
LERROUX
BUSINESS LAWYERS

LERROUX

BUSINESS LAWYERS

REGLAMENTO EUROPEO DE PROTECCIÓN DE DATOS

FREMM

LERROUX BUSINESS LAWYERS

¿Por qué se necesita una nueva normativa en forma de Reglamento Europeo?

- Mayor flujos transfronterizos de datos => Mercado interior
- Rápida evolución tecnológica y globalización
- Tratamiento de datos permite => nuevos y mejores servicios, productos e investigación

Riesgos:

- Datos se multiplican exponencialmente:
- Son más accesibles, mas actores y más fáciles de procesar.
- Más difícil el control: destino y usos
- Mayores flujos transfronterizos
- La tecnología ha transformado la vida social y la economía

- Norma obligatoria en todos sus elementos y directamente aplicable en todos los Estados miembros (artículo 288 TFUE).
- Todos los sujetos el mismo nivel de derechos, obligaciones y responsabilidades
- Garantiza: supervisión coherente
- Sanciones equivalentes
- Cooperación autoridades de control

FREMM

LERROUX
BUSINESS LAWYERS

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El Reglamento General de Protección de Datos (RGPD) tiene como objetivo principal garantizar un nivel equivalente de protección de los datos personales entre los Estados miembros de la Unión Europea y asegurar la libre circulación de los mismos en el territorio europeo.

Entró en aplicación el 25 de mayo de 2018 para todos los Estados Miembros de la UE, tanto las Instituciones como empresas y organizaciones deben adaptarse a sus disposiciones si no quieren enfrentarse a unas sanciones económicas cuya cuantía se ha incrementado considerablemente respecto la anterior legislación.

Aunque el Reglamento resulta de aplicación directa y no requiere desarrollo por parte de los Estados miembros, se está desarrollando una ley de protección de datos que tendrá un carácter residual respecto el RGPD.

FREMM

LERROUX
BUSINESS LAWYERS

REGLAMENTO GENERAL DE PROTECCIÓN DE DATOS

El Reglamento regula el tratamiento total o parcialmente automatizado, de datos personales así como el tratamiento no automatizado de datos personales contenidos o destinados a ser incluidos en un fichero.

El RGPD se aplicará al tratamiento de datos en el contexto de las actividades de un establecimiento del responsable o del encargado de la Unión, independientemente de que el tratamiento tenga lugar en la Unión o no.

También resultará de aplicación al tratamiento de datos personales cuyos titulares residan en la Unión, independientemente de que el responsable tenga establecimiento en la Unión o no, cuando el tratamiento se relaciona con la oferta de **bienes o servicios dirigidos a ciudadanos europeos** o cuando está relacionado con el control de su comportamiento en la medida en que este tiene lugar en territorio de la Unión.

FREMM

LERROUX BUSINESS LAWYERS

ÁMBITO DE APLICACIÓN TERRITORIAL

La aplicación del Reglamento se amplía a responsables y encargados **no establecidos en la UE** siempre que realicen tratamientos derivados de:

- Una oferta de bienes o servicios destinados a ciudadanos de la Unión independientemente de que deban pagar o no

- Como consecuencia de un control del comportamiento - monitorización y seguimiento-

Para que esta ampliación del ámbito de aplicación pueda hacerse efectiva, esas organizaciones deberán **nombrar un representante en la Unión Europea**, que actuará como punto de contacto de las Autoridades de supervisión y de los ciudadanos y que, en caso necesario, podrá ser **destinatario de las acciones de supervisión** que desarrollen esas autoridades.

Los datos de contacto de ese representante en la Unión **deberán proporcionarse a los interesados entre la información relativa a los tratamientos de sus datos personales.**

Representante: persona física o juridica establecida en el Unión designada por escrito por el Responsable o encargado para la realización de sus obligaciones.

FREMM

LERROUX
BUSINESS LAWYERS

¿Dónde no entra el Reglamento?

No se aplica:

- Al tratamiento de datos de personas jurídicas
- A datos de personas fallecidas
- Al tratamiento efectuado por una persona física en el ejercicio de actividades **exclusivamente personales o domésticas**.Sin conexión con actividad profesional o comercial (sin lucro) Ejmp: correspondencia, repertorio telefónico, actividades en redes sociales, actividades en línea siempre dentro del contexto.

FREMM

LERROUX BUSINESS LAWYERS

RESPONSABLE Y ENCARGADO

La normativa contempla dos figuras: El responsable del tratamiento y el encargado del tratamiento.

El responsable es la persona física o jurídica que determina los fines y medios del tratamiento puede ser persona física o jurídica, de naturaleza pública o privada, u órgano administrativo, que sólo o conjuntamente con otros decida sobre la finalidad, contenido y uso del tratamiento, aunque no lo realizase materialmente.

El encargado es la persona física o jurídica que trata los datos personales por cuenta del responsable.

La responsabilidad última sobre el tratamiento de los datos recae en el responsable, no obstante puede tener responsabilidad el encargado e incluso pueden tener una **responsabilidad compartida**.

La relación entre el responsable y el encargado deberá formalizarse mediante un contrato con un contenido mínimo regulado por el RGPD entre cuyas exigencias se encuentras establecer el objeto, duración y finalidad del tratamiento de los datos o los tipo de datos que van a ser tratados.

Al margen de este contenido mínimo regulado por contrato, el RGPD exige tanto al responsable como al encargado que lleve a cabo un registro de las actividades de tratamiento de datos personales así como de las medidas de seguridad aplicables.

A la hora de elegir a un encargado del tratamiento, el Reglamento exige al responsable que debe seleccionar a un encargado que ofrezca garantías suficientes respecto su adecuación a las disposiciones del RGPD.

FREMM

LERROUX BUSINESS LAWYERS

REQUISITOS DE CALIDAD

Requisitos de calidad para el tratamiento de datos de carácter personal:

- Han de ser los, pertinentes y no excesivos(para la finalidad perseguida)
- Tratados para finalidades determinadas, explícitas y legítimas.
- No podrán usarse para finalidades incompatibles.
- Deben ser exactos y puestos al día (de oficio o a instancia del interesado).
- Serán cancelados cuando hayan dejado de ser necesarios o pertinentes.
- No serán conservados durante un período superior al necesario.
- Serán almacenados de forma que permitan el ejercicio de derechos.
- Se prohíbe la recogida de datos por medios fraudulentos, desleales o ilícitos.

FREMM

LERROUX
BUSINESS LAWYERS

MINIMIZACION DE DATOS

Los datos personales tratados serán adecuados, pertinentes y limitados a lo necesario en relación con los fines para los que son tratados:

• Solo deben tratarse si la finalidad del tratamiento no pudiera lograrse razonablemente por otros medios (principios de proporcionalidad y necesidad)

• Es necesario garantizar que se limite a un mínimo estricto su plazo de conservación.

EXACTITUD DE DATOS

Los datos personales serán exactos y, si fuera necesario, actualizados.

Se adoptarán todas las medidas razonables para que se supriman o rectifiquen sin dilación los datos personales que sean inexactos con respecto a los fines para los que se tratan.

Se habilitarán medios para permitir a los afectados informar de las variaciones que puedan afectar a los datos tratados.

FREMM

LERROUX BUSINESS LAWYERS

LIMITACIÓN DEL PLAZO DE CONSERVACIÓN

Los datos personales serán mantenidos de forma que se permita la identificación de los interesados durante no más tiempo del necesario para los fines del tratamiento de los datos personales (excepciones en caso de fines de archivo en interés público, fines de investigación científica o histórica o fines estadísticos)

Para garantizar que los datos personales no se conservan más tiempo del necesario, el responsable del tratamiento ha de establecer plazos para su supresión o revisión periódica.

Se debe aportar información a los interesados para que al menos puedan valorar cuando van a ser suprimidos sus datos personales

FREMM

LERROUX BUSINESS LAWYERS

LICITUD DEL TRATAMIENTO

Respecto el principio de licitud, el RGPD establece un listado cerrado de causas por las cuales se considerará que el tratamiento es lícito:

-Obtención de los datos por el consentimiento del interesado
-La existencia de una relación contractual cuando los datos son necesarios para su ejecución
-Mandato legal
-Protección de intereses vitales
-Intereses legítimos del responsable o de un tercero siempre que sobre dichos intereses no prevalezcan los derechos fundamentales del interesado, en especial cuando sea menor

En relación al consentimiento del interesado, el responsable debe ser capaz de demostrar que aquel consintió de forma expresa, el tratamiento de sus datos. No es válido el consentimiento tácito o por omisión. Si el consentimiento se otorgara en una declaración en la que se haga referencia a otros asuntos, éste se prestara de tal forma que se distinga claramente del resto de asuntos.

