



GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO						
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025	
				Página:	1 de 13	

TABLA DE CONTENIDO

1.	BASE LEGAL Y ÁMBITO DE APLICACIÓN	2
2.	DEFINICIONES.....	3
3.	PRINCIPIOS DE LA PROTECCIÓN DE DATOS.....	4
4.	CATEGORÍAS ESPECIALES DE DATOS.....	6
4.1.	Datos sensibles	6
4.2.	Derechos de los niños, niñas y adolescentes	6
5.	FUNCIONES Y OBLIGACIONES	7
5.1.	Responsable del tratamiento	7
5.2.	Funciones del oficial de protección de datos	8
5.3.	Responsables de administrar las bases de datos	10
5.4.	Usuarios	10

GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>	
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO							
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025		
						Página:	2 de 13

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 en el Decreto 1377 de 2013, por el cual se reglamenta parcialmente la Ley anterior y compilado en 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 *PO-DE-01 Política de tratamiento de datos personales* y en el *AA-DE-02 Manual de Sistema de Seguridad de la Información*; y deben cumplir con las obligaciones en materia de seguridad de los datos correspondientes a sus funciones y cargo.

Para velar con el cumplimiento de sus obligaciones de seguridad, la COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CRÉDITO “COONFIE” nombra o designa colaboradores responsables de la seguridad de la información y encargados de desarrollar, coordinar, controlar y verificar el cumplimiento de las medidas de seguridad recogidas en el *AA-DE-02 Manual de Sistema de Seguridad de la Información*.

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 COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CRÉDITO “COONFIE”.


Todos los usuarios o colaboradores están obligados a cumplir con las medidas de seguridad establecidas para el tratamiento de los datos en el documento *AA-DE-02 Manual de Sistema de Seguridad de la Información* y están sujetos al deber de confidencialidad, incluso después de acabada su relación laboral o profesional con la organización o empresa 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.

GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO						
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025	
				Página:	3 de 13	

2. DEFINICIONES

Establecidas en el artículo 3 de la Ley 1581 de 2012 y el artículo 2.2.2.25.1.3 Decreto 1074 de 2015 (artículo 3 del Decreto 1377 de 2013):

- **Autorización:** Consentimiento previo, expreso e informado del Titular para llevar a cabo el tratamiento de datos personales.
- **Base de Datos:** Conjunto organizado de datos personales que sea objeto de tratamiento.
- **Dato personal:** Cualquier información vinculada o que pueda asociarse a una o varias personas naturales determinadas o determinables.
- **Dato público:** Es el dato que no sea semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.
- **Dato Privado:** Es un dato personal que por su naturaleza íntima o reservada solo interesa a su titular y para su tratamiento requiere de su autorización previa, informada y expresa. Bases de datos que contengan datos como números telefónicos y correos electrónicos personales; datos laborales, sobre infracciones administrativas o penales, administrados por administraciones tributarias, entidades financieras y entidades gestoras y servicios comunes de la Seguridad Social, bases de datos sobre solvencia patrimonial o de crédito, bases de datos con información suficiente para evaluar la personalidad del titular, bases de datos de los responsables de operadores que presten servicios de comunicación electrónica.
- **Dato Semiprivado:** Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no solo a su titular sino a cierto sector o grupo de personas o a la sociedad en general, como son: Bases de datos que contengan Información financiera, crediticia, comercial, de servicios y la proveniente de terceros países.
- **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.

GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO						
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025	
				Página:	4 de 13	


- **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.
- **Usuario:** Persona natural o jurídica con un vínculo laboral o contractual con el Responsable y que por sus funciones o relación comercial tiene acceso o trata los datos contenidos en las bases de datos.

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 en las demás disposiciones que la desarrollen. De acuerdo con la Corte Constitucional en virtud del principio de legalidad el Titular tiene derecho a que sus datos sean tratados de conformidad con los límites establecidos en la normatividad vigente y en especial a tomar acciones cuando su Tratamiento esté expresamente prohibido¹.
- **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 de manera clara y expresa. Ello implica que los datos de carácter personal únicamente pueden recolectarse para un fin necesario y determinado que justifique el uso de los mismos sin que se rompa el equilibrio entre el interés del Responsable y el Titular.
- **Principio de libertad:** Los Titulares de los datos tienen la potestad de autorizar o no el uso de sus datos personales, por tanto, el uso y/o tratamiento de los datos solo puede ejercerse con el consentimiento previo, expreso e informado del Titular, con lo cual, se prohíbe el uso de autorizaciones con finalidades abiertas, no específicas o de un consentimiento tácito del Titular.

¹ Corte Constitucional. Sentencia C - 748 de 2011. M.P. Jorge Ignacio Pretelt Chaljub

GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO						
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025	
				Página:	5 de 13	

Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento.

