

EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS

Guía gratuita para abogados

**Las claves básicas
para su elaboración**

edj
XTech
Law
School

¡Hola!

¡Bienvenidos a la guía de evaluación de impacto de protección de datos para despachos de abogados!

Es un honor para mí darles la más cordial bienvenida a EDJ XTECH Law School, la escuela de negocios que ha sido mi sueño y pasión durante mucho tiempo. Soy Leyre Pérez, CEO y Co-Fundadora de la primera escuela de negocios online para abogados especializada en tecnología.

En un mundo cada vez más digitalizado y con transmisiones constantes de información, la protección de datos se ha convertido en un aspecto fundamental en nuestros despachos. Todas las gestiones o tratamientos de datos que no se realicen siguiendo unos estándares de seguridad pueden comprometer los datos de nuestros clientes, y verse dañada nuestra imagen empresarial. Por ello, nos complace presentarles esta guía gratuita de protección de datos, la cual tiene como objetivo principal elaborar un plan de evaluación de impacto de protección de datos en nuestros despachos.

¡Creemos firmemente en el acceso equitativo a la información y en brindar recursos que ayuden a contrarrestar los riesgos asociados al tratamiento de datos.

Apoyamos el acceso a formación gratuita generando recursos que ayuden a un entorno legal innovador y actualizado.



Leyre Pérez
Co-fundadora y CEO
EDJ XTECH Law School

Índice

Como institución educativa, tenemos la responsabilidad de fomentar una cultura de seguridad y promover buenas prácticas en el uso de la información.



Índice de vulneraciones de datos 04

¿Qué es una Evaluación de Impacto de Protección de Datos? 05

¿Es obligatoria la EIPD en mi despacho? 06

¿Qué debe contener una EIPD? 08

¿Qué medidas debo implantar? 09

¿Cuáles son las consecuencias de no realizar una EIPD? 12

Índice de vulneración de datos

El auge de las tecnologías, la navegación continua por Internet, con la consiguiente aceptación de cookies, la descarga de aplicaciones y el registro continuo en plataformas y negocios creando perfiles de usuarios, implican nuevos riesgos en materia de protección de datos.

En el año 2022 el sector legal ha visto incrementarse un 57% los ataques cibernéticos por ransomware, es decir, por secuestro de datos y la consiguiente extorsión para su liberación. Igualmente, este año el 69% de las empresas españolas sufrió alguna vulneración de datos, según el informe de Infoblox de 2022; y esta cifra alcanza el 83% en las empresas de América Latina, según IBM Security.

Ante esta situación, las empresas deben desarrollar un protocolo de actuación adecuado para la protección de los datos, y con carácter previo, una evaluación de impacto de protección de dichos datos.

Aunque tu empresa o despacho sea muy responsable en el cumplimiento de las leyes de protección de datos... ¡Debes mostrarlo!

Tus clientes deben conocer el compromiso de tu despacho con la protección de datos y el respeto absoluto de la privacidad personal.

El sector legal ha visto un 57% más de ataques cibernéticos consistentes en secuestro de datos

¿Qué es una

Evaluación de impacto

de protección de datos?

Una de las primeras medidas para velar por la protección de los datos de las personas físicas recabados en nuestro despacho o negocio, es elaborar una Evaluación de Impacto de Protección de Datos (EIPD) o PIAS (por sus siglas en inglés, Privacy Impact Assessments) recogida en el RGPD.

La EIPD es la herramienta utilizada para el análisis de los riesgos que entraña un producto o servicio para la protección de datos de personas físicas.

El propósito principal es mantener la seguridad de la información de nuestros clientes, mediante la adopción de medidas técnicas y organizativas necesarias para eliminar riesgos que se hubieran detectado.



The background of the page is a dark blue gradient. On the left side, there is a vertical strip of white binary code (0s and 1s) and the word "DATA" in white capital letters. At the bottom of the page, there is a blurred image of a computer keyboard with white keys on a dark background.

¿Es obligatoria la EIPD en mi despacho?

En todo caso, la EIPD siempre es recomendable pues permite demostrar que se cumple con el principio de responsabilidad proactiva de la normativa y que se están implementando todas las medidas necesarias para garantizar el RGPD.

Pero NO. La EIPD no es obligatoria en todos los tratamientos, sino que es obligatoria para tratamientos que implican alto riesgo para los derechos y libertades de las personas físicas. El artículo 24 RGPD determina que se tendrán en cuenta la naturaleza, el ámbito, el contexto, los fines del tratamiento y riesgos de diversa probabilidad y gravedad para derechos de personas físicas.