De acuerdo al RGPD, cuando el interesado sea menor de 16 años no podrá otorgar consentimiento sobre el tratamiento de sus datos, se deberá recabar para ello el consentimiento de quien ostente su patria potestad. Los estados podrán rebajar la edad mínima hasta los 13 años. La LOPD situó el umbral en los 14 y el anteproyecto parece rebajarlos a los 13 años.

FREMM

LERROUX BUSINESS LAWYERS

PRIVACIDAD POR DISEÑO Y POR DEFECTO

Los datos personales serán tratados de tal manera que se garantice una seguridad adecuada de los datos personales, incluida la protección contra el tratamiento no autorizado o ilícito y contra su pérdida, destrucción o daño accidental, mediante la aplicación de medidas técnicas u organizativas apropiadas. El responsable del tratamiento debe adoptar políticas internas y aplicar medidas que cumplan en particular los principios de protección de datos desde el diseño y por defecto.

Por Diseño: Tanto en el momento de determinar los medios de tratamiento como en el momento del propio tratamiento, el responsable del tratamiento aplicará medidas técnicas y organizativas apropiadas, como la seudonimización, concebidas para aplicar de forma efectiva los principios de protección de datos, como la minimización de datos, e integrar las garantías necesarias en el tratamiento, a fin de cumplir los requisitos del presente Reglamento y proteger los derechos de los interesados.

Por Defecto: El responsable del tratamiento aplicará las medidas técnicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento los datos personales que sean necesarios para cada uno de los fines específicos del tratamiento.

FREMM

LERROUX BUSINESS LAWYERS

TRANSPARENCIA DE LA INFORMACIÓN

El responsable del tratamiento deberá facilitar al interesado, en el momento de obtener sus datos, la información establecida en el RGPD. Esta información hace referencia a la identificación del responsable del tratamiento, la finalidad del tratamiento, la legitimación del mismo, posibles destinatarios, derechos de los interesados y, en su caso, procedencia de los datos. Para facilitar su presentación, se contempla la posibilidad de mostrar la información a diferentes niveles o capas, incluyendo en el primer nivel la información básica y remitir a un segundo nivel la información adicional.

Esta información deberá presentarse de forma concisa, transparente, inteligible y de fácil acceso, con un lenguaje claro y sencillo; en particular cuando la información vaya dirigida a niños.

FREMM

LERROUX BUSINESS LAWYERS

¿De qué debemos informar?

Los interesados a los que se soliciten datos personales deberán ser previamente informados de modo expreso, preciso e inequívoco:

- De la existencia de un fichero o tratamiento de datos de carácter personal, de la finalidad de la recogida de éstos, de las categorías de datos que se van a tratar y de los destinatarios de la información.
- De la existencia de perfiles, de haberlos
- Del carácter obligatorio o facultativo de su respuesta a las preguntas que les sean planteadas.
- De las consecuencias de la obtención de los datos o de la negativa a suministrarlos.
- De la posibilidad de ejercitar los derechos que veremos en un apartado posterior
- De la identidad y dirección del responsable del tratamiento o, en su caso, de su representante.
- Cuando los datos de carácter personal no hayan sido recabados del interesado, éste deberá ser informado dentro de los tres meses siguientes.
- No será necesario informar cuando expresamente una ley lo prevea, (o cuando la información al interesado resulte imposible o exija esfuerzos desproporcionados o fuentes accesibles al público – que deberá identificarse-).

FREMM

LERROUX BUSINESS LAWYERS

RESPONSABILIDAD PROACTIVA

A parte de respetar y hacer respetar los principios que rigen el tratamiento de datos, el responsable, o el encargado, debe llevar a cabo una serie de medidas concretas encaminadas a preservar la seguridad de los datos y a mitigar los efectos adversos que puedan producirse por una posible quiebra en la seguridad.

El Reglamento hace especial hincapié respecto la anterior normativa en la responsabilidad proactiva del encargado y del encargado con los efectos de reforzar la seguridad desde el diseño y por defecto en el tratamiento de los datos personales. Estas medidas deben implementarse y además documentarse de tal manera que puedan ser analizadas por requerimiento de la autoridad competente.

Las medidas concretas que debe llevar a cabo el responsable o encargado son:

-Llevar a cabo un registro de actividades
-Realizar análisis de riesgo
-Implantar y documentar las medidas de seguridad
-Marcar un mecanismo de notificaciones de quiebras de seguridad
-Realizar evaluaciones de impacto

FREMM

LERROUX
BUSINESS LAWYERS

De la inscripción de los ficheros hacia la llevanza interna de un registro de actividades

La Directiva 95/46/CE estableció la obligación general de notificar el tratamiento de datos personales a las autoridades de control.

Pese a implicar cargas administrativas y financieras, dicha obligación, sin embargo, no contribuyó en todos los casos a mejorar la protección de los datos personales.

Por tanto, estas obligaciones generales de notificación indiscriminada deben eliminarse y sustituirse por procedimientos y mecanismos eficaces que se centren, en su lugar, en los tipos de operaciones de tratamiento que, por su naturaleza, alcance, contexto y fines, entrañen probablemente un alto riesgo para los derechos y libertades de las personas físicas.

Estos tipos de operaciones de tratamiento pueden ser, en particular, las que implican el uso de nuevas tecnologías, o son de una nueva clase y el responsable del tratamiento no ha realizado previamente una evaluación de impacto relativa a la protección de datos, o si resultan necesarias visto el tiempo transcurrido desde el tratamiento inicial.

FREMM

LERROUX
BUSINESS LAWYERS

¿Qué debe contener el registro de actividades?

Cada **responsable** y, en su caso, su representante, llevarán un **registro de las actividades de tratamiento efectuadas bajo su responsabilidad**. Dicho registro deberá contener toda la información indicada a continuación:

- El nombre y los datos de contacto del responsable y, en su caso, del corresponsable, del representante del responsable, y del delegado de protección de datos.
- Los fines del tratamiento.
- Una descripción de las categorías de interesados y de las categorías de datos personales.
- Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones internacionales.
- En su caso, las transferencias de datos personales a un tercer país o una organización Internacional.
- Cuando sea posible, los plazos previstos para la supresión de las diferentes categorías de datos.
- Cuando sea posible, una descripción general de las medidas técnicas y organizativas de seguridad.

FREMM

LERROUX
BUSINESS LAWYERS

REGISTRO DE ACTIVIDADES

El registro de actividades consiste en documentar las operaciones de tratamientos de datos de acuerdo a las exigencias y formalidades establecidas en el Reglamento.

El registro de actividades deberá contener cuestiones como:

-Nombre y datos de contacto del responsable o su representante así como del delegado
-Fines del tratamiento
-Descripción de la categoría de interesados y de la categoría de los datos personales
-Categoría de los destinatarios a los que se les comunicará los datos personales
-En su caso, transferencias internacionales y plazos de supresión de los datos

Las empresas de menos de 250 trabajadores estarán exentas de la obligación a menos que el tratamiento que realicen pueda entrañar un riesgo para los derechos y libertades de los interesados, no sea ocasional, o incluya categorías especiales datos (origen étnico o racial, orientaciones políticas o religiosas, datos genéticos o biométricos, salud o vida sexual) o datos relativos a condenas e infracciones penales .

FREMM

LERROUX BUSINESS LAWYERS

ANÁLISIS DE RIESGO

El análisis de riesgo consiste en analizar los posibles fallos en la seguridad que pueda haber en el transcurso del tratamiento de datos con el objetivo de corregir los mismos y reforzar la seguridad. El transcurso del tratamiento se inicia con la obtención de los datos y sigue con el almacenamiento, uso o tratamiento, cesión a terceros y, finalmente, destrucción.

Para realizar el análisis, debe atenderse a la tecnología que se utiliza en el tratamiento, a la naturaleza de los datos, a las distintas operaciones e intervinientes en las mismas, así como al posible volumen de afectados en el caso de una quiebra en la seguridad la magnitud del daño producido

La obligación de llevar a cabo el análisis de riesgo rige para cualquier persona física o jurídica que realiza un tratamiento de datos personales sujeto al Reglamento.

La Agencia Española de Protección de datos ha confeccionado una guía, disponible en su página web, para ayudar a los obligados a realizar el análisis de riesgos.