- **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:** El Responsable del tratamiento o el Encargado del tratamiento deben garantizarle al Titular de los datos el derecho a obtener en cualquier momento y sin restricciones, información acerca de la existencia de los datos que le conciernen. En el momento de solicitar la autorización al Titular, se informa 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 de todo el 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 las Prácticas Generales de Seguridad de la Información, 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

GESTIÓN ADMINISTRATIVA							
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO							
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025		
						Página:	6 de 13

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

El Usuario o colaborador deberá tener en cuenta el alcance de los datos sensibles como aquellos que afectan la intimidad del Titular o cuyo uso indebido puede generar 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.


El Usuario o colaborador tendrá en cuenta en el uso de datos sensibles, lo indicado en 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 Usuario o colaborador deberá tener en cuenta en el tratamiento de datos personales de niños, niñas y adolescentes sus prohibiciones, 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.

GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>	
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO							
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025		
						Página:	7 de 13

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

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

Todo responsable y encargado involucrado en el tratamiento de los datos personales de niños, niñas y adolescentes, deberá velar por el uso adecuado de los mismos, cumpliendo en todo momento con los principios y obligaciones recogidos en la LEPD y el Decreto 1377 de 2013 compilado en el Capítulo 25 del 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 Y OBLIGACIONES

5.1. Responsable del tratamiento

El Usuario o colaborador deberá tener en cuenta los deberes de COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CREDITO "COONFIE" como Responsable del Tratamiento, sin perjuicio de las demás disposiciones previstas en el marco legal que rige la protección de datos personales. En todo caso, deberá conocer y coadyuvar en el cumplimiento de las siguientes obligaciones:

1. Garantizar al Titular, en todo tiempo, el pleno y efectivo ejercicio del derecho de hábeas data.
2. Solicitar y conservar, en las condiciones previstas en la presente ley, copia de la respectiva autorización otorgada por el Titular.
3. Informar debidamente al Titular sobre la finalidad de la recolección y los derechos que le asisten por virtud de la autorización otorgada.
4. Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.
5. Garantizar que la información que se suministre al Encargado del Tratamiento sea veraz, completa, exacta, actualizada, comprobable y comprensible.
6. Actualizar la información, comunicando de forma oportuna al Encargado del Tratamiento, todas las novedades respecto de los datos que previamente le haya suministrado y adoptar las demás medidas necesarias para que la información suministrada a este se mantenga actualizada.
7. Rectificar la información cuando sea incorrecta y comunicar lo pertinente al Encargado del Tratamiento.


GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO						
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025	
				Página:	8 de 13	

8. Suministrar al Encargado del Tratamiento, según el caso, únicamente datos cuyo Tratamiento esté previamente autorizado de conformidad con lo previsto en la presente ley.
9. Exigir al Encargado del Tratamiento en todo momento, el respeto a las condiciones de seguridad y privacidad de la información del Titular.
10. Tramitar las consultas y reclamos formulados en los términos señalados en la ley y en la política.
11. Adoptar un manual interno de políticas y procedimientos para garantizar el adecuado cumplimiento de la ley y en especial, para la atención de consultas y reclamos.
12. Informar al Encargado del Tratamiento cuando determinada información se encuentra en discusión por parte del Titular, una vez se haya presentado la reclamación y no haya finalizado el trámite respectivo.
13. Informar a solicitud del Titular sobre el uso dado a sus datos.
14. Informar a la autoridad de protección de datos cuando se presenten violaciones a los códigos de seguridad y existan riesgos en la administración de la información de los Titulares.
15. Cumplir las instrucciones y requerimientos que imparta la Superintendencia de Industria y Comercio.

5.2. Funciones del oficial de protección de datos

El Usuario o colaborador tendrá en cuenta las siguientes funciones del Oficial de Protección de Datos Personales de COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CREDITO "COONFIE", para acudir en caso de requerirlo:


1. Ejecutar en las distintas áreas de la organización el Programa Integral de Protección de Datos Personales.
2. Realizar seguimiento y control al Programa Integral de Protección de Datos Personales.
3. Realizar las gestiones para mantener actualizadas las políticas y estrategias necesarias para generar una cultura de protección de datos dentro de la organización.
4. Coordinar la implementación del programa de protección de datos con los procesos que faciliten la documentación e inventario de las bases de datos en poder de la organización.
5. Responder por el registro de las bases de datos de la organización en el Registro Nacional de Bases de Datos y mantenerlo actualizado, atendiendo a las políticas internas y a la normatividad expedida por la Superintendencia de Industria y Comercio o cualquier entidad que así lo requiera.
6. Gestionar ante la Superintendencia de Industria y Comercio las declaraciones de conformidad de la organización, cuando sea del caso.
7. Coordinar y hacer seguimiento, a un plan de capacitación en Protección de Datos personales que garantice el conocimiento por parte de los empleados y colaboradores de la organización de dicha normatividad.
8. Gestionar el cumplimiento de los planes de auditoría interna para verificar el cumplimiento del Programa de Protección de datos personales.
9. Acompañar y asesorar a la organización en la atención de las visitas y los requerimientos que realice la Superintendencia de Industria y Comercio y otras entidades públicas relacionadas con protección de datos personales.

GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO						
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025	
				Página:	9 de 13	

10. Coordinar el comité de Habeas Data o área responsable y someter a aprobación de dicho comité las modificaciones o ajustes al programa integral de protección de datos personales, así como los asuntos que por su complejidad o impacto deban ser resueltos en dicho comité.
11. Asesorar y conceptuar sobre los asuntos relacionados con manejo de información de la organización en la clasificación de pública y privada a fin de garantizar el cumplimiento de habeas data.
12. Asesorar al comité o área responsable de manejo de datos de terceros en cuanto a los temas relacionados con protección de datos personales.
13. Asesorar y conceptuar sobre asuntos relacionados con acceso a la información pública de acuerdo con la ley de transparencia.
14. Asesorar y conceptuar sobre los resultados de consultas a listas restrictivas.
15. Demás asuntos relacionados con la protección y respeto del derecho de protección de datos funciones asignadas por su Jefe Inmediato.

De otra parte, el Oficial de Protección de Datos de acuerdo con la Guía de Responsabilidad Demostrada coordinará con los Administradores de bases de datos la implementación de buenas prácticas en la gestión de datos personales y administración del programa que le permita cumplir las normas sobre protección de datos personales, así como, establecer los controles al mismo, su evaluación y revisión. 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.

GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO						
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025	
				Página:	10 de 13	

5.3. Responsables de administrar las bases de datos


El Usuario o colaborador tendrá en cuenta el rol que cumplen los responsables de administrar las bases de datos señaladas en el "**DA-DE-01 Organización Bases de Datos**" y acatará las instrucciones que le sean impartidas en concordancia con las siguientes funciones:

1. Coordinar y controlar la implantación de las medidas de seguridad, y colaborar con el responsable del tratamiento en la difusión del *AA-DE-02 Manual de Sistema de Seguridad de la Información*.
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. Controlar los permisos de acceso a los datos por parte de los usuarios autorizados identificados en el *AA-DE-02 Manual de Sistema de Seguridad de la Información*.
4. Reportar 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 del *AA-DE-02 Manual de Sistema de Seguridad de la Información* 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.
9. Informar semestralmente al oficial de protección de datos personales, las modificaciones de la base de datos a su cargo, para efectos de que el oficial de protección de datos pueda proceder con la actualización en el RNBD.
10. Gestionar y administrar los soportes de los consentimientos obtenidos de los Titulares de la base de datos a su cargo.
11. Coordinar y verificar la calidad de los Titulares de las consultas y reclamos relacionados con la base de datos a su cargo.

5.4. Usuarios

COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CREDITO "COONFIE" consciente de la importancia del adecuado tratamiento de los datos por parte de todas las personas que intervienen en el almacenamiento, tratamiento, consulta o cualquier otra actividad relacionada con los datos personales y sistemas de información establece de conformidad con las funciones y obligaciones recogidas en la relación contractual, los siguientes criterios que deberán cumplir a partir de la expedición de este documento.

COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CREDITO "COONFIE" cumple con el deber de información con la inclusión de acuerdos de confidencialidad y deber de secreto suscritos con los


GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO						
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025	
				Página:	11 de 13	

colaboradores y los usuarios de sistemas de identificación sobre bases de datos y sistemas de información, y mediante una circular informativa dirigida a los mismos sobre el contenido del presente documento.

Las funciones y obligaciones del personal de COOPERATIVA NACIONAL EDUCATIVA DE AHORRO Y CREDITO "COONFIE" se definen, con carácter general, según el tipo de actividad que desarrollan dentro de la organización y, específicamente, por el contenido de este Manual. Los usuarios y perfiles con acceso a los recursos protegidos, tales como, documentos o soportes que contienen datos personales tienen el deber de custodiarlos, así como de vigilar y controlar que personas no autorizadas puedan tener acceso a ellos y el incumplimiento de las obligaciones y medidas de seguridad establecidas será sancionable de acuerdo con la normativa aplicable a la relación jurídica existente entre el empleado y la organización.

