

**TALLERES FORMATIVOS GRATUITOS PARA
ENTIDADES SIN ÁNIMO DE LUCRO**

**modo
dataprotección**

**Las herramientas clave para las
organizaciones del tercer sector en
materia de Protección de Datos**

HERRAMIENTAS GRATUITAS DE LA AEPD

Andrea Sánchez

Este documento consiste en un breve resumen sobre las herramientas gratuitas que la Agencia Española de Protección de Datos pone a disposición de las empresas, principalmente dirigido a las PYMES, para facilitarles la comprensión y cumplimiento de las obligaciones en materia de protección de datos establecidas en el RGPD y la Ley Orgánica 3/2018. En particular, las herramientas abordadas en el presente documento permiten ayudar a que las empresas sepan cómo gestionar los riesgos y realizar una evaluación de impacto, así como identificar la necesidad de notificar una brecha de seguridad a las personas físicas afectadas. Adicionalmente y en última instancia, se hace una breve referencia a las ocasiones en que se debe utilizar y cómo el canal de consultas de los delegados de protección de datos.

Pérez-Llorca

UNA INICIATIVA DE:



Coordinadora de
ONG para el Desarrollo
Región de Murcia

www.coordinadoraongdrm.org



Fundación
Pro Bono
España

www.probonoespana.org

FORMACIÓN IMPARTIDA POR:

C L I F F O R D
C H A N C E

Pérez-Llorca



Pinsent Masons



Ramón y Cajal
ABOGADOS

CON EL APOYO DE:



El presente documento no constituye ningún asesoramiento jurídico por parte de las y los profesionales del Derecho que lo distribuyen, sino que está elaborado con el único propósito de difundir conocimientos de interés general en torno a la normativa de protección de datos para que las entidades sin ánimo de lucro puedan basarse en el mismo para

trabajar su documentación propia. Por tanto, los autores del documento están exonerados de cualquier responsabilidad por la utilización del mismo.

RECUERDA:

- ❑ Tendremos una segunda sesión **NO GRABADA** para revisar el trabajo que habéis realizado y resolver vuestras dudas. No obstante, puedes **enviar cualquier consulta o duda a nuestro equipo a través del correo mododataprotection@gmail.com**

- ❑ **La segunda sesión del taller será el día 23 de junio de 2022.**

HERRAMIENTAS GRATUITAS DE LA AEPD PARA EL CUMPLIMIENTO EN MATERIA DE PROTECCIÓN DE DATOS

La Agencia Española de Protección de Datos (AEPD) proporciona una serie de herramientas gratuitas a las empresas que facilitan la comprensión y cumplimiento de aquellas obligaciones que la normativa de protección de datos, principalmente el Reglamento General de Protección de Datos (UE) 2016/279 (RGPD) y la Ley Orgánica 3/2018 de Protección de Datos y Garantía de los Derechos Digitales (LOPDGDD), establecen para los responsables y encargados del tratamiento de datos personales.

Estas herramientas se pueden encontrar en la página oficial de la AEPD en la sección de Guías y Herramientas > Herramientas.

HERRAMIENTAS GESTIÓN DEL RIESGO

En primer lugar, a lo largo del transcurso de nuestra primera sesión [8 de junio] abordaremos **las herramientas de la AEPD destinadas a facilitar la identificación y gestión de los riesgos** que pueda conllevar el tratamiento de los datos personales que efectúa una empresa, así como ayudar a identificar las ocasiones donde resulte necesario elaborar una evaluación de impacto, y cómo hacerlo, y aquellas donde resulte necesario efectuar una consulta previa ante la AEPD.

Antes de proceder a explicar el funcionamiento de las herramientas de gestión del riesgo, debemos hacer un breve recordatorio de los

artículos 35 y 36 del RGPD que desarrollan las obligaciones del responsable del tratamiento de los datos de realizar una evaluación de impacto (EIPD) y una consulta previa a la autoridad de control.

El tratamiento de los datos personales puede generar un impacto adverso en las personas físicas afectadas por el mismo. Es por ello que el RGPD demanda al responsable del tratamiento, en virtud del principio de responsabilidad proactiva, la identificación, evaluación y mitigación realizadas de una forma objetiva, del riesgo para los derechos y libertades de las personas en los tratamientos de datos personales. La mitigación ha de realizarse mediante la adopción de medidas técnicas y organizativas que garanticen y, además, permitan demostrar la protección de dichos derechos.

Con carácter general, el RGPD no exige ningún requisito explícito a la hora de ejecutar la gestión del riesgo. En consecuencia, todas las empresas con independencia del tratamiento que lleven a cabo, deben identificar aquellos riesgos que se deriven de su tratamiento y buscar y aplicar medidas que permitan mitigar su impacto. No obstante, y para aquellos tratamientos que impliquen un alto riesgo, el RGPD sí establece unos requisitos mínimos que ha de tener su gestión. Estos se derivan, especialmente, de las obligaciones establecidas en los artículos 35 “Evaluación de impacto relativa a la protección de datos” (EIPD), y el artículo 36 “Consulta previa” del RGPD.

La Evaluación de Impacto (EIPD) es una especificidad dentro de la gestión del riesgo. Mientras que, como hemos dicho previamente, la gestión del riesgo es obligatoria para todo tratamiento, las

obligaciones concretas que se establecen para la EIPD son obligatorias, exclusivamente, para tratamientos de alto riesgo. La autoridad de control es la que establece con carácter general aquellos tratamientos que requieren de una evaluación de impacto, no obstante, podemos citar como ejemplo aquellos que implican un tratamiento automatizado como la elaboración de perfiles, aquellos que implican un tratamiento a gran escala de categorías especiales de datos, etc.

Por otro lado, las consultas previas son aquellas consultas que se efectúan a la autoridad de control para buscar asesoramiento sobre las medidas mitigadoras a aplicar cuando, tras haber realizado una EIPD, el riesgo residual resultante es elevado y podría poner en riesgo los derechos y libertades de las personas físicas afectadas.

Pues bien, para facilitar el cumplimiento de estas obligaciones, la AEPD pone a disposición de las empresas las siguientes herramientas:

1. FACILITA RGPD
2. FACILITA EMPRENDE
3. GESTIONA EIPD
4. EVALÚA RIESGO RGPD

Para conocer cuándo utilizar cada una de estas herramientas, dejamos a continuación un cuadro explicativo.

¿El tratamiento de datos personales conlleva un riesgo escaso o bajo?

- FACILITA RGPD: La herramienta permite a la empresa generar documentación para cumplir con los requisitos del RGPD cuando el tratamiento conlleva un riesgo bajo. Si la herramienta de FACILITA RGPD considera que no aplica a la empresa por ser el riesgo del tratamiento no escaso, la misma indica a la empresa la necesidad de llevar a cabo una gestión de riesgos.

¿La empresa que trata los datos personales es una empresa de nueva creación que aplica herramientas innovadoras o novedosas relacionadas con las nuevas tecnologías?

- FACILITA EMPRENDE: Es una herramienta que sirve de apoyo para caracterizar los tratamientos realizados por empresas con nuevas tecnologías y startups de reciente creación (que suelen ser de mayor dificultad en este tipo de empresas que utiliza tecnologías innovadoras). Este tipo de empresas al utilizar tecnologías muy innovadoras muchas veces implican un tratamiento de datos de alto riesgo por lo que en ocasiones esta herramienta te remite a GESTIONA EIPD para que evalúes el riesgo y veas si es necesario una EIPD.

¿Se desconoce el riesgo que implica el tratamiento de datos?

- GESTIONA EIPD: Esta herramienta es un asistente previo para preparar la gestión del riesgo para los derechos y libertades y permite a la empresa saber si resulta necesario que efectúe una evaluación de impacto en protección de datos.

¿El tratamiento de los datos personales conlleva un riesgo alto?

- EVALÚA- RIESGO RGPD: Esta herramienta permite a las empresas hacer una primera evaluación del riesgo intrínseco; establece la necesidad de realizar una Evaluación de Impacto y estima el riesgo residual si se utilizan medidas y garantías para mitigar los factores de riesgo específicos. Al estimar este riesgo residual te permite saber si resulta necesario que se efectúe una consulta previa a la AEPD.

En adelante pasamos a desarrollar estas cuatro herramientas de forma individualizada.

HERRAMIENTA 1: FACILITA RGPD

¿En qué consiste la herramienta?

FACILITA RGPD es una herramienta de ayuda para las empresas que realicen un tratamiento de datos personales de escaso riesgo (e.g. tratamientos de datos de contacto y facturación de los clientes o proveedores de una pequeña empresa) para facilitarles la adaptación al cumplimiento del Reglamento General de Protección de Datos. **ES DE LAS HERRAMIENTAS MÁS UTILIZADAS POR LAS EMPRESAS.**

En concreto, la herramienta permite, a través de tres pantallas de preguntas valorar la situación de la empresa en términos de tratamiento de los datos personales. En base a ello, FACILITA RGPD genera documentos de protección de datos adaptados a la empresa concreta, entre otros, cláusulas informativas que debe incluir en sus formularios de recogida de datos personales, el registro de actividades de tratamiento.

