfiles de usuarios, y de los accesos autorizados para cada uno de ellos. Además, contará con mecanismos para evitar el acceso a datos con derechos distintos de los autorizados. En el caso de soportes informáticos, puede consistir en la asignación de contraseñas, y en el caso de documentos, en la entrega de llaves o mecanismos de apertura de dispositivos de almacenamiento donde se archive la documentación.

La modificación sobre algún dato o información, así como la concesión, alteración, inclusión o anulación de los accesos autorizados y de los usuarios recogidos en la lista actualizada mencionada en el párrafo anterior, corresponde de manera exclusiva al personal autorizado, cualquier personal ajeno a la Institución que, de forma autorizada y legal, tenga acceso a los recursos protegidos, estará sometido a las mismas condiciones y tendrá las mismas obligaciones de seguridad que el personal propio.

1.3. Ejecución del tratamiento fuera de las infraestructuras

El almacenamiento de datos personales del responsable del tratamiento o encargado del tratamiento en dispositivos portátiles y su tratamiento fuera de las infraestructuras institucionales,

requiere una autorización previa por parte de la Institución y el cumplimiento de las garantías de seguridad correspondientes al tratamiento de este tipo de datos.

1.4. Bases de datos temporales, copias y reproducciones

Las bases de datos temporales o copias de documentos creadas para trabajos temporales o auxiliares deben cumplir con el mismo nivel de seguridad que corresponde a las bases de datos o documentos originales. Una vez que dejan de ser necesarias, estas bases de datos temporales o copias serán borradas o destruidas, impidiéndose así el acceso o recuperación de la información que contienen.

Solamente el personal autorizado puede realizar copias o reproducir los documentos.

1.5. Responsable de seguridad

La Institución designará a un responsable de seguridad encargado de coordinar y controlar las medidas de seguridad contenidas en el presente manual. El mismo responsable de la seguridad será el encargado de las bases de datos sensibles y de la seguridad de las bases de datos no automatizadas.

De acuerdo con la normativa sobre protección de datos, la designación de los responsables de seguridad no exonera de responsabilidad al responsable del tratamiento o encargado del tratamiento.

1.6. Auditorías

Las bases de datos que contengan datos personales, objeto de tratamiento por parte de la Institución clasificadas con nivel de seguridad sensible o privado, se han de someter, al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento de las medidas de seguridad contenidas en este manual.

Serán objeto de auditoría tanto los sistemas de información como las instalaciones de almacenamiento y tratamiento de datos.

La Institución realizará una auditoría extraordinaria, siempre que se realicen modificaciones sustanciales en el sistema de información que puedan afectar al cumplimiento de las medidas de seguridad, con el fin de verificar la adaptación, adecuación y eficacia de las mismas.

Las auditorías concluirán con un informe de auditoría, que contendrá:

a. El dictamen sobre la adecuación de las medidas y controles a la normativa sobre protección de datos.
b. La identificación de las deficiencias halladas y la sugerencia de medidas correctoras o complementarias necesarias.
c. La descripción de los datos, hechos y observaciones en que se basen los dictámenes y las recomendaciones propuestas.

El responsable de seguridad**,** estudiará el informe e implementará las medidas correctoras a lugar. Los informes de auditoría serán adjuntados a los registros pertinentes y quedarán a disposición de la autoridad de control.

2. Medidas de seguridad para bases de datos no automatizadas

2.1. Archivo de documentos

La Institución fijará los criterios y procedimientos de actuación que se deben utilizar para el archivo de documentos que contengan datos personales conforme a la Ley. Los criterios de archivo garantizarán la conservación, localización y consulta de los documentos y harán posible los derechos de consulta y reclamo de los Titulares.

El archivo considerará entre otros, criterios como el grado de utilización de los usuarios con acceso autorizado a los mismos, la actualidad de su gestión y/o tratamiento y la diferenciación entre bases de datos históricas y de administración o gestión de la empresa.

Los dispositivos de almacenamiento de documentos deben disponer de llaves u otros mecanismos que dificulte su apertura, excepto cuando las características físicas de éstos lo impidan, en cuyo caso se adoptarán las medidas necesarias para impedir el acceso de personas no autorizadas.

Cuando los documentos que contienen datos personales se encuentren en proceso de revisión o tramitación y, por tanto, fuera de los dispositivos de almacenamiento, ya sea antes o después de su archivo, la persona que se encuentre a cargo de los mismos debe custodiarlos e impedir en todo caso que personas no autorizadas puedan acceder a ellos.

Los dispositivos de almacenamiento que contengan documentos con datos personales clasificados con nivel de seguridad sensible deben encontrarse en áreas o locales en las que el acceso esté protegido con puertas de acceso con sistemas de apertura de llave u otros mecanismos similares. Estas áreas deben permanecer cerradas cuando no se precise el acceso a dichos documentos. Si no fuera posible cumplir con lo anterior, se podrán adoptar medidas alternativas debidamente motivadas que se incluirán en el presente manual.

2.2. Acceso a los documentos

El acceso a los documentos ha de realizarse exclusivamente por el personal autorizado en el numeral siguiendo los mecanismos y procedimientos definidos. Estos últimos deben identificar y conservar los accesos realizados a la documentación clasificada con nivel de seguridad sensible, tanto por usuarios autorizados como por personas no autorizadas tal y como se refleja en el numeral referido anteriormente.

El procedimiento de acceso a los documentos que contienen datos clasificados como sensibles implica el registro de accesos a la documentación, la identidad de quien accede, el momento en que se produce el acceso y los documentos a los que se han accedido. El acceso a documentos con este tipo de datos se realiza por personal autorizado, si se realiza por personas no autorizadas deberá supervisarse por algún usuario autorizado o por el responsable de seguridad.

3. MEDIDAS DE SEGURIDAD PARA BASES DE DATOS AUTOMATIZADAS

3.1. Identificación y autenticación.

La Institución instalará un sistema de seguridad informática que permitirá identificar y autenticar de forma correcta a los usuarios de los sistemas de información, con el fin de garantizar que solo el personal autorizado pueda acceder a las bases de datos.

También ha de establecerse un mecanismo que permita la identificación personalizada e inequívoca de todo usuario que intente acceder al sistema de información y que verifique si está autorizado. La identificación debe realizarse mediante un sistema único para cada usuario que accede a la información teniendo en cuenta el nombre de usuario, la identificación de empleado, el nombre del departamento entre otros.

Cuando el sistema de autenticación esté basado en la introducción de contraseña, se ha de implantar un procedimiento de asignación, distribución y almacenamiento de contraseñas; para garantizar la integridad y confidencialidad de estas últimas, se recomienda que tengan un mínimo de ocho caracteres y contengan mayúsculas, minúsculas, números y letras.

Por otra parte, la Institución debe vigilar que las contraseñas se cambien de forma periódica, nunca por un tiempo superior a 365 días, igualmente se garantizará el almacenamiento automatizado, interno y cifrado, de las contraseñas mientras estén vigentes, y adoptará un mecanismo para limitar los intentos reiterados de accesos no autorizados.

3.2. Entrada y salida de documentos o soportes

La entrada de documentos o soportes debe registrarse indicando el tipo de documento o soporte, la fecha y hora, el emisor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable de la recepción. La salida o envío de documentos o soportes, debidamente autorizada, ha de registrarse indicando el tipo de documento o soporte, la fecha y hora, el receptor, el número de documentos o soportes incluidos en el envío, el tipo de información que contienen según el nivel de seguridad, la forma de envío y la persona responsable del envió. .

3.3. Control de acceso físico

Los lugares que sean sede de los sistemas de información que contienen datos personales deben estar debidamente protegidos con el fin de garantizar la integridad y confidencialidad de dichos datos; asimismo, han de cumplir con las medidas de seguridad físicas correspondientes.