FREMM

LERROUX
BUSINESS LAWYERS

EVAUACIÓN DE IMPACTO

En el caso de que un tratamiento de datos pueda conllevar un alto riesgo para los derechos y libertades de los interesados, el responsable deberá realizar, antes del tratamiento, una evaluación de impacto, la cual deberá contemplar:

-Una descripción de las operaciones de tratamiento previstas, fines e interés perseguido
-Detalle de la necesidad y proporcionalidad de las operaciones respecto a su finalidad
-Evaluación de los riesgos para los derechos y libertades de los interesados
-Medidas previstas para afrontar los riesgos

El Reglamento contempla una serie de tratamientos que requerirán evaluaciones de impacto

-Tratamientos a gran escala de datos sensible
-Observación sistemática a gran escala de una zona de acceso público
-Evaluación sistemática y exhaustiva de aspectos personales de personas físicas que se base en un tratamiento automatizado, como la elaboración de perfiles, y sobre cuyas bases se tomen decisiones que produzcan efectos jurídicos a los titulares o les afecte significativamente.

En el caso de que la evaluación muestre un alto riesgo, deberá comunicar el hecho a la autoridad competente.

FREMM

LERROUX
BUSINESS LAWYERS

¿Qué debemos preguntarnos?

- ¿Se tratan datos **sensibles**?
- ¿Se incluyen datos de una **gran cantidad** de personas?
- ¿Incluye el tratamiento la **elaboración de perfiles**?
- ¿Se **cruzan los datos** obtenidos de los interesados con otros disponibles en otras fuentes?
- ¿Se pretenden utilizar los datos obtenidos para una finalidad para **otro tipo de finalidades**?
- ¿Se están tratando **grandes cantidades de datos**, incluido con técnicas de análisis masivo tipo big data?
- ¿Se utilizan tecnologías especialmente **invasivas para la privacidad**, como las relativas a geolocalización, videovigilancia a gran escala o ciertas aplicaciones del Internet de las Cosas?

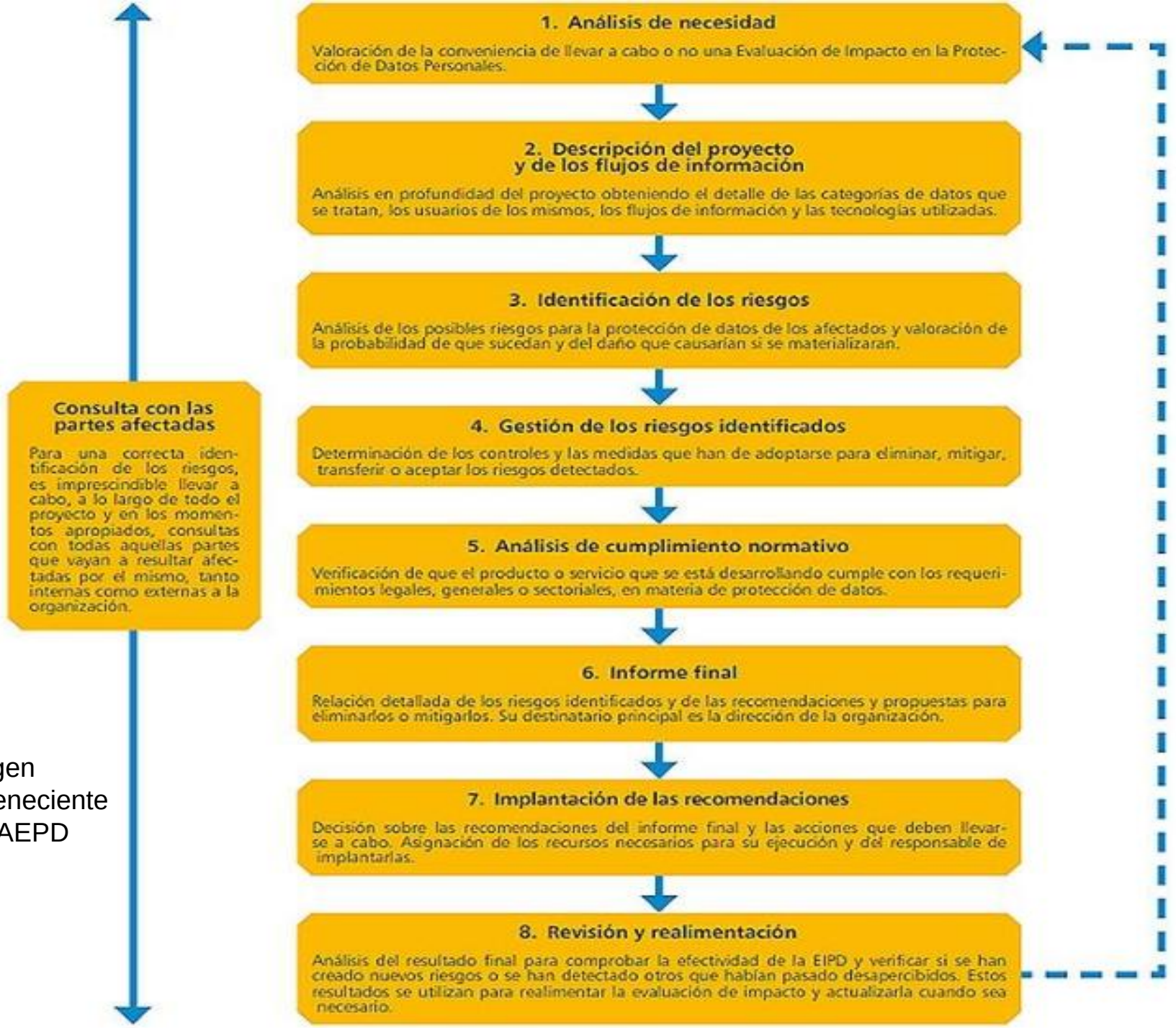

Imagen perteneciente a la AEPD

FREMM

LERROUX BUSINESS LAWYERS

MEDIDAS DE SEGURIDAD

En función del análisis efectuado, se deberán adoptar aquellas medidas de seguridad necesarias para la protección de los datos personales.

Estas medidas de seguridad variarán según la naturaleza y alcance de los datos personales, así como la finalidad del tratamiento y los riesgos para los derechos y libertades de los titulares de los datos. También se tendrá en cuenta el estado y coste de la técnica en el momento.

Una novedad del Reglamento respecto la LOPD es la valoración de los datos en su conjunto, no se trata de diferenciar los datos según un tipo de categorías y en base a la misma establecer una medida de seguridad u otra, sino de valorar el conjunto de datos que son tratados y en base a su conjunto establecer las medidas de seguridad. Por este motivo, las medidas de seguridad implantadas en atención a la LOPD podrían ser insuficientes con el nuevo Reglamento.

FREMM

LERROUX
BUSINESS LAWYERS

NOTIFICACIÓN DE LA VIOLACIÓN DE LOS DATOS

La violación de la seguridad de los datos es toda quiebra en la seguridad que ocasione la destrucción, pérdida o alteración accidental o ilícita de los datos personales, transmitidos, conservados o tratados de otra forma, o la comunicación o acceso no autorizado a dichos datos.

El responsable del tratamiento debe prever la posibilidad de que exista una quiebra en la protección de los datos personales. En base a esta previsión, debe marcar los mecanismos para mitigar el posible daño y comunicar la violación a la Agencia en el plazo de 72h si puede suponer un riesgo para los derechos y libertados de los titulares de los datos.
En el caso de que la quiebra pudiese tener un gran impacto, se deberá comunicar también la misma a los interesados para que adopten las medidas necesarias.

La violación en la seguridad de los datos no sólo se limita a hackers y grandes multinacionales, la pérdida de un teléfono móvil o un ordenador abierto en un espacio de acceso público pueden suponer una quiebra en la seguridad.
El responsable tiene la obligación de documentar todas las violaciones en la seguridad de los datos producidas.

FREMM

LERROUX
BUSINESS LAWYERS

SANCIONES

El Reglamento prevé un incremento de las sanciones económicas respecto a la anterior normativa:

La obtención de datos de un niño sin el consentimiento de sus tutores, el incumplimiento de la obligación de llevar a cabo un registro de las actividades del tratamiento o de la comunicación de las violaciones de seguridad de los datos así como de realizar las evaluaciones de impacto o de designar a un delegado de protección de datos cuando sea obligatorio, son ejemplos de infracciones que podrán sancionarse con una multa económica de hasta 10 millones de euros o de una cuantía equivalente al 2% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la suma de mayor cuantía.