El enlace para acceder a dicha herramienta es el siguiente:

<https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQwMjAzNDkxNjUxNzUxOTk1NTgw?updated=true>.

Cuestiones a tener en consideración

- La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la

LOPDGDD para los responsables y encargados de tratamiento, únicamente proporciona orientación y facilita la comprensión de dichas obligaciones.

- La herramienta NO PUEDE utilizarse para tratamientos de datos personales que entrañen un elevado riesgo para los derechos y libertades de las personas físicas como tratamientos masivos, generación y uso de perfiles, video vigilancia, etc.
- Los datos subidos o aportados a esta herramienta SE ELIMINAN tras finalizar su uso, por lo que la AEPD no conocerá la información aportada.
- La ayuda proporcionada es general, por lo que puede NO ADAPTARSE a las características concretas de todas las empresas.

Instrucciones para su uso

Accediendo al enlace que se ha aportado anteriormente, la herramienta FACILITA RGPD despliega un cuestionario o auto test que la empresa debe ir completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto.

Primero, la herramienta hace tres preguntas acerca del tratamiento de datos para asegurar que el tratamiento efectuado por la empresa no entraña un elevado riesgo para los derechos y libertades de las

personas físicas. **[Ver las capturas de pantalla que se adjuntan a continuación]**

Si la actividad de su organización pertenece a alguno de estos sectores, márquelo:

- Sanidad
- Solvencia patrimonial y crédito
- Generación y uso de perfiles
- Actividades políticas, sindicales o religiosas
- Servicios de telecomunicaciones
- Seguros
- Entidades bancarias y financieras
- Actividades de servicios sociales
- Publicidad
- Videovigilancia masiva (Videovigilancia de grandes infraestructuras como estaciones de ferrocarril o centros comerciales)
- Ninguno de los anteriores

Si su organización trata alguno de los datos de la lista, márquelos:

- Datos que revelen origen étnico o racial
- Datos de opiniones políticas o religión
- Datos de afiliación sindical (excepto cuotas sindicales)
- Datos genéticos
- Datos biométricos dirigidos a identificar de manera unívoca a una persona
- Datos de salud física o mental
- Datos relativos a la vida sexual o a la orientación sexual
- Datos relativos a condenas o infracciones penales
- Geolocalización
- Ninguno de los anteriores

Si su organización realiza alguno de los siguientes tratamientos, márquelo:

- Hacer o analizar perfiles
- Hacer publicidad y prospección comercial masiva a potenciales clientes
- Prestación de servicios de explotación de redes públicas o servicios de comunicación electrónica (proveedor de servicios de internet (LGT))
- Gestionar los asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical
- Gestión, control sanitario o venta de medicamentos
- Historial clínico o sanitario
- Ninguna de las anteriores

Si de la respuesta que se proporcione a las preguntas la herramienta entiende que no hay un riesgo alto para los derechos y libertades de las personas afectadas, la herramienta pasa a la segunda fase del cuestionario. Si no es el caso, la herramienta muestra un mensaje emergente señalando que la herramienta no es adecuada para el que la está utilizando y que debe realizar un análisis de riesgos.



Con los datos que ha proporcionado este programa no es adecuado para usted, ya que su empresa no cumple con los requisitos para seguir. Debe realizar un análisis de riesgos.

Si se supera la primera fase, la herramienta señala que es adecuada para el tratamiento y procede a recabar información de la empresa para generar los formularios correspondientes de protección de datos.

“Ha respondido de forma negativa a todas las cuestiones anteriores, por tanto, se podría entender que los tratamientos realizados por su entidad entrañan, a priori, un escaso nivel de riesgo para los derechos y libertades de los interesados y por tanto se encontraría en disposición de utilizar el siguiente programa.”

Las preguntas que se formulan para generar los formularios hacen referencia a las siguientes cuestiones:

1. Datos identificativos de la empresa (nombre, dirección de correo electrónico, NIF, teléfono, etc.). Estos datos sirven para personalizar los documentos o formularios de protección de datos que emite la herramienta.

Los datos que incorpore en el programa desde esta pantalla hasta la finalización del programa, se van a utilizar para elaborar los documentos que se generan automáticamente adaptados a su organización

Nombre de la empresa

Dirección completa de la empresa

N.I.F.:

Teléfono

Dirección de correo electrónico:

Descripción de la actividad

2. A continuación, la herramienta pregunta las categorías de interesados de los cuales se tratan los datos: (i) clientes personas físicas, (ii) empleados, (iii) candidatos, (iv) proveedores personas físicas. Si se responde afirmativamente a la categoría de interesado, la herramienta desplegará un

cuestionario con preguntas acerca de los datos que se recaban de esas categorías de interesados (tipos de datos (bancarios, identificativos, etc.); para que finalidades los recaba (prestar servicio, etc.) y a quién entrega esos datos).
[Ver captura de pantalla ejemplificativa de esta cuestión]

| | |
|---|--|
| ¿Su organización trata datos personales de clientes (personas físicas)? Se refiere a datos personales de aquellas personas con las que usted mantiene una relación comercial. | |
| <input checked="" type="radio"/> Sí <input type="radio"/> No | |

| | |
|---|--|
| A continuación marque qué datos personales trata de sus clientes | Marque para qué utiliza los datos personales que solicita a sus clientes |
| <input type="checkbox"/> Identificación (nombre, apellidos, NIF, dirección postal, teléfono, email) <input type="checkbox"/> Características personales (estado civil, fecha y lugar de nacimiento, edad, sexo, nacionalidad) <input type="checkbox"/> Datos académicos <input type="checkbox"/> Datos bancarios | <input type="checkbox"/> Prestarles un servicio <input type="checkbox"/> Facturar <input type="checkbox"/> Enviar publicidad postal o por correo electrónico <input type="checkbox"/> Servicio postventa y fidelización |

Marque a quien entrega los datos personales de sus clientes

| | |
|---|-----------------------------------|
| Cumplimiento de obligaciones legales: | Otros: |
| <input type="checkbox"/> Agencia Estatal de Administración Tributaria <input type="checkbox"/> Instituto Nacional de la Seguridad social <input type="checkbox"/> Bancos y entidades financieras <input type="checkbox"/> Fuerzas y Cuerpos de Seguridad <input type="checkbox"/> Otros | <input type="checkbox"/> Gestoría |

Asimismo, la herramienta también pregunta las siguientes cuestiones (las mismas se preguntan porque la comunicación de datos a terceros subcontratados o la recogida de imágenes con cámaras de video vigilancia puede conllevar un riesgo alto):

- ¿Su organización capta imágenes mediante cámaras de video vigilancia con fines de seguridad?

- ¿Su organización tiene contratadas terceras empresas que le prestan servicios como pueden ser los de mantenimiento de su página web, desarrollo de programas informáticos, proveedor de correo electrónico, hosting, servicio de limpieza, servicio de video vigilancia u otros?

Una vez respondido el cuestionario, la herramienta generará los documentos de protección de datos adaptados a la empresa. Estos documentos se descargarán en formato Word que podrá ser editado por la empresa a su discreción para adaptar y personalizar en mayor medida el tratamiento de los datos que realiza.



Facilita.docx

REMINDER: La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la LOPDGG.

HERRAMIENTA 2: FACILITA EMPRENDE

¿En qué consiste la herramienta?

Esta herramienta busca dar apoyo a personas emprendedoras y startups (menos de 10 años de creación) cuyos tratamientos se

caracterizan por un fuerte componente innovador, con empleo de tecnologías emergentes.

En concreto, la herramienta permite caracterizar los tipos de tratamientos realizados y proporcionar los documentos que se enumeran a continuación y que dan apoyo a la empresa para cumplir con las obligaciones de protección de datos:

1º) Una política de información en dos niveles compuesta por las cláusulas de informativas a proporcionar en el momento de la recogida de datos y una política de privacidad.

2º) El Registro de Actividades de Tratamiento (RAT) pre cumplimentado.

3º) El modelo de hoja de registro de incidentes para cumplir con el artículo 33.5 relativo a la documentación de las brechas de seguridad que afecten o puedan afectar a datos personales.

4º) Un conjunto de cláusulas contractuales a incluir en los contratos que suscriba con las personas encargadas de tratamientos de datos y proveedores.

5º) Si su empresa cuenta con una página web que utiliza cookies y tecnologías similares, una política de cookies.

6º) Un conjunto de directrices y recomendaciones, para ayudarle en el proceso de adecuación, en relación con la gestión de brechas de seguridad, la atención al ejercicio de los derechos,

recomendaciones sobre video vigilancia, indicaciones específicas con relación a la gestión de los riesgos de sus tratamientos, así como a las estrategias de privacidad y medidas de seguridad que deberá implementar.

