POLÍTICA DE PROTECCIÓN DE DATOS PERSONALES

Versión: 09/10/2022

Responsable: Legal & Regulatory

Aprobado por: Valeria Plastino

Entrada en vigor: 1 / 04 /2016

Contacto:

byron.pabon@cirion technologies.com

Octubre 2022

ÍNDICE

1. INTRODUCCIÓN

Esta **Política de Protección de Datos Personales** (la "Política") ha sido desarrollada a los efectos de garantizar el cumplimiento de la normativa vigente en materia de protección de datos personales.[1]

Este documento está basado en determinados criterios del Estándar Internacional ISO/IEC 27002, como marco de referencia.

El presente documento tiene por objeto cumplir, por un lado, con el artículo 48, fracción I del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (el "Reglamento de la LFPD"), en el que se prevé que el Responsable podrá adoptar políticas de privacidad obligatorias y exigibles al interior de su organización como medida para garantizar el debido tratamiento de los datos personales, privilegiando los intereses del titular y la expectativa razonable de privacidad.

Asimismo, tiene por objeto cumplir con el artículo 61, fracción II en relación con el artículo 2, fracción V, también del Reglamento de la LFPD; en donde de forma clara y concisa se indica que el Responsable deberá adoptar las medidas organizativas necesarias para que el personal conozca las normas de seguridad en materia de protección de datos personales que afecten al desarrollo de sus funciones, así como las consecuencias en que pudiera incurrir en caso de incumplimiento.

Además, contiene la regulación de las condiciones organizativas de las bases de datos que tratan datos personales en posesión de **CIRION TECHNOLOGIES MÉXICO, S. R. L. y CIRION TECHNOLOGIES MEXICO II, S. DE R.L. DE C.V.** (en adelante y conjuntamente, "**CIRION**"), existentes en la actualidad o que puedan crearse en el futuro; así como de las condiciones para la obtención de dichos datos personales, la entrega y transferencia de los datos a un tercero y los procedimientos a seguir para atender solicitudes relativas al ejercicio de los derechos de acceso, rectificación, cancelación y oposición de los datos por los titulares (derechos ARCO) y de revocación del consentimiento.

Se determinarán los Responsables Funcionales y los Responsables Operativos (ANEXO SEGUNDO) de cada base de datos, señalando las condiciones de seguridad del entorno, programas y equipos, el uso de los datos y los procedimientos de autorización para accesos.

Esta Política es de aplicación a la obtención y tratamiento de los datos personales que figuren en bases de datos en posesión de **CIRION**, así como a toda modalidad de uso posterior, incluso no automatizada, de datos personales registrados en soportes físicos susceptibles de tratamiento automatizado, no automatizado o mixto.

Quedan exceptuados de la aplicación de esta política:

- Las bases de datos relativas a personas morales (sociedades anónimas, fundaciones, asociaciones, y otros tipos de personas jurídicas),

[1] Dicha normativa comprende, entre otras, las siguientes disposiciones: (i) Ley Federal de Protección de Datos Personales en Posesión de los Particulares ("LFPD"); (ii) Reglamento de la LFPD; (iii) Lineamientos del Aviso de Privacidad; (iv) RECOMENDACIONES en materia de seguridad de datos personales; (v) Modelo de Aviso de Privacidad Corto para Video-Vigilancia publicado por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (INAI, antes IFAI), y (vi) Recomendaciones aplicables emitidas por el INAI.

- Las bases de datos de información tecnológica o comercial que reproduzcan datos ya publicados en diarios oficiales u otras publicaciones oficiales,
- Las bases de datos mantenidas por personas físicas en el ejercicio de sus actividades exclusivamente personales o domésticas.

1.1. Alcance

El presente documento define y documenta las funciones y obligaciones de cada una de las partes que accedan a bases de datos con tratamiento automatizado o no automatizado de datos personales.

Este documento afecta a todas las Áreas de **CIRION** y, en particular, a aquéllas que intervienen en la obtención, tratamiento y entrega de datos personales obrantes en bases de datos automatizadas y no automatizadas en **CIRION**, así como a los directivos titulares de dichas Áreas, como Responsables Funcionales de las Bases de Datos, al Responsable, al Departamento de Datos de Personales de la organización, y al personal autorizado para acceder a los mismos (personal descrito en el ANEXO SEGUNDO de la presente Política)

Se recomienda facilitar este documento a cada una de estas personas a través de un correo electrónico personalizado y con acuse de recibo en donde se expondrá la obligación de su lectura y el cumplimiento de las medidas reflejadas.

El incumplimiento de las directrices, principios y obligaciones definidas en la presente Política puede ser motivo de rescisión de la relación de trabajo, por desobediencia relacionada con el trabajo contratado o por dar a conocer asuntos de carácter reservado, con perjuicio de la empresa (artículo 47 de la Ley Federal del Trabajo) y demás medias que CIRION considere pertinentes.

La presente normativa incorpora una serie de modelos de cláusulas, contratos e impresos, que deben ser considerados orientativos. Antes de ser usados y/o implementados deberán contar con la autorización del **Departamento de Datos Personales de CIRION, en la persona del funcionario encargado según el área de que se trate**.

2. OBTENCIÓN, UTILIZACIÓN, CONSERVACIÓN Y CANCELACIÓN DE DATOS PERSONALES

La obtención de los datos personales, así como su uso, tratamiento automatizado y no automatizado, conservación, cancelación, bloqueo y supresión deberá realizarse en **CIRION** con sujeción a lo dispuesto en los apartados siguientes.

2.1. Obtención de los datos personales

La obtención de datos personales se realizará con fines determinados, explícitos y legítimos.

Los datos a recoger deben ser necesarios, adecuados y relevantes en relación con el ámbito y los fines para los que se han obtenido, no pudiendo obtenerse por medios fraudulentos, desleales o ilícitos y apegándose en todo momento a la presente política, así como a las políticas globales de **CIRION**.

La obtención de datos puede realizarse recabándolos personal o directamente del propio titular, o a través de terceros o de fuentes de acceso público (obtención indirecta). La obtención de datos personales origina el nacimiento del derecho de sus titulares a la información preceptiva que se indica en el siguiente apartado.

El hecho de que los datos personales sean tratados posteriormente con fines históricos, estadísticos y/o científicos, no se considerará incompatible con la finalidad que originó su obtención.

CIRION está obligado a mantener datos personales exactos y actualizados, de forma que respondan con veracidad a la situación actual de sus titulares, debiendo cancelar dichos datos una vez que hayan dejado de ser necesarios o pertinentes para las finalidades para las cuales hubieran sido recabados; respetando en todo momento los posibles plazos legales de conservación de la información establecidos disposiciones legales distintas a la normativa de protección de datos personales.

2.1.1. El derecho de información en la obtención de datos personales

Conforme a la normativa vigente – adicional a la Ley Federal de Protección de Datos Personales en Posesión de los Particulares (la LFPD) y su Reglamento – denominada "*Lineamientos del Aviso de Privacidad*", **CIRION** debe facilitar a los titulares de datos personales que trata para finalidades determinadas, la siguiente información, a través de los Avisos de Privacidad correspondientes (revisados y aprobados por el Área Legal:

1. La identidad y domicilio del responsable que trata los datos personales;

2. Los datos personales que serán sometidos a tratamiento;

3. En su caso, el señalamiento expreso de los datos personales sensibles que se tratarán;

4. Las finalidades del tratamiento;

5. Los mecanismos para que el titular pueda manifestar su negativa para el tratamiento de sus datos personales para aquellas finalidades que no son necesarias, ni hayan dado origen a la relación jurídica con el responsable;

6. Las transferencias de datos personales que, en su caso, se efectúen; el tercero receptor de los datos personales, y las finalidades de las mismas;

7. La cláusula que indique si el titular acepta o no la transferencia, cuando así se requiera;

8. Los medios y el procedimiento para ejercer los derechos ARCO;

9. Los mecanismos y procedimientos para que, en su caso, el titular pueda revocar su consentimiento al tratamiento de sus datos personales;

10. Las opciones y medios que el responsable ofrece al titular para limitar el uso o divulgación de los datos personales;

11. La información sobre el uso de mecanismos en medios remotos o locales de comunicación electrónica, óptica u otra tecnología, que permitan recabar datos personales de manera automática y simultánea al tiempo que el titular hace contacto con los mismos, en su caso, y

12. Los procedimientos y medios a través de los cuales el responsable comunicará a los titulares los cambios al aviso de privacidad.

Cuando los datos personales sean obtenidos **de manera indirecta** del titular, el responsable deberá observar lo siguiente para la puesta a disposición del Aviso de Privacidad correspondiente:

1. Cuando los datos personales sean tratados para una finalidad prevista en una transferencia consentida o se hayan obtenido de una fuente de acceso público, **CIRION** dará a conocer el Aviso de Privacidad respectivo **en el primer contacto que se tenga con el titular**, o

2. Si **CIRION** pretende utilizar los datos para una finalidad distinta a la originalmente consentida, es decir, vaya a tener lugar un cambio de finalidad, el Aviso de Privacidad deberá darse a conocer antes de realizar el aprovechamiento de dichos datos personales.

Si el Aviso de Privacidad no se hace del conocimiento del titular de manera directa o personal, el titular tendrá un plazo de cinco días (contados a partir de la fecha en que se haya puesto a su disposición el Aviso de Privacidad) para que, de ser el caso, manifieste su negativa para el tratamiento de sus datos personales para las finalidades que sean distintas a aquéllas que son necesarias y den origen a la relación jurídica entre el responsable y el titular**. Si el titular no manifiesta su negativa para el tratamiento de sus datos de conformidad con lo anterior, se entenderá que ha otorgado su consentimiento para el tratamiento de los mismos, salvo prueba en contrario**.

No será necesario informar directamente a los titulares en el supuesto anterior, cuando resulte imposible dar a conocer el Aviso de Privacidad al titular o exija esfuerzos que vayan más allá de lo razonable, en consideración del número de titulares, o a la antigüedad de los datos.

En estos casos, **CIRION** podrá instrumentar **medidas compensatorias** de comunicación masiva de acuerdo con los criterios generales expedidos por el Instituto Nacional de Transparencia, Acceso a la Información y Protección de Datos Personales (**INAI)** (*antiguo IFAI*) y publicados en el Diario Oficial de la Federación el pasado 18 de abril de 2012, y demás órganos o normativas que sean aplicables, bajo los cuales podrán utilizarse los medios que se establecen en el artículo 35 del Reglamento de la LFPD.

Los casos que no actualicen los criterios generales emitidos por el INAI requerirán la autorización expresa de este Instituto, previo a la instrumentación de la medida compensatoria correspondiente.

En el supuesto de querer recurrir a medidas compensatorias con motivo de la imposibilidad de dar a conocer el Aviso de Privacidad o por requerir esta acción un esfuerzo desproporcionado, el Área captadora de los datos lo pondrá en conocimiento del Departamento de Datos Personales para coordinar el inicio del procedimiento a que se refieren los artículos 33 y 34 del Reglamento de la LFPD.

El Área captadora de la información deberá presentar al Departamento de Datos Personales las causas o justificación de la imposibilidad de dar a conocer el aviso de privacidad a los titulares o el esfuerzo

desproporcionado que esto exige. Se deberá también recabar información relativa al número de titulares afectados, antigüedad de los datos, si existe o no contacto directo con los titulares, y la capacidad económica de **CIRION** con el fin de determinar qué medios puede utilizar como alternativas para difundir el aviso de privacidad correspondiente.

Adicionalmente, deberá recabarse la siguiente información/documentación:

a) Tratamiento al que pretende aplicar la medida compensatoria y sus características principales, tales como finalidad; tipo de datos personales tratados; si se efectúan transferencias; particularidades de los titulares, entre ellas edad, ubicación geográfica, nivel educativo y socioeconómico, entre otros;

b) Tipo de medida compensatoria que se pretende aplicar y por qué periodo la publicaría;

c) Texto propuesto para la medida compensatoria, y

d) Cualesquiera otros documentos que **CIRION** considere necesarios presentar ante el INAI.

El Reglamento de la LFPD prevé los siguientes medios para la publicación de los Avisos de Privacidad que se den a conocer como medida compensatoria a la comunicación directa de los mismos a los titulares:

1. Diarios de circulación nacional;

2. Diarios locales o revistas especializadas, cuando se demuestre que los titulares de los datos personales residan en una determinada entidad federativa o pertenezcan a una determinada actividad;

3. Página de Internet del responsable;

4. Hiperenlaces o hipervínculos situados en una página de Internet del Instituto, habilitados para dicho fin, cuando el responsable no cuente con una página de Internet propia;

5. Carteles informativos;

6. Difusión en cápsulas informativas en radiodifusoras, o

7. Otros medios alternos de comunicación masiva.

Dada la diversa cantidad de supuestos que puede suponer la decisión de optar por medidas compensatorias, el Departamento de Datos Personales, en coordinación con el Área captadora de los datos deberán definir caso por caso el escrito que dé inicio al procedimiento para la autorización de este tipo de medidas y dejar evidencia de que se discutió la medida compensatoria, proporcionando los argumentos que llevaron a esa decisión.

2.1.2. Requisitos internos previos para la obtención de datos personales

Cualquier Área Gerencial o de Dirección que vaya a proceder a recabar datos personales a través de cualquier medio: electrónicamente, contractualmente, a través de medios impresos o formularios, telefónicamente, etc., deberá someter la captación de dichos datos a las directrices aquí expuestas.

Con el objeto de vigilar internamente que se cumpla el deber de información en la obtención de los datos personales, se describe el siguiente **procedimiento interno**:

a) Cuando el titular de cualquier Área de **CIRION** (que asume internamente y a efectos de la presente Política el carácter de Responsable Funcional) decida emprender actos, campañas o cualesquiera actos que vayan a significar, entre otros, la obtención de datos personales de cualquier persona física, deberá notificar al Departamento de Datos Personales sobre la siguiente información:

1) Procedencia de la información.

2) Tipología de los datos personales.

3) Finalidades para las cuales se van a utilizar los datos.

4) Sistema de información en el que se procederá a tratar dicha información.

b) El Departamento de Datos Personales procederá a analizar la situación de hecho para redactar el o los correspondientes Avisos de Privacidad, que cumplan con las especificaciones descritas.

c) El Responsable Funcional de la Base de Datos implantará el o los Avisos de Privacidad dentro de su proceso de captación de datos (mediante su colocación en los medios que vayan a ser empleados para recabar datos personales), conforme a las instrucciones que obtenga del Departamento de Datos Personales.

El Responsable Funcional de la Base de Datos comunicará al Departamento de Datos Personales sobre esta nueva fuente de información y el sistema en el que procederá a tratar los datos, con el objeto de que el segundo analice si es necesario modificar la Relación de Medidas de Seguridad correspondiente y/o el Inventario de Bases de Datos y Sistemas de Información.

2.1.3. El consentimiento del titular para el tratamiento de sus datos personales

El tratamiento de datos personales requiere, como norma general, del consentimiento del titular, salvo que:

1. Esté previsto en una Ley;

2. Los datos figuren en fuentes de acceso público;

3. Los datos personales se sometan a un procedimiento previo de disociación;

4. Tenga el propósito de cumplir obligaciones derivadas de una relación jurídica entre el titular y el responsable;

5. Exista una situación de emergencia que potencialmente pueda dañar a un individuo en su persona o en sus bienes;

6. Sean indispensables para la atención médica, la prevención, diagnóstico, la prestación de asistencia sanitaria, tratamientos médicos o la gestión de servicios sanitarios, mientras el titular no esté en condiciones de otorgar el consentimiento, en los términos que establece la Ley General de Salud y demás disposiciones jurídicas aplicables y que dicho tratamiento de datos se realice por una persona sujeta al secreto profesional u obligación equivalente, o

7. Se dicte resolución de autoridad competente.

La obtención del consentimiento deberá ser:

- **Libre**: sin que medie error, mala fe, violencia o dolo, que puedan afectar la manifestación de voluntad del titular;
- **Específica**: referida a una o varias finalidades determinadas que justifiquen el tratamiento, e
- **Informada**: que el titular tenga conocimiento del aviso de privacidad previo al tratamiento a que serán sometidos sus datos personales y las consecuencias de otorgar su consentimiento.