La Institución tiene el deber de poner en conocimiento de su personal las obligaciones que les competen con el objetivo de proteger físicamente los documentos o soportes en los que se encuentran las bases de datos, no permitiendo su manejo, utilización o identificación por personas no autorizadas. Las infraestructuras donde se ubican las bases de datos se señalarán en los correspondientes formatos institucionales. Solamente el personal autorizado puede tener acceso a los lugares donde estén instalados los equipos que dan soporte a los sistemas de información, de acuerdo con lo dispuesto en numeral antes referido.

3.4. Copias de respaldo y recuperación de datos

La Institución llevará a cabo los procedimientos de actuación necesarios para realizar copias de respaldo, al menos una vez a la semana, excepto cuando no se haya producido ninguna

actualización de los datos durante ese periodo. Todas las bases de datos deben tener una copia de respaldo a partir de las cuales se puedan recuperar los datos.

De igual modo, ha establecido procedimientos para la recuperación de los datos con el objetivo de garantizar en todo momento la reconstrucción al estado en el que éstos se encontraban antes de su pérdida o destrucción. Cuando la pérdida o destrucción afecte a bases de datos parcialmente automatizadas se grabarán manualmente los datos dejando constancia de ello.

Igualmente la Institución se encargará de controlar el correcto funcionamiento y aplicación de los procedimientos de realización de copias de respaldo y recuperación de los datos cada 6 meses, adicionalmente se debe conservar una copia de respaldo de los datos y de los procedimientos de recuperación de los mismos en un lugar distinto a aquel en el que se encuentren los equipos donde se lleva a cabo su tratamiento. Este lugar deberá cumplir en todo caso las mismas medidas de seguridad exigidas para los datos originales.

3.5. Registro de acceso.

De los intentos de acceso a los sistemas de información la Institución conservará, como mínimo, la identificación del usuario, la fecha y hora en que se lleva a cabo, la base de datos a la que se accede, el tipo de acceso y si ese acceso ha sido autorizado o no autorizado. En caso de que el registro haya sido autorizado, se guarda la información que permita identificar el registro consultado.

La Institución por intermedio de su responsable de seguridad de las bases de datos automatizadas se encargará de controlar los mecanismos que permiten el registro de acceso, revisar con carácter mensual la información de control registrada y elaborar un informe de las revisiones realizadas y los problemas detectados. Además, debe impedir la manipulación o desactivación de los mecanismos que permiten el registro de acceso.

Los datos que contiene el registro de acceso deben conservarse, al menos, durante dos años.

No será necesario el registro de acceso cuando el responsable del tratamiento sea una persona natural y garantice que solamente él tiene acceso y trata los datos personales. Estas circunstancias deben hacerse constar expresamente.

3.6. Redes de comunicaciones

El acceso a datos personales a través de redes de comunicaciones, públicas o privadas, debe someterse a medidas de seguridad equivalentes al acceso local de datos personales.

La transmisión de datos personales mediante redes públicas o inalámbricas de comunicaciones electrónicas se tiene que llevar a cabo cifrando dichos datos, o utilizando otro mecanismo similar que garantice que la información no sea inteligible ni manipulada por terceras personas.

ARTÍCULO 11: FUNCIONES Y OBLIGACIONES: 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 Institución deben actuar de conformidad con las funciones y obligaciones recogidas en el presente documento.

La Institución debe informar a su personal de servicio sobre las medidas y normas de seguridad que compete al desarrollo de sus funciones, así como de las consecuencias de su incumplimiento, mediante cualquier medio de comunicación que garantice su recepción o difusión (correo electrónico, tablón de anuncios entre otros.) De igual modo, debe poner a disposición del personal el presente manual para que puedan conocer la normativa de seguridad de la empresa y sus obligaciones en esta materia en función del cargo que ocupan.

La Institución cumplirá con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscriben las personas responsables de manejo de información.

PARAGRAFO PRIMERO: Las funciones y obligaciones del personal de la Institución se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la organización y específicamente, por el contenido de esta norma. La lista de usuarios y perfiles con acceso a los recursos protegidos estarán recogidos en los formatos dispuestos para el efecto.

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 este acuerdo por parte del personal al servicio de la Institución es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y la Institución.

PARAGRAFO SEGUNDO: Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de la Institución son las siguientes:

a. **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 Institución 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.

b. **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 conforme las disposiciones institucionales que al respecto se expidieren.

c. **Obligaciones relacionadas con las medidas de seguridad implementadas:**

1. Acceder a las bases de datos solamente con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
2. No revelar información a terceras personas ni a usuarios no autorizados.
3. Observar las normas de seguridad y trabajar para mejorarlas.
4. No realizar acciones que supongan un peligro para la seguridad de la información.
5. No sacar información de las infraestructuras de la Institución sin la debida autorización.

d. **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 a los responsables de seguridad que podrán autorizarla y, en su caso, registrarla.

e. **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.

f. **Obligación de notificar incidencias:** Los usuarios tienen la obligación de notificar las incidencias de las que tenga conocimiento a los responsables de seguridad, quienes se encargarán 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 pérdida 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 entre otros.

g. **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.

h. **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.

i. **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 empresa.

j. **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.

k. **Copias de respaldo y recuperación de datos:** Debe realizarse copia de seguridad de toda la información de bases de datos personales de la Institución.

l. **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad establecidas.

6. Bases de datos y sistemas de información

Las bases de datos almacenadas y tratadas por la Institución se recogen en la siguiente tabla (Tabla I), donde se indica el nivel de seguridad y el sistema de tratamiento de cada una de ellas.

TABLA I. BASES DE DATOS Y NIVEL DE SEGURIDAD

BASE DE DATOS	NIVEL DE SEGURIDAD	SISTEMA DE TRATAMIENTO	FINALIDAD
ASPIRANTES O PROSPECTOS	SENSIBLE	FÍSICO	Seguimiento de prospectos de alumnos en cualquier metodología y con fines comerciales.
INSCRITOS	SENSIBLE	FÍSICO	Seguimiento de prospectos que han iniciado su solicitud de cupo en los programas de la Institución cualquiera sea su naturaleza
ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS	SENSIBLE	FÍSICO	Seguimiento de personal docente o administrativo de la Institución así como estudiantes que desempeñan movilidad internacional o son beneficiarios de relaciones convencionales dentro del marco de funciones sustantivas o adjetivas
SOFTWARE CONTABLE	PRIVADO	FÍSICO	Gestión de la información financiera de personas naturales o jurídicas con relacionamiento con la Institución sea en calidad de acreedores, deudores, contratistas, contratantes o cualquiera otra.
PROVEEDORES	SENSIBLE	FÍSICO	Gestión de la información de proveedores de bienes o servicios de la Institución
EMPRENDIMIENTO (ESTUDIANTES ACTIVOS, EGRESADOS Y EMPRESAS)	SENSIBLE	FÍSICO	Gestión de estudiantes, docentes y personas naturales o jurídicas asociadas a procesos de emprendimiento como parte o no de un proceso académico
BENEFICIARIOS DE PROYECTOS Y ACTIVIDADES DE	SENSIBLE	FÍSICO	Registro y gestión de información de personas naturales o personas jurídicas, por lo general sin ánimo de lucro que son beneficiarias o aliadas en

