1000

CIRCULAR 009/17

Medellín, 30 MAY 2017

PARA: COLABORADORES Y CONTRATISTAS DE LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR

ASUNTO: MANUAL DE SEGURIDAD DEL USUARIO PARA EL TRATAMIENTO DE LA INFORMACIÓN DE LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR

Mediante la presente circular se presenta el manual de seguridad del usuario para el tratamiento de la información de la Corporación para el fomento de la educación superior, que obedece al mandato legal, en cuanto al derecho constitucional que tiene todas las personas a conocer, actualizar y rectificar la información que se haya recogido sobre ellas en base de datos o archivos, y los demás derechos, libertades y garantías frente a la materia que desarrolle la Ley y la Constitución Política.

Atentamente,

LICETH KARINE MENESES YARURO
Directora Ejecutiva

Transcribió: Xiomara Gaviria Cardona, Abogada
Anexo: Manual de seguridad del usuario para el tratamiento de la información.
Anexo Roles y Responsabilidades

1000

RESOLUCIÓN Nº 0047/17

POR MEDIO DE LA CUAL SE ADOPTA EL MANUAL DE SEGURIDAD DEL USUARIO PARA EL TRATAMIENTO DE LA INFORMACIÓN DE LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR

LA DIRECTORA EJECUTIVA DE LA CORPORACION PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR

En ejercicio de sus facultades legales y conforme a los artículos 35 y 37 de los estatutos de la organización y

CONSIDERANDO QUE:

1. Que la Corporación para el Fomento de la Educación Superior es una asociación mixta sin ánimo de lucro, descentralizada de forma indirecta del orden departamental de Antioquia, perteneciente a la rama del poder ejecutivo, que entre sus asociados están La Fundación EPM, La Gobernación de Antioquia y el Instituto para el Desarrollo de Antioquia-IDEA-. Fue constituida por Acta No. 1, otorgada por la Asamblea de Asociados, en octubre 24 de 2013, por lo tanto se denomina ENTIDAD ESTATAL, conforme lo establece el literal a) numeral 1 del artículo 2 de la ley 80 de 1993, es así como, en lo relativo a sus actos y contratos, la legislación aplicable es la que rige la contratación administrativa.

2. Que el objeto de la misma es gerenciar la política de acceso y permanencia en la educación superior a través de la promoción, administración, financiación y operación de programas para la educación superior de jóvenes de escasos recursos de estratos 1, 2 y 3 en el Departamento de Antioquia; así como la gestión, promoción y consolidación de mecanismos para la formación en Educación Superior.

3. Que la Ley 1581 DE 2012 por la cual se dictan disposiciones generales para la protección de datos personales, tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma disposición normativa.

4. Que de conformidad con el literal k del artículo 17 de la Ley 1581 de 2012, es un deber de los responsables del tratamiento adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la presente ley y en especial, para la atención de consultas y reclamos.

5. Que el artículo 2.2.2.25.3.1 del decreto 1074 de 2015 establece que los responsables del tratamiento deberán desarrollar sus políticas para el tratamiento de los datos personales y velar porque los Encargados del Tratamiento den cabal cumplimiento a las mismas.

6. Que de acuerdo a lo anterior, mediante resolución 0052 del 31 de octubre de 2016, la Corporación adopta la política de tratamiento de la información.

7. Que en mérito de lo expuesto la Directora Ejecutiva de la CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR.

RESUELVE:

ARTÍCULO PRIMERO: Adoptar el manual de seguridad del usuario para el tratamiento de la información de la Corporación para el Fomento de la Educación Superior.

ARTÍCULO SEGUNDO: El presente manual rige a partir de la fecha de su publicación, se divulgará a través del portal institucional, y estará sujeto actualizaciones en la medida en que se modifiquen o se dicten nuevas disposiciones legales sobre la materia.