El consentimiento expreso también deberá ser inequívoco, es decir, que existan elementos que de manera indubitable demuestren su otorgamiento.

En **CIRION**, los datos personales que se tratan proceden, en la gran mayoría de los casos, de una relación contractual existente con clientes, de empleados o candidatos a puestos de trabajo; y en menor medida de proveedores de servicios.

Ello acarrea que en la mayoría de los casos no sea necesaria la obtención del consentimiento expreso de los titulares para el tratamiento de sus datos personales por parte de **CIRION**, ya que dicho consentimiento se otorgaría de forma implícita en el momento en que el titular los proporciona y, previamente, ha tenido a su disposición el Aviso de Privacidad correspondiente. En su caso, y en aquellos casos enumerados anteriormente, el consentimiento para el tratamiento de los datos personales no sería siquiera necesario.

En este sentido, **es importante diferenciar entre la necesidad de obtener el consentimiento y la obligación de informar a los titulares sobre el tratamiento de sus datos, a través de Avisos de Privacidad. El primero, podrá no ser necesario en algunas ocasiones, pero la obligación de informar a los titulares sobre el tratamiento de sus datos, nunca puede dejar de cumplirse**.

Por otro lado, la legislación sobre protección de datos personales establece la obligación de obtener un **consentimiento expreso y por escrito** de los titulares cuando se recaben de éstos datos personales sensibles (que revelen ideología, afiliación sindical, religión, creencias, datos de salud, etc.)

En **CIRION** existe tratamiento de datos personales sensibles para finalidades específicas que justifican su recabo y procesamiento. En todo caso, es necesario subrayar que sólo se procederá a tratar este tipo de datos gestionando esta información con estricta confidencialidad y con las medidas de seguridad aplicables, y exclusivamente a efectos de cumplir con las **finalidades legítimas y justificadas** a que se refieran los Avisos de Privacidad que actualmente han sido emitidos, o que en el futuro sea necesario adoptar.

Los datos personales sensibles no podrán ser usados con fines discriminatorios, ni en perjuicio de ningún titular de los mismos.

Como regla general, **se prohíbe expresamente la creación de bases de datos que traten datos personales sensibles**, sin que se justifique la creación de las mismas para finalidades legítimas, concretas y acordes con las actividades o fines explícitos perseguidos por **CIRION**.

Cualquier duda o consulta sobre el tratamiento de datos personales sensibles deberá dirigirse al Departamento de Datos Personales de **CIRION**.

2.2. Conservación y cancelación de datos personales

Los datos deben conservarse de forma diligente y con las medidas de seguridad necesarias. La conservación diligente exige que los datos estén actualizados y que sean almacenados de forma que permitan el ejercicio de los **derechos ARCO** por parte del titular, debiendo durar el tiempo necesario para que se cumplan los fines para los cuales se recabaron y registraron.

Los plazos de conservación pueden depender, por una parte, de la relación jurídica existente entre **CIRION** y los titulares, en cuyo caso deberá mantenerse conservados, con carácter general, mientras subsista esta relación y una vez concluida como máximo, por los plazos siguientes:

- **Diez años** para los datos de clientes y proveedores, tratados en cualquier documentación relativa a la actividad de **CIRION** (cumplimiento de las disposiciones de los artículos 38 y 46 del Código de Comercio).
- **Cinco años** para la documentación relativa a la contabilidad de la empresa y para los Comprobantes Fiscales Digitales.

Por ello, el Responsable Funcional de la Base de Datos correspondiente debe proceder a eliminar los datos del sistema, una vez hayan vencido los plazos de conservación y aquéllos hayan dejado de ser útiles o pertinentes.

En todo caso, debe tomarse en cuenta que los plazos anteriormente indicados pueden variar en función de diversas circunstancias, como pueden ser el inicio de procedimientos judiciales o administrativos basados en la información contenida en la documentación genéricamente identificada.

La norma general al respecto, que establece actualmente el artículo 37 del Reglamento de la LFPD, es la siguiente:

> *Los plazos de conservación de los datos personales* ***no deberán exceder aquéllos que sean necesarios para el cumplimiento de las finalidades que justificaron el tratamiento****, y deberán atender las disposiciones aplicables a la materia de que se trate****, y tomar en cuenta los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información****. Una vez cumplida la o las finalidades del tratamiento, y cuando no exista disposición legal o reglamentaria que establezca lo contrario, el responsable deberá proceder a la cancelación de los datos en su posesión previo bloqueo de los mismos, para su posterior supresión.*

En otras palabras: **CIRION** no deberá conservar datos personales más allá del tiempo que sea necesario para el cumplimiento de las finalidades que justificaron su recabo, procesamiento, uso, aprovechamiento y conservación, incluyendo los períodos que sea necesario conservar dichos datos para acreditar el cumplimiento de obligaciones o cualesquiera otras relaciones jurídicas.

La LFPD establece que esta **CIRION**, en su calidad de responsable, procurará que los datos personales contenidos en las bases de datos sean pertinentes, correctos y actualizados para los fines para los cuales fueron recabados. Esta obligación de actualización recae sobre **CIRION** pero **será realizada por el Responsable Funcional de la Base de Datos** que requiera corregir o actualizar datos personales, y en especial en aquellos casos en que el titular de los datos ha ejercido su derecho de rectificación, definido más adelante.

La obligación de cancelación de los datos recae sobre el Responsable Funcional de la Base de Datos, quien de oficio cancelará los datos una vez haya finalizado el plazo de conservación, o a instancia del titular en ejercicio de su derecho de cancelación, definido más adelante.

No se procederá a la cancelación anteriormente referida, en cualquiera de los siguientes supuestos:

1. Se refiera a las partes de un contrato privado, social o administrativo y sean necesarios para su desarrollo y cumplimiento;

2. Deban ser tratados por disposición legal;

3. Obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas;

4. Sean necesarios para proteger los intereses jurídicamente tutelados del titular;

5. Sean necesarios para realizar una acción en función del interés público;

6. Sean necesarios para cumplir con una obligación legalmente adquirida por el titular, y

7. Sean objeto de tratamiento para la prevención o para el diagnóstico médico o la gestión de servicios de salud, siempre que dicho tratamiento se realice por un profesional de la salud sujeto a un deber de secreto.

Cualquier duda o consulta sobre la cancelación de datos personales en las bases de datos de **CIRION** deberá dirigirse al Departamento de Datos Personales.

3. EJERCICIO DE LOS DERECHOS DE LOS TITULARES DE DATOS PERSONALES

Cuando las personas físicas titulares de los datos personales que son objeto de tratamiento por parte de **CIRION** ejerzan alguno de los derechos que les corresponden (relacionados a continuación), se actuará de acuerdo con el procedimiento establecido en el apartado 3.2 (Procedimiento de ejercicio de los derechos ARCO y plazos legales).

La atención de dichos derechos lleva implícito el cumplimiento de los plazos señalados en la LFPD y su Reglamento, que se identifican en la presente Política.

Cualquier duda respecto al alcance de los derechos ARCO o de las solicitudes sobre revocación del consentimiento, deberá dirigirse al Departamento de Datos Personales.

3.1. Derechos ARCO, revocación del consentimiento y limitación sobre el uso o divulgación de datos personales

Los derechos de los titulares reconocidos en nuestro ordenamiento jurídico, con relación al tratamiento de sus datos personales, son:

a) Derecho de Acceso:

Se refiere al derecho de los titulares para obtener información sobre sus datos personales en posesión del responsable, así como información relativa a las condiciones y generalidades del tratamiento.

b) Derecho de Rectificación:

Los titulares podrán solicitar, en todo momento, que el responsable rectifique sus datos personales que resulten ser inexactos o incompletos.

c) Derecho de Cancelación:

Los titulares podrán solicitar, en todo momento, la cancelación de los datos personales cuando consideren que su tratamiento ya no es necesario para las finalidades para las cuales fueron recabados en primer lugar, o cuando consideren que no están siendo tratados conforme a los principios y deberes que establece la LFPD y su Reglamento.

La cancelación procederá respecto de la totalidad de los datos personales del titular, contenidos en una base de datos del responsable, o de sólo una parte de ellos, según lo haya solicitado.

La cancelación implica el cese en el tratamiento por parte del responsable, a partir de un bloqueo de los mismos y su posterior supresión.

En el caso de que exista una obligación de conservación de los datos y se hubiere solicitado la cancelación conforme a derecho y por persona legitimada para hacerlo, los datos deberán ser conservados, pero se bloqueará el acceso a los mismos datos por el personal de **CIRION** y se evitará cualquier proceso ulterior de utilización.

En el apartado 2.2 se han indicado los casos en que no resulta procedente la cancelación de los datos, a pesar de haberlo solicitado en tiempo y forma el titular de los mismos.

d) Derecho de Oposición al tratamiento de datos personales

Los titulares podrán, en todo momento, oponerse al tratamiento de sus datos personales o exigir que se cese en el mismo cuando:

1. Exista causa legítima y su situación específica así lo requiera. En estos casos, deberá justificarse que aun siendo lícito el tratamiento, éste debe cesar para evitar que su persistencia cause un perjuicio al titular, o
2. Requiera manifestar su oposición para el tratamiento de sus datos personales a fin de que no se lleve a cabo el tratamiento para fines específicos.

No procederá el ejercicio del derecho de oposición en aquellos casos en los que el tratamiento sea necesario para el cumplimiento de una obligación legal impuesta al responsable.

e) Revocación del consentimiento:

En cualquier momento, el titular podrá revocar su consentimiento para el tratamiento de sus datos personales, para lo cual el responsable deberá establecer mecanismos sencillos y gratuitos, que permitan al titular revocar su consentimiento al menos por el mismo medio por el que lo otorgó, siempre y cuando no lo impida una disposición legal.

f) Limitación sobre el uso o divulgación de datos personales.

Los titulares puedes solicitar la limitación del uso o divulgación de sus datos personales por parte del responsable o de terceros, mediante su inclusión en listados de exclusión propios o comunes. En su caso, puede darse a conocer a los titulares la existencia de los Registros Públicos de Consumidores y de Usuarios que prevén la Ley Federal de Protección al Consumidor y la Ley de Protección y Defensa al Usuario de Servicios Financieros, respectivamente.

3.2. Procedimiento de ejercicio de los derechos ARCO y revocación del consentimiento. Plazos legales

El ejercicio de cualquiera de los derechos ARCO no excluye la posibilidad de ejercer alguno de los otros, ni puede constituir requisito previo para el ejercicio de cualquier otro de ellos. Las revocaciones del consentimiento para el tratamiento de datos personales deben tramitarse dentro de los mismos plazos legales aplicables para atender solicitudes de ejercicio de derechos ARCO.

La LFPD y su Reglamento reconocen a dos personas facultadas para ejercer los derechos ARCO:

a) Por el titular, previa acreditación de su identidad, a través de la presentación de copia de su documento de identificación.
b) Por el representante del titular, previa acreditación de su identidad, del titular al que representa y de la existencia de la representación.

Asimismo, el Reglamento de la LFPD establece que para el ejercicio de los derechos ARCO en relación con datos personales de menores de edad o de personas que se encuentren en estado de interdicción o incapacidad establecida por ley, se estará a las reglas de representación dispuestas en el Código Civil Federal.

En relación con las bases de datos de **CIRION**, se facilitará este ejercicio de acuerdo con el procedimiento que se establece a continuación.

3.2.1. Requisitos comunes al ejercicio de los derechos de Acceso, Rectificación, Cancelación y Oposición (derechos ARCO), revocaciones del consentimiento y solicitudes de limitación sobre el uso o divulgación de datos personales

El ejercicio de los derechos ARCO tendrá carácter gratuito, debiendo cubrir el titular únicamente los gastos justificados de envío o con el costo de reproducción en copias u otros formatos (art. 35 de la LFPD).

Sólo deben recibirse solicitudes de atención de derechos ARCO, de revocación del consentimiento, o de limitación del uso o divulgación de datos personales (conjuntamente y en adelante, Solicitudes de Derechos), a través de dos vías:

- Vía postal, a la dirección Lago Zurich 96, Colonia Ampliación Granada, Delegación, Miguel Hidalgo, México D.F. 11529, o
- Vía correo electrónico, a la siguiente cuenta: privacy.latam@ciriontechnologies.com

La solicitud deberá dirigirse a:

[EMPRESA CIRION RESPONSABLE, DEFINIDA EN EL AVISO DE PRIVACIDAD CORRESPONDIENTE]

Departamento de Datos Personales

Referencia: Protección de Datos - Derechos ARCO / Revocación del Consentimiento

Y contendrá:

1. El nombre del titular y domicilio u otro medio para comunicarle la respuesta a su solicitud;
2. Los documentos que acrediten la identidad o, en su caso, la representación legal del titular;
3. La descripción clara y precisa de los datos personales respecto de los que se busca ejercer alguno de los derechos antes mencionados, y
4. Cualquier otro elemento o documento que facilite la localización de los datos personales.

Toda persona que reciba una Solicitud de Derechos, por cualquier medio de los indicados, (correo postal o correo electrónico) deberá canalizarla de manera inmediata hacia CIRION, ya que se tiene un plazo de 20 días hábiles para contestar.

El único medio habilitado y aceptable para recibir las Solicitudes de Derechos por correo electrónico es a través de la cuenta: privacy.latam@cirion technologies.com, misma que se encuentra señaladas en los Avisos de Privacidad pertinentes de **CIRION**. En caso de recibir una solicitud de derechos, por cualquier motivo, a través de otra dirección, deberá responderse indicando cual es la dirección habilitada para ello.

Si cualquier área de **CIRION** recibe una solicitud a través de un correo electrónico que no sea el anteriormente señalado, deberá consultar con el Departamento de Datos Personales para poder contestar al titular, invitándolo a dirigir su solicitud a través del correo habilitado.

Si la solicitud no reúne los requisitos citados (solicitud incompleta), **CIRION**, a través del Departamento de Datos Personales, solicitará al titular la subsanación de los mismos.

Se contestarán por escrito con acuse de recibo, con el fin de acreditar el envío y la recepción de todas las solicitudes de ejercicio de los derechos ARCO, incluso en aquellos casos en que no existiera en las bases de datos de **CIRION** información sobre el titular que remitió la solicitud. Deberá crearse un archivo, ya sea físico o electrónico de cada uno de los casos atendidos.

3.2.2. Áreas competentes para tramitar las solicitudes

Para atender y tramitar las solicitudes de ejercicio de estos derechos efectuadas por los titulares, así como para remitir la información correspondiente, serán conjuntamente competentes las siguientes Áreas:

1. Distintas Áreas de **CIRION** (Responsables Funcionales de las Bases de Datos), con el objeto de analizar la existencia de tratamiento y la trascripción de los datos tratados en las diversas bases de datos:

    - Si se ejercitan por empleados o candidatos: el Área de Recursos Humanos
    - Si se ejercitan por personal de proveedores: el Área de Procurement
    - Si se ejercitan por los clientes o representantes legales de clientes: Sales
    - Si se ejercitan por proveedores o suministradores: el Área de Procurement

- Cualquier otra Área que haya asumido el rol de Responsable Funcional de la base de datos que contenga los datos personales a que se refiere la solicitud.

2. El Departamento de Datos Personales, con el objeto de comunicar al titular de forma fehaciente la determinación adoptada en relación con el derecho ejercido, y llevar a cabo el archivo de toda la documentación generada para poder acreditar el cumplimiento de los plazos, en caso de verificación por parte del INAI.