PROYECCION SOCIAL			procesos de intervención en comunidades.
EGRESADOS	PRIVADO	FÍSICO	Registro y gestión de personas naturales que han culminado su proceso académico en virtud de titulación.
EMPLEADOS	SENSIBLE	FÍSICO	Registro y gestión de información de personas naturales con relaciones contractuales debidamente legalizadas con la Institución .
ESTUDIANTES	PRIVADO	FÍSICO	Seguimiento, control y registro de estudiantes activos en todo su proceso formativo
HOJAS DE VIDA DE POSIBLES TRABAJADORES	PRIVADO	FÍSICO	Registro y uso de información de aspirantes a ingresar a la Institución en calidad de trabajadores
PRACTICAS (EMPRESAS)	PRIVADO	FÍSICO	Registro y gestión de información de estudiantes en unidades de negocio que permiten culminar sus procesos de formación en instancias prácticas
ACCIDENTALIDAD ENFERMEDADES Y AUSENTISMOS	PRIVADO	FÍSICO	Registro y uso de información asociada a la condición médica de los trabajadores de la Institución
CONTRATOS Y/O CONVENIOS PÚBLICOS Y/O PRIVADOS	SENSIBLE	FÍSICO	Registro de información asociada a las etapas pre, post y contractuales de los contratos o convenios suscritos por la Institución
ASEGURADORAS Y ASISTENCIAS	SENSIBLES	FÍSICO	Registro y gestión de información de personas naturales cubiertas por los seguros institucionales cualquiera sea su calidad o sus condiciones especiales
PROCESOS JURIDICOS	SENSIBLES	FÍSICO	Registro y gestión de la información asociada a la defensa judicial o extrajudicial de la Institución sea en instancias jurisdiccionales o en instancias de policial administrativa o cualquiera otra
BASE DE DATOS	**NIVEL DE SEGURIDAD**	**SISTEMA DE TRATAMIENTO**	**FINALIDAD**
ASPIRANTES O PROSPECTOS	SENSIBLE	AUTOMATIZADO	Seguimiento de prospectos de alumnos en cualquier metodología y con fines comerciales.

INSCRITOS	SENSIBLE	AUTOMATIZADO	Seguimiento de prospectos que han iniciado su solicitud de cupo en los programas de la Institución cualquiera sea su naturaleza
ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS	SENSIBLE	AUTOMATIZADO	Seguimiento de personal docente o administrativo de la Institución así como estudiantes que desempeñan movilidad internacional o son beneficiarios de relaciones convencionales dentro del marco de funciones sustantivas o adjetivas
SOFTWARE CONTABLE	PRIVADO	AUTOMATIZADO	Gestión de la información financiera de personas naturales o jurídicas con relacionamiento con la Institución sea en calidad de acreedores, deudores, contratistas, contratantes o cualquiera otra.
PROVEEDORES	SENSIBLE	AUTOMATIZADO	Gestión de la información de proveedores de bienes o servicios de la Institución
EMPRENDIMIENTO (ESTUDIANTES ACTIVOS, EGRESADOS Y EMPRESAS)	SENSIBLE	AUTOMATIZADO	Gestión de estudiantes, docentes y personas naturales o jurídicas asociadas a procesos de emprendimiento como parte o no de un proceso académico
BENEFICIARIOS DE PROYECTOS Y ACTIVIDADES DE PROYECCION SOCIAL	SENSIBLE	AUTOMATIZADO	Registro y gestión de información de personas naturales o personas jurídicas, por lo general sin ánimo de lucro que son beneficiarias o aliadas en procesos de intervención en comunidades.
EGRESADOS	PRIVADO	AUTOMATIZADO	Registro y gestión de personas naturales que han culminado su proceso académico en virtud de titulación.
EMPLEADOS	SENSIBLE	AUTOMATIZADO	Registro y gestión de información de personas naturales con relaciones contractuales debidamente legalizadas con la Institución .
ESTUDIANTES	PRIVADO	AUTOMATIZADO	Seguimiento, control y registro de estudiantes activos en todo su proceso formativo
HOJAS DE VIDA DE POSIBLES TRABAJADORES	PRIVADO	AUTOMATIZADO	Registro y uso de información de aspirantes a ingresar a la Institución en calidad de trabajadores
PRACTICAS (EMPRESAS)	PRIVADO	AUTOMATIZADO	Registro y gestión de información de estudiantes en unidades de negocio que permiten culminar

			sus procesos de formación en instancias prácticas
ACCIDENTALIDAD ENFERMEDADES Y AUSENTISMOS	PRIVADO	AUTOMATIZADO	Registro y uso de información asociada a la condición médica de los trabajadores de la Institución
CONTRATOS Y/O CONVENIOS PÚBLICOS Y/O PRIVADOS	SENSIBLE	AUTOMATIZADO	Registro de información asociada a las etapas pre, post y contractuales de los contratos o convenios suscritos por la Institución
ASEGURADORAS Y ASISTENCIAS	SENSIBLES	AUTOMATIZADO	Registro y gestión de información de personas naturales cubiertas por los seguros institucionales cualquiera sea su calidad o sus condiciones especiales
PROCESOS JURIDICOS	SENSIBLES	AUTOMATIZADO	Registro y gestión de la información asociada a la defensa judicial o extrajudicial de la Institución sea en instancias jurisdiccionales o en instancias de policial administrativa o cualquiera otra
ASPIRANTES O PROSPECTOS	SENSIBLE	AUTOMATIZADO	
INSCRITOS	SENSIBLE	AUTOMATIZADO	
ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS	SENSIBLE	AUTOMATIZADO	
SOFTWARE CONTABLE	PRIVADO	AUTOMATIZADO	
PROVEEDORES	SENSIBLE	AUTOMATIZADO	

TABLAS II. ESTRUCTURA DE LAS BASES DE DATOS SENSIBLES

	ASPIRANTES O PROSPECTOS, INSCRITOS, ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS, SOFTWARE CONTABLE, PROVEEDORES, EMPRENDIMIENTO (ESTUDIANTES ACTIVOS, EGRESADOS Y EMPRESAS,) BENEFICIARIOS DE PROYECTOS Y ACTIVIDADES DE PROYECCION SOCIAL, EGRESADOS, EMPLEADOS, ESTUDIANTES, HOJAS DE VIDA DE POSIBLES TRABAJADORES, PRACTICAS (EMPRESAS,) ACCIDENTALIDAD ENFERMEDADES Y AUSENTISMOS, CONTRATOS Y/O CONVENIOS PÚBLICOS Y/O PRIVADOS, ASEGURADORAS Y ASISTENCIAS y PROCESOS JURIDICOS.
Responsable del tratamiento	**ESCUELA LATINOAMERICANA DE INGENIEROS, TECNOLOGOS Y EMPRESARIOS - ELITE**, NIT 900534524 – 4, Dirección Calle 70 No. 10 A-39 de la ciudad de Bogotá D.C., Teléfono: (571) 552-1860, Correo electrónico: basesdedatos@elite.edu.co
Encargado de consultas y reclamos	**ALVARO LEANDRO BARRETO SANDOVAL**, 1049605806, Teléfono: (571) 552-1860, Correo electrónico: basesdedatos@elite.edu.co
Tipos de datos	**SENSIBLES**
Sistema de tratamiento	**AUTOMATIZADO Y FÍSICO**
Origen y procedencia de los datos	**Recogidos por el responsable y de bases de datos de terceros**

TABLAS III. ESTRUCTURA DE LAS BASES DE DATOS PRIVADOS

	ASPIRANTES O PROSPECTOS, INSCRITOS, ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS, SOFTWARE CONTABLE, PROVEEDORES, EMPRENDIMIENTO (ESTUDIANTES ACTIVOS, EGRESADOS Y EMPRESAS,) BENEFICIARIOS DE PROYECTOS Y ACTIVIDADES DE PROYECCION SOCIAL, EGRESADOS, EMPLEADOS, ESTUDIANTES, HOJAS DE VIDA DE POSIBLES TRABAJADORES, PRACTICAS (EMPRESAS,) ACCIDENTALIDAD ENFERMEDADES Y AUSENTISMOS, CONTRATOS Y/O CONVENIOS PÚBLICOS Y/O PRIVADOS, ASEGURADORAS Y ASISTENCIAS y PROCESOS JURIDICOS.
Responsable del tratamiento	**ESCUELA LATINOAMERICANA DE INGENIEROS, TECNOLOGOS Y EMPRESARIOS - ELITE,** NIT 900534524 – 4, Dirección Calle 70 No. 10 A-39 de la ciudad de Bogotá D.C., Teléfono: (571) 552-1860, Correo electrónico: basesdedatos@elite.edu.co
Encargado de consultas y reclamos	**ALVARO LEANDRO BARRETO SANDOVAL,** 1049605806, Teléfono: (571) 552-1860, Correo electrónico: basesdedatos@elite.edu.co
Tipos de datos	**PRIVADOS**