Anexo: Manual de seguridad del usuario para el tratamiento de la información.
Anexo Roles y Responsabilidades

PUBLIQUESE Y CÚMPLASE

Dada en Medellín, 30 MAY 2017

LICETH KARINE MENESES YARURO
Directora Ejecutiva

Proyectó
Xiomara Gaviria Cardona
Abogada

corpoeducacionsuperior.org

MANUAL DE SEGURIDAD DEL USUARIO PARA EL TRATAMIENTO DE LA INFORMACIÓN DE LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR

1. BASE LEGAL Y ÁMBITO DE APLICACIÓN

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, por la cual se dictan disposiciones generales para la Protección de Datos Personales (LEPD); y el Capítulo 25 del Decreto 1074 de 2015.

Cuando el Titular de los datos 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.

Si bien la responsabilidad del tratamiento de los datos recae en la organización u empresa responsable del tratamiento, sus competencias se materializan en las funciones que corresponden a su personal de servicio. El personal de la organización u empresa responsable del tratamiento con acceso, directo o indirecto, a bases de datos que contienen datos personales han de conocer la normativa de protección de datos, la política de protección de datos de la entidad y el Manual Interno de Seguridad; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones, actividades y cargos.

Para velar con el cumplimiento de sus obligaciones de seguridad, LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR nombra a número de responsables de seguridad encargados de desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en el Manual Interno de Seguridad.

Esta política será aplicable a todos los datos personales registrados en bases de datos que sean objeto de tratamiento por el responsable del tratamiento y se encuentra dirigida a todos los usuarios de datos, que son tanto el personal propio como al personal externo de LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR.

Todos los usuarios identificados en el Manual Interno de Seguridad 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 acabada su relación laboral o profesional con la entidad responsable del tratamiento. El deber de confidencialidad, recogido en el artículo 4 literal h) de la LEPD, se formaliza a través de la firma de un acuerdo de confidencialidad suscrito entre el usuario y el responsable del tratamiento.

Para todos los efectos del presente documento, entiéndase la abreviatura LEPD como Ley estatutaria de protección de datos personales 1581 de 2012.

2. DEFINICIONES

Establecidas en el artículo 3 de la Ley 1581 de 2012 y el artículo 2.2.2.25.1.3 y el Decreto 1074 de 2015

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

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

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

Dato público: Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Datos sensibles: Se entiende por datos 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.

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

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

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

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

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

Transferencia: La transferencia de datos tiene lugar cuando el responsable y/o encargado del tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que a su vez es responsable del tratamiento y se encuentra dentro o fuera del país.

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

3. PRINCIPIOS DE LA PROTECCIÓN DE DATOS

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

Principio de legalidad: El tratamiento de los datos es una actividad reglada que debe sujetarse a lo establecido en la LEPD y Decreto 1074 de 2015 y en las demás disposiciones concordantes.

Principio de finalidad: El tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular.

Principio de libertad: El tratamiento solo puede ejercerse con el consentimiento previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que revele el consentimiento. El tratamiento de los datos requiere la autorización previa e informada del Titular por cualquier medio que permita ser consultado con posterioridad, salvo en los siguientes casos que exceptúa el artículo 10 de la LEPD:

- Información requerida por una entidad pública o administrativa en ejercicio de sus funciones legales o por orden judicial.
- Datos de naturaleza pública.
- Casos de urgencia médica o sanitaria.
- Tratamiento de información autorizado por la Ley para fines históricos, estadísticos o científicos.
- Datos relacionados con el Registro Civil de las personas.
- Principio de veracidad o calidad: La información sujeta a tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

Principio de transparencia: En el tratamiento debe garantizarse el derecho del Titular a obtener del responsable del tratamiento o del encargado del tratamiento, en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan. En el momento de solicitar la autorización al titular, el responsable del tratamiento deberá informarle de manera clara y expresa lo siguiente, conservando prueba del cumplimiento de este deber:

- El tratamiento al cual será sometidos sus datos y la finalidad del mismo.
- El carácter facultativo de la respuesta del Titular a las preguntas que le sean hechas cuando éstas traten sobre datos sensibles o sobre datos de niños, niñas o adolescentes.
- Los derechos que le asisten como Titular.
- La identificación, dirección física, correo electrónico y teléfono del responsable del tratamiento.

Principio de acceso y circulación restringida: El tratamiento se sujeta a los límites que se derivan de la naturaleza de los datos personales, de las disposiciones de la LEPD y la Constitución. En este sentido, el tratamiento solo podrá hacerse por personas autorizadas por el titular y/o por las personas previstas en la Ley. Los datos personales, salvo la información pública, no podrán estar disponibles en Internet y otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados conforme a la Ley.