7º) Una relación de recomendaciones para prevenir el acoso digital.

El enlace para acceder a esta herramienta es el siguiente:

<https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQwMjY4MzAxNjUxOTI3NzM2MjM5?updated=true>.

Cuestiones a tener en consideración

- La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la LOPDGDD.
- Cabe la posibilidad de por los tipos de tratamiento que suelen ir asociados a los modelos de negocios de emprendedores y startups, la empresa no tenga un riesgo bajo para los derechos y libertades de las personas físicas y entonces, tenga que personalizar y complementar los entregables facilitados por esta herramienta.
- La información SE ELIMINA terminada la sesión por lo que la AEPD no puede conocer ni tratar dicha información.

Instrucciones para su uso

Accediendo al enlace que se ha aportado anteriormente, la herramienta FACILITA EMPRENDE despliega un cuestionario o auto test que la empresa debe ir completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto.

El proceso de cumplimentación está estructurado en tres partes:

En primer lugar, se evalúa si la empresa encuadra en el perfil de una startup tecnológica, identificando las tecnologías utilizadas (e.g. plataformas colaborativas, aplicaciones móviles, etc.) y recogiendo los datos para generar el documento personalizado (i.e. nombre de la empresa, NIF, descripción de la actividad etc.). **[Ver las capturas de pantalla que se adjuntan a continuación]**

SECCIÓN 1 de 3: IDENTIFICACIÓN DE LA ENTIDAD Y ACTIVIDADES DESARROLLADAS

Marque las opciones que caracterizan a su empresa y al modelo de negocio que desarrolla:

De acuerdo con el criterio seguido por el [EU Startup Monitor](#) en el estudio de la evolución del ecosistema europeo de emprendimiento, una empresa, para ser considerada startup, debe cumplir los siguientes requisitos:

- Tener un máximo de 10 años de antigüedad
- Mostrar un fuerte carácter innovador en productos y servicios
- Contar con expectativas de crecimiento del número de empleados o de los mercados en los que opera.

¿Considera que su empresa reúne los requisitos enunciados?

- Sí
- No

Marque las tecnologías o desarrollos innovadores que aplican en su modelo de negocio:

- Plataformas colaborativas
- Marketplace y/o comercio electrónico
- Desarrollo de soluciones SaaS (Software as a Service)
- Desarrollo de aplicaciones web/móviles
- Juegos
- Análisis masivo de datos
- Otras

Nombre o razón social de la empresa

N.I.F.:

Dirección completa de la empresa a efectos legales (vía, número, código postal, localidad y provincia)

| | |
|----------------------|---|
| Teléfono | Dirección de correo electrónico: |
| <input type="text"/> | <input type="text"/> |

Una vez recogidos estos datos, la herramienta pregunta en calidad de qué se está tratando datos personales: (i) responsable; (ii) encargado; (iii) desarrollador. Identificado el rol, la herramienta pasa a solicitar información sobre aquellos tratamientos de tipo básico que la empresa puede estar gestionando como responsable (datos de clientes potenciales, clientes, empleados, candidatos, proveedores personas físicas y qué datos en concreto o para qué finalidad) así como los datos de identificación de aquellas terceras

partes que le estén prestando un servicio a su entidad. A partir de esta información la herramienta generará información de utilidad para ayudar a la empresa en el cumplimiento de sus obligaciones: elaboración de los registros de actividades de tratamiento, cláusulas informativas, modelos de contratos con encargados de tratamiento, etc.

SECCIÓN 2 de 3: ANÁLISIS BÁSICO DE LOS TRATAMIENTOS

Aplicando la terminología del Reglamento Europeo de Protección de Datos, usted es **responsable de un tratamiento** cuando es quien decide acerca de la finalidad a la que se destinan los datos o informaciones que pueda recopilar relativas a personas físicas y cuando toma decisiones acerca de los medios o formas en los que dichos datos o informaciones personales van a ser tratados o procesados. En este caso, como responsable de un tratamiento de datos personales, debe de abordar todas las obligaciones señaladas en el RGPD y en la LOPDGDD.

Por el contrario, si en el marco de una relación contractual, usted procesa datos o informaciones personales relativas a personas físicas a requerimiento o solicitud de un tercero que es quién decide sobre la finalidad y los medios o formas en la que los datos van a ser procesados, siguiendo sus instrucciones en todo momento, entonces usted es **encargado de tratamiento**.

Además, en calidad de startup, su empresa podría estar realizando el diseño y desarrollo de productos y servicios adquiridos posteriormente por terceros, ya sean responsables o encargados, actuando como **desarrollador o fabricante** de productos tecnológicos en el contexto de lo que podemos denominar la economía digital. Aunque en ese caso no juegue un papel de responsabilidad desde el punto de vista de las obligaciones del RGPD, pueden resultarle de utilidad las pautas facilitadas en la documentación generada por la herramienta a la hora de incorporar a sus productos aquellas estrategias de diseño y opciones de configuración que ayuden a responsables y encargados a cumplir con sus obligaciones en materia de protección de datos.

En base a lo indicado, seleccione de las siguientes opciones aquellas en las que considera que se desarrollan sus actividades empresariales en las que se tratan o procesan datos y/o informaciones personales:

- Soy responsable
- Soy encargado
- Soy desarrollador

SECCIÓN 2 de 3: ANÁLISIS BÁSICO DE LOS TRATAMIENTOS

¿Su startup trata datos personales de potenciales clientes (personas físicas)?

Se refiere a datos personales de aquellas personas físicas con la que usted todavía no mantiene una relación comercial.

Sí No

A continuación marque qué datos personales trata de sus potenciales clientes

- Datos de identificación (nombre, apellidos, NIF, dirección postal, teléfono, email)
- Características personales (estado civil, fecha y lugar de nacimiento, edad, género, nacionalidad)
- Datos profesionales (cargo, lugar de trabajo, sector de actividad)

Marque de donde obtiene los datos personales de su potenciales clientes

- Los facilitan ellos
- Los compro a una tercera empresa

SECCIÓN 2 de 3: ANÁLISIS BÁSICO DE LOS TRATAMIENTOS

¿Su startup trata datos personales de proveedores (personas físicas)?

Se refiere a datos personales de aquellas personas físicas que le proveen de productos o servicios necesarios para su actividad como entidad empresarial (servicios de cloud, alojamiento web, servicios de IA, hardware, software, etc.), proveedor de hardware o cualquier otro producto.

Sí No

A continuación marque qué datos personales trata de sus proveedores

- Datos de identificación (nombre, apellidos, dirección postal, teléfono, email)
- Datos bancarios (número de cuenta corriente de abono)

Marque para qué utiliza los datos personales que solicita a sus proveedores

Introduzca otras finalidades:

Finalidad 1

Asimismo, la herramienta también pregunta las siguientes cuestiones (las mismas se preguntan porque la comunicación de datos a terceros subcontratados o la recogida de imágenes con cámaras de video vigilancia puede conllevar un riesgo alto):

- ¿Su startup capta imágenes mediante cámaras de video vigilancia con fines de seguridad?

- ¿Su startup dispone de empresas contratadas que le prestan servicios como por ejemplo los de mantenimiento o alojamiento web, desarrollo de software, servicios de correo electrónico, servicio de limpieza, video vigilancia, etc.?

[Si estas preguntas se responden afirmativamente la herramienta te solicita datos relacionados con ellas].

Finalizadas estas secciones anteriores, existe una tercera fase que es variable en función de la información previamente aportada. En concreto, se analizan aquellas actividades de tratamiento que se soportan sobre las tecnologías empleadas por la empresa, caracterizando, para cada una de ellas, el nivel de riesgo que representan.

A modo de ejemplo, en esta fase la herramienta te hace preguntas como las que mostramos a continuación: ¿Su tratamiento está basado en el desarrollo o la prestación de servicios a usuarios a través de aplicaciones web o móviles? / ¿Realiza algún tratamiento, distinto de los anteriores, que haga uso de tecnologías altamente innovadoras? / ¿Su tratamiento está basado en el desarrollo de soluciones o en la prestación de servicios a usuarios que realicen un análisis masivo de datos? Estas preguntas varían en función de lo contestado en las fases anteriores. Si se contesta afirmativamente a las mismas (identificando este tratamiento), la herramienta despliega una serie de cuestionarios sobre el tipo de datos, las finalidades e identifica los factores de riesgo.