El incumplimiento por parte del responsable de respetar los principios del tratamiento de datos personales o de los derechos que asisten a los interesados, podrá sancionarse con una multa económica de hasta 20 millones de euros o del equivalente al 4% del volumen de negocio total anual global del ejercicio financiero anterior, optándose por la suma de mayor cuantía.

FREMM

LERROUX BUSINESS LAWYERS

DERECHOS DE LOS INTERESADOS

El interesado ostenta una serie de derechos respecto al tratamiento de sus datos y el responsable está obligado a informarle de ello. Estos derechos son:

-Derecho a conocer la existencia del tratamiento de sus datos y a obtener una copia de los mismos
-Derecho a rectificar los datos personales inexactos que le conciernen
-Derecho a la supresión de sus datos, el llamado derecho al olvido, bajo las condiciones marcadas en el RGPD
-Derecho a la limitación del tratamiento de sus datos
-Derecho a la portabilidad de los datos
-Derecho a oponerse al tratamiento de sus datos
-Derecho a no ser objeto de una decisión basada únicamente en el tratamiento automatizado de sus datos

FREMM

LERROUX BUSINESS LAWYERS

DERECHOS DE LOS INTERESADOS

El responsable del tratamiento deberá facilitar al interesado la posibilidad de ejercer sus derechos mediante una vía de comunicación análoga a la que utilizó para recabar los datos personales.

El responsable tendrá un plazo de contestación de un mes a partir de la recepción de la solicitud del interesado, plazo que podrá prorrogarse otros dos meses en atención a la complejidad y número de peticiones. En todo caso, el responsable deberá informar al interesado, durante el primer mes de plazo, de la prórroga de la contestación así como de los motivos de la misma.

Si el responsable no da curso a la solicitud del interesado, deberá informarle de las razones de su no actuación así como de la posibilidad que tiene el interesado de presentar una reclamación ante la autoridad de control y de ejercer acciones judiciales.

FREMM

LERROUX
BUSINESS LAWYERS

¿Qué comprende el derecho de acceso?

Únicamente el conocimiento de la información sometida a tratamiento:

- Datos personales
- Finalidad
- Origen de los datos
- Cesiones realizadas y que se prevén realizar,etc.

No comprende qué personas, dentro del ámbito de organización del responsable del fichero han podido tener acceso a dicha información.

FREMM

LERROUX BUSINESS LAWYERS

DERECHO DE SUPRESIÓN

El responsable del tratamiento está obligado a suprimir sin dilación indebida cuando:

- Los datos personales que **no sean necesarios** en relación con los fines para los que fueron recogidos o tratados de otro modo
- El interesado **retire el consentimiento** en que se basa el tratamiento y este **no se base en otro fundamento jurídico**

Cuando la supresión derive del ejercicio del derecho de oposición el responsable **podrá conservar** los datos identificativos del afectado **necesarios** con el fin de **impedir tratamientos futuros para fines de mercadotecnia directa**.

Listas Robinson

Debemos tener en cuenta los periodos legales de conservación

FREMM

LERROUX BUSINESS LAWYERS

BLOQUEO DE DATOS

Bloqueo de datos: la identificación y reserva de datos con el fin de impedir su tratamiento.

La obligación de bloqueo garantiza la adecuada aplicación y supervisión del cumplimiento de las normas de protección de datos.

El responsable del tratamiento estará obligado a bloquear los datos cuando proceda a su rectificación o supresión.

En el tiempo que dure la limitación, el responsable sólo podrá tratar los datos afectados, más allá de su conservación:

- Con el consentimiento del interesado
- Para la formulación, el ejercicio o la defensa de Reclamaciones
- Para proteger los derechos de otra persona física o jurídica
- Por razones de interés público importante de la Unión o del Estado miembro

El hecho de que el tratamiento de los datos personales esté limitado **debe constar claramente en el sistema.**

FREMM

LERROUX
BUSINESS LAWYERS

PORTABILIDAD DE DATOS

Es una **forma avanzada** del derecho de acceso

El interesado tendrá **derecho a recibir los datos personales que le incumban**, que haya facilitado a un responsable del tratamiento, en *un formato estructurado, de uso común y lectura mecánica*, y a **transmitirlos a otro responsable** del tratamiento sin que lo impida el responsable al que se los hubiera facilitado

Este derecho sólo puede ejercerse:

- Cuando el tratamiento se efectúe por medios automatizados.
- Cuando el tratamiento se base en el consentimiento o en un contrato.
- Cuando el interesado lo solicita respecto a los datos que haya proporcionado al responsable y que le conciernan, incluidos los datos derivados de la propia actividad del interesado.

El derecho a la portabilidad implica que los datos personales del interesado *se transmiten directamente de un responsable a otro*, sin necesidad de que sean transmitidos previamente al propio interesado, siempre que ello sea técnicamente posible.

FREMM

LERROUX
BUSINESS LAWYERS

PERFILES

«elaboración de perfiles»*: toda forma de tratamiento automatizado de datos personales consistente en utilizar datos personales* ***para evaluar determinados aspectos pe****rsonales de una persona física, en particular para* ***analizar o predecir*** *aspectos relativos al rendimiento profesional, situación económica, salud, preferencias personales, intereses, fiabilidad,*

comportamiento, ubicación o movimientos de dicha persona física

Todo interesado tiene derecho a no ser objeto de una **decisión basada únicamente** en el tratamiento automatizado, **incluida la elaboración de perfiles**, que **produzca efectos jurídicos** en él o **le afecte significativamente** de modo similar.

Excepciones:

- Cuando es necesaria para la celebración o la ejecución de un contrato entre el interesado y un responsable del tratamiento;
- Está **autorizada por el Derecho** de la Unión o de los Estados miembros que se aplique al responsable del tratamiento
- Se basa en el **consentimiento explícito** del interesado

FREMM

LERROUX BUSINESS LAWYERS

¿Cómo se ejercitan los derechos? GRATUIDAD

Los responsables deben facilitar la presentación de **solicitudes por medios electrónicos**, especialmente cuando el tratamiento se realiza por estos medios.

Cuando el **interesado presente la solicitud por medios electrónicos**, la información se facilitará en un formato electrónico de uso común.

En todo caso, el interesado puede solicitar que se facilite la contestación de otro modo

El ejercicio del derecho no podrá ser denegado por el solo motivo de optar el afectado por otro medio

Será gratuito para el interesado.

Excepción:

Cuando se formulen solicitudes **manifiestamente infundadas o excesivas**, especialmente por repetitivas

- Corresponde al **responsable demostrar** el carácter infundado o excesivo de las solicitudes que tengan un coste para el interesado.
- Debe corresponder efectivamente con el verdadero coste de la tramitación de la solicitud

Se prevé **gratuidad** por primera **copia** pero cobro por otras copias

El responsable del tratamiento **facilitará una copia** de los datos personales objeto de tratamiento.

El responsable **podrá percibir por cualquier otra copia** solicitada por el interesado un canon

razonable basado en los costes administrativos.

Los responsables deben utilizar todas las medidas razonables para verificar la identidad de quienes ejerzan los derechos.

FREMM

LERROUX
BUSINESS LAWYERS

¿Cuándo se puede denegar el ejercicio de un derecho?

Los derechos serán **denegados** cuando la solicitud **sea formulada por persona distinta del afectado** y no se acredita que el mismo actúa en representación de aquél.

También serán **denegados** cuando:

- Ejercicio manifiestamente infundado o
- Repetitivo
- Ejercicio del derecho de acceso en más de una ocasión durante el plazo de seis meses, a menos que exista causa legítima para ello.
- Cuando el afectado solicite que se facilite la contestación de su derecho de otro modo que resulta imposible

El responsable que **trate una gran cantidad** de información sobre un interesado podrá pedir a éste que **especifique la información** a que se refiere su solicitud de acceso.

FREMM

LERROUX
BUSINESS LAWYERS

¿Qué pasa si no lo atiendes el derecho?

Si el responsable **decide no atender** una solicitud, debe:

- Informar al interesado
- **Motivar la negativa**
- Contestar sin dilación y a más tardar dentro del plazo de un mes desde su presentación.
- Que puede presentar una reclamación a la autoridad de control
- Que puede ejercitar acciones judiciales

El responsable deberá informar al interesado sobre las actuaciones derivadas de su petición en el plazo de **un mes** –**tenga o no datos-**

Se puede **extender otros dos meses** cuando sea necesario –complejidad y número de solicitudes-

FREMM

LERROUX
BUSINESS LAWYERS

SOLICITUD DEL CONSENTIMIENTO

- Cuando el tratamiento se base en el consentimiento del interesado, el responsable deberá ser capaz de **demostrar** que aquel consintió el tratamiento de sus datos personales.