3.2.3. Derecho de Acceso

Cada titular de datos personales sólo podrá ejercer este derecho a intervalos no inferiores a doce meses, salvo que hubiesen ocurrido modificaciones sustanciales al Aviso de Privacidad correspondiente. El Área responsable (Responsable Funcional de las Bases de Datos Personales) deberá dejar constancia de la fecha de ejercicio de este derecho, por cada solicitud recibida, a efectos de control de este plazo.

Para permitir el ejercicio de este derecho a los titulares, se podrá optar por uno o varios de los siguientes sistemas de consulta a la base de datos correspondiente:

- Visualización en pantalla.
- Impresión del registro correspondiente.
- Escrito descriptivo.
- Fotocopia de documentos.
- Cualquier otro procedimiento que pueda ofrecerse, adecuado a la configuración e implantación material de la base de datos.

Si el titular de los datos no elige en su petición la forma de acceso, el Departamento de Datos Personales podrá remitir una carta indicando:

- Que el acceso a sus datos personales lo podrá realizar en las oficinas de **CIRION**, durante un plazo no menor a quince días hábiles contados a partir de la fecha de envío de la respuesta, salvo que el tipo de solicitud de acceso aconseje que la información se proporcione por escrito (por ejemplo, al haber sido solicitado el acceso por titulares que no tienen su domicilio en la misma localidad que **CIRION**), o
- Que **CIRION** le remite la información solicitada en alguno de los formatos indicados, según sea definido por el Departamento de Datos Personales.

Si el titular no acude para tener acceso a sus datos personales dentro del plazo otorgado, será necesaria la presentación de una nueva solicitud. En dichos casos, se recomienda que **CIRION** remita una comunicación informativa mediante la cual haga conocer al titular y deje constancia (unilateral) de su inasistencia para acceder a los datos, esta constancia deberá ser archivada por el Departamento de Datos Personales de **CIRION**.

En todo caso, la información, cualquiera que sea la forma en que se facilite, se dará de forma legible e inteligible, transcribiendo los datos personales solicitados y los resultantes de cualquier elaboración o proceso informático, así como el origen de los mismos; los receptores de transferencias realizadas (si los hubiere), y los usos y finalidades para los que se obtuvieron y conservaron.

La petición de acceso se resolverá por el Responsable Funcional de la Base de Datos o, en su caso, por el Responsable Operativo en el que haya delegado este trámite, **en el plazo máximo de doce días hábi**les, a contar desde la recepción de la solicitud que previamente analizó el Departamento de Datos Personales.

Si la determinación adoptada es positiva para el acceso a los datos, ésta se hará efectiva mediante la comunicación por escrito del resultado obtenido de las búsquedas realizadas (si el titular optó por este medio) o bien **dentro de un plazo no menor a quince días hábiles** si el titular optó por acudir personalmente a la consulta de sus datos, contados a partir de que la determinación sea comunicada al titular.

Si la solicitud fuese desestimada o hubiese transcurrido el plazo de veinte días hábiles sin que CIRION hubiese dado contestación a la misma, el titular puede iniciar el procedimiento de protección de derechos ante el INAI. CIRION nunca debe permitir que una solicitud no sea atendida en el plazo legal.

Como regla general, únicamente se denegará el acceso cuando la solicitud sea formulada por persona distinta del titular o cuando no existan datos del solicitante en las bases de datos del responsable.

Si el titular ejerce el derecho de acceso en un intervalo inferior a doce meses sin que se hubiesen realizado modificaciones sustanciales al Aviso de Privacidad que pudieran motivar nuevas consultas, el responsable podrá optar por solicitar al primero que cubra los costos de búsqueda y respuesta, que en ningún caso podrán ser superiores a tres días de Salario Mínimo General Vigente en el Distrito Federal (artículo 35 de la LFPD).

3.2.4. Derechos de rectificación, cancelación y oposición

Las personas físicas (titulares) tienen derecho a que sus datos personales sometidos a tratamiento sean rectificados sin son erróneos o están desactualizados.

También tienen derecho a indicar que no desean que se traten para una finalidad específica por parte del Responsable (por ejemplo, que no desean recibir publicidad, pero desean mantener vigente una relación contractual con el Responsable).

La solicitud de cancelación deberá indicar si se trata de un dato erróneo o inexacto o si revoca la autorización para el tratamiento del dato.

No procederá la cancelación de los datos:

1. Cuando el solicitante no sea el titular de los datos personales, o el representante legal no esté debidamente acreditado para ello;
2. Cuando no se encuentren los datos personales del solicitante en ninguna base de datos de **CIRION**;
3. Cuando se lesionen los derechos de un tercero;
4. Cuando exista un impedimento legal, o la resolución de una autoridad competente, que restrinja el acceso a los datos personales, o no permita la rectificación, cancelación u oposición de los mismos, y
5. Cuando la rectificación, cancelación u oposición haya sido previamente realizada.

Cuando procediendo la cancelación no sea posible la supresión física de los datos personales, deberán bloquearse con el fin de impedir su ulterior proceso o utilización, conservándose con el único propósito de determinar posibles responsabilidades en relación con su tratamiento hasta el plazo de prescripción legal o contractual de éstas. Cumplido el citado plazo deberá procederse a su supresión.

Si por cualquier motivo el Responsable Funcional de la Base de Datos que le compete no tuviere acceso a esta última para atender el derecho ejercido por los titulares, deberá canalizar la solicitud al Departamento de Datos Personales.

La procedencia de la rectificación, cancelación u oposición se hará efectiva **dentro de los quince días siguientes** a la comunicación de la determinación adoptada.

Si lo procedente es negar la rectificación, cancelación u oposición ejercidas, deberá comunicarse al titular la razón motivada de la denegación **dentro del plazo de veinte días** a que se refiere el artículo 32 de la LFPD.

3.2.5. Procedimiento y cómputo ordinario de plazos para atender el ejercicio de derechos de los titulares

Los plazos y el procedimiento general descrito con anterioridad, se desarrolla con mayor detalle a continuación. Por consiguiente, y siguiendo el mismo sistema de cómputo de días hábiles y las partes intervinientes, se describe los siguientes **plazos internos**:

Plazos internos ordinarios para atender el ejercicio de los derechos ARCO (días hábiles):

- Desde la entrada de la solicitud en cualquier área de **CIRION** (fecha de comienzo del cómputo del plazo legal) se remitirá la solicitud al Departamento de Datos Personales, **como máximo al día siguiente**.

- **Dentro de los 4 (cuatro) días siguientes**, el Departamento de Datos Personales analizará la solicitud para determinar si la misma cumple con los requisitos formales que marca la LFPP y su Reglamento.

- Si la solicitud cumple con los requisitos establecidos, el Departamento de Datos Personales remitirá por correo electrónico y con categoría de urgente la solicitud del titular a cada uno de los Responsables Funcionales de las Bases de Datos.

- Los Responsables Funcionales dispondrán, desde la recepción de la solicitud remitida por el Departamento de Datos Personales, de un **plazo interno de 12 (doce) días** para tramitar y recopilar la información del interesado que ejercita cualquiera de los derechos ARCO.

  Los Responsables Funcionales (asistidos en su caso por el Departamento de Datos Personales) deberán:

  a. Analizar la legitimación de la solicitud del titular; es decir, si resulta posible y procedente:
     i. Acceder a sus datos;
     ii. Rectificar sus datos;
     iii. Cancelar sus datos, u
     iv. Oponerse al tratamiento de sus datos.
  b. Realizar búsquedas (manuales y electrónicas) sobre la base de datos a los efectos de identificar los datos.
  c. En su caso, identificar la información en las bases de datos no automatizadas.

- Una vez llevada a cabo esta tarea y **dentro del plazo marcado (doce días)**, cada uno de los Responsables Funcionales remitirá al Departamento de Datos Personales la

información/documentación con los datos personales existentes sobre el titular que remitió la solicitud atendida.

A tales efectos, deberán indicar:

- Si el acceso a los datos personales es posible, conforme a la información que remitan; o
- Si la rectificación de datos es procedente y ejecutable; o
- Si la cancelación es procedente y ejecutable; o
- Si la oposición al tratamiento es procedente y ejecutable.

- El Departamento de Datos Personales, tras la revisión y supervisión correspondiente, contará con tres días para remitir al titular la determinación adoptada en relación con su ejercicio de derechos ARCO.

- Si la solicitud ha resultado procedente, el Departamento de Datos Personales deberá coordinar con los Responsables Funcionales correspondientes que la determinación adoptada se haga efectiva dentro de los siguiente 15 (quince) días a la comunicación de la respuesta.

El siguiente flujo de trabajo ilustra las etapas que han sido descritas anteriormente:

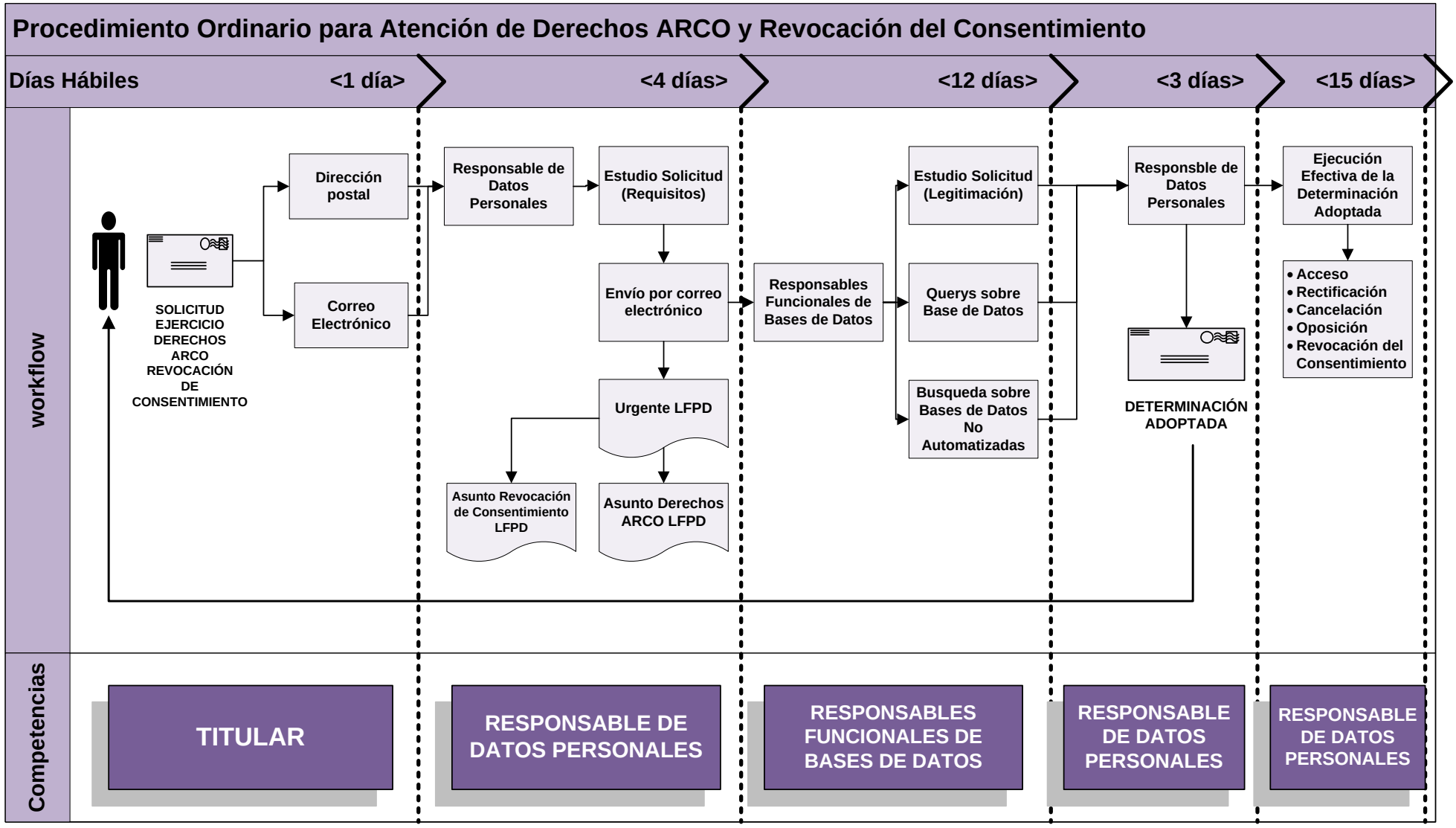

Ilustración 1. Procedimiento Ordinario Derechos ARCO

3.2.6. Computo de plazos en caso de solicitudes incompletas o erróneas

En aquellos casos en que el titular presente una solicitud errónea o incompleta, se procederá conforme al siguiente procedimiento:

- Desde la entrada de la solicitud (fecha de comienzo del cómputo del plazo legal) ésta se remitirá al Departamento de Datos Personales, **como máximo al día siguiente**.

- **Dentro de los 4 (cuatro) días siguientes**, el Departamento de Datos Personales analizará la solicitud para determinar si la misma cumple con los requisitos formales que marcan la LFPP y su Reglamento.

- Si la solicitud está incompleta o contiene errores que no permiten su tramitación, el Departamento de Datos Personales **deberá comunicar de inmediato esta situación al solicitante**, remitiéndole una comunicación en la que explique las causas por las cuales no se cumplen los requisitos legales necesarios para tramitarla; Indicando al titular que cuenta con **diez días hábiles** para subsanar su solicitud.

- Si el titular no subsana su solicitud dentro del plazo anteriormente indicado, el Departamento de Datos Personales deberá archivar toda la documentación relacionada con aquélla para efectos de verificación por parte del INAI, y podrá tenerla por no presentada.

- Si el titular subsana adecuadamente su solicitud, **comenzarán a contar los plazos** a que se refiere el artículo 32 de la LFPD y, por lo tanto, el Departamento de Datos Personales debe tratar la solicitud **dentro del procedimiento ordinario** a que se refiere el apartado inmediato anterior.