SECCIÓN 3 de 3: ANÁLISIS DE TRATAMIENTOS BASADOS EN NUEVOS DESARROLLOS TECNOLÓGICOS Y SOLUCIONES INNOVADORAS

TIPOS DE DATOS

Marque los tipos de datos que trata su empresa en este tratamiento

- Datos que revelen origen étnico o racial
- Datos de opiniones políticas o religión
- Datos de afiliación sindical (excepto cuotas sindicales)
- Datos genéticos
- Datos biométricos dirigidos a identificar de manera unívoca a una persona
- Datos de salud física o mental (excepto grado de discapacidad)
- Datos relativos a la vida sexual o a la orientación sexual
- Datos de servicios sociales
- Datos relativos a condenas penales
- Datos relativos a la situación financiera o patrimonial
- Datos sobre preferencias o intereses personales
- Datos sobre el comportamiento de las personas

SECCIÓN 3 de 3: ANÁLISIS DE TRATAMIENTOS BASADOS EN NUEVOS DESARROLLOS TECNOLÓGICOS Y SOLUCIONES INNOVADORAS

FINALIDADES

Marque las finalidades que persigue su entidad con este tratamiento

- Geolocalización
- Hacer o analizar perfiles
- Hacer publicidad y prospección comercial masiva a potenciales clientes
- Gestionar los asociados o miembros de partidos políticos, sindicatos, iglesias, confesiones o comunidades religiosas, fundaciones y otras entidades sin ánimo de lucro, cuya finalidad sea política, filosófica, religiosa o sindical
- Gestión, control sanitario o venta de medicamentos
- Mantenimiento y gestión de historiales clínicos o sanitarios en el marco de investigación sanitaria
- Mantenimiento de plataformas colaborativas
- Prestación de servicios a través de un marketplace y/o comercio electrónico
- Desarrollo de aplicaciones web/móviles/juegos dirigidas a múltiples potenciales usuarios
- Ninguno de los anteriores

SECCIÓN 3 de 3: ANÁLISIS DE TRATAMIENTOS BASADOS EN NUEVOS DESARROLLOS TECNOLÓGICOS Y SOLUCIONES INNOVADORAS

FACTORES DE RIESGO DE LOS TRATAMIENTOS

Marque los factores de riesgo que afectan a este tratamiento

- ¿Se recaban datos o información de personas en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), relativos a varios aspectos de su personalidad o sus hábitos?
- Partiendo de la información recopilada ¿se lleva a cabo la toma de decisiones automatizadas o la toma de decisiones que contribuyan en gran medida a la toma de tales decisiones automatizadas, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato?
- ¿Se lleva a cabo labores de observación, monitorización, supervisión, geolocalización o seguimiento/control de personas de forma directa o indirecta y de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, seguimiento de vehículos, etc.?
- ¿Realiza alguno de los siguientes tratamientos?
 - ¿Recopila o procesa información sobre personas relativa a informaciones de tipo étnico o racial, opiniones de índole política, información sobre convicciones religiosas o filosóficas, afiliación sindical, información de tipo genético, información biométrica que permita identificar de manera unívoca a una persona física, datos de salud, información sobre la vida sexual o la orientación sexual?
 - ¿Trata datos relativos a condenas o infracciones penales?
 - ¿Lleva a cabo análisis para determinar la situación financiera o patrimonial de las personas?
 - ¿Lleva a cabo actividades que permitan deducir alguna de las informaciones mencionadas sobre personas físicas?
- ¿Se realizan actividades en las que se tratan o procesan datos o informaciones biométricas para identificar unívocamente a las personas?
- ¿Se almacenan o procesan datos genéticos con algún fin?

A partir del análisis de los datos, las finalidades y los factores de riesgo que incorporan la herramienta realiza una recomendación respecto a la aproximación a la gestión del riesgo que debería seguir la empresa.

Como resultado final, la herramienta de FACILITA EMPRENDE te facilita:

- El saber si procede o no realizar una gestión del riesgo y una evaluación de impacto por ser el tratamiento de los datos que lleva a cabo la empresa tecnológica de alto riesgo.
- Un documento base adaptado a los tratamientos que realiza la empresa (cláusulas de firmantes, cartel de video vigilancia, etc.) y señalando aquellas cuestiones necesarias para que cumpla con la adaptación a la normativa de protección de datos. Este documento es una versión de mínimos y deberá ser validado por el responsable. El documento se descarga en formato Word, pudiendo ser editado por la empresa a su gusto.

La recogida de información a través de cuestionarios ha concluido.

RECUERDE que FACILITA – EMPRENDE es sólo una herramienta de ayuda y que el documento obtenido constituye sólo una base de mínimos que deberá estar adaptada y actualizada a la situación de los tratamientos que se lleven a cabo en su entidad. **La obtención del documento no implica, por sí misma y de forma automática, el cumplimiento automático del RGPD.**

Al pulsar el botón FINALIZAR la herramienta procederá a generar el documento en formato editable. En todo caso, no olvide realizar las siguientes actuaciones:

- Incluir las **cláusulas informativas** de primer nivel en los formularios de solicitud de información (ya sean en papel o en formato electrónico) y enlazarlos con la política de privacidad de segundo nivel en la que se pueda ampliar la información.
- Revisar los contratos de los que dispone actualmente e incluir las **cláusulas contractuales relativas a las obligaciones de los encargados** en materia de protección de datos.
- Elaborar aquellos contratos de los que todavía no dispone e igualmente incluir las cláusulas contractuales arriba referidas.
- Si dispone de cámaras de videovigilancia, debe colocar en un lugar visible el cartel informativo de **zona videovigilada** para que los interesados afectados estén informados de la existencia de los dispositivos.
- Si de su tratamiento se deriva la necesidad de contar con un **Delegado de Protección de Datos**, no olvide analizar las distintas fórmulas existentes (contratación en plantilla, subcontratación a través de una empresa especializada) para poner en marcha sus servicios.
- Implantar las medidas de seguridad, tanto técnicas como organizativas, que se le indican en el documento correspondiente.
- Documentar cualquier decisión tomada en relación con los tratamientos de datos personales, así como cualquier incidente que sufra y que pueda tener afectación en los mismos.
- Custodiar y mantener actualizados todos los documentos.



FacilitaEmprende....docx

HERRAMIENTA 3: GESTIONA EIPD

¿En qué consiste la herramienta?

Es una herramienta que funciona como asistente previo (i.e. aspectos básicos a tener en cuenta) para proporcionar ayuda en la elaboración de una evaluación de impacto (EIPD o PIA), la cual se debe llevar a cabo para ver los riesgos que suponen ciertos tratamientos de datos en los derechos y libertades de las personas físicas (no siempre se requiere una EIPD); o una gestión de los riesgos.

La herramienta está destinada para los pequeños y medianos responsables (PYMES) del tratamiento de datos personales que no dispongan en su organización de un marco para la gestión del riesgo.

En concreto, GESTIONA EIPD es como una especie de una lista cerrada de elementos a tener en cuenta, y aporta a las personas responsables las bases mínimas para iniciar las actividades de análisis y gestión de riesgos en el ámbito del RGPD, incluyendo requisitos de cumplimiento normativo y medidas encaminadas a reducir o mitigar el riesgo del tratamiento.

El enlace para acceder a esta herramienta es el siguiente:

<https://gestion.aepd.es/>

Cuestiones a tener en consideración

- La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la LOPDGDD para los responsables y encargados de tratamiento, únicamente proporciona orientación y facilita la comprensión.
- La herramienta NO SUPONE la realización de una evaluación de impacto, sino que sirve como punto de partida. En concreto, el empleo de esta herramienta se debe realizar teniendo en consideración la Guía de Gestión de riesgo y evaluación de impacto en tratamientos de datos personales de la AEPD, la lista de verificación para determinar la adecuación formal de una EIPD y la presentación de consulta previa.

- Esta herramienta NO PUEDE ENTENDERSE como una forma de aplicar las medidas técnicas y organizativas de seguridad incluidas en el artículo 32 del RGPD.
- Esta herramienta se utiliza en conjunción con el listado de tratamientos de datos personales en los que es obligatorio hacer una EIPD: https://www.aepd.es/es/documento/listas-dpia-es-35-4_0.pdf.
- Los datos que se señalen e incluyan en el cuestionario de GESTIONA EIPD se guardarán de forma local en el ordenador. Ello permite iniciar la gestión de riesgos y cerrar la sesión y luego volver a donde lo dejaste metiendo el nombre que has decidido darle al análisis. Para ello hay que pinchar al inicio de la herramienta en la opción señalada como “CARGAR ANÁLISIS PREVIOS”.



eipd
EIPD

Instrucciones para su uso

Accediendo al enlace que se ha aportado anteriormente, la herramienta GESTIONA EIPD despliega un cuestionario o auto test que la empresa debe ir completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto.

En primer lugar, para iniciar sesión la herramienta te solicita que elijas entre iniciar una EIPD o una gestión de los riesgos. Una vez seleccionas un nombre denominar a la EIPD o para la gestión de riesgos comienza el análisis.

OPCIÓN EIPD:

Si seleccionas EIPD, se formulan ocho preguntas sobre los siguientes temas:

- (i) el tipo de tratamientos que lleva a cabo tu empresa se incluye entre aquellos que la AEPD considera que requieren una EIPD;

Análisis de la necesidad de realizar una EIPD

1 Tipos de operaciones específicamente considerados por la Autoridad de control

2 3 4 5 6 7 8

¿El tratamiento a analizar se encuentra dentro de la lista de tipos de tratamientos de datos publicados por la AEPD que requieren una EIPD?