- Si el consentimiento del interesado se da en el contexto de una declaración escrita que también se refiera a otros asuntos, la solicitud de consentimiento se **presentará de tal forma que se distinga claramente de los demás asuntos**, de forma inteligible y de fácil acceso y utilizando un lenguaje claro y sencillo.

- El interesado tendrá derecho a **retirar su consentimiento en cualquier momento**. La retirada del consentimiento no afectará a la licitud del tratamiento basada en el consentimiento previo a su retirada. Antes de dar su consentimiento, el interesado será informado de ello. Será tan fácil retirar el consentimiento como darlo.

- Al evaluar si el consentimiento se ha dado **libremente**, se tendrá en cuenta en la mayor medida posible el hecho de si, entre otras cosas, la ejecución de un contrato, incluida la prestación de un servicio, **se supedita al consentimiento al tratamiento de datos personales que no son necesarios** para la ejecución de dicho contrato.

FREMM

LERROUX
BUSINESS LAWYERS

CONDICIONES PARA EL CONSENTIMIENTO

El consentimiento debe darse mediante un **acto afirmativo** claro que refleje una manifestación de voluntad libre, específica, informada, e inequívoca del interesado de aceptar el tratamiento de datos de carácter personal que le conciernen, como una declaración por escrito, inclusive por medios electrónicos, o una declaración verbal.

Por tanto, el **silencio**, las casillas ya marcadas o la inacción no deben constituir consentimiento.

El consentimiento debe darse para todas las actividades de tratamiento realizadas con el mismo o los mismos fines. Cuando el tratamiento tenga varios fines, debe darse el consentimiento para todos ellos.

Para garantizar que el consentimiento se haya dado libremente, este no debe constituir un fundamento jurídico válido para el tratamiento de datos de carácter personal en un caso concreto en el que exista un desequilibro claro entre el interesado y el responsable del tratamiento.

Se **presume que el consentimiento no se ha dado libremente** cuando no permita autorizar por separado las distintas operaciones de tratamiento de datos personales pese a ser adecuado en el caso concreto, o cuando el cumplimiento de un contrato, incluida la prestación de un servicio, sea dependiente del consentimiento, aún cuando este no sea necesario para dicho cumplimiento.

Cuando el tratamiento se base en el consentimiento de conformidad con la Directiva 95/46/CE, no es necesario que el interesado dé su consentimiento de nuevo si la forma en que se dio el consentimiento se ajusta a las condiciones del presente Reglamento.

FREMM

LERROUX
BUSINESS LAWYERS

¿Qué pasa si no conseguimos el consentimiento?

No será preciso el consentimiento cuando:

- Sean tratados por las Administraciones públicas en el ámbito de sus competencias
- Se refieran a las partes de un contrato o precontrato de una relación negocial, laboral o administrativa y sean necesarios para su mantenimiento o cumplimiento
- El tratamiento de los datos tenga por finalidad proteger un interés vital del interesado.
- Figuren en fuentes accesibles al público (y su tratamiento sea necesario para la satisfacción del interés legítimo perseguido por el responsable del fichero o por el del tercero a quien se comuniquen los datos, siempre que no se vulneren los derechos y libertades fundamentales del interesado).

FREMM

LERROUX BUSINESS LAWYERS

DETERMINADAS PROHIBICIONES

- Nadie podrá ser obligado a declarar sobre su ideología, religión o creencias.
- Cuando en relación con estos datos se proceda a recabar el consentimiento a que se refiere el apartado siguiente, se advertirá al interesado acerca de su derecho a no prestarlo.
- Quedan prohibidos los ficheros creados con la finalidad exclusiva de almacenar datos de carácter personal que revelen la ideología, afiliación sindical, religión, creencias, origen racial o étnico, o vida sexual.
- Los datos de carácter personal relativos a la comisión de infracciones penales o administrativas sólo podrán ser incluidos en ficheros de las Administraciones públicas competentes en los supuestos previstos en las respectivas normas reguladoras.

FREMM

LERROUX
BUSINESS LAWYERS

EXCEPCIONES A LAS PROHIBICIONES

Excepciones:

• Tratamiento necesario para la prevención o para el diagnóstico médicos, la prestación de asistencia sanitaria o tratamientos médicos o la gestión de servicios sanitarios, siempre que dicho tratamiento de datos se realice por un profesional sanitario sujeto al secreto profesional o por otra persona sujeta asimismo a una obligación equivalente de secreto.

• Tratamiento necesario para salvaguardar el interés vital del afectado o de otra persona, en el supuesto de que el afectado esté física o jurídicamente incapacitado para dar su consentimiento.

• Tratamiento realizado por instituciones y los centros sanitarios públicos y privados y los profesionales correspondientes podrán proceder al tratamiento de los datos de carácter personal relativos a la salud de las personas que a ellos acudan o hayan de ser tratados en los mismos, de acuerdo con lo dispuesto en la legislación estatal o autonómica sobre sanidad.

• Consentimiento expreso

FREMM

LERROUX BUSINESS LAWYERS

ASEGURAMIENTO Y CONFIDENCIALIDAD DE FICHEROS.

El responsable del fichero (o el encargado del tratamiento) deberán:

- Adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y los riesgos a que están expuestos, ya provengan de la acción humana o del medio físico o natural.

- El responsable del fichero y quienes intervengan en cualquier fase del tratamiento de los datos de carácter personal están obligados al secreto profesional respecto de los mismos y al deber de guardarlos, obligaciones que subsistirán aun después de finalizar sus relaciones con el responsable del fichero.

FREMM

LERROUX BUSINESS LAWYERS

NIVELES DE SEGURIDAD

El reglamento de desarrollo de la antigua LOPD fija **tres niveles de seguridad** atendiendo a la naturaleza de la información.

Los niveles de seguridad son **acumulativos** de modo que un fichero de nivel alto deberá aplicar también las medidas previstas en los niveles básico y medio.

• **Básico**: Todos los ficheros.

• **Medio**: Ficheros que contienen datos relativos a infracciones penales o administrativas, Hacienda Pública, servicios financieros o solvencia. Aquellos que sean responsables las entidades gestoras y Servicios Comunes de la Seguridad Social, las mutuas de accidentes de trabajo y enfermedades profesionales de la Seguridad Social.

• **Alto**: Ficheros que contienen datos de ideología, religión, creencias, origen racial, salud, vida sexual, datos policiales, datos derivados de actos de violencia de género, y ficheros o tratamientos de los que sean responsables los operadores que presten servicios de comunicaciones electrónicas disponibles al público o exploten redes públicas de comunicaciones electrónicas respecto a los datos de tráfico y localización.

FREMM

LERROUX BUSINESS LAWYERS

MEDIDAS DE SEGURIDAD. FICHEROS AUTOMATIZADOS

Medidas de seguridad de nivel básico.

- Funciones y obligaciones del personal.
- Registro de incidencias.
- Control de acceso.
- Gestión de soportes y documentos.
- Identificación y autenticación.
- Copias de respaldo y recuperación.

Medidas de seguridad de nivel medio

.

- Responsable de seguridad.
- Auditoría.
- Gestión de soportes y documentos.
- Identificación y autenticación.
- Control de acceso físico.
- Registro de incidencias.

Medidas de seguridad de nivel alto.

- Gestión y distribución de soportes.
- Copias de respaldo y recuperación.
- Registro de accesos.
- Telecomunicaciones.

FREMM

LERROUX
BUSINESS LAWYERS

MEDIDAS DE SEGURIDAD. FICHEROS NO AUTOMATIZADOS

Medidas de seguridad de nivel básico.

- Obligaciones comunes.
- Criterios de archivo.
- Dispositivos de almacenamiento.
- Custodia de los soportes.

Medidas de seguridad de nivel medio.

- Responsable de seguridad.
- Auditoría.

Medidas de seguridad de nivel alto.

- Almacenamiento de la información.
- Copia o reproducción.
- Acceso a la documentación.
- Traslado de documentación.

FREMM

LERROUX BUSINESS LAWYERS

AUDITORIA COMO MEDIDA DE SEGURIDAD

Auditoría (medidas de seguridad de nivel medio)

Los sistemas de información e instalaciones de tratamiento y almacenamiento de datos se someterán, **al menos cada dos años, a una auditoría interna o externa que verifique el cumplimiento del presente título**.