El siguiente flujo de trabajo ilustra las etapas que se recomienda seguir en aquellos casos en que debe solicitarse la subsanación de una solicitud de ejercicio de derecho ARCO:

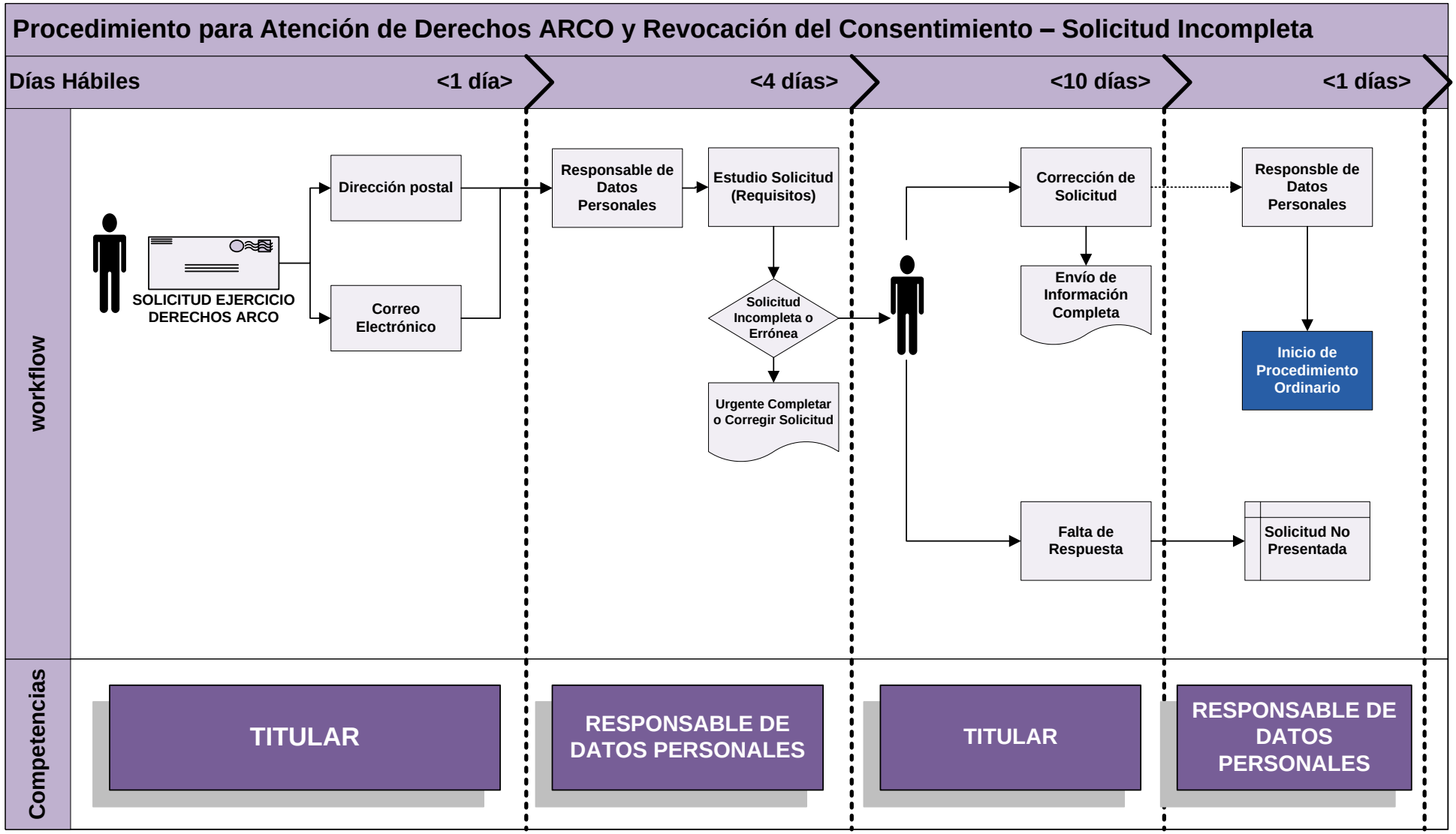

Ilustración 2. Procedimiento para atención de solicitudes incompletas

4. ACCESO A LOS DATOS. RECURSOS CONTENIDOS EN BBDD AUTOMATIZADAS Y NO AUTOMATIZADAS

Únicamente podrán acceder a bases de datos que procesan o contienen datos personales (BBDD) las personas especialmente autorizadas para ello, y sólo tendrán acceso a la información o recursos autorizados.

Cuando una persona o Área precise, para el cometido de sus funciones en **CIRION**, acceder por primera vez a datos personales o a recursos de bases de datos automatizadas o no automatizadas que contengan este tipo de datos, debe solicitar la oportuna autorización al Departamento de Datos Personales, informándole de las razones por las que necesita el acceso y el tipo o tipos de datos que precisa consultar.

El Departamento de Datos Personales sólo autorizará el acceso a aquellos datos o recursos que sean precisos para el desarrollo de las funciones del peticionario.

El Responsable Funcional de la Base de Datos deberá mantener una lista actualizada de usuarios autorizados de conformidad con lo establecido en el apartado 9.1.2.3 de este documento. Esta responsabilidad se podrá delegar en el Departamento de Datos Personales.

4.1. Obligaciones del personal con acceso a datos personales

Las obligaciones que deben conocer los colaboradores de **CIRION** en el desarrollo de sus funciones, derivadas de la LFPD y de su Reglamento, son las siguientes:

- Quienes intervengan en cualquier fase del tratamiento de datos personales están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, subsistiendo estas obligaciones aún después de haber finalizado su relación con **CIRION**, o de haber cambiado de función.

- La violación del deber de secreto tendrá la consideración de falta laboral muy grave y dará lugar al inicio del Procedimiento Disciplinario vigente en **CIRION**, sin perjuicio de otras responsabilidades a que hubiere lugar. La inobservancia de las demás obligaciones se calificará según la gravedad del hecho, en aplicación de normativa aplicable.

- Aplicar las directrices de seguridad que impone la Normativa Interna de la Firma y habilitar aquellas otras medidas de seguridad necesarias para una correcta protección de su entorno de trabajo.

- Usar los datos exclusivamente para el fin que han sido facilitados y de acuerdo con la función que le ha sido encomendada.

- Utilizar software aprobado/homologado por el área de TI.

- Utilizar las funciones de control de acceso, a todos los niveles, en computadoras que almacenan datos personales: setup, protector de pantallas, etc.
- Proteger y mantener en secreto las contraseñas utilizadas para su gestión y cambiarlas con la periodicidad que establezca el área de TI.

- Apagar de forma ordenada los equipos de trabajo, al finalizar la jornada de trabajo, salvo que por razones específicas éstos deban permanecer encendidos, y exista control sobre aquéllos en esta situación.

- Comunicar cualquier anomalía por mal funcionamiento (hardware, software, virus informáticos) a TI, así como cualquier incidencia de seguridad (intentos de acceso no autorizados, manejo inadecuado de datos, etc.) mediante el correspondiente Registro de Incidencias.

- Habilitar los medios necesarios para proteger los soportes que contengan datos de personales.

- Utilizar los medios necesarios para destruir los soportes antes de desecharlos o reutilizarlos cuando la información contenida en estos así lo requiera.

- Guardar los soportes que contengan datos personales en armarios o escritorios protegidos con llave o con un sistema de combinación, al finalizar la jornada de trabajo.

- Comunicar a través del correspondiente modelo de entrada y salida de soportes cualquier tipo de soportes que entre o salga de las instalaciones de **CIRION**.

- Utilizar los equipos informáticos exclusivamente para la finalidad para la que han sido facilitados y nunca para trabajos o comunicaciones personales.

- Utilizar trituradoras de papel para la destrucción de documentación donde se alberguen datos personales y/o en contenedores de papel para su posterior destrucción, cuando dicha documentación deje de ser necesaria o pertinente, tal como se señala en las políticas internas en relación al manejo de información confidencial.

Todas las funciones de cada una de las personas con acceso a los datos personales y a los sistemas de información deberán estar definidas y documentadas en la Relación de Medidas de Seguridad que apruebe y determine el área de TI de **CIRION**.

A fin de que todas las personas que intervienen en el tratamiento de datos personales conozcan sus funciones y obligaciones respecto a la confidencialidad de la información, el Departamento de Datos Personales dará publicidad a las presentes obligaciones, así como a las obligaciones adicionales que deban observarse en razón de los datos personales tratados.

5. TRATAMIENTO DE DATOS PERSONALES POR CUENTA DE CIRION, PARA LA PRESTACIÓN DE SERVICIOS (ENCARGADOS)

La entrega de datos personales a terceros para su tratamiento por cuenta de **CIRION** o la solicitud genérica para que los traten en cualquier fase del tratamiento (obtención, procesamiento, consulta, custodia, destrucción, etc.) se realizará siempre en virtud de una relación contractual y por escrito entre **CIRION** y el tercero (denominado por la normativa como "Encargado"), sin que los datos se puedan utilizar para una finalidad distinta a la que figure en el contrato de prestación de servicios. Dentro de esta relación contractual, los datos no podrán ser transferidos a otras personas, ni siquiera para su conservación, salvo que dicha transferencia forme parte del propio servicio o sea instruida por **CIRION**.

Los contratos de prestación de servicios variarán según la tipología de los datos personales entregados para tratamiento y, por tanto, contendrán disposiciones específicas en relación con el nivel de seguridad aplicable a dichos datos.

Una vez cumplida la prestación contractual, los datos personales deberán ser destruidos o devueltos al Responsable (**CIRION**), al igual que cualquier soporte o documento en que conste algún dato personal objeto de tratamiento. No obstante, si el Área de **CIRION**, gestora del contrato, presume la posibilidad de ulteriores encargos al mismo tercero prestador del servicio, podrá admitir el almacenamiento de los datos por este último, con las debidas garantías de seguridad.

Con carácter general, no se permitirá la subcontratación en los contratos que conlleven entrega/comunicación de datos personales a un Encargado, si no existe la correspondiente autorización de los Responsables Funcionales implicados y del Departamento de Datos Personales.

Si la subcontratación fuera necesaria por así requerirlo el tipo de servicios contratado, deberán observarse las disposiciones del artículo 54 del Reglamento de la LFPD y todas las Disposiciones que de esta actividad emanen.

Por todo ello, cuando un Área de **CIRION** (Responsable Funcional) necesite facilitar datos personales a un tercero para la prestación o gestión de un servicio, seguirá las siguientes recomendaciones:

a) Lo comunicará al Departamento de Datos Personales con el objeto de acordar y definir el correspondiente contrato de prestación de servicios que cumpla con las disposiciones de los artículos 51, 52 y 54 del Reglamento de la LFPD.

En dicho contrato, **CIRION** promoverá la inclusión de las cláusulas necesarias para regular el tratamiento de los datos por parte del Encargado (prestador del servicio), cuyo modelo aparece en el **ANEXO PRIMERO** de esta Política.

b) El Departamento de Datos Personales archivará una copia del contrato firmado con el prestador del servicio (Encargado), y lo pondrá a disposición del INAI en caso de requerimiento.

c) El Departamento de Datos Personales junto con el área de TI analizará, si es necesario, implementar alguna de las siguientes medidas:

1. Inventario del soporte a través del cual se vaya a remitir la información.

2. Llenar el correspondiente registro de salida de soportes existente a estos efectos.

3. Implementar algún mecanismo de cifrado en el soporte para evitar que terceros ajenos a la relación contractual puedan acceder a datos personales sensibles o a información clasificada como confidencial por **CIRION**.

4. Implementar algún mecanismo de cifrado en la remisión de los datos si ésta se realiza a través de redes de telecomunicaciones.

6. TRANSFERENCIAS DE DATOS. RECURSOS CONTENIDOS EN UNA BASE DE DATOS PERSONALES

Por transferencia de datos se entiende "*toda comunicación de datos realizada a persona distinta del responsable o encargado del tratamiento*" (art. 3, fracción XIX de la LFPD).

Dadas las consecuencias e implicaciones que conlleva la transferencia de datos personales contenidos en las bases de datos de **CIRION**, para su realización se seguirán las siguientes reglas:

6.1. Regla general

Con carácter general, no se transferirán datos personales a terceros.

Se exceptúan de dicha regla los siguientes supuestos:

1. Cuando la transferencia esté prevista en una Ley o Tratado en los que México sea parte;
2. Cuando la transferencia sea necesaria para la prevención o el diagnóstico médico, la prestación de asistencia sanitaria, tratamiento médico o la gestión de servicios sanitarios;
3. Cuando la transferencia sea efectuada a sociedades controladoras, subsidiarias o afiliadas bajo el control común del responsable, o a una sociedad matriz o a cualquier sociedad del mismo grupo del responsable que opere bajo los mismos procesos y políticas internas;
4. Cuando la transferencia sea necesaria por virtud de un contrato celebrado o por celebrar en interés del titular, por el responsable y un tercero;
5. Cuando la transferencia sea necesaria o legalmente exigida para la salvaguarda de un interés público, o para la procuración o administración de justicia;
6. Cuando la transferencia sea precisa para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial, y
7. Cuando la transferencia sea precisa para el mantenimiento o cumplimiento de una relación jurídica entre el responsable y el titular.

Podrán llevarse a cabo transferencias de datos personales en aquellos supuestos que se obtenga el consentimiento del titular, siempre que el Responsable-Receptor trate los datos personales conforme a lo establecido en el Aviso de Privacidad que el Responsable-Transferente (**CIRION**) le comunique en todos los casos.

6.2. Control de la transferencia efectuada

El Responsable Funcional de la base de datos a la que correspondan los datos personales objeto de transferencia deberá informar al Departamento de Datos Personales sobre:

- La finalidad de la transferencia,
- Los datos que se transfieren,
- La identidad y el domicilio del responsable receptor de los datos.

Si la transferencia de datos se efectúa mediante la entrega de soportes (informáticos o papel), ésta deberá autorizarse por el Departamento de Datos Personales, y anotarse en un Registro si los datos se extraen de una base de datos con nivel recomendable de seguridad medio o alto, mediante el modelo correspondiente (apartado 9.1.2.2).

7. BASES DE DATOS QUE TRATAN DATOS PERSONALES

Las bases de datos existentes en **CIRION** con datos personales constan en el ***Inventario de Bases de Datos y Sistemas de Información*** disponible en el ANEXO TERCERO.

Estas bases de datos pueden ser clasificadas en:

7.1. Clasificación

1. **En razón de su uso:**

   - **CORPORATIVAS**: Aquellas que son básicas para la gestión de **CIRION**, independientemente del entorno donde residan o del lugar de su ubicación y que normalmente son utilizadas por más de una Dirección y/o Gerencia.

   - **NO CORPORATIVAS**: Aquellas que son utilizadas por una sola Dirección, Gerencia, Jefatura o Área de **CIRION**.

2. **En razón de las medidas de seguridad que deberían adoptar tomando en cuenta la sensibilidad de los datos personales tratados:**

   - **Bases de datos que deben contar con medidas de seguridad de nivel básico**: Por defecto, todas las bases de datos automatizadas deben disponer de medidas de seguridad de nivel básico.

   - **Bases de datos que deben contar con medidas de seguridad de nivel medio**: Contendrán las medidas de nivel básico más las de nivel medio aquellas bases de datos que traten, además de datos personales “genéricos”, datos de tipo financiero y/o patrimonial.

   - **Bases de datos que deben contar con medidas de seguridad de nivel alto**: Contendrán medidas de nivel básico, medio y alto las bases de datos que traten datos personales considerados como sensibles por la LFPD.

Dependiendo de la clasificación de las bases de datos por el nivel de las medidas de seguridad que deberían adoptar en consideración de la sensibilidad de los datos tratados, **CIRION** implementará las medidas de seguridad descritas en el apartado 9 de la presente Política de Protección de Datos Personales.

Lo anterior, con independencia de que por sí mismo o mediante la ejecución de un proyecto específico adopte en el plazo que considere pertinente las "*Recomendaciones en materia de seguridad de datos personales*" publicadas en el Diario Oficial de la Federación el pasado 30 de octubre de 2013 y todas las modificaciones que de ella deriven.

7.2. Creación de nuevas bases de datos

Cuando se trate de crear nuevas bases de datos personales distintas a las inventariadas en la fecha de publicación de la primera versión de esta Política de Protección de Datos Personales, se deberá contar con la autorización del Titular del Área correspondiente, que lo comunicará por escrito al Departamento de Datos Personales, informando de todos los extremos que figuran en el Inventario de Bases de Datos y dejando el correspondiente registro de dicha actualización.

Las pruebas previas a la creación o modificación de bases de datos, consistentes en la grabación o volcado de datos personales, no se realizarán con datos reales salvo que se garantice el nivel de seguridad correspondiente al tipo de datos personales tratado.

7.3. Modificaciones o supresiones de bases de datos

Las supresiones de bases de datos, o las modificaciones que se realicen de cualquier extremo que figura en el Inventario, se comunicarán por parte del Responsable Funcional al Departamento de Datos Personales y al Área Marketing, Seguridad, Procurement o Sales, según corresponda, para que estos últimos ejecuten las modificaciones procedentes en los sistemas de información, en el Inventario de Bases de Datos de **CIRION** y en la Relación de las Medidas de Seguridad de la base de datos afectada que al efecto haya adoptado el Área de TI.

En aquellos casos en que se suprima una base de datos, deberá quedar constancia del destino de los datos personales, indicando si los mismos han sido suprimidos o transferidos a otra base de datos.