NO

Tratamientos que impliquen perfilado o valoración de sujetos, incluida la recogida de datos del sujeto en múltiples ámbitos de su vida (desempeño en el trabajo, personalidad y comportamiento), que cubran varios aspectos de su personalidad o sobre sus hábitos.

NO SI

Tratamientos que impliquen la toma de decisiones automatizadas o que contribuyan en gran medida a la toma de tales decisiones, incluyendo cualquier tipo de decisión que impida a un interesado el ejercicio de un derecho o el acceso a un bien o un servicio o formar parte de un contrato.

NO SI

Tratamientos que impliquen la observación, monitorización, supervisión, geolocalización o control del interesado de forma sistemática y exhaustiva, incluida la recogida de datos y metadatos a través de redes, aplicaciones o en zonas de acceso público, así como el procesamiento de identificadores únicos que permitan la identificación de usuarios de servicios de la sociedad de la información como pueden ser los servicios web, TV interactiva, aplicaciones móviles, etc.

NO SI

Tratamientos que impliquen el uso de categorías especiales de datos a las que se refiere el artículo 9.1 del RGPD, datos relativos a condenas o infracciones penales a los que se refiere el artículo 10 del RGPD o datos que permitan determinar la situación financiera o de solvencia patrimonial o deducir información sobre las personas relacionada con categorías especiales de datos.

NO SI

(ii) si se van a tratar categorías especiales de datos;

¿Se van a tratar categorías especiales de datos?

NO

Justifique su respuesta

¿Se van a tratar categorías especiales de datos a gran escala?

NO

Justifique su respuesta

(iii) finalidades del tratamiento (menores de edad, hacer perfiles, datos a gran escala de zonas de acceso público, etc.);

¿El tratamiento involucra datos de menores de edad en materia de Protección de Datos (14 años según la LOPDGDD)?

SI

Justifique su respuesta

¿La finalidad del tratamiento implica el uso específico de datos de personas con discapacidad o cualquier otro colectivo en situación de especial vulnerabilidad?

SI

Justifique su respuesta

(iv) tecnologías empleadas para el tratamiento;

1 2 3 4 5 **Tecnologías empleadas para el tratamiento** 6 7 8

¿Se prevé el uso de tecnologías que se pueden percibir como inmaduras, de reciente creación o salida al mercado o con elevado riesgo para el acceso no autorizado ? ? SI

Justifique su respuesta

(v) existencia de encargados de tratamiento, cesiones o transferencias internacionales de datos;

1 2 3 4 5 6 **Encargados de tratamiento, cesiones de datos y transferencias internacionales de datos** 7 8

¿Se ha delegado alguna de las tareas que compone el tratamiento a un proveedor externo a la entidad? (en caso afirmativo detallar cuales) ? SI

Justifique su respuesta

¿Se realizan cesiones de datos a otras entidades, ya sean del mismo grupo o proveedores externos al mismo? (en caso afirmativo detallar cuales) ? SI

(vi) percepción del riesgo por el responsable del tratamiento y por el delegado de protección de datos (DPO) y;

1 2 3 4 5 6 7 **Percepción del riesgo por el responsable del tratamiento y DPO** 8

¿Es este tratamiento es similar a otro para el que haya sido necesario realizar una EIPD ? ? SI

Justifique su respuesta

¿Se considera, con independencia de las preguntas indicadas en este formulario, que es recomendable

(vii) base jurídica del tratamiento.

¿Tiene el tratamiento su base jurídica en el derecho de la Unión Europea o de un Estado miembro y la EIPD ya se ha realizado en este contexto?



SI

Justifique su respuesta

Las preguntas anteriores sirven para determinar el riesgo que entraña el tratamiento de los datos y si se precisa hacer una evaluación de impacto.

Una vez se responden las preguntas anteriores, se inicia una nueva fase que consta de las siguientes secciones:

- Ciclo de vida de los datos
- Análisis de la necesidad y proporcionalidad del tratamiento
- Identificación de los riesgos
- Gestión de los riesgos

Las mismas son comunes al proceso de gestión de los riesgos por lo que las desarrollaremos una única vez, para el proceso de gestión de los riesgos.

Tras haber incluido la información que precisaban los campos anteriores, la herramienta genera un resultado que puede ser “ACEPTABLE” o “NO ACEPTABLE”. Asimismo, te da la opción de generar un informe de riesgos para continuar con la EIPD o un informe para seguir identificando los riesgos y salvaguardas del tratamiento.

Resultados EIPD

Existen las siguientes opciones:

- Mitigar o volver a revisar los riesgos residuales en caso de no obtener un resultado "aceptable"
- Generar el informe de riesgos para continuar con la evaluación de impacto del tratamiento
- Generar el informe final para continuar identificando riesgos y salvaguardas del tratamiento
- Terminar para salir de la aplicación y eliminar la información almacenada en su ordenador

Resultado: ACEPTABLE

Generar informe de riesgos ?

Generar informe final ?

Terminar

OPCIÓN GESTIÓN DEL RIESGO:

Si seleccionas la opción de gestión de riesgos, la herramienta inicia un cuestionario con preguntas. En primer lugar, la herramienta recoge información sobre el ciclo de vida de los datos. En concreto, información sobre (i) el proceso de captura de los datos; (ii) la clasificación y almacenamiento de los datos; (iii) el uso y tratamiento de los datos; (iv) la cesión o transferencia de los datos a un tercero para su tratamiento; y (v) la destrucción de los datos. **[A modo ejemplificativo se muestra a continuación capturas de pantalla de esta primera fase de ciclo de los datos.]**

Ciclo de vida de los datos

1 Captura de datos 2 3 4 5

Actividades de los procesos de captura de datos ?

Justifique su respuesta

Categorías de datos adquiridos ?

Justifique su respuesta

Intervinientes en la captura de los datos ?

Justifique su respuesta

Tecnologías aplicadas ?

Justifique su respuesta

Actividades de almacenamiento y clasificación ?

Justifique su respuesta

Categorías de datos almacenados o clasificados ?

Justifique su respuesta

Para cada de estas categorías se deben rellenar cuatro campos: actividades; categorías de datos; intervinientes y tecnologías aplicadas.

Una vez completada esta primera fase, la herramienta procede a identificar los riesgos y amenazas. Seleccionadas las amenazas, la herramienta mostrará las amenazas seleccionadas con las posibles medidas de control asociadas a cada una de ellas. La empresa debe seleccionar aquellas medidas que sean necesarias para mitigar el riesgo de la amenaza. Además, deberá seleccionar la probabilidad y el impacto de que ocurra dicha amenaza.

Después de seleccionar las medidas de control, se debe evaluar la probabilidad y el impacto calculando nuevamente el riesgo residual. Este proceso es necesario realizarlo para cada una de las amenazas seleccionadas.

Identificación de riesgos

1 Amenazas/Riesgos 2

- | | |
|--|---|
| 1. No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender | <input type="radio"/> NO <input type="radio"/> SI |
| 2. Carecer de una base jurídica sobre la que se sustenten los tratamientos realizados sobre los datos | <input type="radio"/> NO <input type="radio"/> SI |
| 3. Tratar datos inadecuados y excesivos para la finalidad del tratamiento | <input type="radio"/> NO <input type="radio"/> SI |
| 4. Tratar datos personales con una finalidad distinta para la cual fueron recabados | <input type="radio"/> NO <input type="radio"/> SI |
| 5. Almacenar los datos por periodos superiores a los necesarios para la finalidad del tratamiento y a la legislación vigente | <input type="radio"/> NO <input type="radio"/> SI |
| 6. No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la privacidad en la organización | <input type="radio"/> NO <input type="radio"/> SI |
| 7. Realizar transferencias internacionales a países que no ofrezcan un nivel de protección adecuado | <input type="radio"/> NO <input type="radio"/> SI |
| 8. No tramitar o dificultar el ejercicio de los derechos de los interesados | <input type="radio"/> NO <input type="radio"/> SI |

Gestion de riesgos

No facilitar la información en materia de protección de datos o no redactarla de forma accesible y fácil de entender

Medidas

Identificación de la finalidad del tratamiento
Cláusulas y locuciones para cumplir con el deber de información

Probabilidad: Máxima | Impacto: Máxima | Riesgo residual: Muy Alto

Almacenar los datos por periodos superiores a los necesarios para la finalidad del tratamiento y a la legislación vigente

Medidas

Actividades del tratamiento
Identificación de la finalidad del tratamiento
Definición de los plazos de conservación de los datos
Descripción del ciclo de vida del dato asociado a un tratamiento

Probabilidad: Máxima | Impacto: Máxima | Riesgo residual: Muy Alto

No disponer de una estructura organizativa, procesos y recursos para una adecuada gestión de la privacidad en la organización

Medidas

Política de privacidad
Gobierno de la privacidad

Cuando se hayan rellenado todas las medidas de control, probabilidades e impactos de las amenazas, la herramienta generará un resultado que puede ser “ACEPTABLE” o “NO ACEPTABLE” que, en última instancia, deberá ser validado por el responsable.