Principio de seguridad: La información sujeta a tratamiento por el responsable del tratamiento o encargado del tratamiento se deberá manejar con las medidas técnicas, humanas y administrativas que sean necesarias para otorgar seguridad a los registros evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento. El responsable del tratamiento tiene la responsabilidad de implantar las medidas de seguridad correspondientes y de ponerlas en conocimiento todo personal que tenga acceso, directo o indirecto, a los datos. Los usuarios que accedan a los sistemas de información del responsable del tratamiento deben conocer y cumplir con las normas y medidas de seguridad que correspondan a sus funciones. Estas normas y medidas de seguridad se recogen en el Manual Interno de Seguridad, de obligado cumplimiento para todo usuario y personal de la

empresa. Cualquier modificación de las normas y medidas en materia de seguridad de datos personales por parte del responsable del tratamiento ha de ser puesta en conocimiento de los usuarios.

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

4. CATEGORÍAS ESPECIALES DE DATOS

4.1. Datos sensibles

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

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

- El Titular haya dado su autorización explícita a dicho tratamiento, salvo en los casos que por ley no sea requerido el otorgamiento de dicha autorización.
- El tratamiento sea necesario para salvaguardar el interés vital del Titular y éste se encuentre física o jurídicamente incapacitado. En estos eventos, los representantes legales deberán otorgar su autorización.
- El tratamiento sea efectuado en el curso de las actividades legítimas y con las debidas garantías por parte de 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.
- El tratamiento se refiera a datos que sean necesarios para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial.
- El tratamiento tenga una finalidad histórica, estadística o científica. En este evento deberán adoptarse las medidas conducentes a la supresión de identidad de los Titulares.

4.2. Derechos de los niños, niñas y adolescentes

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

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

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

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

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1074 de 2015. 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.

5. FUNCIONES YOBLIGACIONES

5.1. Responsable del tratamiento

Las obligaciones en materia de seguridad de los datos de LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR son las siguientes:

- Coordinar e implantar las medidas de seguridad recogidas en el Manual Interno de Seguridad.
- Difundir el referido documento entre el personal afectado.
- Mantener el Manual Interno de Seguridad actualizado y revisado siempre que se produzcan cambios relevantes en el sistema de información, el sistema de tratamiento, la organización de la entidad, el contenido de la información de las bases de datos, o como consecuencia de los controles periódicos realizados. De igual modo, se revisará su contenido cuando se produzca algún cambio que pueda afectar al cumplimiento de las medidas de seguridad.
- Designar uno o más responsables de seguridad e identificar a los usuarios autorizados para acceder a las bases de datos.
- Cuidar que el acceso mediante sistemas y aplicaciones informáticas se lleve a cabo mediante acceso identificado y contraseña.
- Autorizar, salvo delegación expresa a usuarios autorizados, la salida de soportes fuera de los establecimientos donde se encuentran las bases de datos; las entradas y salidas de información por red, mediante dispositivos de almacenamiento electrónico o en papel; y el uso de módems y las descargas de datos.
- Verificar semestralmente la correcta aplicación del procedimiento de copias de respaldo y recuperación de datos.
- Garantizar la existencia de una lista de usuarios autorizados y perfiles de usuario.
- Analizar, junto con el responsable de seguridad correspondiente, las incidencias registradas para establecer las medidas correctoras oportunas, al menos cada tres meses.
- Realizar una auditoría, interna o externa, para verificar el cumplimiento de las medidas de seguridad en materia de protección de datos, al menos cada dos (2) años.

5.2. Responsables deseguridad

Los responsables de la Seguridad designados por LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR para las bases de datos, Sensibles, automatizadas y no automatizadas se encuentran en el "Anexo Roles y Responsabilidades".