Con carácter extraordinario deberá realizarse dicha auditoría siempre que se realicen **modificaciones sustanciales** en el sistema de información que puedan repercutir en el cumplimiento de las medidas de seguridad implantadas con el objeto de verificar la adaptación, adecuación y eficacia de las mismas.

El informe de auditoría deberá dictaminar sobre la **adecuación de las medidas y controles a la Ley y su desarrollo reglamentario, identificar sus deficiencias y proponer las medidas correctoras o complementarias necesarias**.

Los informes de auditoría serán **analizados por el responsable de seguridad** competente, que elevará las conclusiones al responsable del fichero o tratamiento para que **adopte las medidas correctoras adecuadas** y quedarán a disposición de la **AEPD** o, en su caso, de las autoridades de control de las comunidades autónomas.

FREMM

LERROUX
BUSINESS LAWYERS

OBLIGACIONES DEL RESPONSABLE DE SEGURIDAD

Teniendo en cuenta la naturaleza, el ámbito, el contexto y los fines del tratamiento así como los riesgos de diversa probabilidad y gravedad para los derechos y libertades de las personas físicas, el responsable del tratamiento **aplicará medidas técnicas y organizativas apropiadas a fin de garantizar y poder demostrar que el tratamiento es conforme con el Reglamento**. Dichas medidas incluirán, entre otras:

• La seudonimización y el cifrado de datos personales

• La capacidad de garantizar la confidencialidad, integridad, disponibilidad y resiliencia permanentes de los sistemas y servicios de tratamiento

• La capacidad de restaurar la disponibilidad y el acceso a los datos personales de forma rápida en caso de incidente físico o técnico

• Un proceso de verificación, evaluación y valoración regulares de la eficacia de las medidas técnicas y organizativas para garantizar la seguridad del tratamiento.

La **adhesión a códigos de conducta o a un mecanismo de certificación aprobados** podrán ser utilizados como elementos para demostrar el cumplimiento de las obligaciones por parte del responsable del tratamiento.

FREMM

LERROUX
BUSINESS LAWYERS

DELEGADO DE PROTECCIÓN DE DATOS

El Delegado de Protección de Datos se encarga de asesorar al responsable o al encargado en todo lo relativo a la normativa de protección de datos.

La relación entre el delegado y el responsable o encargado podrá ser mediante contrato laboral o de servicios. A la hora de su designación se exige al responsable o encargado que elijan a una persona con conocimientos legales específicos y suficientes en protección de datos.

Los datos de contacto del delegado deben hacerse público por parte de los responsables y encargados, a su vez deberán comunicarse a las autoridades de supervisión.

FREMM

LERROUX
BUSINESS LAWYERS

DESIGNACION DEL DPO

El responsable y el encargado del tratamiento designarán un delegado de protección de datos siempre que:

• El tratamiento lo lleve a cabo una autoridad u organismo público, excepto los tribunales que actúen en ejercicio de su función judicial.

• Las actividades principales del responsable o del encargado consistan en operaciones de tratamiento que, en razón de su naturaleza, alcance y/o fines, requieran una observación habitual y sistemática de interesados a gran escala, o

• Las actividades principales del responsable o del encargado consistan en el tratamiento a gran escala de categorías especiales de datos personales y de datos relativos a condenas e infracciones penales

Un grupo empresarial podrá nombrar un único delegado de protección de datos siempre que sea fácilmente accesible desde cada establecimiento.

FREMM

LERROUX BUSINESS LAWYERS

CONDICIONES PARA DESIGNAR A UN DPO

El delegado de protección de datos será designado atendiendo a sus cualidades profesionales y, en particular, a sus conocimientos especializados del Derecho y la práctica en materia de protección de datos y a su capacidad para desempeñar sus funciones.

El delegado de protección de datos podrá formar parte de la plantilla del responsable o del encargado del tratamiento o desempeñar sus funciones en el marco de un contrato de servicios.

El responsable o el encargado del tratamiento publicarán los datos de contacto del delegado de protección de datos y los comunicarán a la autoridad de control.

Debe tener cierta independencia

FREMM

LERROUX BUSINESS LAWYERS

COMUNICACIÓN DE DATOS PERSONALES

Los datos de carácter personal objeto del tratamiento sólo podrán ser comunicados a un tercero para el cumplimiento de fines directamente relacionados con las funciones legítimas del cedente y del cesionario con el previo consentimiento del interesado.

Será nulo el consentimiento cuando la información no permita conocer la finalidad o el tipo de actividad de aquel a quien se pretenden comunicar.

Excepciones al consentimiento:

- Cuando la cesión está autorizada en una ley.
- Cuando se trate de datos recogidos de fuentes accesibles al público.
- Cuando responda a la libre y legítima aceptación de una relación jurídica que implique necesariamente esta cesión.
- Cuando la comunicación que deba efectuarse tenga por destinatario al Defensor del Pueblo, el Ministerio Fiscal o los Jueces o Tribunales o el Tribunal de Cuentas, en el ejercicio de las funciones que tiene atribuidas o se realice entre Administraciones públicas para fines históricos, estadísticos o científicos.
- Cuando la cesión de datos de carácter personal relativos a la salud sea necesaria para solucionar una urgencia o para realizar los estudios epidemiológicos.

FREMM

LERROUX BUSINESS LAWYERS

CONTRATO DE ENCARGO DE TRATAMIENTO

No se considerará comunicación de datos el acceso de un tercero a los datos cuando dicho acceso sea necesario para la prestación de un servicio al responsable del tratamiento.

La realización de tratamientos por cuenta de terceros deberá estar regulada en un contrato que:

- Deberá constar por escrito
- Establezca que el encargado del tratamiento únicamente tratará los datos conforme a las instrucciones del responsable del tratamiento, que no los aplicará o utilizará con fin distinto al que figure en dicho contrato, ni los comunicará, ni siquiera para su conservación, a otras personas.
- Estipule las medidas de seguridad que el encargado del tratamiento está obligado a implementar.
- Una vez cumplida la prestación contractual, los datos de carácter personal deberán ser destruidos o devueltos al responsable del tratamiento, al igual que cualquier soporte o documentos en que conste algún dato de carácter personal objeto del tratamiento.
- En el caso de que el encargado del tratamiento destine los datos a otra finalidad, los comunique o los utilice incumpliendo las estipulaciones del contrato, será considerado también responsable del tratamiento, respondiendo de las infracciones en que hubiera incurrido personalmente.

FREMM

LERROUX BUSINESS LAWYERS

Transferencias internacionales, especial referencia al Privacy Shield

La aprobación el 12 de julio de 2016 del nuevo marco del Escudo de la Privacidad (Privacy Shield) entre la UE y EE.UU., para las transferencias de datos personales a entidades situadas en EE.UU., ha aportado un respaldo jurídico a las transferencias internacionales de datos que se Efectúen de la UE a EE.UU.

Sin embargo, algunas Autoridades Nacionales de Control y el propio Grupo del Artículo 29 se muestran recelosas con este nuevo marco y han mostrado sus inquietudes acerca de la estabilidad y durabilidad del acuerdo, pues el texto no varía excesivamente de su predecesor, que fue anulado por el Tribunal de justicia de la Unión Europea.

Aunque existen instrumentos alternativos para efectuar transferencias internacionales de datos a EE.UU., se plantea la misma duda respecto a ellos: qué garantías existen de que esos mecanismos no adolezcan de la misma falta de protección de los derechos y libertades fundamentales garantizados en la UE por la que se anuló el Acuerdo de Puerto Seguro.

Por otro lado, en vista del incremento de los flujos comerciales entre los países de la UE y China y de las transferencias de datos a este país. Existe una gran inseguridad jurídica de las empresas y los ciudadanos europeos, ya que este país no cuenta con una Decisión de la Comisión Europea que declare que garantiza un nivel de protección adecuado en materia de protección de datos. **Las empresas CHINAS se están adaptando al GPDR**.

GPDR COMO MODELO INTERNACIONAL DE PROTECCIÓN DE DATOS.

FREMM

LERROUX
BUSINESS LAWYERS

TRANSFERENCIAS INTERNACIONALES

Sólo se realizarán transferencias de datos personales que sean objeto de tratamiento o vayan a serlo tras su transferencia a un tercer país u organización internacional si el responsable y el

encargado del tratamiento cumplen las condiciones establecidas en el Reglamento.