Sistema de tratamiento	**AUTOMATIZADO Y FÍSICO**
Origen y procedencia de los datos	**Recogidos por el responsable y de bases de datos de terceros**

TABLA IV. RESPONSABLES DE SEGURIDAD Y MEDIDAS DE SEGURIDAD DE LAS BASES DE DATOS

	ASPIRANTES O PROSPECTOS, INSCRITOS, ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS, SOFTWARE CONTABLE, PROVEEDORES, EMPRENDIMIENTO (ESTUDIANTES ACTIVOS, EGRESADOS Y EMPRESAS,) BENEFICIARIOS DE PROYECTOS Y ACTIVIDADES DE PROYECCION SOCIAL, EGRESADOS, EMPLEADOS, ESTUDIANTES, HOJAS DE VIDA DE POSIBLES TRABAJADORES, PRACTICAS (EMPRESAS,) ACCIDENTALIDAD ENFERMEDADES Y AUSENTISMOS, CONTRATOS Y/O CONVENIOS PÚBLICOS Y/O PRIVADOS, ASEGURADORAS Y ASISTENCIAS y PROCESOS JURIDICOS.
Responsables de seguridad	Responsable de seguridad designado por la Institución , esto es el administrador para datos sensibles, automatizados y no automatizados.
Control de acceso físico	**Datos sensibles:** Usuarios autorizados, Doble llave
Gestión documental	Archivo en carpetas AZ o cualquiera otra, almacenamiento en armarios, se realiza transporte de documentos conforme tablas de retención documental, destrucción de documentos mediante quema.
Control de acceso lógico	Usuario y contraseña, registro de entradas, cambio de contraseñas una vez al año, bloqueo de acceso tras tres intentos (esto conforme condiciones de la correspondiente plataforma)
Copias de respaldo y procedimiento	Copias de respaldo cada 30 días, procedimiento de recuperación

de recuperación	
Sistema de identificación y autenticación	Usuario y contraseña, contraseña: longitud mínima: nueve caracteres, números y letras; cambio de contraseña al menos una vez al año, tres intentos de entrada, almacenamiento cifrado.
Registro de acceso a los documentos	Usuarios autorizados

PARAGRAFO: Cuando exista contrato de transmisión de datos, los encargados del tratamiento deberán cumplir con las funciones y obligaciones relacionadas con las medidas en materia de seguridad recogidas en el presente acuerdo.

ARTÍCULO 12: PROCEDIMIENTO DE NOTIFICACIÓN, GESTIÓN Y RESPUESTA ANTE INCIDENCIAS: La Institución establece los lineamientos generales de procedimiento de notificación, gestión y respuesta de incidencias con el fin de garantizar la confidencialidad, disponibilidad e integridad de la información contenida en las bases de datos que están bajo su responsabilidad, este podrá ser desarrollado en los procedimientos institucionales conforme el mapa de procesos institucional.

Todos los usuarios y responsables de procedimientos, así como cualquier persona que tenga relación con el almacenamiento, tratamiento o consulta de las bases de datos recogidas en este documento, deben conocer el procedimiento para actuar en caso de incidencia.

El procedimiento de notificación, gestión y respuesta ante incidencias en su componente genérico es el siguiente:

1. Cuando una persona tenga conocimiento de una incidencia que afecte o pueda afectar la confidencialidad, disponibilidad e integridad de la información protegida de la empresa

deberá comunicarlo de manera inmediata, a los responsables de seguridad, describiendo detalladamente el tipo de incidencia producida, e indicando las personas que hayan podido tener relación con la incidencia, la fecha y hora en que se ha producido, la persona que notifica la incidencia, la persona a quién se le comunica y los efectos que ha producido.

2. Una vez comunicada la incidencia ha de solicitar al responsable de seguridad correspondiente un acuse de recibo en el que conste la notificación de la incidencia con todos los requisitos enumerados anteriormente.

La Institución creará un registro de incidencias que debe contener: el tipo de incidencia, fecha y hora de la misma, persona que la notifica, persona a la que se le comunica, efectos de la incidencia y medidas correctoras cuando corresponda. Este registro es gestionado por el responsable de seguridad de la base de datos.

Asimismo, debe implementar los procedimientos para la recuperación de los datos, indicando quien ejecuta el proceso, los datos restaurados y, en su caso, los datos que han requerido ser grabados manualmente en el proceso de recuperación.

ARTICULO 13: MEDIDAS PARA EL TRANSPORTE, DESTRUCCIÓN Y REUTILIZACIÓN DE DOCUMENTOS Y SOPORTES: Cuando corresponda desechar cualquier documento (original, copia o reproducción) o soporte que contenga datos personales debe procederse a su destrucción o borrado, a través de la implementación de medidas orientadas a evitar el acceso o recuperación de la información contenida en dicho documento o soporte.

Cuando se lleve a cabo el traslado físico de documentos o soportes deben adoptar las medidas necesarias para impedir el acceso indebido, la manipulación, la sustracción o la pérdida de la información. El traslado de soportes que contengan datos personales se realiza cifrando la información, o utilizando cualquier otro mecanismo que garantice que no se manipule ni se acceda a la misma.

Los datos contenidos en dispositivos portátiles deben estar cifrados cuando se hallen fuera de las infraestructuras que están bajo control de la Institución, cuando no sea posible el cifrado, se debe evitar el tratamiento de datos personales mediante este tipo de dispositivos; sin embargo, se podrá proceder al tratamiento cuando sea estrictamente necesario, adoptando para ello medidas de seguridad que tengan en cuenta los riesgos e incluyéndolas en el presente manual.

CAPITULO III.
DISPOSICIONES ASOCIADAS A PROTOCOLOS Y PROCEDIMIENTOS.

ARTÍCULO 14: BASE LEGAL Y ÁMBITO DE APLICACIÓN: El presente capítulo se desarrolla sobre las disposiciones 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 y del artículo 13 del Decreto 1377 de 2013 y las normas que le modifiquen, deroguen o adicionen, en razón de ello será aplicado a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento.

ARTÍCULO 15: DEFINICIONES: Para todos los efectos institucionales y en concordancia con las disposiciones de la Ley 1581 de 2.012 y su Decreto Reglamentario 1377 de 2.013 se tendrán como definiciones las siguientes:

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

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

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

d. **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.

e. **Datos sensibles:** Se entiende por datos sensibles aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar su discriminación, tales como aquellos que revelen el origen racial 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.

f. **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.

g. **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.

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

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

j. **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.

k. **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.

l. **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

ARTÍCULO 16: AUTORIZACIÓN DE LA POLÍTICA DE TRATAMIENTO: De acuerdo con las normas legales aplicables, para el tratamiento de datos personales se requiere la autorización previa e informada del titular, esto 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 Institución en los términos y condiciones recogidos en la misma.

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

a. Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.

b. Datos de naturaleza pública.

c. Casos de urgencia médica o sanitaria.

d. Tratamiento de información autorizado por la ley para fines históricos, estadísticos o científicos.

e. Datos relacionados con el Registro Civil de las personas.

f. A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.

g. Las que tengan por finalidad la seguridad y defensa nacional la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo.

h. Las que tengan como fin y contengan información de inteligencia y contrainteligencia.

i. Las que contengan información periodística y otros contenidos editoriales

j. Las bases de datos con información financiera, crediticia, comercial y de servicios, y de los censos de población y vivienda.

PARAGRAFO PRIMERO: TRATAMIENTO DE DATOS SENSIBLES: El responsable, podrá hacer uso y tratamiento de los datos considerados como sensibles cuando:

a. 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.

b. El Tratamiento sea necesario para salvaguardar el interés vital del titular y este se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.

c. El Tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.

d. El Tratamiento sea realizado en el trascurso de las actividades de obligatorio cumplimiento con base en los principios de legitimidad, legalidad, veracidad, confidencialidad, seguridad y con las debidas garantías por parte de terceros como; entidades prestadoras como escenarios para las prácticas académicas, entidades prestadoras de servicios de salud, cualquier otro organismo cuya finalidad requiera la autorización del titular siempre que se refieran exclusivamente al tratamiento autorizado y que mantenga contacto regularmente razón de su finalidad. En dichos escenarios, los datos no se podrán suministrar a terceros sin la autorización del titular
e. 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.