La EIPD sólo es obligatoria para tratamientos que implican alto riesgo para los derechos y libertades de las personas físicas.

Deberás implantarla si cumples 2 o más de los siguientes criterios:

1	Tratamientos que implican valoración de personas que cubran varios aspectos de su personalidad o hábitos.
2	Uso de datos personales que implican la toma de decisiones automatizadas.
3	Gestión de datos que impliquen observación, monitorización, supervisión, geolocalización o control de las personas de forma sistemática.
4	Tratamientos de datos de categorías especiales (i.e. sanitarios), datos relativos a condenas o infracciones o datos relativos a situación financiera o solvencia patrimonial.
5	Gestión de datos biométricos de identificación de las personas.
6	Uso de datos genéticos.
7	Tratamiento de datos a gran escala.
8	Operaciones que impliquen la asociación o combinación de bases de datos de dos o más tratamientos con finalidades distintas o responsables distintos.
9	Tratamiento de datos de personas vulnerables o en riesgo de exclusión social.
10	Uso de datos de nuevas tecnologías o nuevos usos de tecnologías consolidadas.
11	Operaciones con datos personales que impidan a los interesados ejercer sus derechos, utilizar un servicio o ejecutar un contrato.

¿Qué debe contener una EIPD?

1. Individualización

Una EIPD debe ser detallada e individualizada al despacho teniendo en cuenta:

- Sus actividades.
- Sus riesgos.
- La información contenida.



2. Contenido mínimo

- Identificación de los responsables de las distintas áreas.
- Identificación y clasificación de la información para determinar los datos personales que se tratan.
- Identificar quiénes tendrán acceso a los datos personales y cómo los tratarán.
- Identificar los controles que se implantarán para asegurar que los datos recabados sean solamente los necesarios y para finalidades legítimas.
- Descripción de medidas necesarias para la mitigación de los riesgos.
- Determinar las revisiones ordinarias y extraordinarias que se realizarán a la EIPD.

3. Sin información confidencial

La EIPD debe facilitarse a todo el personal para su conocimiento e implantación durante el desempeño de las labores de la empresa. Por ello, es imprescindible que en la EIPD no se recoja información de carácter confidencial.





Medidas recomendables

¿Qué medidas debo implantar?

Para una adecuada EIPD existen dos tipos de medidas que es conveniente implantar en nuestro despacho:

1. Medidas técnicas: Desde el punto de vista técnico, se han elaborado estándares de gestión de riesgos como:

1.1. *Norma ISO/IEC DIS 29134* sobre la evaluación de impacto en materia de intimidad.

1.2. *Norma UNE-ISO 31000:2009* sobre la gestión de riesgos que es una norma básica para poder implantar otras normas, como la *Norma ISO 27001:2017* de seguridad de la información.

2. Medidas organizativas: Desde el punto de vista organizativo, las medidas organizativas variarán entre empresas, precisamente en atención a los datos recogidos y a las actividades realizadas. No obstante, existe diversos protocolos y medidas de seguridad que serán aplicables con carácter general.

En todo caso, el factor clave para éxito en la implantación de la EIPD será la concienciación y formación al personal.

Medidas técnicas

Medida 1



1. Protección del correo electrónico (antispam).

Medida 2



2. Cortafuegos

Medida 3



3. Realización de copias de seguridad

Medida 4



4. Cifrado de datos

Medida 5



5. Gestión de contraseñas

Medida 6



6. Network Access control para determinar políticas de accesos y conexión.

Medidas organizativas

Medida 1



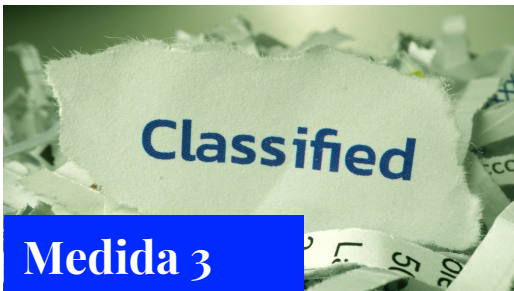
1. Políticas de seguridad

Medida 2



2. Diseño de un plan de tratamiento de datos

Medida 3



3. Protocolos de utilización de información clasificada.

Medida 4



4. Cláusulas de seguridad de proveedores

Medida 5



5. Políticas de intercambio de información: uso de dispositivos móviles, teletrabajo, etc.

Medida 6



6. Política de borrado y destrucción de documentos.

Consecuencias de no elaborar una EIPD

La obligatoriedad o no en la elaboración de la EIPD en tu despacho determina también consecuencias de diversa índole.