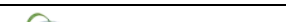
A continuación, se establecen las funciones y obligaciones principales sobre el tratamiento de las bases de datos personales bajo responsabilidad directa o indirecta de los colaboradores y/o usuarios:

- **Deber de secreto:** Aplica a todas las personas que, en el desarrollo de su profesión o trabajo, acceden a bases de datos personales y vincula tanto a usuarios como a prestadores de servicios contratados. En cumplimiento de este deber, los usuarios de la empresa u organización no pueden comunicar o relevar a terceras personas, datos que manejen o de los que tengan conocimiento en el desempeño o cargo de sus funciones, y deben velar por la confidencialidad e integridad de los mismos.
- **Funciones de control y autorizaciones delegadas:** El responsable del tratamiento puede delegar el tratamiento de datos a terceros, para que actúe como encargado del tratamiento, mediante un contrato de transmisión de datos.
- **Obligación de gestionar consentimientos de los Titulares de los datos:** Los datos de los Titulares de los datos solo podrán ser usados previa autorización del Titular, por lo tanto, a falta de esta no podrán ser utilizados en nombre del Responsable.
- **Obligaciones relacionadas con las medidas de seguridad implantadas:** Únicamente se debe acceder a las bases de datos con la debida autorización y cuando sea necesario para el ejercicio de sus funciones.
 - No revelar información a terceras personas ni a usuarios no autorizados.
 - Observar las normas de seguridad y trabajar para mejorarlas.
 - No realizar acciones que supongan un peligro para la seguridad de la información.
 - No sacar información de las instalaciones de la organización sin la debida autorización.
- **Uso de recursos y materiales de trabajo:** Debe estar orientado al ejercicio de las funciones asignadas. No se autoriza el uso de estos recursos y materiales para fines personales o ajenos a las tareas correspondientes al puesto de trabajo. Cuando, por motivos justificados de trabajo, sea necesaria la salida de dispositivos periféricos o extraíbles, deberá comunicarse al responsable de seguridad correspondiente que podrá autorizarla y, en su caso, registrarla.
- **Uso de impresoras, escáneres y otros dispositivos de copia:** Cuando se utilicen este tipo

GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO						
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025	
Página:		12 de 13				

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 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, etc.
- **Deber de custodia de los soportes utilizados:** Obliga al usuario autorizado a vigilar y controlar que personas no autorizadas accedan a la información contenida en los soportes. Los soportes que contienen bases de datos físicas deben identificar el tipo de información que contienen según el tipo de datos (confidencial, reservado o pública clasificada) mediante un sistema de etiquetado y ser inventariados. Cuando la información esté clasificada con nivel de seguridad sensible, el sistema de etiquetado solo debe ser comprensible para los usuarios autorizados a acceder a dicha información.
- **Responsabilidad sobre los terminales de trabajo y portátiles:** Cada usuario es responsable de su propio terminal de trabajo; cuando esté ausente de su puesto, debe bloquear dicho terminal (ej. protector de pantalla con contraseña) para impedir la visualización o el acceso a la información que contiene; y tiene el deber de apagar el terminal al finalizar la jornada laboral. Asimismo, los ordenadores portátiles han de estar controlados en todo momento para evitar su pérdida o sustracción.
- **Uso limitado de Internet y correo electrónico:** El envío de información por vía electrónica y el uso de Internet por parte del personal está limitado al desempeño de sus actividades en la organización.
- **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 empresa.
- **Deber de archivo y gestión de documentos y soportes:** Los documentos y soportes deben de ser debidamente archivados con las medidas de seguridad recogidas en el *PO-DE-01 Política de tratamiento de datos personales* y en el *AA-DE-02 Manual de Sistema de Seguridad de la Información*
- **Capacitaciones:** Asistir puntualmente y participar en las capacitaciones impartidas por el Responsable expresando las inquietudes a las que hubiere lugar para el adecuado uso de los datos personales.

GESTIÓN ADMINISTRATIVA						 Coonfie <i>Es Presente y Futuro Solidario</i>	
MANUAL DE SEGURIDAD EN PDP AL FUNCIONARIO							
Código:	MA-DE-01	Versión:	1	Vigencia:	28 de julio de 2025		
						Página:	13 de 13

CONTROL DE CAMBIOS		
La trazabilidad de los cambios generados en el documento podrá ser consultada en el Listado Maestro de Documentos.		
Versión	Descripción Del Cambio	Fecha de Aprobación
1	Elaboración inicial del documento	28 de julio de 2025
Elaborado Por:		Revisado Por:
YULIANA KARIME OSORIO ACHIPIZ Cargo: Coordinadora de PDP		SERGIO ALEJANDRO CUÉLLAR CARDONA Cargo: Coordinador de PL y SIG
		Aprobado Por:
		NÉSTOR BONILLA RAMÍREZ Cargo: Gerente General