Asimismo, la herramienta te da la opción de generar un informe de riesgos con el resultado del análisis o un informe final con el que iniciar la identificación y gestión de los riesgos para los derechos y libertades de los interesados con el objeto de diseñar el plan de acción con las medidas de control. Todo ello en formato Excel o pdf.



HERRAMIENTA 4: EVALÚA- RIESGO RGPD

¿En qué consiste la herramienta?

Es una herramienta para el análisis de necesidad de una Evaluación de Impacto en Protección de Datos.

La misma tiene un triple objetivo: (i) hace una primera evaluación del riesgo intrínseco; (ii) establece la necesidad de realizar una Evaluación de Impacto y (iii) estima el riesgo residual si se utilizan medidas y garantías para mitigar los factores de riesgo específicos.

El enlace para acceder a esta herramienta es el siguiente:

https://www.aepd.es/es/herramienta/EvaluaRiesgo_RGPD.zip

Cuestiones a tener en consideración

- A diferencia de las herramientas anteriores que se pueden usar en línea, esta herramienta precisa de su descarga para poder ser empleada. La misma se descarga en formato Zip, que contiene el Excel donde se lleva a cabo el proceso.
- Los factores de riesgo desplegados en esta herramienta NO tienen carácter exhaustivo. Esto quiere decir que cada empresa como responsable del tratamiento deberá identificar los aspectos específicos que le afectan en su actividad particular, en el procesamiento de datos personales que requiera el despliegue de su negocio y, previo asesoramiento, incluirlo en su evaluación.
- Esta herramienta se complementa con la GUÍA DE GESTIÓN DEL RIESGO Y EVALUACIÓN DE IMPACTO EN TRATAMIENTOS DE DATOS PERSONALES que unifica los criterios e interpretaciones de las autoridades en materia de protección de datos.

El enlace de acceso a esta guía es el siguiente:

<https://www.aepd.es/es/documento/gestion-riesgo-y-evaluacion-impacto-en-tratamientos-datos-personales.pdf>

Esta guía permite un conocimiento más profundo de la gestión de los riesgos y es aplicable a cualquier tratamiento con

independencia del nivel de riesgo. La misma se estructura en tres apartados: el primero contiene una descripción de los fundamentos de la gestión de riesgos para los derechos y libertades; el segundo incluye un desarrollo metodológico básico para la aplicación de la gestión del riesgo, y el último está enfocado en los casos en los sea preciso realizar una EIPD, con las orientaciones necesarias para llevarla a cabo.

A continuación, se adjunta una pequeña tabla con algunos de los puntos clave de esta guía.

- Se especifica que la gestión del riesgo no puede, en ningún caso, sustituirse por el cumplimiento normativo, o por una póliza de seguros que cubra la responsabilidad de la organización en caso de que haya una infracción de la normativa de protección de datos, sino que, ante cualquier tratamiento, la organización tiene adoptar medidas técnicas y organizativas que protejan los derechos y libertades de las personas.

- Se destaca la importancia que tiene la gestión de la seguridad de la información. En concreto se indica que la implementación en la organización de modelos de gestión, como el Sistema de Gestión de la Seguridad de la Información (SGSI) y de directrices como las normas ISO 27000 o el Esquema Nacional de Seguridad, además de políticas de información de la entidad y las políticas de seguridad, son medios para poder gestionar los riesgos de forma efectiva y eficaz. No obstante, la implementación de estos modelos no es suficiente, sino que las medidas de seguridad que se implementen en la organización tienen que revisarse continuamente dado que la actividad de tratamiento, y por ende el riesgo, puede evolucionar por diversos factores.

- Se incluye el concepto de “Gobernanza de los riesgos para los derechos y libertades” relacionado con el cumplimiento del principio de responsabilidad proactiva, y que indica que en la organización se deben implementar políticas de protección de datos efectivas, prácticas y ejecutivas, no limitadas a una mera declaración de voluntad de compromiso.

- Se introducen se introducen dos nuevos conceptos para el cálculo del nivel del riesgo cuando hay dos o más factores de riesgo que apunten a un determinado nivel de impacto, y cuando haya dos o más indicios que apunten a un determinado nivel de probabilidad: el coeficiente de impacto acumulado y el coeficiente de probabilidad acumulado.
- Se desarrolla la exigencia relativa a la evaluación de la necesidad y proporcionalidad del tratamiento, haciendo una ponderación del juicio de proporcionalidad, del juicio de necesidad y del juicio de proporcionalidad en sentido estricto.

Instrucciones para su uso

En primer lugar, la empresa debe descargarse la herramienta en formato ZIP y abrir el Excel que se contiene en la misma, pues como hemos dicho anteriormente, esta herramienta no puede ser utilizada en línea como las demás.

Una vez descargada, la herramienta despliega un cuestionario o auto test que la empresa debe ir completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto.

En concreto, a través de once pestañas diferentes, EVALÚA – RIESGO RGPD muestra aquellos factores de riesgo que pueden afectar al tratamiento de los datos personales. La empresa, haciendo un recorrido secuencial a través de las once pestañas deberá determinar la aplicabilidad de cada factor de riesgo. Seleccionando el cuadro de aplicabilidad de cada factor de riesgo se desplegarán en muchos casos ejemplos, además de permitir seleccionar “APLICA” o “NO APLICA”.

Asimismo, a lado de la categoría de factor de riesgo, se añade una segunda columna que indica “MITIGACIÓN” de forma que en función de las medidas y garantías con las que cuente la empresa para mitigar dichos factores de riesgo se indique una de las cuatro categorías siguientes: (1) no mitigado; (2) limitadamente mitigado; (3) significativamente mitigado; (4) mitigado.

Las once pestañas que contiene el Excel son las siguientes:

- (i) finalidades del tratamiento (si se lleva a cabo un perfilado, un rastreo de contactos, decisiones automatizadas, localización, etc.);
- (ii) tipos de datos utilizados (datos biométricos, datos genéticos, metadatos, datos sanitarios, datos relativos a condenas, etc.);
- (iii) extensión y alcance del tratamiento (es un tratamiento exhaustivo, el volumen de datos es elevado, es un tratamiento a gran escala, etc.);
- (iv) categorías de interesados que se tratan (discapacitados, colectivos vulnerables, menores de 14 años, personas con enfermedades mentales, etc.);
- (v) factores técnicos empleados en el tratamiento (servicios web, aplicaciones móviles, video vigilancia, reconocimiento facial, etc.);

- (vi) recogida y generación de los datos tratados (acceso a bases de datos sobre fraude, datos personales obtenidos en zonas de acceso público, combinación de conjuntos de datos, etc.);
- (vii) efectos colaterales del tratamiento de los datos (podría determinar la situación financiera, puede provocar o genera discriminación, posible daño reputacional, etc.);
- (viii) el sector donde opera el responsable o encargado (empresa de biotecnología, entidad financiera, hospitales, etc.);
- (ix) comunicaciones de los datos (difusión indiscriminada de identificadores únicos, transferencia a países sin un nivel adecuado de protección, etc.);
- (x) otros factores (este campo es para que rellene la empresa con aquellos otros factores de riesgo que considere que apliquen y que no se encuadren en las categorías anteriores);
- (xi) seguridad en el tratamiento de los datos (pérdida de trazabilidad, fallos en medidas y garantías técnicas de protección, pérdida de integridad, etc.)

[Dejamos debajo capturas de pantalla mostrando algunas de las diferentes once pestañas sobre factores de riesgo.]

Reiniciar

Atras

Siguiente

| OPERACIONES RELACIONADAS CON LOS FINES DE TRATAMIENTO | | |
|---|---------------|------------|
| SIN DEFINIR | Aplicabilidad | Mitigación |
| Perfilado | | |
| Evaluación de sujetos | | |
| Predicción | | |
| Control del empleado | | |
| Control de acceso a internet | | |
| Observación | | |

| TIPOS DE DATOS UTILIZADOS | | |
|---|---------------|------------|
| SIN DEFINIR | Aplicabilidad | Mitigación |
| Documentos personales | | |
| Información de aplicaciones de registro de actividades vitales | | |
| Aspectos personales | | |
| Preferencias de consumo, gustos, hábitos (no categorías especiales) | | |
| Rendimiento laboral | | |

| EXTENSIÓN Y ALCANCE DEL TRATAMIENTO | | |
|--|---------------|------------|
| SIN DEFINIR | Aplicabilidad | Mitigación |
| Sistemático | | |
| Exhaustivo sobre las personas | | |
| Involucra gran número de sujetos | | |
| El volumen de datos tratado es muy elevado | | |
| Diversidad del tratamiento elevada | | |

Las categorías anteriormente enunciadas contienen aquellas categorías de datos, alcances de tratamiento, finalidades del tratamiento, etc. que implican un elevado nivel de riesgo, de forma que, si aplican, normalmente la empresa llevará a cabo un tratamiento de los datos de alto riesgo.