Se recomienda conservar durante al menos dos años la Relación de Medidas de Seguridad de cualquier base de datos que hubiese sido suprimida, a contar desde su fecha efectiva de baja en los sistemas de información.

8. RESPONSABLE, RESPONSABLE FUNCIONAL, DEPARTAMENTO DE DATOS PERSONALES, USUARIOS AUTORIZADOS (Y RESPONSABLE OPERATIVO)

8.1. Concepto y atribución de responsabilidades

Desde el punto de vista legal, **CIRION** es la entidad responsable de las bases de datos personales, frente al INAI y frente a los titulares de dichos datos. Lo anterior, tanto a efectos del cumplimiento de las

obligaciones impuestas por la LFPD, como a efectos del régimen de infracciones y sanciones previsto en el mismo ordenamiento.

No obstante lo anterior, a los efectos de **gestión y organización corporativa** se constituyen tres figuras prácticas (más una figura opcional):

a) Responsable Funcional de la Base de Datos;
b) Departamento de Datos Personales;
c) Usuarios que tratan datos personales, y
d) Responsable Operativo de la Base de Datos (opcional).

8.1.1. Responsable Funcional de la Base de Datos

Persona o personas (empleados o personal externo) cuya función consiste en solicitar y coordinar las acciones/actividades de cumplimiento jurídico en materia de protección de datos personales que corresponden al Responsable (**CIRION**) en posesión de dichos datos.

La asignación de dicho rol no supone la asunción de responsabilidades que sean propias del Responsable (**CIRION**) frente al INAI o los titulares de datos.

La figura de Responsable Funcional, recaerá sobre los siguientes directivos:

a) De las bases de datos CORPORATIVAS será responsable cada uno de los Titulares del Área que haga un uso mayoritario sobre cada una de las bases de datos en cuestión.
b) De las bases de datos NO CORPORATIVAS (Departamentales) será responsable el correspondiente Titular.

La figura de Responsable Funcional de cada base de datos titularidad de **CIRION** constará en el ***Inventario de Bases de Datos***, contenido en el ANEXO TERCERO.

8.1.2. Departamento de Datos Personales

El Departamento de Datos Personales de la organización, identificado como la persona o titular del Departamento a que se refiere el artículo 30 de la LFPD, recaerá sobre las personas determinadas en el Anexo Segundo y Anexo Tercero de la presente Política, en función de la naturaleza de las tareas y responsabilidades a su cargo.

8.1.3. Usuarios autorizados que tratan datos personales

Resto de personas de la organización que, sin tener, por competencia o actividad, responsabilidad directa en la ejecución de las labores de cumplimiento de la legislación sobre protección de datos personales, tratan o pueden llegar a tratar datos personales en el desempeño de sus actividades.

8.1.4. Responsable Operativo

La figura del Responsable Operativo puede recaer en personal autorizado por el Responsable Funcional de cada base de datos, que tendrá encomendadas una serie de actividades de cumplimiento operativo, de coordinación y de ejecución de cumplimiento de actividades relacionadas con la LFPD.

Cuando no existan Responsables Operativos, sus funciones serán asumidas por el Responsable Funcional.

8.2. Funciones y obligaciones

8.2.1. Responsables Funcionales de las Bases de Datos

Los **Responsables Funcionales** de cada base de datos, tendrán las siguientes funciones y obligaciones:

1. Vigilar el contenido y el uso del tratamiento de datos personales.

2. Autorizar a las personas que, de acuerdo con las necesidades de gestión, puedan acceder a la información, estableciendo los mecanismos necesarios para evitar que un usuario acceda a datos distintos de los autorizados.

3. Mantener una relación actualizada de usuarios que tengan acceso autorizado a los sistemas de información correspondientes.

4. Autorizar y controlar las transferencias nacionales e internacionales de datos a terceros o a empresas del Grupo y aprobar el envío de soportes fuera de la organización.

5. Cuando existan encargos del tratamiento de datos personales, revisar previamente a su inicio que se han celebrado los contratos oportunos y que se han establecido las medidas de seguridad adecuadas.

6. Coordinar y controlar las medidas definidas en la Relación de Medidas de Seguridad de la base de datos correspondiente.

7. Gestionar la resolución de incidencias relativas a seguridad de los datos personales.

8. Autorizar y gestionar la implantación de las medidas correctoras adecuadas especificadas en los Informes de Auditoría que se lleguen a producir desde la entrada en vigor de esta Política en **CIRION**.

9. Autorizar las salidas de información que se produzcan por cualquier causa y medio.

10. Guardar el secreto profesional respecto de los datos personales a que tenga acceso con motivo de sus funciones.

11. Asegurar que el personal a su cargo conoce la obligación de secreto profesional que tienen respecto de los datos personales a los que tengan acceso con motivo de sus funciones.

12. Coordinar la creación, modificación y/o supresión de bases de datos que traten datos personales.

13. Coordinar directamente las modificaciones en el tratamiento de los datos personales para determinar si resulta necesaria la actualización o modificación de los Avisos de Privacidad correspondientes.

14. Cualquier otra actividad que, prevista en la presente Política de Protección de Datos Personales, no hubiese sido asignada a otra figura relacionada con el tratamiento de datos personales.

8.2.2. Departamento de Datos Personales

La figura del **Departamento de Datos Personales** tendrá las siguientes funciones y obligaciones:

1. Coordinar, gestionar y ejecutar las medidas y acciones necesarias para tramitar y responder en tiempo y forma las solicitudes de ejercicio de los derechos ARCO y de revocación del consentimiento que formulen los titulares de datos personales, en coordinación con los Responsables Funcionales.

2. Adoptar las medidas necesarias para que el personal conozca las normas de seguridad que afecten al desarrollo de sus funciones, reglas vigentes de aspecto organizativo, así como las consecuencias en que dicho personal pudiera incurrir en caso de incumplimiento. A tales efectos, deberá contar con el apoyo de los Responsables Funcionales.

3. Determinar el nivel de seguridad recomendable para las bases de datos personales, en función de los tipos de datos contenidos en las mismas.

4. Controlar la adopción de las medidas definidas en la Relación de Medidas de Seguridad de cada base de datos.

5. Asegurar el establecimiento de procedimientos de identificación y autenticación para el acceso a los datos personales tratados por **CIRION**.

6. Autorizar las personas y Áreas que, de acuerdo con las necesidades de gestión, puedan acceder a la información, según las solicitudes dirigidas por los Responsable Funcionales de las bases de datos.

7. Actualizar la Relación de Medidas de Seguridad de las bases de datos, cuando sea procedente de conformidad al Reglamento de la LFPD.

8. Realizar revisiones de control sobre el cumplimiento y seguimiento de las normas y procedimientos establecidos en la Relación de Medidas de Seguridad.

9. Analizar, junto con los Responsables Funcionales que correspondan, los Informes de Auditoría que se emitan sobre los sistemas de información que tratan datos personales y elevar las conclusiones a la Dirección General.

10. Coordinar dentro de la organización acciones de formación y concientización periódicas en materia de protección de datos.

11. Revisar periódicamente que los Avisos de Privacidad se encuentren debidamente actualizados.

12. Custodiar debidamente las Relaciones de Medidas de Seguridad, documentación interna en materia de protección de datos; documentación relativa a las funciones y obligaciones del personal que trata datos personales, así como los Informes Jurídicos y de Auditoría elaborados sobre la materia para **CIRION**.

13. En el caso de las bases de datos de **CIRION** que contienen datos personales considerados sensibles (origen racial o étnico, estado de salud presente y futura, información genética, creencias religiosas, filosóficas y morales, afiliación sindical, opiniones políticas y/o preferencia sexual), controlar los

mecanismos de registro de acceso a los datos protegidos, revisar periódicamente la información de control registrada, así como elaborar un informe de las revisiones realizadas y los problemas detectados al menos una vez al mes, elevando las conclusiones de dicho informe al Responsable Funcional de la base de datos correspondiente y, en su caso, al Responsable Operativo de la misma.

14. Guardar el secreto profesional respecto de los datos personales a que tenga acceso con motivo de sus funciones.

15. Actuar como interlocutor, en representación de la empresa, en todas aquellas actuaciones que se lleven a cabo frente al INAI.

16. Cualquier otra actividad prevista en la presente Política de Protección de Datos Personales que le identifique como responsable de su gestión y control.

8.2.3. Usuarios que tratan datos personales

Los **usuarios autorizados** que por motivo de sus funciones tengan acceso a datos personales, tendrán las siguientes funciones y obligaciones:

1. Guardar el secreto profesional respecto de los datos personales a que tenga acceso con motivo de sus funciones.

2. Los puestos de trabajo estarán bajo la responsabilidad del usuario autorizado que garantizará que la información que muestran no pueda ser visible por personas no autorizadas.

3. Cuando se abandone un puesto de trabajo, bien temporalmente o bien al finalizar su turno de trabajo, deberán dejarlo en un estado que impida la visualización de los datos protegidos. Esto podrá realizarse a través de un protector de pantalla que impida la visualización de los datos. La reanudación del trabajo implicará la desactivación de la pantalla protectora con la introducción de la contraseña correspondiente.

4. En el caso de las impresoras, deberán asegurarse que no quedan documentos impresos en la bandeja de salida que contengan datos personales que deban estar protegidos.

5. Cada usuario será responsable de la confidencialidad de su contraseña y, en caso de que la misma sea conocida fortuita o fraudulentamente por personas no autorizadas, deberá registrarlo como incidencia al equipo de Compliance y proceder a su cambio de manera inmediata.

6. No almacenar información fuera de las ubicaciones lógicas y físicas autorizadas para tales efectos.

7. Observar y cumplir todas las Políticas y Procedimientos de seguridad recogidos o previstos en la Relación de Medidas de Seguridad. En concreto, conocer y cumplir con las funciones y obligaciones del personal que trata datos personales.

8. Cualquier otra actividad que prevista en la presente Política de Protección de Datos Personales les identifique como usuarios de datos personales.

8.2.4. Responsable Operativo

En caso de que esta figura sea implementada dentro de **CIRION**, son funciones y obligaciones del Responsable Operativo, las siguientes:

1. Gestionar y controlar las transferencias nacionales e internacionales de datos personales a terceros o empresas de **CIRION** y gestionar el envío de soportes fuera de la Entidad.

2. Gestionar los contratos y anexos necesarios para regular las relaciones con los encargados del tratamiento, previa consulta y aprobación del Departamento de Datos Personales.

3. Verificar los accesos a las aplicaciones con el nivel de tratamiento específico según las necesidades del puesto, validar la relación actualizada de usuarios con acceso a las aplicaciones, así como notificar los errores de asignación detectados.

4. Verificar las salidas de información que se produzcan por cualquier causa y medio.

5. Notificar a las entidades receptoras a las que se han transferido datos personales sobre la rectificación, oposición y/o cancelación de los mismos, en los plazos establecidos por la legislación de protección de datos personales.

6. Supervisar la correcta ejecución de cualquier tipo de rectificación, oposición y/o cancelación de datos personales por el titular de los mismos.

7. Coordinar, gestionar y/o ejecutar las tareas de búsqueda en las bases de datos relacionadas con el ejercicio de los derechos ARCO.

8. En su caso, coordinar, gestionar y/o ejecutar la creación y actualización de listas de exclusión relacionas con el ejercicio del derecho de oposición de los titulares de datos personales.
9. Comunicar las necesidades de altas, bajas y/o modificación de privilegios de los usuarios sobre los recursos.

10. En general, detectar y escalar al Responsable Funcional las necesidades derivadas del cumplimiento de la legislación de protección de datos personales.

9. MEDIDAS DE SEGURIDAD DE LAS BASES DE DATOS

A fin de garantizar la confidencialidad, disponibilidad e integridad de la información, se establecen una serie de medidas técnicas y organizativas aplicables en todo el ámbito de **CIRION** para garantizar la seguridad que deben reunir las bases de datos personales automatizadas y no automatizadas, centros de tratamiento, locales, equipos, sistemas, programas y las personas que intervengan en el tratamiento de los datos personales.

Por defecto, cualquier base de datos que trate datos personales debe adoptar las medidas de seguridad de nivel básico. Asimismo, que aquellas bases de datos que traten, entre otros, datos financieros y/o patrimoniales**, deberán adoptar además medidas de seguridad de nivel medio. Por último, que aquellas**

bases de datos que traten datos personales sensibles**, deberán adoptar medidas de seguridad de nivel alto, en adición a las medidas de nivel básico y medio.**

Las medidas de seguridad que deben implementarse sobre las bases de datos versarán según el sistema de tratamiento y la tipología de los datos personales tratados:

BASES DE DATOS AUTOMATIZADAS

MEDIDAS DE SEGURIDAD	NIVEL DE SEGURIDAD		
	BÁSICO	MEDIO	ALTO
Disponer de una Relación de Medidas de Seguridad	☒	☒	☒
Funciones y obligaciones del personal	☒	☒	☒
Registro de Vulneraciones de Seguridad (Incidencias)	☒	☒	☒
Identificación y autenticación	☒	☒	☒
Sistema de control de accesos lógicos	☒	☒	☒
Sistema de control de acceso físico		☒	☒
Gestión de soportes y documentos	☒	☒	☒
Copias de respaldo y recuperación	☒	☒	☒
Auditorías		☒	☒
No realizar pruebas con datos reales	☒	☒	☒
Distribución de soportes			☒
Disponer de un registro de accesos			☒
Cifrado de las telecomunicaciones			☒

Tabla 1. Medidas de Seguridad para Bases de Datos Automatizadas

BASES DE DATOS NO AUTOMATIZADAS

MEDIDAS DE SEGURIDAD	NIVEL DE SEGURIDAD		
	BÁSICO	MEDIO	ALTO
Disponer de una Relación de Medidas de Seguridad	☒	☒	☒
Funciones y obligaciones del personal	☒	☒	☒
Registro de Vulneraciones de Seguridad (Incidencias)	☒	☒	☒
Control de accesos		☒	☒
Gestión de soportes	☒	☒	☒
Criterios de archivo	☒	☒	☒
Dispositivos de almacenamiento	☒	☒	☒
Custodia de los soportes	☒	☒	☒
Auditorías		☒	☒
Almacenamiento de la información			☒
Copia o reproducción			☒
Acceso a la documentación			☒
Traslado de documentación			☒

Tabla 2. Medidas de Seguridad para Bases de Datos No Automatizadas

Todas las bases de datos personales deberán disponer de su propia “Relación de Medidas de Seguridad” bajo la gestión y control del Departamento de Datos Personales.

9.1. Medidas de seguridad sobre bases de datos automatizadas

9.1.1. Medidas de Seguridad de NIVEL BÁSICO

Todas las bases de datos automatizadas que contengan datos personales deben observar las medidas de seguridad de nivel básico, que deben constar en la "**Relación de Medidas de Seguridad**" existente para cada base de datos. Este documento será de obligado cumplimiento para el personal con acceso a los datos personales automatizados y al sistema de información en cuestión.