PARAGRAFO SEGUNDO: REQUISITOS ESPECIALES PARA EL TRATAMIENTO DE DATOS PERSONALES DE NIÑOS, NIÑAS Y ADOLESCENTES: Está prohibido el tratamiento de datos personales de niños, niñas y adolescentes, salvo aquellos datos de naturaleza pública, siempre y cuando dicho tratamiento cumpla con los siguientes parámetros y requisitos

1. Que responda y respete el superior de los niños, niñas y adolescentes.

2. 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 de su derecho a ser escuchado, opinión que será valorada teniendo en cuenta la madurez, autonomía y capacidad para entender el asunto.

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. Para este fin deberán aplicarse los principios y obligaciones establecidos en la Ley 1581 de 2012 y decretos reglamentarios.

PARAGRAFO TECERO: AUTORIZACIÓN DE LOS ADOLESCENTES PARA OBTENER INFORMACIÓN EN RELACIÓN CON SU EDUCACIÓN: Cuando se trate del tratamiento de datos de adolescentes es posible que la autorización previa sea otorgada directamente por el estudiante, en razón de ello, para el tratamiento de datos personales, es necesario tener en cuenta el principio de libertad, definido en el literal c) del artículo 4 de la Ley 1581 de 2012 así: "c) Principio de libertad: El Tratamiento sólo 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 releve el consentimiento.

Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento. Este principio, pilar fundamental de la administración de datos, permite al adolescente elegir voluntariamente si su información personal puede ser utilizada o no en bases de datos.

ARTÍCULO 17: TRATAMIENTO Y FINALIDADES DE LAS BASES DE DATOS: La Institución en el desarrollo de su actividad, 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 presenta las distintas bases de datos que maneja la Institución y las finalidades asignadas a cada una de ellas.

TABLA V. FINALIDADES SIC.

BASE DE DATOS	**FINALIDAD BASE DE DATOS**	**FINALIDAD SUPERINTENDENCIA**
ASPIRANTES O PROSPECTOS	Seguimiento de prospectos de alumnos en cualquier metodología y con fines comerciales.	• Publicidad y prospección comercial - prospección comercial • Publicidad y prospección comercial – Ofrecimiento productos y servicios

		•Publicidad y prospección comercial - Segmentación de mercados
INSCRITOS	Seguimiento de prospectos que han iniciado su solicitud de cupo en los programas de la Institución cualquiera sea su naturaleza	• Publicidad y prospección comercial - prospección comercial
ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS	Seguimiento de personal docente o administrativo de la Institución así como estudiantes que desempeñan movilidad internacional o son beneficiarios de relaciones convencionales dentro del marco de funciones sustantivas o adjetivas	• Educación • Educación y cultura – Becas y ayudas a estudiantes • Educación y cultura – Encuestas sociológicas y de opinión • Educación y cultura – Enseñanza Universitaria o superior • Educación y cultura – Otras enseñanzas o eventos • Gestión contable, fiscal y administrativa – Gestión administrativa
SOFTWARE CONTABLE	Gestión de la información financiera de personas naturales o jurídicas con relacionamiento con la Institución sea en calidad de acreedores, deudores, contratistas, contratantes o cualquiera otra.	• Gestión contable, fiscal y administrativa - Gestión de clientes
PROVEEDORES	Gestión de la información de proveedores de bienes o servicios de la Institución	• Gestión contable, fiscal y administrativa - Gestión de proveedores. • Gestión contable, fiscal y administrativa - Gestión administrativa
EMPRENDIMIENTO (ESTUDIANTES ACTIVOS, EGRESADOS Y EMPRESAS)	Gestión de estudiantes, docentes y personas naturales o jurídicas asociadas a procesos de emprendimiento como parte o no de un proceso académico	• Finalidades varias - Procedimientos administrativos. • Educación, Educación y cultura - Otras enseñanzas o eventos
BENEFICIARIOS DE PROYECTOS Y ACTIVIDADES DE PROYECCION	Registro y gestión de información de personas naturales o personas jurídicas, por lo general sin ánimo de lucro que son beneficiarias o aliadas en procesos de	• Finalidades varias - Procedimientos administrativos. • Educación, Educación y cultura - Otras enseñanzas o eventos

SOCIAL	intervención en comunidades.	
EGRESADOS	Registro y gestión de personas naturales que han culminado su proceso académico en virtud de titulación.	• Gestión contable, fiscal y administrativa - Gestión administrativa • Finalidades varias - Procedimientos administrativos
EMPLEADOS	Registro y gestión de información de personas naturales con relaciones contractuales debidamente legalizadas con la Institución .	• Recursos Humanos – Control de horario • Recursos Humanos – Formación de personal • Recursos Humanos – Gestión de personal • Recursos Humanos – Gestión de trabajo temporal • Recursos Humanos – Prestaciones sociales • Recursos Humanos – Prevención de riesgos laborales • Recursos Humanos – Promoción y gestión de empleos • Recursos Humanos – Promoción y selección de personal Información de empleados • Gestión contable, fiscal y administrativa - Gestión administrativa
ESTUDIANTES	Seguimiento, control y registro de estudiantes activos en todo su proceso formativo	• Educación • Educación y cultura – Becas y ayudas a estudiantes • Educación y cultura – Deportes • Educación y cultura – Encuestas sociológicas y de opinión • Educación y cultura – Enseñanza Universitaria o superior • Educación y cultura – Otras enseñanzas o eventos • Gestión contable, fiscal y

		administrativa – Gestión administrativa • Gestión contable, fiscal y administrativa - Gestión de cobros y pagos
HOJAS DE VIDA DE POSIBLES TRABAJADORES	Registro y uso de información de aspirantes a ingresar a la Institución en calidad de trabajadores	• Recursos Humanos – Control de horario • Recursos Humanos – Formación de personal • Recursos Humanos – Gestión de personal • Recursos Humanos – Gestión de trabajo temporal • Recursos Humanos – Prestaciones sociales • Recursos Humanos – Prevención de riesgos laborales • Recursos Humanos – Promoción y gestión de empleos • Recursos Humanos – Promoción y selección de personal Información de empleados • Gestión contable, fiscal y administrativa - Gestión administrativa
PRACTICAS (EMPRESAS)	Registro y gestión de información de estudiantes en unidades de negocio que permiten culminar sus procesos de formación en instancias prácticas	• Finalidades varias - Procedimientos administrativos. • Educación, Educación y cultura - Otras enseñanzas o eventos
ACCIDENTALIDAD ENFERMEDADES Y AUSENTISMOS	Registro y uso de información asociada a la condición médica de los trabajadores de la Institución	• Finalidades varias - Custodia y gestión de información de bases de datos. • Recursos humanos - Gestión de personal
CONTRATOS Y/O CONVENIOS PÚBLICOS Y/O	Registro de información asociada a las etapas pre, post y contractuales de los contratos o convenios suscritos por la	• Recursos Humanos – Promoción y selección de personal • Gestión contable, fiscal y

PRIVADOS	Institución	administrativa - Gestión administrativa
ASEGURADORAS Y ASISTENCIAS	Registro y gestión de información de personas naturales cubiertas por los seguros institucionales cualquiera sea su calidad o sus condiciones especiales	• Gestión contable, fiscal y administrativa - Gestión administrativa
PROCESOS JURIDICOS	Registro y gestión de la información asociada a la defensa judicial o extrajudicial de la Institución sea en instancias jurisdiccionales o en instancias de policial administrativa o cualquiera otra	• Justicia - prestación social. • Finalidades varias - Custodia y gestión de información de bases de datos.