1. Consecuencias legales:

En el caso de la elaboración de la EIPD sea obligatoria para el responsable del tratamiento, su incumplimiento puede dar lugar a una infracción del RGPD.

Concretamente, sería una infracción de las disposiciones 35 y 36 del RGPD, generando responsabilidad para el responsable o encargado del tratamiento.

2. Consecuencias económicas:

Por un lado, las infracciones cometidas en función de su gravedad pueden conllevar multas de la AEPD de hasta 20 millones de euros. Por otro, una vulneración de datos puede ocasionar interrupciones de actividad y la consiguiente pérdida de negocios.



3. Consecuencias reputacionales:

Los datos personales de tus clientes pueden quedar expuestos, de forma que se dañe su confianza en la gestión de sus datos por parte de tu despacho legal. Tenemos que considerar, además, que los datos obrantes en un despacho de abogados pueden ser especialmente delicados (i.e. antecedentes penales, pensiones de alimentos, etc.) por lo que la inadecuada protección de datos puede perjudicar tu imagen empresarial.



Gracias por haber tomado el tiempo de leer esta guía sobre protección de datos para abogados. Esperamos que esta guía les haya proporcionado una visión sólida de las claves básicas a tener en consideración para la elaboración de una EIPD, así como de su trascendencia jurídica en un despacho de abogados.

Te animamos a continuar explorando y profundizando en este tema, ya que las vulneraciones de datos son cada vez más frecuentes y es fundamental estar preparados para enfrentar los desafíos que surgen en el mundo digital.

¿QUIERES FORMARTE EN TECNOLOGÍA Y EFICIENCIA DIGITAL?

Infórmate sobre nuestros
cursos de formación continua



ADQUIERE EL MANUAL DEFINITIVO PARA SOBREVIVIR A LA ERA DIGITAL

Si has estado leyendo las noticias, seguramente te hayas dado cuenta de que la tecnología está cambiando la forma en que se llevan a cabo los negocios, las interacciones entre las personas, la adquisición de bienes, la firma de contratos e incluso la contratación de abogados.

Este libro es una guía completa que te ayudará a sumergirte en la ola de la tecnología, automatizar tu despacho, atraer nuevos clientes y evitar ser reemplazado por un abogado innovador (o un robot).

Disponible en
amazon



FUENTES DE INFORMACIÓN

[[1] AEPD (s.f.) Evaluación de impacto. <https://www.aepd.es/es/preguntas-frecuentes/2-rgpd/10-evaluacion-de-impacto>.

[2] Ayudaley (s.f.) Evaluación de impacto de protección de datos. <https://ayudaleyprotecciondatos.es/2019/02/20/evaluacion-impacto-proteccion-datos-rgpd/>

[3] Jiménez, M. (18 jul. 2023) Los grupos de secuestro de datos o ransomware ponen foco en los servicios profesionales. <https://cincodias.elpais.com/companias/2023-07-18/los-grupos-de-secuestro-de-datos-o-ransomware-ponen-foco-en-los-servicios-profesionales.html>

[4] User Tech Business (28 abr. 2023) El 69 % de las organizaciones españolas sufrió al menos una violación de datos en 2022. <https://www.ituser.es/seguridad/2023/04/el-69-de-las-organizaciones-espanolas-sufrio-al-menos-una-violacion-de-datos-en-2022>

[5] Revista economía. (23 feb. 2023). Un 83% de las organizaciones en Latinoamérica ha tenido más de una vulneración de datos. <https://www.revistaeconomia.com/un-83-de-las-organizaciones-en-latinoamerica-ha-tenido-mas-de-una-vulneracion-de-datos-ciberresiliencia-es-el-concepto-que-toma-fuerza-en-el-mundo-virtual/>

[6] Grupo ático 34 (s.f.) Medidas técnicas y organizativas en protección de datos. <https://protecciondatos-lopd.com/empresas/medidas-tecnicas-organizativas/>

EVALUACIÓN DE IMPACTO DE PROTECCIÓN DE DATOS

Guía gratuita para abogados



EDJ EXTECH LAW SCHOOL

@EDJuristas

contacto@eficienciadigitalparajuristas.com

www.eficienciadigitalparajuristas.com

TODOS LOS DERECHOS RESERVADOS.



No se permite la reproducción, transmisión en cualquier forma o medio, electrónico o mecánico, almacenamiento en un sistema de recuperación, fotocopia, grabación, escaneo, o de cualquier otra manera, de ninguna parte de este libro. Cualquiera de estas acciones requiere la debida autorización por escrito de las autoras.