9.1.1.1. Contenido de la Relación de Medidas de Seguridad

Conforme a lo dispuesto por el artículo 61 del Reglamento de la LFPD, esta relación deberá contener las Medidas de Seguridad derivadas de las fracciones contenidas en el mismo numeral, por lo que habrá de tenerse en cuenta cuál es su contenido:

> ***Acciones para la seguridad de los datos personales***
>
> ***Artículo 61****. A fin de establecer y mantener la seguridad de los datos personales, el responsable deberá considerar las siguientes acciones:*
>
> ***I.*** *Elaborar un inventario de datos personales y de los sistemas de tratamiento;*
> ***II.*** *Determinar las funciones y obligaciones de las personas que traten datos personales;*
> ***III.*** *Contar con un análisis de riesgos de datos personales que consiste en identificar peligros y estimar los riesgos a los datos personales;*
> ***IV.*** *Establecer las medidas de seguridad aplicables a los datos personales e identificar aquéllas implementadas de manera efectiva;*
> ***V.*** *Realizar el análisis de brecha que consiste en la diferencia de las medidas de seguridad existentes y aquéllas faltantes que resultan necesarias para la protección de los datos personales;*
> ***VI.*** *Elaborar un plan de trabajo para la implementación de las medidas de seguridad faltantes, derivadas del análisis de brecha;*
> ***VII.*** *Llevar a cabo revisiones o auditorías;*
> ***VIII.*** *Capacitar al personal que efectúe el tratamiento, y*
> ***IX.*** *Realizar un registro de los medios de almacenamiento de los datos personales.*
> ***X.*** *El responsable deberá contar con una relación de las medidas de seguridad derivadas de las fracciones anteriores.*

9.1.1.2. Actualización de la Relación de Medidas de Seguridad

Conforme al artículo 62 del Reglamento de la LFPD, la Relación de Medidas de Seguridad deberá actualizarse, cuando ocurra cualquiera de los siguientes eventos:

> ***I.*** *Se modifiquen las medidas o procesos de seguridad para su mejora continua, derivado de las revisiones a la política de seguridad del responsable;*
> ***II.*** *Se produzcan modificaciones sustanciales en el tratamiento que deriven en un cambio del nivel de riesgo;*
> ***III.*** *Se vulneren los sistemas de tratamiento, de conformidad con lo dispuesto en el artículo 20 de la Ley y 63 del presente Reglamento, o*
> ***IV.*** *Exista una afectación a los datos personales distinta a las anteriores.*

*En el caso de datos personales sensibles, los responsables procurarán revisar y, en su caso, actualizar las relaciones correspondientes **una vez al año**.*

9.1.1.3. Registro de Vulneraciones de Seguridad (Incidencias)

El Departamento de Datos Personales, en la persona de los responsables operativos y funcionales del área de seguridad de CIRION, crearán un Registro de Vulneraciones de Seguridad (Incidencias) para las bases de datos personales existentes o de futura creación **CIRION**; su contenido estará a disposición de los Responsables Funcionales de la base de datos correspondiente.

La comunicación de vulneraciones de seguridad se realizará por parte de los usuarios mediante correo electrónico a la dirección establecida al efecto privacy.latam@ciriontechnologies.com y cumplimentando el impreso generado para tales casos:

Notificación de Vulneración de Seguridad (Incidencia)
Incidencia Nº _____ (Asignado por el Departamento de Datos Personales)
Fecha de notificación: ___/___/___
Descripción detallada de la incidencia:
Fecha y hora en que se produjo la incidencia:
Persona(s) a quien(es) se comunica:
Efectos que puede producir (de no subsanarse o independientemente de ello):
Recuperación de Datos (a rellenar sólo si la incidencia lo amerita): Procedimiento realizado: Datos restaurados: Datos grabados manualmente: Persona que ejecutó el proceso: Firma del Departamento de Datos Personales: _____
Persona que realiza la comunicación: _____

Ilustración 3. Modelo de Impreso para Notificación de Vulneraciones de Seguridad

Cualquier usuario que tenga conocimiento de una incidencia/vulneración de seguridad es responsable de su comunicación al Departamento de Datos Personales.

El conocimiento y la no-notificación de una incidencia/vulneración de seguridad por parte de un usuario será considerado como una falta contra la seguridad de las bases de datos por parte del usuario que omitió la notificación.

¿Qué es una incidencia?

Se considera incidencia cualquier anomalía que afecte o pudiera afectar a la seguridad de los datos, en cualquiera de sus tres vertientes: confidencialidad, integridad o disponibilidad.

Se entiende por:

- **Confidencialidad**: la condición que garantiza que la información no puede estar disponible o ser descubierta por o para personas, entidades o procesos no autorizados. La información únicamente puede ser accedida por los usuarios autorizados.

  Ejemplo de incidencia: El envío involuntario de información a personas no autorizadas o facilitar indebidamente el acceso a personas no autorizadas.

- **Integridad**: El sistema no debe modificar o corromper la información que almacena, ni permitir que alguien no autorizado lo haga. Sólo los usuarios autorizados pueden modificar la información contenida.

  Ejemplo de incidencia: Pérdida de una parte de los datos personales con motivo de un proceso erróneo (humano o técnico).

- **Disponibilidad**: Condición que permite que tanto el hardware como el software funcionen eficientemente de forma continuada y que, en caso de fallo, exista la capacidad de recuperarse rápidamente. Los elementos del sistema deben de estar accesibles y disponibles a los usuarios autorizados.

  Ejemplo de incidencia: Avería del soporte físico que almacena los datos personales o fallo en la realización de las copias de respaldo.

Por su parte, el artículo 63 del Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, establece:

Vulneraciones de seguridad

Artículo 63*. Las vulneraciones de seguridad de datos personales ocurridas en cualquier fase del tratamiento son:*

I. *La pérdida o destrucción no autorizada;*
II. *El robo, extravío o copia no autorizada;*
III. *El uso, acceso o tratamiento no autorizado, o*
IV. *El daño, la alteración o modificación no autorizada.*

Medidas de Seguridad de NIVEL MEDIO

Las bases de datos a las que corresponda este nivel de seguridad deberán contar con todas las medidas de seguridad de nivel básico, más las que adicionalmente se identifican en los siguientes apartados:

9.1.1.4. Auditorias Periódicas

Se procurará que **al menos cada dos años** se lleve a cabo una auditoría de todos los Sistemas de Información que deban adoptar medidas de seguridad de nivel medio, así como de las instalaciones de tratamiento de datos, con el fin de verificar el cumplimiento de las medidas de seguridad en la Relación correspondiente y los procedimientos, criterios y recomendaciones vigentes en materia de protección de datos personales.

La auditoría podrá efectuarse de forma interna, o también por empresas especializadas y contratadas al efecto, cuando así se decida por parte del Departamento de Datos Personales.

Si se decide optar por la contratación de auditorías externas, se recomienda solicitar que los auditores propuestos por la empresa que sea contratada tengan la certificación CISA (*Certified Information Systems Auditor*) de ISACA (*Information System Audit Control Association*) y cuenten con conocimientos jurídicos sobre la aplicación de la normativa de protección de datos personales.

Los informes de auditoría deberán identificar deficiencias y proponer medidas correctoras o complementarias, y serán analizados por el Departamento de Datos Personales, quien elevará sus conclusiones a nivel Corporativo para que se adopten las medidas correctoras adecuadas. A su vez los comunicará a los Responsables Funcionales de las Bases de Datos, para su conocimiento.

El Departamento de Datos Personales deberá archivar los informes de auditoría correspondientes y las conclusiones que emita al respecto, junto a la "Relación de Medidas de Seguridad" de la base de datos correspondiente, para su puesta a disposición en caso de que éstos sean requeridos por el INAI.

9.1.1.5. Registro de entrada y salida de soportes y documentos

Se deberá establecer un sistema de registro de entrada y salida de soportes y documentos que permita conocer el tipo de documento o soporte; la fecha y hora; el emisor y el destinatario; el número de documentos o soportes incluidos en el envío; el tipo de información que contienen; la forma de envío y la persona responsable de la recepción/entrega, que deberán estar debidamente autorizadas:

AUTORIZACIÓN DE SALIDA DE SOPORTES		
	Fecha de salida:	___/___/_____
SOPORTE		
Tipo de soporte y etiqueta		
Contenido		
Base de datos de donde procede la información		
Fecha de creación		
FINALIDAD Y DESTINO		
Finalidad		
Destino		
Destinatario		
FORMA DE ENVÍO		
Medio de envío		
Remitente		
Precauciones para el transporte		
AUTORIZACIÓN		
Persona que autoriza		
Cargo/Puesto		
Observaciones		
Firma		

Ilustración 4. Modelo de Impreso para Autorización de Salida de Soportes

9.1.1.6. Sistemas de identificación y autenticación específicos

Se establecerá un sistema que permita la identificación inequívoca y personalizada de todo usuario que intente acceder al sistema de información, limitando la posibilidad de intentar reiteradamente el acceso no autorizado al sistema de información.

Se deberá mantener una lista actualizada de usuarios autorizados para acceder a los sistemas de información que tratan datos personales.

9.1.1.7. Control de acceso físico a los locales

Únicamente el personal autorizado podrá tener acceso a las instalaciones o locales donde estén ubicados los sistemas de información que tratan datos personales.

9.1.2. Medidas de Seguridad de NIVEL ALTO

Las bases de datos a las que corresponde adoptar medidas de seguridad de nivel alto (que tratan datos personales sensibles) incorporarán las medidas de seguridad de nivel básico, medio y además las que a continuación se identifican:

9.1.2.1. Contenido de la Relación de Medidas de Seguridad

Además de lo dispuesto para los niveles básico y medio de seguridad, **el nivel alto tendrá el siguiente contenido adicional**:

- Medidas que deberán adoptarse con carácter previo a la distribución de soportes, bien mediante el cifrado de datos o bien mediante cualquier otro mecanismo que garantice que la información no sea inteligible ni pueda ser manipulada durante el transporte.

- Existencia de una copia de respaldo y de los procedimientos de recuperación de los datos en un lugar diferente a aquél en que se encuentren los equipos informáticos que los tratan. Dichas copias deberán estar en lugares con las medidas de seguridad adecuadas.

- En el supuesto de que se transmitan datos personales a través de redes de telecomunicación, se deberán cifrar los datos personales sensibles o utilizar cualquier otro medio (que se describirá en la Relación de Medidas de Seguridad), que garantice que la información no sea inteligible, ni manipulada por terceros.

- Deberá existir un "Registro de Accesos", cuyo diseño deberá incorporarse en la Relación de Medidas de Seguridad de la base de datos correspondiente.

9.1.2.2. Registro de accesos

Las bases de datos que deban adoptar un nivel de seguridad alto deberán contar con un registro para guardar, como mínimo durante dos años, la siguiente información:

- Identificación del usuario que ha accedido
- Fecha y hora del acceso.
- Base de datos accedida y tipo de acceso.
- Si se autorizó o se denegó el acceso, guardando información que permita identificar el registro accedido, en su caso.

Este registro estará bajo el control del Departamento de Datos Personales, . Se deberán implementar medidas que impidan la desactivación de los registros. La información de control registrada deberá revisarse periódicamente y elaborarse un informe, al menos cada dos meses, sobre las revisiones realizadas y los problemas detectados.

9.1.2.3. Registro de accesos

Las bases de datos que deban adoptar un nivel de seguridad alto deberán contar con un registro para guardar, como mínimo durante dos años, la siguiente información:

- Identificación del usuario que ha accedido
- Fecha y hora del acceso.
- Base de datos accedida y tipo de acceso.
- Si se autorizó o se denegó el acceso, guardando información que permita identificar el registro accedido, en su caso.

Este registro estará bajo el control del Departamento de Datos Personales en la persona de los responsables operativos y funcionales del área de seguridad de CIRION. Se deberán implementar medidas que impidan la desactivación de los registros. La información de control registrada deberá revisarse periódicamente y elaborarse un informe, al menos cada dos meses, sobre las revisiones realizadas y los problemas detectados.

9.2. Medidas de seguridad sobre bases de datos no automatizadas

Dado que la LFPD y su Reglamento resultan aplicables al tratamiento de datos personales que obren tanto en soportes electrónicos como físicos, también resulta necesario adoptar medidas de seguridad sobre las bases de datos no automatizadas, que deberán desarrollarse en la Relación correspondiente.

Conforme a lo anterior, **CIRION** también deberá tomar en cuenta los factores y elementos a que se refiere el artículo 60 del Reglamento de la LFPD, en relación con las medidas de seguridad aplicables a los sistemas de tratamiento no automatizados.

Siendo lo anterior, a continuación se identifican las medidas de seguridad mínimas aplicables a bases de datos no automatizadas.

9.2.1. Medidas de Seguridad de NIVEL BÁSICO

9.2.1.1. Criterios de archivo y clasificación de los soportes físicos

El archivo de los soportes o documentos se realizará de acuerdo con los criterios previstos en su respectiva legislación.

Estos criterios deberán garantizar la correcta conservación de los documentos, la localización y la consulta de la información; de tal forma que se posibilite y garantice el ejercicio de los derechos ARCO conforme al procedimiento descrito en el apartado 3.2.5 de esta Política.

En aquellos casos en los que no exista norma aplicable sobre el archivo de la documentación, deberá implementarse el procedimiento correspondiente, mismo que deberá ser aprobado por el Departamento de Datos Personales de **CIRION**.

9.2.1.2. Dispositivos de almacenamiento

Los dispositivos de almacenamiento de los documentos que contengan datos personales deberán disponer de mecanismos que obstaculicen su apertura (por ejemplo, cerraduras con llave o con acceso mediante combinación). Cuando las características físicas de aquéllos no permitan adoptar esta medida, **CIRION** adoptará medidas que impidan el acceso de personas no autorizadas a las zonas en que dichos dispositivos se encuentren.

9.2.1.3. Custodia de los soportes

Mientras la documentación con datos personales no se encuentre archivada en los dispositivos de almacenamiento establecidos, por estar en procesos de revisión o tramitación, con carácter previo o posterior a su archivo, la persona que se encuentre a cargo de la misma deberá custodiarla e impedir en todo momento que pueda ser accedida por personas no autorizadas.

9.2.2. Medidas de Seguridad de NIVEL MEDIO

9.2.2.1. Auditoría

Las bases de datos no automatizadas a las que resulten aplicables las medidas de seguridad de este nivel se someterán, al menos cado dos años, a una auditoría interna o externa que verifique el cumplimiento de las disposiciones del Reglamento de la LFPD y de las Recomendaciones en Materia de Seguridad de Datos Personales, emitidas por el entonces IFAI.

9.2.3. Medidas de Seguridad de NIVEL ALTO

9.2.3.1. Almacenamiento de la información

Los armarios, archivadores u otros dispositivos en los que se almacenen las bases de datos no automatizadas que contienen datos personales sensibles deberán encontrarse en áreas en las que el acceso esté protegido con puertas de acceso con sistema de apertura mediante llave, u otro dispositivo equivalente o superior. Dichas áreas deberán permanecer cerradas cuando no sea preciso el acceso a los documentos incluidos en la base de datos.

Si no fuese posible llevar a cabo estas medidas, el Departamento de Datos Personales deberá promover y adoptar medidas alternativas que, debidamente motivadas, deberán incluirse en la correspondiente Relación de Medidas de Seguridad

9.2.3.2. Copia o reproducción

Sólo se podrán realizar copias o reproducciones de los documentos bajo el control y supervisión del personal autorizado para tratar la documentación que contiene datos personales sensibles. Deberá procederse a la destrucción de las copias o reproducciones desechadas, de forma que se evite el acceso a la información contenida en las mismas, o su recuperación posterior.

9.2.3.3. Acceso a la documentación

El acceso a la documentación se limitará exclusivamente al personal autorizado. También se deberán establecer mecanismos que permitan identificar los accesos realizados a los documentos que puedan ser utilizados por varios usuarios autorizados.

El acceso por parte de personas no autorizadas deberá quedar adecuadamente registrado.

9.2.3.4. Traslado de documentos

Siempre que se proceda al traslado físico de la documentación contenida en una base de datos de este tipo, deberán adoptarse medidas dirigidas a impedir el acceso o manipulación de la información que ha de ser trasladada.

10. EFECTIVIDAD Y DEROGACIÓN

El presente documento entrará en vigor el día primero del mes siguiente a la fecha de su comunicación interna a las Áreas involucradas y deroga cualquier otra comunicación interna relativa a la seguridad de datos personales tratados en los sistemas de información de **CIRION**.