ARTÍCULO 18: DERECHOS DE LOS TITULARES: 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:

a. **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 les han dado a sus datos personales.

b. **Derechos de quejas y reclamos.** Serán los siguientes:

    a. **Reclamo de corrección**: Es el derecho del titular a que se actualicen, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

    b. **Reclamo de supresión:** Es 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.

    c. **Reclamo de revocación:** Es el derecho del titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.

    d. **Reclamo de infracción:** Es el derecho del titular a solicitar que se subsane el incumplimiento de la normativa en materia de protección de datos.

c. **Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento**: Este se establece salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en la normatividad vigente.

d. 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.

ARTÍCULO 19: ATENCIÓN A LOS TITULARES DE DATOS: Corresponde inicialmente al Secretario General Dr. Alvaro Leandro Barreto Sandoval con C.C. No. 1049605806, este será el encargado de la atención de peticiones, consultas y reclamos ante la cual el Titular de los datos puede ejercer sus derechos, teléfono: (571) 552-1860, correo electrónico: basesdedatos@elite.edu.co

ARTÍCULO 20: PROCEDIMIENTOS PARA EJERCER LOS DERECHOS DEL TITULAR:

1. Derecho de acceso o consulta

El titular podrá consultar de forma gratuita sus datos personales en dos casos:

a. Al menos una vez cada mes calendario.
b. 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 Institución solamente podrá cobrar al titular 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 Institución enviado al correo electrónico a basesdedatos@elite.edu.co, indicando en el Asunto “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a la dirección Calle 70 No. 10 A-39 de la ciudad Bogotá D.C. La solicitud deberá contener los siguientes datos:

1. Nombre y apellidos del Titular.
2. 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.
3. Petición en que se concreta la solicitud de acceso o consulta.
4. Dirección para notificaciones, fecha y firma del solicitante.
5. 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:

a. Visualización en pantalla.
b. Por escrito, con copia o fotocopia remitida por correo certificado o no.
c. Tele copia.
d. Correo electrónico u otro medio electrónico.
e. Otro sistema adecuado a la configuración de la base de datos o a la naturaleza del tratamiento, ofrecido por la Institución.

Una vez recibida la solicitud, eta será resuelta 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.

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 Institución enviado al correo electrónico a basesdedatos@elite.edu.co, indicando en el Asunto, “Ejercicio del derecho de acceso o consulta”, o a través de correo postal remitido a la dirección Calle 70 No. 10 A-39 de la ciudad de Bogotá D.C. La solicitud deberá contener los siguientes datos:

1. Nombre y apellidos del Titular.
2. 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.
3. Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o infracción.
4. Dirección para notificaciones, fecha y firma del solicitante.
5. 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 Institución 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.

ARTÍCULO 21: MEDIDAS DE SEGURIDAD: La Institución con el fin de cumplir con el principio de seguridad consagrado en el artículo 4 literal g) de la Ley 1581 implementará 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 Institución mediante la suscripción de los correspondientes contratos de transmisión, requerirá a los encargados del tratamiento con los que trabaja la implementación de las medidas de seguridad necesarias para garantizar la seguridad y confidencialidad de la información en el tratamiento de los datos personales, en razón de ello se exponen las medidas de seguridad implantadas:

TABLA VI. 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	Normas asociadas a 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 soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes.	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 distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado	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 de notificación y gestión de incidencias.	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 el personal de las normas y de las consecuencias del incumplimiento de las mismas	1. Elaboración e implementación de los parámetros de obligatorio 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 datos, medidas de seguridad para el transporte, destrucción y reutilización de

				documentos, identificación de los encargados del tratamiento.

TABLA VII. 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 permitan el 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 VIII. 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 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.	1. Designación de uno o varios responsables de seguridad. 2. Designación de uno o varios encargados del control y la coordinación de las medidas dela norma de seguridad. 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.	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 envío, responsable de la recepción o entrega.	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 del tratamiento para la ejecución de los procedimientos de recuperación.

ARTÍCULO 22: TRANSFERENCIA DE DATOS A TERCEROS PAÍSES: Se prohíbe la transferencia de datos personales a países que no proporcionen niveles adecuados de protección de datos, por ende, 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 ley 1581 exige a sus destinatarios. Esta prohibición no regirá cuando se trate de:

1. Información respecto de la cual el titular haya otorgado su autorización expresa e inequívoca para la transferencia.
2. Intercambio de datos de carácter médico, cuando así lo exija el tratamiento del titular por razones de salud o higiene pública.
3. Transferencias bancarias o bursátiles, conforme a la legislación que les resulte aplicable.
4. Transferencias acordadas en el marco de tratados internacionales en los cuales la República de Colombia sea parte, con fundamento en el principio de reciprocidad.
5. 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.
6. 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.

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.

ARTÍCULO 23: VIGENCIA: Las bases de datos responsabilidad de la Institución 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 se 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.

CAPITULO IV.
DISPOSICIONES ASOCIADAS A PROTOCOLOS DE ATENCIÓN AL TITULAR DE DATOS.

ARTICULO 24: ALCANCE: El objetivo del presente capítulo es poner en conocimiento el procedimiento a seguir para dar respuesta a las solicitudes de acceso y reclamos ejercitadas en virtud de los derechos de acceso, corrección, supresión, revocación o reclamo por infracción del titular de los datos personales objeto de tratamiento por la Institución.

La Institución adoptará las medidas oportunas para difundir el presente documento a todas las personas que forman parte de su organización y tienen acceso a los datos personales, para que puedan informar a los titulares del procedimiento a seguir en los casos aquí regulados.

ARTÍCULO 25: PRECEPTO LEGAL Y TITULARIDAD: El derecho a la protección de los datos tiene como finalidad permitir a todas las personas conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en archivos o bases de datos, este derecho constitucional se recoge en los artículos 15 y 20 de la Constitución Política, en la ley estatutaria 1581 de 2012 y en el Decreto 1377 de 2013, de acuerdo con el artículo 8 de la Ley 1581 y los artículos 21 y 22 del Decreto 1377 de 2013, los titulares de los datos pueden ejercer una serie de

derechos en relación con el 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.

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

ARTÍCULO 26: DERECHOS DE LOS TITULARES: Los derechos del titular son los siguientes:

a) **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 se les han dado a sus datos personales.

b) **Derechos de quejas y reclamos.** Corresponde a los siguientes cuatro tipos de reclamos:

   1. **Reclamo de corrección:** Es el derecho del titular a que se actualicen, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.

   2. **Reclamo de supresión:** Es 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.

3. **Reclamo de revocación:** Es el derecho del titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.

4. **Reclamo de infracción**: Es el derecho del titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

c) **Derecho a solicitar prueba de la autorización otorgada al responsable del tratamiento:** Este derecho aplica en toto momento y circunstancia salvo cuando expresamente se exceptúe como requisito para el tratamiento de conformidad con lo previsto en el artículo 10 de la Ley 1581.

d) **Derecho a presentar ante la Superintendencia de Industria y Comercio quejas por infracciones:** Es el derecho por medio del cual 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.

ARTÍCULO 27: ATENCIÓN A LOS TITULARES DE DATOS: De manera inicial tengase como encargado de esta gestión al Coordinador Jurídico de la Institución (Dr. Luis Carlos Restrepo Rojas o quien haga sus veces) como el encargado de la atención de peticiones, consultas y reclamos ante la cual los titulares de los datos personales pueden ejercer sus derechos, esto en la línea 3813222 y al correo electrónico: basesdedatos@cun.edu.co.

ARTICULO 28: LINEAMIENTOS GENERALES DE PROCEDIMIENTO PARA EL EJERCICIO DE DERECHOS: Sin perjuicio de las consideraciones a consignarse en el SIGECC establezcanse los siguientes lineamientos generales de procedimiento en materia de ejercicio de derechos de titulaes:

A. **PROCEDIMIENTO DE ACCESO O CONSULTA:** El titular podrá consultar de forma gratuita sus datos personales en los siguientes eventos:

a. Al menos una vez cada mes calendario.
b. 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 Institución 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.