Los responsables de la seguridad tienen las siguientes funciones:

- Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión del Manual Interno de Seguridad.
- Coordinar y controlar los mecanismos que permiten acceder a la información contenida en las bases de datos y elaborar un informe mensual sobre dicho control.
- Gestionar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en el Manual Interno de Seguridad.
- Habilitar el registro de incidencias a todos los usuarios para que comuniquen y registren las incidencias relacionadas con la seguridad de los datos; así como acordar con el responsable del tratamiento las medidas correctoras y registrarlas.
- Comprobar, al menos cada tres (3) meses, la validez y vigencia de la lista de usuarios autorizados, la existencia y validez de las copias de seguridad para la recuperación de los datos, la actualización del Manual Interno de Seguridad y el cumplimiento de las medidas relacionadas con las entradas y salidas de datos.
- Definir el proyecto de auditoría, interna o externa, al menos cada dos (2) años.
- Recibir y analizar el informe de auditoría para elevar sus conclusiones y proponer medidas correctoras al responsable del tratamiento.
- Gestionar y controlar los registros de entradas y salidas de documentos o soportes que contengan datos personales

5.3. Usuarios

Todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información de LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR deben actuar de conformidad a las funciones y obligaciones recogidas en el presente documento.

LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR cumple con el deber de información con su inclusión de acuerdos de confidencialidad y deber de secreto que suscribe.

Las funciones, actividades y obligaciones del personal de LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la entidad.

El incumplimiento de las obligaciones y medidas de seguridad establecidas en este Manual por parte de las personas internas o externas de LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR es sancionable de acuerdo a la normativa aplicable a la relación jurídica existente entre el usuario y la entidad.

Las funciones y obligaciones de los usuarios de las bases de datos personales bajo responsabilidad de LA CORPORACIÓN PARA EL FOMENTO DE LA EDUCACIÓN SUPERIOR son las siguientes:

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

la cambie. Cuando sea necesario restaurar la contraseña, el usuario debe comunicarlo al administrador del sistema.

- **Copias de respaldo y recuperación de datos:** Debe realizarse copia de seguridad de toda la información de bases de datos personales de la entidad.
- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en la Política de tratamiento de la información y en el Manual de políticas de seguridad de la información.

LICETH KARINE MENESES YARURO
Directora Ejecutiva.
Corporación para el Fomento de la Educación Superior.

Reviso: Xiomara Gaviria Cargo: Abogada Firma:	Revisó: Andrés Felipe Domínguez Cargo: Prof. Sistemas Firma:	Revisó: Sandra Paola Nohavá Cargo : Subdirectora Técnica Firma:	Revisó: Carlos Mario Garcés Díaz Cargo: Subdirector Administrativo y Financiero Firma:

ANEXO 3

ROLES Y RESPONSABILIDADES

ANEXO

ROLES Y RESPONSABILIDADES OFICIAL DE PROTECCIÓN DE DATOS

OFICIAL DE PROTECCIÓN DE DATOS

- Cargo: PROFESIONAL EN SISTEMAS
- Nombre: ANDRES FELIPE DOMINGUEZ RENDON,
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 1.037.594.073
- Correo electrónico: contacto@corpoeducacionsuperior.org

La figura de Oficial de Protección de Datos tiene fundamento legal en el artículo 2.2.2.25.4.4. del Decreto compilatorio 1074 de 2015, el cual señala la obligación de los Responsables y Encargados de designar a una persona o área para la protección de datos personales quien tendrá como función dar trámite a las solicitudes de los Titulares, para el ejercicio de los derechos establecidos en la Ley 1581 de 2012 y normas concordantes.

Por otra parte, la Delegatura de Protección de Datos Personales de la Superintendencia de Industria y Comercio en ejercicio de sus funciones publicó la "Guía para la Implementación del Principio de Responsabilidad Demostrada (Accountability)" el 28 de mayo de 2015. Directriz que acoge los planteamientos formulados por la Organización para la Cooperación y el Desarrollo Económico (OCDE), específicamente en lo relativo al Programa Integral de Gestión de Datos Personales.

La citada guía desarrolla la obligación de formular las políticas y procedimientos para el tratamiento de los datos personales y la articulación de las diferentes áreas internas de la empresa encabezada por la alta gerencia en colaboración con el oficial de protección de datos personales y demás empleados de la organización.