Principio general de las transferencias:

- Cada responsable y encargado llevarán un registro de las actividades de tratamiento efectuadas bajo su responsabilidad o por cuenta de un responsable respectivamente. Dicho registro deberá contener la siguiente información:

  Las categorías de destinatarios a quienes se comunicaron o comunicarán los datos personales, incluidos los destinatarios en terceros países u organizaciones

  internacionales.

El responsable del tratamiento deberá facilitar la siguiente información en el momento en que se obtengan los datos:

Entre otros aspectos de la intención del responsable de transferir datos personales

a un tercer país u organización internacional.

FREMM

LERROUX BUSINESS LAWYERS

TRANSFERENCIAS INTERNACIONALES

Principio general de las transferencias:

En el marco del GPDR las transferencias se pueden llevar a cabo sin necesidad de autorización previa: Cuando se aporten garantías suficientes a través de un contrato ad hoc o de un acuerdo administrativo entre autoridades públicas.

Podrá realizarse una transferencia de datos personales a un tercer país u organización internacional cuando la Comisión haya decidido que el tercer país, un territorio o uno o varios sectores específicos de ese tercer país, o la organización internacional de que se trate garantizan un nivel de protección adecuado. Dicha transferencia no requerirá ninguna autorización específica.

Si no estamos en el caso de una transferencia basada en una decisión de adecuación de la Comisión, el responsable o el encargado del tratamiento solo podrá transmitir datos personales a un tercer país u organización internacional si hubiera ofrecido garantías adecuadas y a condición de que los interesados cuenten con derechos exigibles y acciones legales efectivas. Se materializará mediante:

- Instrumentos jurídicos vinculantes.
- Normas corporativas vinculantes.
- Cláusulas tipo de protección de datos.
- Código de conducta o mecanismo de certificación con compromisos vinculantes.

FREMM

LERROUX
BUSINESS LAWYERS

TRANSFERENCIAS INTERNACIONALES

En ausencia de una decisión de adecuación de conformidad o de garantías adecuadas de conformidad, una transferencia de datos personales a un tercer país u organización internacional únicamente se realizará si se cumple alguna de las condiciones:

• El interesado haya dado explícitamente su consentimiento a la transferencia propuesta, tras haber sido informado de los posibles riesgos para él de dichas transferencias debido a la ausencia de una decisión de adecuación y de garantías adecuadas.
• La transferencia sea necesaria para la ejecución de un contrato entre el interesado y el responsable del tratamiento.
• La transferencia sea necesaria por razones importantes de interés público.
• La transferencia sea necesaria para proteger los intereses vitales del interesado o de otras personas.

Las transferencias de datos son importantes en el contexto de los datos de RR.HH cuando los empresarios utilizan servicios basados en la nube o proveedores de servicios de externalización de RR.HH.

Conocer el lugar en que residen los datos físicamente, y en particular si se encuentran fuera de la UE, constituye un requisito legal para los empresarios.

FREMM

LERROUX
BUSINESS LAWYERS

TRANSFERENCIAS INTERNACIONALES

La exportación de datos fuera de la UE es perfectamente legal, sin embargo, se debe hacer teniendo en cuenta alguno de los diferentes mecanismos de supervisión reglamentaria.

Estos incluyen:

• Transferencias sobre la base de la idoneidad: la UE mantiene una lista de países con leyes de protección de datos consideradas adecuadas (o equivalentes) al GDPR. Solo hay 12 países en esa lista.

Andorra
Argentina
Canadá
Estados Unidos. Solo si la entidad está adherida a “Privacy Shield”.
Guernesey
Isla de Man
Islas Feroe
Jersey
Israel
Nueva Zelanda
Suiza
Uruguay

FREMM

LERROUX
BUSINESS LAWYERS

ACUERDOS DE ADECUACIÓN

El otro mecanismo fundamental para las transferencias de datos legales se da cuando existe un acuerdo específico entre la UE y el país tercero. Este enfoque se utiliza normalmente cuando no ha sido concedida una decisión de idoneidad. El mejor ejemplo de esta situación es el Privacy Shield, un acuerdo bilateral entre EE.UU. y la UE que permite la transferencia de datos a los responsables de tratamiento adheridos al acuerdo. Sin embargo, el Privacy Shield probablemente se someta a los tribunales, como lo fue su predecesor, el Safe Harbor. IDC opina que las empresas con sede en EE.UU. que quieran demostrar su compromiso a largo plazo con los principios del GDPR deberían seguir la senda de las BCR.

Una oportuna ilustración del régimen de transferencia de datos es por supuesto el Brexit. El Brexit es en gran medida irrelevante en lo que se refiere a la protección de datos. Esto se debe a las reglas de transferencia de datos del GDPR: si cualquier empresa de Reino Unido desea comerciar con un socio de la UE, o tratar datos de carácter personal de la UE, tendrá que suscribir las reglas de transferencias de datos incluidas en el GDPR. Dado el volumen de negocio actual entre Reino Unido y la UE, es probable que el primero adopte una ley similar al GDPR cuando abandone la UE. De hecho el ICO (Information Comissioner's Office) ya lo ha indicado.

FREMM

LERROUX BUSINESS LAWYERS

SOLUCIONES CLOUD

La mayoría de las soluciones cloud requerirán transferencias de datos en el exterior de la UE en menor o mayor medida. Los proveedores han desarrollado soluciones para proteger los datos de carácter personal que incluyen modelos de cláusulas contractuales.

La nube es diferente en términos de la multiplicidad de factores involucrados. Las empresas han de abordar la auditoría de manera práctica mediante diversas preguntas sobre el nivel de seguridad y los procesos de protección de datos existentes, y mediante el análisis de informes de auditoría, incluyendo los informes independientes de terceros, posiblemente facilitados por el proveedor de servicios cloud.

Resulta crítico, por ejemplo, entender la seguridad física del centro de datos en que se alojan los datos de carácter personal. Un proveedor de confianza dispondrá al menos de una solución en materia de seguridad tan buena como la de la mayor empresa, y probablemente considerablemente superior a la de la organización de un empresario medio. Incluirá probablemente la certificación ISO 27001 y (cada vez más) 27018, centrada en los datos de carácter personal en las nubes públicas.

No existe por tanto ningún impedimento legal ni técnico para el almacenamiento de datos de recursos humanos en la nube. Algunas empresas pueden optar por una configuración con un centro de datos ubicado en la UE, con certificaciones probadas de seguridad física y seguridad lógica.

Además, el acceso a los datos de la UE se debe producir únicamente desde el interior de la UE: el acceso desde el exterior constituiría una transferencia de datos (efectuado por datos en tránsito) y disminuiría la eficacia de los centros de datos de la UE.

FREMM

LERROUX BUSINESS LAWYERS

GUÍAS, HERRAMIENTAS Y CERTIFICACIONES

Como herramientas más destacadas, la Agencia española de Protección de datos facilita en su página web diversas guías con el objetivo de ayudar a los obligados a cumplir con sus diversas responsabilidades. A su vez, pone a disposición de los usuarios la herramienta “facilita” se trata de una plataforma que ayuda a las empresas con un bajo volumen de tratamiento de datos a adaptarse al reglamento.

A su vez, el RGPD potencia la creación de mecanismos de certificación en materia de protección de datos, así como sellos y marcas con el fin de demostrar el cumplimiento, por parte del obligado, de las disposiciones del RGPD.
Estas certificaciones en todo caso serán voluntarias y su objetivo es el de añadir valor al obligado y seguridad al interesado a la hora elegir a quien le confía sus datos.

FREMM

LERROUX BUSINESS LAWYERS

CLAUSULA LÍCITA

La AEPD a través de los informes emitidos por su Gabinete Jurídico, ha considerado que el consentimiento prestado a través de cláusulas como la siguiente, contiene los requisitos de licitud, lealtad, transparencia, sencillez, inequívoco.

En cumplimiento del RGPD 2016/679, sobre protección de Datos de Carácter Personal .....nombre del responsable del fichero..... informa a los usuarios de que los Datos de Carácter Personal que recoge son objeto de tratamiento automatizado y se incorporan en los ficheros correspondientes, debidamente registrados en la Agencia Española de Protección de Datos.