Cualquier propuesta de modificación, corrección o mejora de la presente Política de Protección de Datos Personales se dirigirá al Departamento de Datos Personales:

DATOS DE CONTACTO		
VP, General Counsel Latam	**Litigation & Employment**	**valeria.plastino@ciriontechnologies.com**

Tabla 3. Datos de Contacto - Departamento de Datos Personales

11. ANEXO PRIMERO. Modelo de cláusulas para regular el encargo de tratamiento de datos personales

11.1. Convenio de Protección de Datos Personales para contratos preexistentes con proveedores (prestadores de servicios) con acceso a datos personales

El siguiente Convenio Modificatorio deberá ser añadido en todos aquellos contratos preexistentes celebrados con Proveedores o Prestadores de Servicios que en función de sus actividades tengan acceso a, y traten datos personales.

Para el caso de contratos de nueva celebración, se recomienda su implementación a través de un Anexo (Convenio de Protección de Datos Personales) que, adaptado al caso concreto, reproduzca las definiciones y cláusulas que a continuación se refieren:

CONVENIO DE PROTECCIÓN DE DATOS PERSONALES CELEBRADO ENTRE [*] **[Entidad de CIRION] Y** [*] **("EL PRESTADOR").**

DEFINICIONES

A efectos de lo dispuesto en el presente Convenio, se entenderá por:

a) **RESPONSABLE**: [*] [Entidad de **CIRION**].

b) **ENCARGADO**: [*] [SOCIEDAD ENCARGADA DEL TRATAMIENTO POR CUENTA DEL RESPONSABLE].

c) **Partes**: El RESPONSABLE y ENCARGADO, en conjunto.

d) **Contrato de Servicios**: Aquél o aquellos celebrado(s) entre el ENCARGADO y el RESPONSABLE, que regula(n) la prestación del primero al segundo de Servicios, en los términos y condiciones pactados en el(los) mismo(s).

e) **Convenio:** El presente convenio de protección de datos personales.

f) **LFPD:** La Ley Federal de Protección de Datos Personales en Posesión de los Particulares, vigente en el territorio de los Estados Unidos Mexicanos (en adelante, "México").

g) **RLFPD**: El Reglamento de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, vigente en el territorio de México.

PERSONAL DATA PROTECTION AGREEMENT [*] **BETWEEN** [*] **[CIRION Entity] AND** [*] **[NAME OF THE SERVICE PROVIDER] (THE PROVIDER) TO REGULATE DATA PROCESSING.**

DEFINITIONS

For the purposes of the provisions of this Agreement, the following definitions shall apply:

a) **DATA CONTROLLER OR CONTROLLER:** [*] [**CIRION** Entity].

b) **DATA PROCESSOR OR PROCESSOR:** [*] [Processing Entity in the name of the Data Controller].

c) **Parties:** The DATA CONTROLLER and DATA PROCESSOR, jointly.

d) **Service Agreement:** means the agreement(s) dated between the Processor and Controller, consisting on the regulation of Services, in the terms and conditions established in said agreement(s).

e) **Agreement:** This personal data protection agreement.

f) **LFPD:** The Federal Law on the Protection of Personal Data held by Private Parties, in force in Mexico.

g) **RLFPD:** The Regulations of the Federal Law on the Protection of Personal Data held by Private Parties, in force in Mexico.

h) **Lineamientos:** Los Lineamientos del Aviso de Privacidad, vigentes en el territorio de México.

i) **Recomendaciones:** Las Recomendaciones en Materia de Seguridad de Datos Personales, vigentes en el territorio de México.

i) **DATOS:** Datos personales, en los términos a que se refiere el artículo 3, fracción V de la LFPD, contenidos en BASES DE DATOS titularidad del RESPONSABLE.

k) **BASES DE DATOS:** Conjunto organizado de DATOS, en los términos a que se refiere el artículo 3, fracción II de la LFPD.

l) **TITULARES:** Las personas físicas a quienes corresponden los DATOS.

m) **SUBCONTRATADO:** Conforme al artículo 54 del RLFPD, la persona física o moral subcontratada por el ENCARGADO, con autorización del RESPONSABLE, para la prestación de servicios que impliquen el tratamiento de DATOS o BASES DE DATOS del RESPONSABLE, en el marco de ejecución del Contrato de Servicios.

n) **Tratamiento:** Conforme al artículo 3, fracción XVIII de la LFPD, la obtención, uso, divulgación o almacenamiento de datos personales, por cualquier medio. El uso abarca cualquier acción de acceso, manejo, aprovechamiento, transferencia o disposición de datos personales.

o) **Vulneración de Seguridad de Datos Personales**: Conforme a lo dispuesto por el artículo 64 del RLFPD, y en cualquier fase del tratamiento:

- La pérdida o destrucción no autorizada de DATOS o BASES DE DATOS;
- El robo, extravío o copia no autorizada de DATOS o BASES DE DATOS;
- El uso, acceso o tratamiento no autorizado de DATOS o BASES DE DATOS, o
- El daño, la alteración o modificación no autorizada de DATOS o BASES DE DATOS.

h) **Guidelines:** The Privacy Notice Guidelines, in force in Mexico.

i) **Recommendations:** The Recommendations on Security of Personal Data, in force in Mexico.

j) **DATA:** Personal data, in the terms of the LFPD, article 3, section V, contained in the DATABASES under the control of the Controller.

k) **DATABASES:** The ordered set of personal DATA, in terms of the LFPD, article 3, section II.

l) **DATA SUBJECTS:** The individuals to whom DATA relates.

m) **SUBCONTRACTOR:** In terms of the RLFPD, article 54, the individual or legal entity subcontracted by the PROCESSOR, authorized by the CONTROLLER, for the provision of services involving the processing of DATA or DATABASES, under the execution of the Service Agreement.

n) **Processing:** In accordance with the LFPD, article 3, section XVIII, the retrieval, use, disclosure or storage of personal data by any means. Use covers any action of access, management, exploitation, transfer or disposal of personal data.

o) **Data Security Breaches:** In accordance with the RLFPD, article 63:

- The loss or unauthorized destruction of DATA or DATABASES;
- The theft, misplacement or unauthorized copying of DATA or DATABASES;
- The Unauthorized use, access or processing of DATA or DATABASES;
- The Unauthorized damage, alteration or modification of DATA or DATABASES.

DECLARACIONES

PRIMERA.- Que en el marco del Contrato de Servicios, el RESPONSABLE y el ENCARGADO acordaron el marco de términos y condiciones en el que el ENCARGADO prestará al RESPONSABLE los servicios especificados en el Contrato de Servicios.

RECITALS

FIRST.- In the framework of the Service Agreement, the CONTROLLER and PROCESSOR agreed the terms and conditions upon which the PROCESSOR will provide to the CONTROLLER the services defined in the Service Agreement.

SEGUNDA.- Que el RESPONSABLE y el ENCARGADO acuerdan mantener en todo su alcance y contenido las disposiciones y cláusulas del Contrato de Servicios, salvo que cualquiera de sus disposiciones contradiga la normativa de protección de datos personales vigente en México, en cuyo caso prevalecerá lo dispuesto en el presente Convenio de Protección de Datos Personales.

SECOND.- The CONTROLLER and PROCESSOR shall maintain in all its scope and content the provisions and clauses of the Service Agreement, unless any of its provisions contradict the Mexican data protection legislation, in which case, shall prevail this Data Protection Agreement.

TERCERA.- Que el RESPONSABLE, por aplicación y en cumplimiento de la LFPD, lleva a cabo el tratamiento de DATOS de los cuales es responsable en los términos previstos en dicho ordenamiento.

THIRD.- Pursuant to and in compliance with the LFPD, the CONTROLLER will process DATA, for which it is responsible in the terms of such law.

En consecuencia, las Partes acuerdan suscribir el presente Convenio de Protección de Datos Personales, sujeto a las siguientes:

In accordance with the aforesaid, the Parties agree to subscribe this Data Protection Agreement, subject to the following:

CLÁUSULAS

CLAUSES

PRIMERA.- OBJETO

FIRST.- PURPOSE

Que el presente Convenio tiene por objeto el establecimiento y definición de las obligaciones a que se refiere el artículo 50 del RLFPD, en el marco de las cuales el ENCARGADO podrá llevar a cabo el tratamiento de los DATOS a que tenga acceso en virtud del Contrato de Servicios, y que están contenidos en las BASES DE DATOS del RESPONSABLE, con la finalidad de realizar las actividades encomendadas por el RESPONSABLE al ENCARGADO a través del Contrato de Servicios.

The purpose of this Agreement is to establish and define the obligations in accordance with the RLFPD, article 50, by which the PROCESSOR may process and transfer DATA that it might have access to, contained in the CONTROLLER's DATABASES. The aforesaid, with the purpose of performing the activities per instructions of the CONTROLLER according to the Service Agreement.

SEGUNDA. TRATAMIENTO Y PROTECCIÓN DE DATOS PERSONALES

SECOND.- PERSONAL DATA PROCESSING AND PROTECTION

El RESPONSABLE reconoce que, en el marco de ejecución y cumplimiento del Contrato de Servicios celebrado con el ENCARGADO, el primero podrá encargar al segundo el tratamiento de DATOS contenidos en las BASES DE DATOS del primero. El ENCARGADO se obliga a respetar todas y cada una de las obligaciones que pudieran corresponderle como "encargado" con arreglo a las disposiciones de la LFPD, su Reglamento, y cualquier otra disposición complementaria o regulación que resulte aplicable.

The DATA CONTROLLER, in accordance with the execution and compliance to the Service Agreement, may request the PROCESSOR the processing of DATA contained in the CONTROLLER's DATABASES; for this reason, the PROCESSOR agrees to respect all of its obligations under the LFPD, RLFPD, and if applicable, other Mexican data protection provisions.

En concreto, el ENCARGADO deberá cumplir con las siguientes obligaciones:

In particular, the PROCESSOR shall comply with the following obligations:

a) Tratar los DATOS contenidos en las BASES DE DATOS única y exclusivamente conforme a las instrucciones que reciba expresamente del RESPONSABLE.

a) Process all DATA contained in the DATABASES, uniquely and exclusively pursuant the explicit instructions of the CONTROLLER.

b) No destinar o utilizar los DATOS para cualquier otro fin distinto al expresamente indicado por el RESPONSABLE, o de cualquier otra forma que suponga un incumplimiento de las instrucciones expresas que el RESPONSABLE le proporcione.

b) Not to use the DATA for any other purposes than those explicitly indicated by the CONTROLLER, or in any other form fail to comply with the explicit instructions provided by the CONTROLLER.

c) No revelar, transferir, ceder o de otra forma comunicar las BASES DE DATOS ni los DATOS en ellas contenidos, ya sea verbalmente o por escrito, por medios electrónicos, papel o mediante acceso informático, ni siquiera para su conservación, a ningún tercero. A tal efecto, el ENCARGADO sólo podrá permitir el acceso a los DATOS a aquellos empleados que tengan necesidad de conocerlos, exclusivamente, para la prestación de los servicios contratados y siempre que tales empleados estén sujetos a las mismas obligaciones de confidencialidad y protección de datos personales que aquí se establecen.

c) Not to disclose, transfer, assign or otherwise communicate the DATABASES or the DATA contained thereof to third parties. The aforesaid, including through verbal, written, or electronic means, not even for DATA storage. In these terms, the PROCESSOR shall guarantee that the DATA is accessible only to its personnel who need to have access to such DATA in order to carry out the contracted services, and with the condition that the personnel shall be subject to the same confidentiality and data protection obligations established herein.

d) Garantizar al RESPONSABLE la adopción y el mantenimiento de las medidas de seguridad que correspondan al tipo de DATOS objeto del tratamiento, de conformidad con lo dispuesto en la LFPD, el RLFPD y las Recomendaciones.

   En concreto, el ENCARGADO garantiza al RESPONSABLE, con carácter previo a la prestación de los servicios relacionados con el tratamiento de los DATOS, que reúne las condiciones necesarias para cumplir con las disposiciones del RLFPD y las Recomendaciones, correspondientes al tipo de DATOS contenidos en las BASES DE DATOS cuyo tratamiento le es encargado.

d) Guarantee the DATA CONTROLLER the adoption and maintenance of security measures according with the type of DATA to be processed, in terms of the LFPD, RLFPD and the Recommendations.

   In particular, the Processor guarantees the Controller, prior to the provision of the Services that it reunites all the necessary conditions to comply with the RLFPD and the Recommendations, in accordance with the type of DATA contained in the DATABASES that will be processed upon request.

e) Destruir o devolver al RESPONSABLE (según éste le indique a la terminación por cualquier causa del Contrato de Servicios, o de los servicios relativos a las BASES DE DATOS o los DATOS, o parte de ellos) la totalidad o aquella parte de las BASES DE DATOS o DATOS correspondientes, así como cualesquiera copias o soportes en los que éstos estuviesen contenidos, debiendo certificar inmediatamente por escrito dicha devolución o destrucción.

e) Destroy or return to the CONTROLLER (as the latter prescribes, on termination of the Service Agreement, or of the services regarding in its whole, or part of, the DATABASES or the DATA), the totality or part of the corresponding DATABASES or DATA, as well as any other copies or supports in which they are being held. Moreover the PROCESSOR shall confirm promptly in writing to the CONTROLLER that the PROCESSOR has complied with such destruction or return.

TERCERA.- VULNERACIONES DE SEGURIDAD DE DATOS PERSONALES

El ENCARGADO estará obligado a comunicar al RESPONSABLE cualquier vulneración de seguridad relacionada con los DATOS a su cargo, que pudiese ocurrir en cualquier fase del tratamiento bajo su responsabilidad o bajo la responsabilidad de un SUBCONTRATADO, en su caso.

A tales efectos, y con el objeto de que el RESPONSABLE cuente con la información y documentación necesaria para actuar conforme lo dispuesto por los artículos 64 y 65 del RLFPD, si el ENCARGADO sufre una vulneración de seguridad relacionada con dichos DATOS, éste deberá comunicar la ocurrencia de la vulneración de seguridad al RESPONSABLE, tan pronto tenga conocimiento de la misma, trasladando a este último, al menos, la siguiente información:

1. La naturaleza del incidente (incluyendo la información sobre las circunstancias en que éste ocurrió);
2. Los datos personales comprometidos;
3. Las acciones correctivas que hubiese realizado de forma inmediata, una vez haya confirmado que ocurrió la vulneración de seguridad;
4. Cualquier información que permita al RESPONSABLE comunicar a los TITULARES las medidas que puedan adoptar para proteger sus intereses, y
5. Los medios a través de los cuales podrá obtener más información sobre la vulneración, para poder informar a los TITULARES cualquier información relevante al respecto

CUARTA.- PRESTACIÓN DE SERVICIOS EN LAS INSTALACIONES O LOCALES DEL ENCARGADO

Cuando en atención a la naturaleza de los servicios contratados los DATOS deban ser tratados fuera de las instalaciones del RESPONSABLE, las Partes reconocen que el ENCARGADO deberá prestar los servicios comprendidos en el Contrato de Servicios, en sus propias instalaciones.

En virtud de lo anterior, el RESPONSABLE autoriza expresamente al ENCARGADO para que en ejecución y cumplimiento de dicho Contrato preste los servicios contratados y por lo tanto trate los DATOS de las BASES DE DATOS en sus propias instalaciones o locales.

THIRD.- PERSONAL DATA SECURITY BREACHES

The PROCESSOR shall inform the CONTROLLER any security breach affecting the DATA or the DATABASES, which may occur at any phase of the data processing, either at its responsibility or, if applicable, under the responsibility of a SUBCONTRACTOR.