Así pues, la adecuada implementación del marco legal en datos personales señalado en la guía de responsabilidad demostrada está relacionado con la designación de competencias que realice la alta gerencia en las diferentes áreas de su organización y de la designación del el Oficial de Protección de Datos Personales encargado de coordinar, conocer y verificar que la implementación del Sistema Integral de Gestión de Datos Personales se ejecute de acuerdo con el marco legal vigente. El Sistema Integral de Gestión de Datos Personales, se entiende como un programa corporativo basado en controles, que responde al tamaño y estructura de la organización, destinado al cumplimiento, implementación y consolidación del régimen de protección de datos.

Las funciones principales del Oficial de Protección de Datos Personales, entre otras son:

- Controlar y actualizar el inventario de información personal continuamente para identificar y evaluar nuevas recolecciones, usos y divulgaciones.
- Revisar las políticas siguiendo los resultados de las evaluaciones o auditorías.

- Mantener como documentos históricos las evaluaciones de impacto y las de amenazas a la seguridad y riesgos.

- Revisar y modificar la formación y la educación en forma periódica como consecuencia de evaluaciones continuas y comunicar los cambios realizados a los controles del programa.

- Revisar y adaptar los protocolos de respuesta en el manejo de violaciones e incidentes para implementar las mejores prácticas o recomendaciones y lecciones aprendidas de revisiones posteriores a esos incidentes.

- Revisar y, en su caso, modificar los requisitos establecidos en los contratos suscritos con los Encargados del Tratamiento.

- Actualizar y aclarar las comunicaciones externas para explicar las políticas de tratamiento de datos.

- Reportar semestralmente al Representante Legal la evolución del riesgo, los controles implementados, el monitoreo y en general del programa.

En este sentido, es necesario tener en cuenta la responsabilidad demostrada que señala el artículo 2.2.2.25.6.1 del Decreto compilatorio 1074 de 2015 para dar cumplimiento a la Ley 1581 de 2012, por cuanto, la figura de Oficial de Protección de Datos se desarrolla en la citada guía como la persona que debe elegirse al interior de las compañías para coordinar la implementación de buenas prácticas de gestión de datos personales, la cual, tendrá la función de estructurar, diseñar y administrar el programa que permita a la organización cumplir las normas sobre protección de datos personales, así como establecer los controles de ese programa, su evaluación y revisión permanente. Para ello deberá tener en cuenta las siguientes directrices:

- Establecer e implementar los controles del Programa Integral de Gestión de Datos Personales.
- Servir de enlace y coordinador con las demás áreas de la organización para asegurar una implementación transversal del Programa Integral de Gestión de Datos Personales.
- Promover una cultura de protección de datos dentro de la organización.
- Mantener un inventario de las bases de datos personales en poder de la organización y clasificarlas según su tipo.
- Registrar las bases de datos de la organización en el Registro Nacional de Bases de Datos y actualizar el reporte atendiendo a las instrucciones que sobre el particular emita la SIC.
- Obtener las declaraciones de conformidad de la SIC cuando sea requerido.
- Redactar y validar los contenidos de los contratos de transmisiones internacionales de datos que se suscriban con Encargados no residentes en Colombia.
- Analizar las responsabilidades de cada cargo de la organización, para diseñar un programa de entrenamiento en protección de datos específico para cada uno de ellos.
- Realizar un entrenamiento general en protección de datos para todos los empleados de la compañía.
- Realizar el entrenamiento necesario a los nuevos empleados, que tengan acceso por las condiciones de su empleo, a datos personales gestionados por la organización.
- Integrar las políticas de protección de datos dentro de las actividades de las demás áreas de la organización (talento humano, seguridad, call centers y gestión de proveedores).
- Medir la participación, y calificar el desempeño, en los entrenamientos de protección de datos.

- Requerir que, dentro de los análisis de desempeño de los empleados, se encuentre haber completado satisfactoriamente el entrenamiento sobre protección de datos personales.

De modo que, la designación del Oficial de Protección de Datos Personales obedece a un deber legal que corresponde cumplir a todas las empresas para la protección y garantía de derechos constitucionales de los titulares de los datos que se están almacenando en sus organizaciones.