En virtud de lo establecido en la Ley 34/2002, de 11 de julio, de Servicios de la Sociedad de la Información y de Comercio Electrónico, ...nombre del responsable del fichero..... informa que podrá utilizar las direcciones de correo electrónico facilitadas por usted, para mantenerle informado de sus novedades comerciales y sus distintas ofertas promocionales. Usted da su consentimiento expreso para que .....nombre del responsable del fichero..... pueda utilizar su dirección de correo electrónico con este fin concreto. El usuario podrá, en todo momento, ejercitar los derechos reconocidos en el RGPD, de Derecho de acceso, Derecho de rectificación, Derecho de supresión, Derecho de oposición, Derecho a la limitación del tratamiento, Derecho a la portabilidad de los datos, Derechos en relación con las decisiones individuales automatizadas . El ejercicio de estos derechos puede realizarlo el propio usuario acompañando copia del DNI de manera presencial en las oficinas de .....nombre del responsable del fichero....., mediante correo electrónico a: .....@..... o bien mediante comunicación escrita a la siguiente dirección postal: .....dirección para ejercicio de derechos .....

¿Como serán las solicitudes de derechos?

A.1. EJERCICIO DEL DERECHO DE ACCESO(1).
DATOS DEL RESPONSABLE DEL FICHERO(2).
Nombre / razón social: ..... Dirección de la Oficina / Servicio ante el que se ejercita el derecho de acceso: C/Plaza ..... no ..... C.Postal ..... Localidad ..... Provincia ..... Comunidad Autónoma ..... C.I.F./D.N.I. .....
DATOS DEL INTERESADO O REPRESENTANTE LEGAL(3.
D./ Da. ....., mayor de edad, con domicilio en la C/Plaza ..... no....., Localidad ..... Provincia ..... C.P . ..... Comunidad Autónoma ..... con D.N.I....., del que acompaña copia, por medio del presente escrito ejerce el derecho de acceso, de conformidad con lo previsto en el artículo 15 de la Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal y en los artículos 27 y 28 del Real Decreto 1720/2007, de 21 de diciembre, por el que se desarrolla la misma, y en consecuencia,
SOLICITA,
Que se le facilite gratuitamente el derecho de acceso a sus ficheros en el plazo máximo de un mes a contar desde la recepción de esta solicitud, y que se remita por correo la información a la dirección arriba indicada en el plazo de diez días a contar desde la resolución estimatoria de la solicitud de acceso.
Asimismo, se solicita que dicha información comprenda, de modo legible e inteligible, los datos de base que sobre mi persona están incluidos en sus ficheros, los resultantes de cualquier elaboración, proceso o tratamiento, así como el origen de los mismos, los cesionarios y la especificación de los concretos usos y finalidades para los que se almacenaron.
En .....a.....de.....de 20..... Firmado
1 Se trata de la petición de información sobre los datos personales incluidos en un fichero. Este derecho se ejerce ante el responsable del fichero (Organismo Público o entidad privada) que es quien dispone de los datos. La Agencia Española de Protección de Datos no dispone de sus datos personales sino solamente de la ubicación del citado responsable si el fichero está inscrito en el Registro General de Protección de Datos.
2 Si Vd. desconoce la dirección del responsable del fichero puede dirigirse a la Agencia Española de Protección de Datos para solicitar esta información en el teléfono 901 100 099.
3 También podrá ejercerse a través de representación legal, en cuyo caso, además del DNI del interesado, habrá de aportarse

DNI y documento acreditativo auténtico de la representación del tercero

FREMM

LERROUX BUSINESS LAWYERS

DESTRUCCIÓN DE DOCUMENTOS

Destrucción de documentos. Plazo de conservación. Cancelación. Técnicas de destrucción

Los datos sólo deben conservarse durante el tiempo necesario para las finalidades del tratamiento para las que han sido recogidos y podrán ser suprimidos una vez cumplidos los plazos legales de conservación.

Además respecto del encargado del tratamiento el artículo 28.3.g) establece como una de sus obligaciones *"a elección del responsable, suprimirá o devolverá todos los datos personales una vez finalice la prestación de los servicios de tratamiento, y suprimirá las copias existentes a menos que se requiera la conservación de los datos personales en virtud del Derecho de la Unión o de los Estados miembros"*

Por lo que parece deducirse que los Estados miembros podrán a través de su legislación interna imponer plazos para la conservación de datos personales, como ya se viene haciendo con la LOPD y diversas normas sectoriales dependiendo de la rama de actividad, Un ejemplo es el plazo de conservación por un mínimo de 5 años que establece el artículo 17 de la Ley de Autonomía del Paciente.

Si un interesado deseara cancelar un dato no se procedería a su destrucción sino que se produciría un bloqueo con miras a imposibilitar su acceso por parte del personal, pero con acceso a Administraciones Públicas o de Jueces y Tribunales debido a posteriores reclamaciones. Prescritas dichas responsabilidades deberá procederse a la supresión.

FREMM

LERROUX BUSINESS LAWYERS

CICLO DE VIDA DE LA INFORMACIÓN Y NORMATIVA APLICABLE

El ciclo de vida de la información consta de tres etapas: generación, conservación y destrucción. Nos vamos a centrar en la etapa de destrucción donde son aplicables diferentes normas y certificaciones entre ellas cabe destacar:

- ISO 15713: 2010 Destrucción segura del material confidencial, código de buenas prácticas. Complemento a la normativa de protección de datos personales y garantiza la destrucción de dichos datos en todo tipo de soportes, indicando los niveles de destrucción según el tipo de información y el tipo de soporte donde se encuentre, donde un nivel alto de protección significará que la recuperación de los datos tiene mayor dificultad

- DIN 66399: Establece el grado de confidencialidad e irrecuperabilidad de los documentos en función del tamaño de las tiras o partículas una vez triturado el documento físico. Sustituye a la antigua DIN 32757, su nivel de seguridad mas alto es el 7 donde los documentos físicos quedarán reducidos a partículas de menos de 5 mm2 o lo que es lo mismo, 12474 tiras o partículas por cada folio DIN-A4. Se utiliza para todo aquello que tenga formato físico como papel, radiografías, soportes ópticos, tarjetas, cinta de film o discos duros entre otros.

FREMM

LERROUX
BUSINESS LAWYERS

METODOS DE BORRADO DE DATOS

Métodos no seguros de borrado serian:

- Aquel dispuesto por el sistema operativo mediante las opciones eliminar, suprimir o delete ya que solo eliminan el contenido de la lista de archivos permaneciendo el archivo en el almacenamiento.

- Tampoco es un método seguro de borrado aquel ejecutado mediante comandos donde el contenido permanece realmente intacto.

- Formatear el dispositivo tampoco es la mejor alternativa ya que no altera el área de datos donde se encuentra el contenido.

Métodos seguros de borrado:

Hay diferentes métodos que persiguen la destrucción de la información y que realizados correctamente impedirán su recuperación. Los mas fiables evitando la recuperación del contenido son:

- Desmagnetización: Intensa exposición de dispositivos electrónicos a campas magnéticos, se utiliza para discos duros, cintas magnéticas de backup, disquetes y otros de similares características.

- Destrucción física: Inutilización del soporte que almacena la información mediante técnicas de desintegración, pulverización, fusión incineración o trituración dependiendo del soporte que almacene la información. Implicando la imposibilidad de recuperación posterior

- Sobre-escritura: Escritura de un patrón de datos sobre los datos contenidos en los dispositivos de almacenamiento, accediendo a su contenido y modificando los valores almacenados. Se debe escribir la totalidad de la superficie de almacenamiento.

FREMM

LERROUX BUSINESS LAWYERS

BORRADO POR LA PROPIA EMPRESA O POR UN TERCERO

Caben dos supuestos que la propia empresa destruya la documentación o que encargue o ceda dicha tarea a un tercero:

- En el primer caso la empresa tiene la obligación de cerciorarse de que se cumplan todos los requisitos normativos y de la efectiva destrucción de los documentos mediante alguna de las técnicas anteriormente expuestas, así como mediante las certificaciones correspondientes, para acreditar su destrucción y aquellos errores que puedan darse en el proceso sean solucionados. También se debe cerciorar de que el acceso a las copias de seguridad de los datos se realice mediante una política de seguridad que evite fugas de información y asegure la cadena de custodia

- En el segundo caso, aquel en el que se encarga o cede a un tercero la tarea de destrucción. La empresa cesionaria debe asegurarse de que la tercera cumpla la normativa de protección de datos y de destrucción de documentación, pudiendo contar y siendo beneficioso que estuviera inscrita en algún mecanismo de certificación como la ISO 1573:2010 ya citada anteriormente.

Madrid Office
Calle Claudio Coello, 124, 4º Izq
28006-Madrid
T (+34) 915 930 072
F (+34) 915 942 824

www.lerroux.com

©Lerroux 2017 - Map pictures and images used under CC license (Heraldry)