Una vez se hayan completado todos los campos con los factores de riesgo y el nivel de protección que tiene la empresa para mitigar esos factores, la herramienta te ofrece un resultado donde se indica

el nivel de riesgo intrínseco y se valora la necesidad de que la empresa realice una evaluación de impacto.

- Si el riesgo intrínseco es alto, significa que, en principio, deberá llevarse a cabo una evaluación de impacto.
- Si el riesgo residual es alto, significa que, en principio, deberá efectuarse una consulta previa ante la autoridad de control.

No obstante, la decisión final debe ser valorada por el responsable del tratamiento, que es quien tiene conocimiento pleno del caso.

En concreto, en la pestaña de resultados la herramienta te indica la valoración del riesgo intrínseco y del riesgo residual, señalando si el riesgo es alto o bajo. Asimismo, la empresa tiene la opción de generar un informe con los resultados, así como de obtener una lista de fuentes de riesgo por categorías.

En segundo lugar, a lo largo del transcurso de nuestra segunda sesión [23 de junio] abordaremos las herramientas de la AEPD destinadas a la identificación de aquellas brechas de seguridad que, por su carácter, requieran ser comunicadas a las personas físicas aceptadas; así como el canal de consultas de la AEPD destinado a los delegados de protección de datos, que actúan como intermediarios entre las empresas y las autoridades de control en materia de protección de datos.

HERRAMIENTA BRECHA DE SEGURIDAD

Antes de proceder a explicar el funcionamiento de la herramienta de comunicación de la brecha de seguridad, debemos hacer un breve recordatorio de los artículos 33 y 34 del RGPD que desarrollan las obligaciones del responsable del tratamiento de los datos de comunicar a la autoridad de control competente y a las personas físicas afectadas, aquellas brechas de seguridad que constituyan un riesgo alto para los derechos y las libertades de las personas físicas.

Una brecha de datos personales es un incidente de seguridad que ocasiona la destrucción, pérdida o alteración accidental o ilícita de los datos personales tratados por un responsable, o bien la comunicación o acceso no autorizados a los mismos.

Una brecha de datos personales puede tener efectos adversos sobre las personas físicas titulares de los datos afectados, susceptibles de ocasionar daños y perjuicios físicos, materiales o inmateriales; por lo que hay que intentar evitarlas y en caso de que sucedan gestionarlas adecuadamente, especialmente cuando puedan poner en riesgo los derechos y libertades de las personas físicas.

El artículo 33 del RGPD impone a los responsables de un tratamiento de datos personales la obligación de notificar a la autoridad de control competente las brechas de datos personales cuando sea probable que constituyan un riesgo para los derechos y libertades de las personas. El responsable de tratamiento debe

valorar el nivel de riesgo de una brecha de datos personales y notificarla a la autoridad de control cuando exista tal riesgo, y además cuando el riesgo sea alto el responsable también deberá comunicar la brecha a las personas afectadas conforme al artículo 34 del RGPD.

Esta comunicación con carácter general, deberá contener los siguientes requisitos:

- a) describir la naturaleza de la violación de la seguridad de los datos personales, inclusive, cuando sea posible, las categorías y el número aproximado de interesados afectados, y las categorías y el número aproximado de registros de datos personales afectados;
- b) comunicar el nombre y los datos de contacto del delegado de protección de datos o de otro punto de contacto en el que pueda obtenerse más información;
- c) describir las posibles consecuencias de la violación de la seguridad de los datos personales;
- d) describir las medidas adoptadas o propuestas por el responsable del tratamiento para poner remedio a la violación de la seguridad de los datos personales, incluyendo, si procede, las medidas adoptadas para mitigar los posibles efectos negativos.

Para ayudar en la toma de esta decisión la AEPD pone a disposición de las empresas la herramienta COMUNICA BRECHA, la cual ayuda a determinar si se debe notificar a las personas físicas por la brecha de seguridad.

HERRAMIENTA: COMUNICA BRECHA

¿En qué consiste la herramienta?

Es una herramienta que permite a la empresa valorar la obligación de informar a las personas físicas afectadas por una brecha de seguridad de los datos personales (artículo 34 RGPD), pues una brecha de seguridad que ponga en riesgo la integridad de los datos puede suponer una imposición de sanciones económicas por la AEPD.

Sirve de ayuda principalmente a las PYMES y autónomos para saber cómo actuar en caso de sufrir una brecha de seguridad.

La herramienta tiene un formato de auto test y está destinada al responsable de protección de datos para que sepa si tiene que notificar o no la brecha en función de la importancia, el tipo de datos afectados y la gravedad del incidente.

Una vez recopilada la información, la herramienta emite un informe, incluyendo las posibles acciones a realizar. Asimismo, la herramienta emitirá una de las tres respuestas:

- Es necesario informar de la brecha de seguridad a las personas afectadas.
- No es necesario informar de la brecha de seguridad, pues se considera que la información expuesta no afecta de forma relevante a las personas físicas.
- La información suministrada no es suficiente para determinar el riesgo.

El enlace para acceder a esta herramienta es el siguiente:

<https://servicios.aepd.es/AEPD/view/form/MDAwMDAwMDAwMDAwMDQwMjY4MzExNjUxOTI3ODQ1NDg3?updated=true>

Cuestiones a tener en consideración

- La mera obtención de los documentos NO SUPONE el cumplimiento automático de las obligaciones del RGPD y la LOPDGDD para los responsables y encargados de tratamiento, únicamente proporciona orientación y facilita la comprensión de dichas obligaciones.
- Los datos subidos o aportados a esta herramienta SE ELIMINAN tras finalizar su uso, por lo que la AEPD no conocerá la información aportada.
- Esta herramienta ayuda a la toma de decisiones, pero es responsabilidad última del responsable del tratamiento ver si corresponde notificar la brecha de seguridad.

Instrucciones para su uso

Accediendo al enlace que se ha aportado anteriormente, la herramienta COMUNICA BRECHA despliega un cuestionario o auto test que la empresa debe ir completando, marcando las respectivas casillas que resulten de aplicación a su caso concreto.

En primer lugar, la herramienta te pedirá que selecciones el sector de actividad al que se dedica la empresa de entre 10 opciones (e.g. telecomunicaciones, solvencia patrimonial, publicidad, entidades bancarias, etc.) y 1 categoría adicional para el caso de que la empresa identifique con ninguna de las categorías anteriores.

Sobre el responsable

Indique el sector de actividad del responsable de tratamiento: *

Servicios de telecomunicaciones

En segundo lugar, la empresa deberá facilitar los detalles sobre el incidente o la brecha de seguridad, facilitando información cómo, por ejemplo, si el incidente ha sido accidental o intencionado; cuál ha sido el origen del incidente; si ha sido o no un ciberincidente.

Sobre la brecha de seguridad de los datos personales

El incidente ha sido: *

- Accidental o sin intencionalidad
- Intencionado
- Desconocido

El origen del incidente ha sido: *

- Interno: Personal o sistemas del responsable de tratamiento
- Interno: Personal o sistemas del encargado de tratamiento
- Externo: Otros, ajenos al responsable y encargado de tratamiento

¿La brecha de seguridad es consecuencia de un ciberincidente?: *

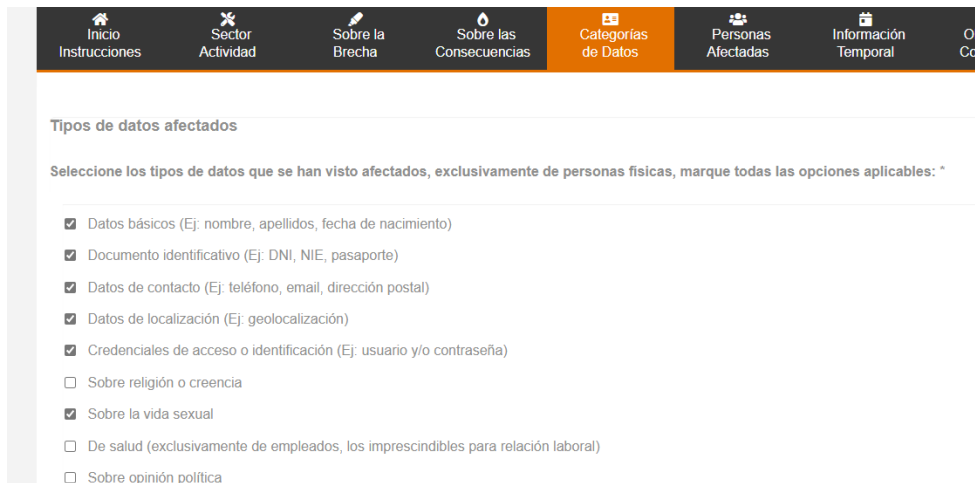
- Si
- No

Posteriormente, la empresa debe facilitar las consecuencias de dicho incidente y en qué grado podrían afectar las consecuencias identificadas a las personas físicas afectadas, indicando el nivel de gravedad que en su opinión merezca el incidente.