RESPONSABLES DE LA SEGURIDAD DE LAS BASES DE DATOS:

BASES DE DATOS: EMPLEADOS ACTIVOS

Responsable de la seguridad de las bases de datos físicos:

- Cargo: SUBDIRECTOR ADMINISTRATIVO Y FINANCIERO
- Nombre: CARLOS MARIO GARCES DIAZ
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 71.670.120

Responsable de la seguridad de las bases de datos sistematizada:

- Cargo: PROFESIONAL EN SISTEMAS
- Nombre: ANDRES FELIPE DOMINGUEZ RENDON
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 1.037.594.043

BASES DE DATOS: BECARIOS

Responsable de la seguridad de las bases de datos físicos:

- Cargo: SUBDIRECTOR ADMINISTRATIVO Y FINANCIERO
- Nombre: CARLOS MARIO GARCES DIAZ
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 71.670.120

Responsable de la seguridad de las bases de datos sistematizada:

- Cargo: PROFESIONAL EN SISTEMAS
- Nombre: ANDRES FELIPE DOMINGUEZ RENDON
- Tipo de Documento: Cédula de ciudadanía

- Número de Documento: 1.037.594.043

BASES DE DATOS: JUNTA DIRECTIVA

Responsable de la seguridad de las bases de datos físicos:

- Cargo: DIRECTORA EJECUTIVA
- Nombre: LICETH KARINE MENESES YARURO
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 1.128.415.272

Responsable de la seguridad de las bases de datos sistematizada:

NO APLICA

BASES DE DATOS: CONTRATISTA Y PROVEEDORES ACTIVOS Y NO ACTIVOS

Responsable de la seguridad de las bases de datos físicos:

- Cargo: SUBDIRECTOR ADMINISTRATIVO Y FINANCIERO
- Nombre: CARLOS MARIO GARCES DIAZ
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 71.670.120

Responsable de la seguridad de las bases de datos sistematizada:

- Cargo: PROFESIONAL EN SISTEMAS
- Nombre: ANDRES FELIPE DOMINGUEZ RENDON
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 1.037.594.043

BASES DE DATOS: CORPORADOS

Responsable de la seguridad de las bases de datos físicos:

- Cargo: DIRECTORA EJECUTIVA
- Nombre: LICETH KARINE MENESES YARURO

- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 1.128.415.272

Responsable de la seguridad de las bases de datos sistematizada:

NO APLICA

BASES DE DATOS: POSTULANTES BECARIOS

Responsable de la seguridad de las bases de datos físicos:

NO APLICA

Responsable de la seguridad de las bases de datos sistematizada:

- Cargo: PROFESIONAL EN SISTEMAS
- Nombre: ANDRES FELIPE DOMINGUEZ RENDON
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 1.037.594.043

BASES DE DATOS: CAPACITACIONES Y EVENTOS

Responsable de la seguridad de las bases de datos físicos:

- Cargo: SUBDIRECTORA TÉCNICA
- Nombre: SANDRA PAOLA NOHAVA BRAVO
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 43263680

Responsable de la seguridad de las bases de datos sistematizada:

- Cargo: PROFESIONAL EN SISTEMAS
- Nombre: ANDRES FELIPE DOMINGUEZ RENDON
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 1.037.594.043

BASES DE DATOS: EMPLEADOS INACTIVOS

Responsable de la seguridad de las bases de datos físicos:

- Cargo: SUBDIRECTOR ADMINISTRATIVO Y FINANCIERO
- Nombre: CARLOS MARIO GARCES DIAZ
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 71.670.120

Responsable de la seguridad de las bases de datos sistematizada:

- Cargo: PROFESIONAL EN SISTEMAS
- Nombre: ANDRES FELIPE DOMINGUEZ RENDON
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 1.037.594.043

BASES DE DATOS: ALIADOS ESTRATEGICOS

Responsable de la seguridad de las bases de datos físicos:

- Cargo: SUBDIRECTOR ADMINISTRATIVO Y FINANCIERO
- Nombre: CARLOS MARIO GARCES DIAZ
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 71.670.120

Responsable de la seguridad de las bases de datos sistematizada:

- Cargo: SUBDIRECTOR ADMINISTRATIVO Y FINANCIERO
- Nombre: CARLOS MARIO GARCES DIAZ
- Tipo de Documento: Cédula de ciudadanía
- Número de Documento: 71.670.120