Accordingly, and in order to provide the CONTROLLER with the necessary information and documentation to act pursuant to articles 64 and 65 of the RLFPD, if the PROCESSOR suffers a Data Security Breach, the PROCESSOR shall notify it immediately to the CONTROLLER, while providing at least, the following information:

1. The nature of the breach (including the circumstances in which it happened);
2. The personal data compromised;
3. Corrective actions immediately implemented, once the breach has being confirmed;
4. Any information that allows the CONTROLLER to notify DATA SUBJECTS about the measures that they may adopt to protect their interests, and
5. The means by which the CONTROLLER may obtain more information regarding the breach. The aforesaid, in order that the CONTROLLER may inform DATA SUBJECTS.

FOURTH.- PROVISION OF SERVICES IN THE FACILITIES OF THE PROCESSOR

When the nature of the contracted services require that DATA must be processed off-site the CONTROLLER's premises the PROCESSOR shall perform such services at its own premises or facilities.

Pursuant the foregoing, the CONTROLLER explicitly authorizes the PROCESSOR that in virtue of the execution and compliance of the Service Agreement, to provide the services and therefore process the DATA contained in the DATABASES in its own premises or facilities.

QUINTA. MEDIDAS DE SEGURIDAD

Conforme a lo dispuesto en el artículo 50, fracción III del RLFPD y las Recomendaciones, las partes contratantes acuerdan que, en relación con las BASES DE DATOS, el ENCARGADO deberá implementar las medidas de seguridad correspondientes, y cualesquiera otras que le fueren impuestas para garantizar la correcta protección de los DATOS en cada caso, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a los que estén expuestos.

SEXTA. POSIBILIDAD DE SUBCONTRATACIÓN DE LOS SERVICIOS

Cuando el ENCARGADO subcontrate cualquiera de los servicios previstos en el Contrato de Servicios (siempre y cuando dicha subcontratación esté permitida en el Contrato de Servicios), y dicha subcontratación implique acceso o tratamiento de los DATOS o BASES DE DATOS del RESPONSABLE, el ENCARGADO deberá formalizar la relación con el SUBCONTRATADO a través de un acuerdo que satisfaga los términos previstos en el artículo 54 del RLFPD. Para tales efectos, el ENCARGADO deberá suscribir un acuerdo por escrito en el que se deberá hacer constar que el tratamiento de los DATOS por parte del SUBCONTRATADO se ajustará a las instrucciones del RESPONSABLE y que el SUBCONTRATADO último asume las mismas obligaciones que se establecen para los encargados en la LFPD, en el RLFPD y demás disposiciones aplicables.

Hasta en tanto el ENCARGADO no hubiere celebrado con el SUBCONTRATADO el contrato a que se refiere el párrafo anterior, el primero no podrá comunicar, otorgar acceso, ni de ninguna otra forma permitir que el segundo trate DATOS o BASES DE DATOS del RESPONSABLE.

SÉPTIMA. DERECHOS DE LOS TITULARES

Los derechos de acceso, rectificación, cancelación y oposición (derechos ARCO) a que se refiere la LFPD y su Reglamento se ejercitarán por los Titulares frente al RESPONSABLE, debiendo el ENCARGADO remitir de forma inmediata a aquél cualquier solicitud que pudiese recibir en dicho sentido.

FIFTH.- SECURITY MEASURES

Pursuant to the RLFPD, article 50, section III, and the Recommendations, the Parties agree that the DATA PROCESSOR shall implement the appropriate security measures (and any others required by sectorial laws and/or regulations) in order to guarantee the DATA integrity, disposition and confidentiality, in every case. For these purposes, the DATA PROCESSOR shall take into account state of the art technology and the risks to which DATA and DATABASES may be exposed.

SIXTH. SUB-CONTRATING OF SERVICES

When the PROCESSOR sub-contracts any of the services defined in the Service Agreement (provided such sub-contacting is permitted under the Service Agreement), and the sub-contracting implies access or processing of the CONTROLLER's DATA or DATABASES, the PROCESSOR shall formalize the relationship with the SUB-CONTRACTOR, by entering into an agreement in the terms of the RLFPD article 54. In these terms, the DATA PROCESSOR shall subscribe a written agreement, in which explicitly shall be stated that the DATA processing requested to the SUB-CONTRACTOR shall always be in accordance with the instructions of the CONTROLLER, and that the SUB-PROCESSOR assumes the same obligations established to data processors pursuant to the LFPD, RLFPD and other applicable legislation.

If the PROCESSOR does not have entered into the aforesaid agreement with the SUB-CONTRACTOR, the PROCESSOR may not communicate, grant access or in any other way allow the SUB-CONTRACTOR to process the CONTROLLER's DATA or DATABASES.

SEVENTH.- DATA SUBJECTS' RIGHTS

The rights of access, rectification, cancelation and opposition (ARCO rights), referred in the LFPD and RLFPD, must be requested before the CONTROLLER by DATA SUBJECTS. The PROCESSOR shall immediately communicate to the CONTROLLER any kind of request filed before said PROCESSOR.

OCTAVA. RESPONSABILIDAD

El ENCARGADO será responsable e indemnizará al RESPONSABLE por cualquier reclamación, costo, pérdida, daño de terceros o responsabilidad contraída y que se derive directa o indirectamente del incumplimiento del presente Convenio o de las disposiciones normativas aplicables de protección de datos personales.

En particular, si el ENCARGADO destina los DATOS a otra finalidad que la prevista en el Contrato de Servicios, los comunica o los utiliza incumpliendo las estipulaciones del presente Convenio o en las disposiciones legales aplicables, será considerado también como "responsable" en los términos establecidos en la LFPD.

EIGHT.- LIABILITY

The PROCESSOR will be liable and shall indemnify the CONTROLLER from all third party claims, costs, losses, or damages arising directly or indirectly out of any breach of this Agreement or the provisions of the data protection legislation in force in Mexico.

In particular, if the PROCESSOR processes the DATA for any other purposes than those established in the Services Agreement, or the applicable legal provisions, communicates or uses said DATA violating the provisions established herein, it shall be considered as a "controller" in accordance with the LFPD.

NOVENA. COMUNICACIÓN DEL AVISO DE PRIVACIDAD

En los términos previstos en el Lineamiento Decimoquinto de los Lineamientos del Aviso de Privacidad publicados en el Diario Oficial de la Federación de fecha 17 de enero de 2013, el RESPONSABLE comunica al ENCARGADO el Aviso de Privacidad que regula el tratamiento de los DATOS necesario para la ejecución del Contrato de Servicios, mediante la entrega de copia íntegra del mismo que se anexa al presente Convenio.

El ENCARGADO también podrá acceder a dicho Aviso de Privacidad a través del siguiente enlace: [*] donde podrá consultar cualquier modificación o actualización que el RESPONSABLE pudiera implementar sobre el mismo, sin perjuicio de que el RESPONSABLE comunique al ENCARGADO cualquier modificación o actualización a través de los medios convenidos para el envío de notificaciones entre las partes.

NINTH.- PRIVACY NOTICE COMMUNICATION

In terms of the Fifteenth Guideline of the Privacy Notice Guidelines, published on January 17, 2013 in the Mexican Official Gazette, the CONTROLLER shall communicate to the PROCESSOR the Privacy Notice, regulating the necessary DATA processing for the execution of the Services Agreement. The CONTROLLER shall give the PROCESSOR a full copy of the Privacy Notice, enclosed herein.

The PROCESSOR may as well have access to the aforementioned Privacy Notice through the following link: [*]; in which it may consult any further modification or amendment made by the CONTROLLER, notwithstanding that the CONTROLLER shall communicate those modifications or amendments through the established means between the Parties.

DÉCIMA.- IDIOMA

El texto íntegro de este Convenio ha sido redactado en los idiomas español e inglés, considerándose ambas versiones como válidas. No obstante, para efectos de interpretación legal prevalecerá la versión en idioma español.

TENTH.- LANGUAGE

The full text of this Agreement has been drafted in Spanish and English languages, both versions being authentic. However, for legal interpretations, the Spanish version shall prevail.

DÉCIMA PRIMERA.- JURISDICCIÓN Y LEY APLICABLE

Para todo lo relativo a la interpretación, cumplimiento y ejecución del presente Convenio, serán aplicables las leyes de los Estados Unidos Mexicanos.

Para el presente Convenio, serán competentes los tribunales de la Ciudad de México, Distrito Federal.

ELEVENTH.- JURISDICTION AND APPLICABLE LAW.

For all matters relating to the interpretation, compliance and enforcement of this Agreement, the laws of Mexico shall apply.

For this Agreement, the courts of Mexico City, Federal District shall be competent.

Las Partes se reconocen mutuamente la personalidad con que comparecen y en pleno conocimiento y entendimiento del contenido y alcance del presente Convenio, lo firman y ratifican por duplicado en [*] el día [*] de [*].

In witness whereof, this Agreement has been signed in [*] originals, of which the Parties have received one each, on [*].

11.2. Modelo de cláusulas para contratos con proveedores (prestadores de servicios) sin acceso a datos personales

El presente modelo de cláusulas debe ser adoptado por **CIRION** para ser incluido en aquellos servicios que por su propia naturaleza no requieren que los prestadores del servicio tengan acceso a datos personales, pero que por su naturaleza podrían permitir que sus empleados o personal lo tuviesen (p.e. servicio de limpieza, mantenimiento de equipo, etc.):

***INFORMACIÓN CONFIDENCIAL Y DATOS PERSONALES**. Las Partes manifiestan y reconocen que para la ejecución y cumplimiento del presente contrato, ni [PRESTADOR DEL SERVICIO], ni su personal (propio o externo) requieren tener acceso, disponer de copias ni de ninguna otra forma acceder, tratar, manejar o copiar: (i) información confidencial, (ii) información financiera, (iii) información sujeta al secreto bancario, (iv) información relativa a la propiedad industrial o intelectual y/o (v) datos personales, de cuyo tratamiento sea responsable [ENTIDAD DE CIRION].*

No obstante lo anterior, si por cualquier motivo o causa ajena a la voluntad expresa de cualquiera de las Partes, el personal de [PRESTADOR DEL SERVICIO] dedicado a la ejecución y cumplimiento de los servicios objeto del contrato de prestación de servicios en las instalaciones o sistemas de [ENTIDAD CIRION] tuviese acceso, por cualquier medio, a cualquier tipo de información a la que no deba tener acceso, desde ese momento quedará individualmente sujeto al deber de confidencialidad, y en particular a lo dispuesto artículo 21 de la Ley Federal de Protección de Datos Personales en Posesión de los Particulares, y demás disposiciones aplicables.

[PRESTADOR DEL SERVICIO] será responsable de comunicar a su personal la existencia del deber de confidencialidad a que se refiere el párrafo anterior, con independencia de las instrucciones que deba trasladar a aquéllos para que se abstengan de acceder a cualquier tipo de información cuyo tratamiento sea responsabilidad de [ENTIDAD CIRION], cuando presten sus servicios en cualesquiera de sus instalaciones.

12. ANEXO SEGUNDO. Departamento de Datos Personales y Responsables Funcionales

DEPARTAMENTO DE DATOS PERSONALES

Figura	Cargo	Área
Responsables Funcionales y Operativos de Datos Personales en México	Sr Mgr, Marketing and Communication - Cluster	Strategic Marketing
	Training & Development Coordinator Regional	Human Resources Operations
	Senior Physical Security Regional	Global Security
	Dir, Sales	Enterprise Latam
	Dir, Legal and Compliance Cluster	Litigation & Employment
	Senior Procurement Manager I	Strategic Sourcing Procurement

** Se aclara que los cargos de los Responsables Funcionales y Operativos constantes en el presente Anexo, recaen en aquellas personas que ocupen las posiciones determinadas y que se encuentren a cargo del manejo de la operación de CIRION México bajo cualquier de sus denominaciones actuales o futuras.

13. ANEXO TERCERO. Inventario de Bases de Datos Personales y Sistemas de Tratamiento

BASE DE DATOS	RESPONSABLES FUNCIONALES Y OPERATIVOS	ÁREA	TIPO DE TRATAMIENTO	SISTEMA DE INFORMACIÓN	NIVEL DE SEGURIDAD	ENCARGOS DEL TRATAMIENTO	TRANSFERENCIAS
EMPLEADOS	**Training & Development Coordinator Regional (A cargo de México)**	**Human Resources Operations**	**Mixto**	**Oracle EBS**	**Alto**	**Procesamiento Externo de Información, S.C.**	• Compañías matrices, afiliadas o subsidiarias de CIRION, • Organismos públicos, administraciones públicas federales, estatales o municipales u órganos judiciales, • Bancos u otras entidades financieras, • Agentes de seguros o sociedades aseguradoras, • Sindicatos, • Organismos, entidades o autoridades en el extranjero, • Terceros nacionales o extranjeros, • Propietarios o representantes legales de inmuebles ocupados por CIRION, y • Prestadores de servicios.
CANDIDATOS	**Training & Development Coordinator Regional (A cargo de México)**	**Human Resources Operations**	**Mixto**	**Oracle EBS**	**Medio**	**N/A**	• Compañías matrices, afiliadas o subsidiarias de CIRION, y • Prestadores de servicios.
CONTROL DE ACCESOS	**Senior Physical Security Regional (A cargo de México)**	**Global Security**	**No Automatizado**	**Bitácora de Visitantes**	**Básico**	**N/A**	No existen para las finalidades del tratamiento.
VIDEOVIGILANCIA	**Senior Physical Security Regional (A cargo de México)**	**Global Security**	**Automatizado**	**Sistema de CCTV (local)**	**Básico**	**N/A**	No existen para las finalidades del tratamiento.
CLIENTES	**Sr Mgr, Marketing and Communication – Cluster (A cargo de México)**	**Strategic Marketing**	**Mixto**	**SIEBEL, ELOQUA, SMCM y OUTLOOK**	**Medio**	**N/A**	• Compañías matrices, afiliadas o subsidiarias de CIRION, • Organismos públicos; administraciones públicas

BASE DE DATOS	RESPONSABLES FUNCIONALES Y OPERATIVOS	ÁREA	TIPO DE TRATAMIENTO	SISTEMA DE INFORMACIÓN	NIVEL DE SEGURIDAD	ENCARGOS DEL TRATAMIENTO	TRANSFERENCIAS
CLIENTES	**Dir, Sales (A cargo de México)**	**Enterprise Latam**					federales, estatales o municipales u órganos judiciales, • Organismos, entidades o autoridades en el extranjero, • Prestadores de servicios • Terceros (alianzas comerciales).
LIBROS Y ACTAS	**Dir, Legal and Compliance Cluster (A cargo de México)**	**Litigation & Employment**	**Mixto**	**Libro de Actas** **Servidor con copias electrónicas de las actas**	**Básico**	**N/A**	• Compañías matrices, afiliadas o subsidiarias de CIRION, y • Organismos Públicos; administraciones públicas federales, estatales o municipales; comisiones; institutos y/o entidades reguladoras.
PROVEEDORES	**Senior Procurement Manager I (A cargo de México)**	**Strategic Sourcing Procurement**	**Mixto**	**SIEBEL y OUTLOOK**	**Medio**	**N/A**	• Compañías matrices, afiliadas o subsidiarias de CIRION, y • Organismos Públicos; administraciones públicas federales, estatales o municipales; comisiones; institutos y/o entidades reguladoras

** Se aclara que los cargos de los Responsables Funcionales y Operativos constantes en el presente Anexo, recaen en aquellas personas que ocupen las posiciones determinadas y que se encuentren a cargo del manejo de la operación de CIRION México bajo cualquier de sus denominaciones actuales o futuras .09

14. ANEXO CUARTO. Ediciones y revisiones

EDICIÓN	REVISIÓN	FECHA	APARTADOS	OBSERVACIONES
PRIMERA	15/03/2016	15/03/2016		Creación
	09/10/2020	09/10/2020		Modificación para incorporar cambio a LUMEN
	09/10/2020	09/10/2022		Modificación para incorporar cambio a CIRION TECHNOLOGIES
SEGUNDA				
TERCERA				