El titular de los datos puede ejercitar el derecho de acceso o consulta de sus datos mediante un escrito dirigido a la Institución bien sea al correo electrónico basesdedatos@elite.edu.co, indicando en el asunto, "Ejercicio del derecho de acceso o consulta", o a través de correo postal remitido a la Calle 70 No. 10 A-39 de la ciudad de Bogotá D.C., en uno u otro caso la solicitud deberá contener los siguientes datos:

i. Nombre y apellidos del titular.
ii. 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.
iii. Petición en que se concreta la solicitud de acceso o consulta.
iv. Dirección para notificaciones, fecha y firma del solicitante.
v. 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:

i. Visualización en pantalla.
ii. Por escrito, con copia o fotocopia remitida por correo certificado o no.
iii. Tele copia.
iv. Correo electrónico u otro medio electrónico.
v. Otro sistema adecuado a la configuración de base de datos o a la naturaleza del tratamiento, ofrecido por la Institución.

Una vez recibida la solicitud, la misma será resuelta 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.

B. **PROCEDIMIENTO DE QUEJAS Y RECLAMOS:** El titular de los datos puede ejercitar los derechos de reclamo sobre sus datos mediante un escrito dirigido la Institución enviado, bien al correo electrónico basesdedatos@elite.edu.co indicando en el asunto, "Ejercicio del derecho de acceso o consulta", o bien a través de correo postal remitido a la dirección Calle 70 No. 10 A-39 de la ciudad de Bogotá D.C. La solicitud deberá contener los siguientes datos:

i. Nombre y apellidos del Titular.
ii. 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.
iii. Descripción de los hechos y petición en que se concreta la solicitud de corrección, supresión, revocación o infracción.
iv. Dirección para notificaciones, fecha y firma del solicitante.
v. 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 Institución 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.

CAPITULO V.
DISPOSICIONES ASOCIADAS A MANEJO WEB.

ARTÍCULO 29: DEFINICIONES: Para todos los efectos institucionales y en concordancia con las disposiciones de la Ley 1581 de 2012 y su Decreto Reglamentario 1377 de 2013 se tendrán como definiciones las siguientes:

a. **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.

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

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

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

e. **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.

f. **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.

g. **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.

h. **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.

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

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

k. **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.

l. **Transmisión:** Tratamiento de datos personales que implica la comunicación de los mismos dentro o fuera del territorio de la República de Colombia cuando tenga por objeto la realización de un tratamiento por el encargado por cuenta del responsable.

ARTÍCULO 30: DATOS DE NAVEGACIÓN: El sistema de navegación y el software necesario para el funcionamiento de la página web institucional recoge 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 de 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.

ARTÍCULO 30: COOKIES O WEB BUGS: El sitio Web institucional 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.

ARTÍCULO 31: DERECHOS DE LOS TITULARES: 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.
5. 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:

a. **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 les han dado a sus datos personales.

b. Derechos de quejas y reclamos. La Ley distingue cuatro tipos de reclamos:

   i. **Reclamo de corrección:** el derecho del Titular a que se actualice, rectifique o modifiquen aquellos datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado.
   ii. **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.

iii. **Reclamo de revocación:** el derecho del Titular a dejar sin efecto la autorización previamente prestada para el tratamiento de sus datos personales.

iv. **Reclamo de infracción:** el derecho del Titular a solicitar que se subsane el incumplimiento de la normativa en materia de Protección de Datos.

c. **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 las normas legales.

d. **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.

APENDICE

INFORME TECNICO INICIAL

En cumplimiento del principio de seguridad consagrado en el artículo 4 literal g) de la Ley Estatutaria 1581 de 2012 de Protección de Datos Personales, la Institución, responsable del tratamiento de datos personales, así como sus encargados del tratamiento, implementará 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.

No se permitirá el registro de bases de datos personales que no reúnan las condiciones mínimas de seguridad expuestas en el presente informe.

Las medidas de seguridad se clasifican en tres niveles de seguridad según el tipo de datos: público-semiprivado, privado y sensible. Los niveles de seguridad son acumulativos, de forma que las medidas de seguridad para datos sensibles incluyen también las medidas de seguridad

para los niveles, privado y público-semiprivado; y las medidas de seguridad para datos privados incluyen, a su vez, las del nivel público-semiprivado. La clasificación de los niveles de seguridad se realiza atendiendo a la tipología de los datos, la finalidad del tratamiento y la actividad del responsable del tratamiento (Tabla I).

TABLA I. BASES DE DATOS Y NIVEL DE SEGURIDAD

BASE DE DATOS	**NIVEL DE SEGURIDAD**	**SISTEMA DE TRATAMIENTO**	**FINALIDAD**
ASPIRANTES O PROSPECTOS	SENSIBLE	FÍSICO	Seguimiento de prospectos de alumnos en cualquier metodología y con fines comerciales.
INSCRITOS	SENSIBLE	FÍSICO	Seguimiento de prospectos que han iniciado su solicitud de cupo en los programas de la Institución cualquiera sea su naturaleza
ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS	SENSIBLE	FÍSICO	Seguimiento de personal docente o administrativo de la Institución así como estudiantes que desempeñan movilidad internacional o son beneficiarios de relaciones convencionales dentro del marco de funciones sustantivas o adjetivas
SOFTWARE CONTABLE	PRIVADO	FÍSICO	Gestión de la información financiera de personas naturales o jurídicas con relacionamiento con la Institución sea en calidad de acreedores, deudores, contratistas, contratantes o cualquiera otra.
PROVEEDORES	SENSIBLE	FÍSICO	Gestión de la información de proveedores de bienes o servicios de la Institución
EMPRENDIMIENTO (ESTUDIANTES ACTIVOS, EGRESADOS Y EMPRESAS)	SENSIBLE	FÍSICO	Gestión de estudiantes, docentes y personas naturales o jurídicas asociadas a procesos de emprendimiento como parte o no de un proceso académico
BENEFICIARIOS DE PROYECTOS Y ACTIVIDADES DE	SENSIBLE	FÍSICO	Registro y gestión de información de personas naturales o personas jurídicas, por lo general sin ánimo de lucro que son beneficiarias o aliadas en

PROYECCION SOCIAL			procesos de intervención en comunidades.
EGRESADOS	PRIVADO	FÍSICO	Registro y gestión de personas naturales que han culminado su proceso académico en virtud de titulación.
EMPLEADOS	SENSIBLE	FÍSICO	Registro y gestión de información de personas naturales con relaciones contractuales debidamente legalizadas con la Institución .
ESTUDIANTES	PRIVADO	FÍSICO	Seguimiento, control y registro de estudiantes activos en todo su proceso formativo
HOJAS DE VIDA DE POSIBLES TRABAJADORES	PRIVADO	FÍSICO	Registro y uso de información de aspirantes a ingresar a la Institución en calidad de trabajadores
PRACTICAS (EMPRESAS)	PRIVADO	FÍSICO	Registro y gestión de información de estudiantes en unidades de negocio que permiten culminar sus procesos de formación en instancias prácticas
ACCIDENTALIDAD ENFERMEDADES Y AUSENTISMOS	PRIVADO	FÍSICO	Registro y uso de información asociada a la condición médica de los trabajadores de la Institución
CONTRATOS Y/O CONVENIOS PÚBLICOS Y/O PRIVADOS	SENSIBLE	FÍSICO	Registro de información asociada a las etapas pre, post y contractuales de los contratos o convenios suscritos por la Institución
ASEGURADORAS Y ASISTENCIAS	SENSIBLES	FÍSICO	Registro y gestión de información de personas naturales cubiertas por los seguros institucionales cualquiera sea su calidad o sus condiciones especiales
PROCESOS JURIDICOS	SENSIBLES	FÍSICO	Registro y gestión de la información asociada a la defensa judicial o extrajudicial de la Institución sea en instancias jurisdiccionales o en instancias de policial administrativa o cualquiera otra
BASE DE DATOS	**NIVEL DE SEGURIDAD**	**SISTEMA DE TRATAMIENTO**	**FINALIDAD**
ASPIRANTES O PROSPECTOS	SENSIBLE	AUTOMATIZADO	Seguimiento de prospectos de alumnos en cualquier metodología y con fines comerciales.