| Inicio Instrucciones | Sector Actividad | Sobre la Brecha | Sobre las Consecuencias | Categorías de Datos | Personas Afectadas | Información Temporal | Obligación Comunicar |
|---|------------------|-----------------|-------------------------|---------------------|--------------------|----------------------|----------------------|
| Sobre las consecuencias | | | | | | | |
| Como consecuencia del incidente: * | | | | | | | |
| <input type="checkbox"/> Personas u organizaciones que no están autorizadas, o no tienen un propósito legítimo para acceder a los datos, han podido acceder y/o extraerlos. | | | | | | | |
| <input checked="" type="checkbox"/> Se han destruido, perdido o cifrado datos personales, de forma que no pueden ser tratados. | | | | | | | |
| <input type="checkbox"/> Se han alterado los datos personales y el tratamiento con datos alterados/inexactos puede suponer un daño para los afectados. | | | | | | | |
| Referido específicamente a los datos afectados. ¿Se ha recuperado la disponibilidad de los datos personales de forma que pueden ser tratados con normalidad? * | | | | | | | |
| <input checked="" type="radio"/> No | | | | | | | |
| <input type="radio"/> Si | | | | | | | |
| <input type="radio"/> Todavía no, pero se recuperará en breve | | | | | | | |

A continuación, la empresa deberá introducir los tipos de datos que se han visto afectados y las personas afectadas, con especial


referencia a si hay colectivos vulnerables como menores de edad, o si se trata de un número amplio de personas afectadas.



The screenshot shows a navigation menu at the top with the following items: Inicio (Instrucciones), Sector (Actividad), Sobre la Brecha, Sobre las Consecuencias, Categorias de Datos (highlighted in orange), Personas Afectadas, Información Temporal, and Ob (Con). Below the menu is a section titled "Tipos de datos afectados" with the instruction: "Seleccione los tipos de datos que se han visto afectados, exclusivamente de personas físicas, marque todas las opciones aplicables: *". The form contains the following options:

- Datos básicos (Ej: nombre, apellidos, fecha de nacimiento)
- Documento identificativo (Ej: DNI, NIE, pasaporte)
- Datos de contacto (Ej: teléfono, email, dirección postal)
- Datos de localización (Ej: geolocalización)
- Credenciales de acceso o identificación (Ej: usuario y/o contraseña)
- Sobre religión o creencia
- Sobre la vida sexual
- De salud (exclusivamente de empleados, los imprescindibles para relación laboral)
- Sobre opinión política

Asimismo, la empresa deberá facilitar información temporal sobre la brecha, señalando la fecha en que se detectó el incidente con certeza y la fecha en que se inició la brecha de seguridad.



The screenshot shows a section titled "Información temporal de la brecha" with the instruction: "Indique la fecha de detección de la brecha, entendida como la fecha en la que el responsable tiene la certeza de que se han visto personales: *". Below this is a date input field containing "02/05/2022". Below the date field is the question: "¿Conoce la fecha en la que se inició la brecha?: *". Below this question is a radio button option: La fecha exacta.

Toda la información anterior sirve para determinar el nivel de riesgo de la brecha, pues sólo un nivel alto de riesgo para los derechos y libertades de las personas físicas afectadas implica la necesidad de notificarles la brecha de seguridad.

En último lugar, la herramienta proporciona un resultado, señalando si de acuerdo a los datos facilitados procede o no comunicar la brecha de seguridad a las personas físicas afectadas.

Resultado

Según los datos facilitados,

DEBERÍA COMUNICAR LA BRECHA DE SEGURIDAD A LOS AFECTADOS

conforme al art. 34 del RGPD al apreciarse que puede existir un riesgo alto o muy alto para los derechos y libertades de los sujetos afectados por la brecha de seguridad.

Si la comunicación a los afectados supone un esfuerzo desproporcionado, podrá optar por una comunicación pública o medida semejante por la que se informe de manera igualmente efectiva a los interesados, en virtud del artículo 34.2c del RGPD.

HERRAMIENTA CANAL DE CONSULTAS DELEGADO DE PROTECCIÓN DE DATOS

Antes de proceder a explicar el funcionamiento del canal de consultas del delegado de protección de datos, debemos hacer un breve recordatorio de los artículos 37 y 39 del RGPD que desarrollan la figura del delegado de protección de datos, cuándo debe ser designado el mismo y las funciones que se le atribuyen.

Para cumplir con la normativa de protección de datos y disponer de un intermediario entre las empresas que tratan los datos personales de las personas físicas y las autoridades de control en materia de protección de datos, el RGPD establece en su artículo 37 la designación de un delegado de protección de datos (DPD o DPO).

Este nombramiento resulta obligatorio en ciertas ocasiones (el tratamiento de datos es por un organismo público, hay un tratamiento a gran escala de categorías especiales de datos, etc.) que vienen recogidos en los artículos 37 del RGPD y 34 de la

LOPDGDD, y que coinciden con aquellas que suelen entrañar un riesgo para los derechos y libertades de los titulares de los datos.

Estos DPD deben ser comunicados a través de la sede electrónica a la AEPD.

Asimismo, y para el cumplimiento de sus funciones establecidas en el artículo 39 del RGPD (e.g. informar de sus obligaciones al responsable y encargado de tratamiento, cooperar con la autoridad de control, actuar como punto de contacto con la autoridad de control, etc.), la AEPD pone a disposición de los DPD de las empresas, el CANAL DE DPO para que los mismos puedan formular aquellas consultas que sean necesarias a la autoridad de control de los datos.

HERRAMIENTA: CANAL DEL DPD

¿En qué consiste la herramienta?

Esta herramienta tiene como finalidad atender las consultas planteadas ante la AEPD por las personas DPD, tanto del sector público como del privado, al desempeñar las funciones encomendadas en el artículo 39 del RGPD.

Podrán plantear las consultas utilizando este canal:

1. Los DPD designados por las personas responsables y encargadas del tratamiento que hayan sido comunicados a la

AEPD. La inclusión en la relación de DPD será suficiente para acreditar la designación.

2. Las organizaciones y asociaciones representativas de personas responsables y encargadas del tratamiento que ofrezcan a sus miembros los servicios de DPD.

Asimismo, existen una serie de requisitos que deben cumplirse para poder utilizar el CANAL DEL DPD:

- Identificarse como DPD, bien con un certificado electrónico, un certificado Clave PIN o una clave permanente. Las consultas anónimas no están permitidas en este canal.
- Facilitar toda aquella información que resulte necesaria sobre la cuestión o consulta que se plantea a la AEPD.
- El análisis que haya desarrollado previamente en el ejercicio de sus funciones como DPD.

El enlace para acceder a esta herramienta es el siguiente:

<https://www.aepd.es/es/guias-y-herramientas/herramientas/canalDPD>

Cuestiones a tener en consideración

Este canal no podrá ser empleado para:

1. Cuestiones planteadas desde un punto de vista hipotético.

2. Cuestiones que pudiesen estar relacionadas con procedimientos que esté tramitando la AEPD, incluidas las relativas al estado de tramitación.
3. Cuestiones que pretendan la validación de documentos elaborados por responsables y encargados en materia de protección de datos, cuya responsabilidad recae sobre ellos en virtud del principio de responsabilidad proactiva.
4. Solicitudes de acceso a la información pública.
5. Consultas que se hayan presentado por el Canal de la Ciudadanía.
6. Consultas que se refieran a cuestiones que se encuentran ya explicadas y son accesibles en los materiales publicados en la página web de la AEPD, tales como las Guías, Preguntas Frecuentes y Herramientas elaboradas para facilitar el cumplimiento del RGPD.

Instrucciones para su uso

Accediendo al enlace que se ha aportado anteriormente, la empresa accederá a la herramienta. Una vez en ella, deberá seleccionar “SEDE ELECTRÓNICA” > CANAL DEL DPD y se le solicitará un certificado clave pin, un certificado electrónico o una clave permanente a través de la cual el DPD podrá acceder.

REMINDER: este canal solo puede ser utilizado por DPD previamente comunicados y registrados en la AEPD.

Una vez se haya accedido se podrá formular la consulta, la cual será respondida por la AEPD atendiendo a cuestiones de eficiencia y optimización de recursos, lo que puede repercutir en el tiempo de respuesta o la forma en que se responda.

Asimismo, y debido a ello, se recomienda consultar antes las PREGUNTAS FRECUENTES que ya contienen muchas de las respuestas a las preguntas más habituales que se suelen formular en materia de protección de datos: <https://www.aepd.es/es/preguntas-frecuentes>. Estas preguntas frecuentes además se encuentran categorizadas por temas: video vigilancia, publicidad no deseada, tus derechos, etc.