INSCRITOS	SENSIBLE	AUTOMATIZADO	Seguimiento de prospectos que han iniciado su solicitud de cupo en los programas de la Institución cualquiera sea su naturaleza
ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS	SENSIBLE	AUTOMATIZADO	Seguimiento de personal docente o administrativo de la Institución así como estudiantes que desempeñan movilidad internacional o son beneficiarios de relaciones convencionales dentro del marco de funciones sustantivas o adjetivas
SOFTWARE CONTABLE	PRIVADO	AUTOMATIZADO	Gestión de la información financiera de personas naturales o jurídicas con relacionamiento con la Institución sea en calidad de acreedores, deudores, contratistas, contratantes o cualquiera otra.
PROVEEDORES	SENSIBLE	AUTOMATIZADO	Gestión de la información de proveedores de bienes o servicios de la Institución
EMPRENDIMIENTO (ESTUDIANTES ACTIVOS, EGRESADOS Y EMPRESAS)	SENSIBLE	AUTOMATIZADO	Gestión de estudiantes, docentes y personas naturales o jurídicas asociadas a procesos de emprendimiento como parte o no de un proceso académico
BENEFICIARIOS DE PROYECTOS Y ACTIVIDADES DE PROYECCION SOCIAL	SENSIBLE	AUTOMATIZADO	Registro y gestión de información de personas naturales o personas jurídicas, por lo general sin ánimo de lucro que son beneficiarias o aliadas en procesos de intervención en comunidades.
EGRESADOS	PRIVADO	AUTOMATIZADO	Registro y gestión de personas naturales que han culminado su proceso académico en virtud de titulación.
EMPLEADOS	SENSIBLE	AUTOMATIZADO	Registro y gestión de información de personas naturales con relaciones contractuales debidamente legalizadas con la Institución .
ESTUDIANTES	PRIVADO	AUTOMATIZADO	Seguimiento, control y registro de estudiantes activos en todo su proceso formativo
HOJAS DE VIDA DE POSIBLES TRABAJADORES	PRIVADO	AUTOMATIZADO	Registro y uso de información de aspirantes a ingresar a la Institución en calidad de trabajadores
PRACTICAS (EMPRESAS)	PRIVADO	AUTOMATIZADO	Registro y gestión de información de estudiantes en unidades de negocio que permiten culminar

			sus procesos de formación en instancias prácticas
ACCIDENTALIDAD ENFERMEDADES Y AUSENTISMOS	PRIVADO	AUTOMATIZADO	Registro y uso de información asociada a la condición médica de los trabajadores de la Institución
CONTRATOS Y/O CONVENIOS PÚBLICOS Y/O PRIVADOS	SENSIBLE	AUTOMATIZADO	Registro de información asociada a las etapas pre, post y contractuales de los contratos o convenios suscritos por la Institución
ASEGURADORAS Y ASISTENCIAS	SENSIBLES	AUTOMATIZADO	Registro y gestión de información de personas naturales cubiertas por los seguros institucionales cualquiera sea su calidad o sus condiciones especiales
PROCESOS JURIDICOS	SENSIBLES	AUTOMATIZADO	Registro y gestión de la información asociada a la defensa judicial o extrajudicial de la Institución sea en instancias jurisdiccionales o en instancias de policial administrativa o cualquiera otra
ASPIRANTES O PROSPECTOS	SENSIBLE	AUTOMATIZADO	
INSCRITOS	SENSIBLE	AUTOMATIZADO	
ESTUDIANTES, DOCENTES Y ADMINISTRATIVOS NACIONALES E INTERNACIONALES POR CONVENIOS	SENSIBLE	AUTOMATIZADO	
SOFTWARE CONTABLE	PRIVADO	AUTOMATIZADO	
PROVEEDORES	SENSIBLE	AUTOMATIZADO	

A continuación, se exponen y describen las medidas de seguridad mínimas implementadas por la Institución:

TABLA VI. 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	Normas asociadas a 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 soportes por medio físico o electrónico. 4. Sistema de etiquetado o identificación del tipo de información. 5. Inventario de soportes.	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 distintos de los autorizados. 4. Concesión, alteración o anulación de permisos por el personal autorizado	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 de notificación y gestión de incidencias.	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 el personal de las normas y de las consecuencias del incumplimiento de las mismas	1. Elaboración e implementación de los parámetros de obligatorio 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 datos, medidas de seguridad para el transporte, destrucción y reutilización de documentos, identificación de los encargados del tratamiento.

TABLA VII. 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 permitan el 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 VIII. 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.	1. Designación de uno o varios responsables de	1. Controles periódicos de cumplimiento	1. Registro de entrada y salida de documentos y	1. Control de acceso al lugar o lugares donde	1. Mecanismo que limite el número de	1. Registro de los procedimientos de recuperación de los datos,

2. Auditoría extraordinaria por modificaciones sustanciales en los sistemas de 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.	seguridad. 2. Designación de uno o varios encargados del control y la coordinación de las medidas dela norma de seguridad. 3. Prohibición de delegación de la responsabilidad del responsable del tratamiento en el responsable de seguridad.		soportes: fecha, emisor y receptor, número, tipo de información, forma de envío, responsable de la recepción o entrega.	se ubican los sistemas de información.	intentos reiterados de acceso no autorizados.	persona que los ejecuta, datos restaurados y datos grabados manualmente. 2. Autorización del responsable del tratamiento para la ejecución de los procedimientos de recuperación.

TABLA IX. 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.	1. Archivadores, armarios u otros ubicados en áreas de acceso	1. Solo por usuarios autorizados.	1. Medidas que impidan el acceso o manipulación de	1. Sistema de etiquetado confidencial.	1. Registro de accesos: usuario, hora, base de datos a la que	1. Transmisión de datos mediante redes electrónicas cifradas.

2. Mecanismo de identificación de acceso. 3. Registro de accesos de usuarios no autorizados.	protegidas con llaves u otras medidas.	2. Destrucción que impida el acceso o recuperación de los datos.	documentos.	2. Cifrado de datos. 3. Cifrado de dispositivos portátiles cuando salgan fuera.	accede, tipo de acceso, registro al que accede. 2. Control del registro de accesos por el responsable de seguridad. Informe mensual. 3. Conservación de los datos: 2 años.	

Artículo Segundo: Remítase copia del presente acuerdo a las Vicerrectorías, Direcciones y demás dependencias de la Institución para los fines correspondientes.

Artículo Tercero: Por la Secretaria General de la Institución realícense las acciones pertinentes para la publicidad de la presente disposición.

Artículo Cuarto: Este acuerdo rige a partir de la fecha de su expedición.

COMUNÍQUESE Y CÚMPLASE.

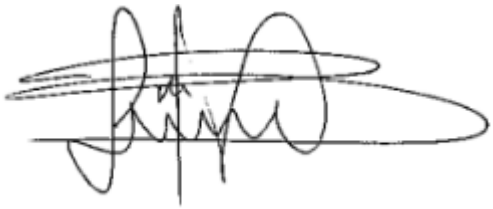
Dado en Bogotá D.C. a los veintiún (21) días del mes de diciembre de dos mil dieciocho (2018)

JAIME ALBERTO RINCÓN PRADO
Presidente del Consejo Directivo

ALVARO LEANDRO BARRETO SANDOVAL
Secretario General

El presente acuerdo es fiel copia del original que reposa en el archivo de la Secretaria General de la Escuela Latinoamericana de Ingenieros, Tecnólogos y Empresarios - ELITE

Cordialmente



ALVARO LEANDRO BARRETO SANDOVAL
Secretario General
ELITE