Análisis de la necesidad de la realización de una PIA

¿Qué es una evaluación de impacto?

La EIPD es una herramienta con carácter preventivo que debe realizar el responsable del tratamiento para poder identi car, evaluar y gestionar los riesgos a los que están expuestas sus actividades de tratamiento con el objetivo de garantizar los derechos y libertades de las personas físicas. En la práctica, la EIPD permite determinar el nivel de riesgo que entraña un tratamiento, con el objetivo de establecer las medidas de control más adecuadas para reducir el mismo hasta un nivel considerado aceptable.

¿Cuándo debe realizarse la evaluación de impacto?

Artículo 35 ***del RGPD***

Establece que ante la probabilidad de que un tratamiento *"entrañe un alto riesgo para los derechos y libertades de las personas físicas"* será necesario llevar a cabo una EIPD antes de la puesta en marcha del tratamiento. Esta obligación está alineada con el principio de privacidad que tiene como objetivo analizar un tratamiento desde su fase de diseño y garantizar una adecuada gestión de los riesgos, además de cumplir con los principios de necesidad y proporcionalidad.

¿Cuándo debe realizarse la evaluación de impacto?

Cuando sea probable que un tipo de tratamiento, en particular si utiliza nuevas tecnologías, por su naturaleza, alcance, contexto o fines, entrañe un alto riesgo para los derechos y libertades de las personas físicas, el responsable del tratamiento realizará, antes del tratamiento, una evaluación del impacto de las operaciones de tratamiento en la protección de datos personales. Una única evaluación podrá abordar una serie de operaciones de tratamiento similares que entrañen altos riesgos similares.

Listas de tratamientos que requieren PIA

Art. 35 RGPD

4. La autoridad de control establecerá y **publicará una lista de los tipos de operaciones de tratamiento que requieran una evaluación de impacto** relativa a la protección de datos de conformidad con el apartado 1. La autoridad de control comunicará esas listas al Comité a que se refiere el artículo 68.

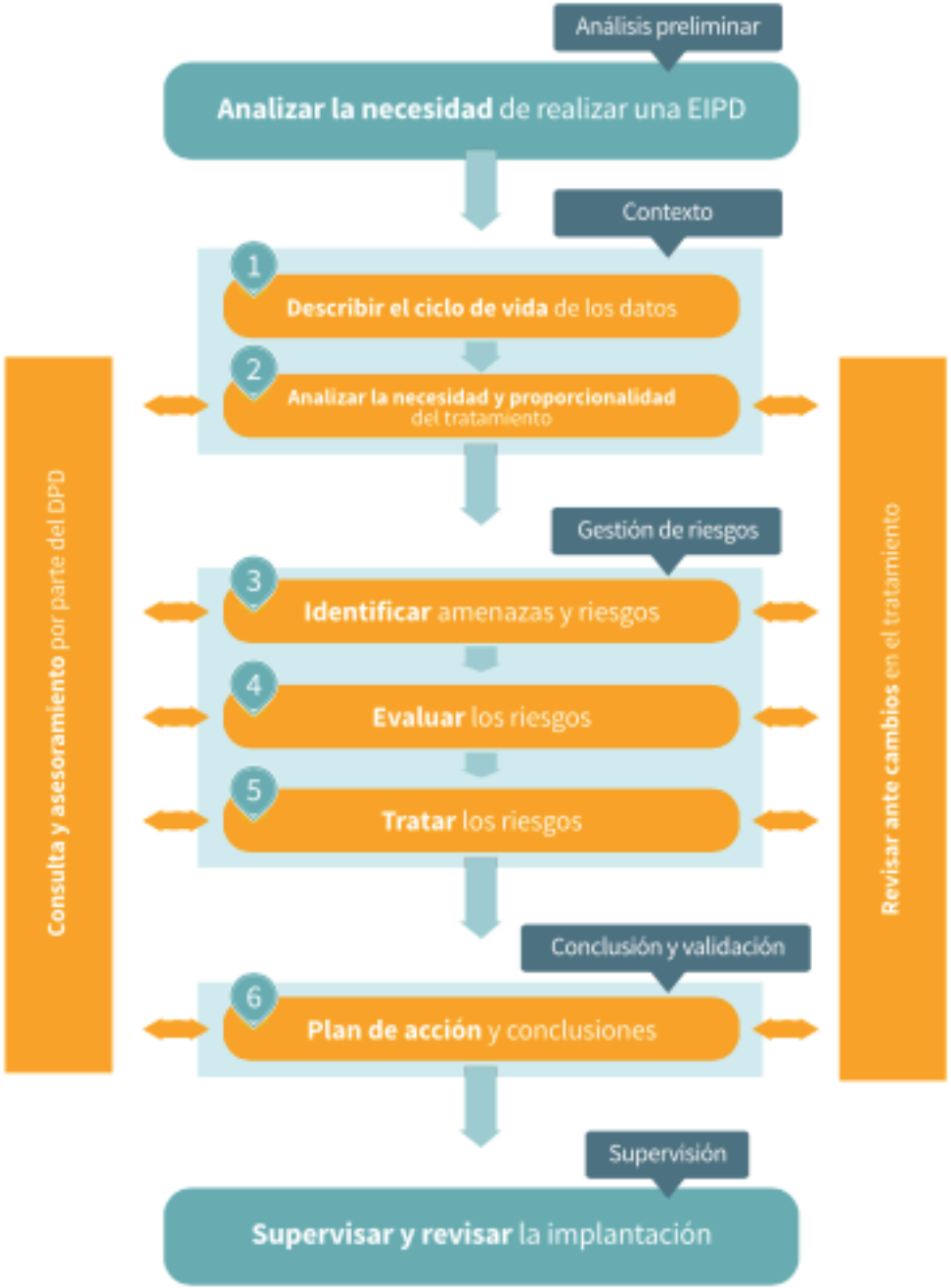
5. La autoridad de control podrá asimismo establecer y publicar la lista de los tipos de tratamiento que **no requiere**n evaluaciones de impacto relativas a la protección de datos. La autoridad de control comunicará esas listas al Comité.

6. Antes de adoptar las listas a que se refieren los apartados 4 y 5, la autoridad de control competente aplicará el mecanismo de coherencia contemplado en el artículo 63 si esas listas incluyen actividades de tratamiento que guarden relación con la oferta de bienes o servicios a interesados o con la observación del comportamiento de estos en varios Estados miembros, o actividades de tratamiento que puedan afectar sustancialmente a la libre circulación de datos personales en la Unión.

Tipos de tratamientos que se realizan en un laboratorio

- Tratamientos de datos sensibles
- Información biométrica
- Bio bancos
- Utilización de nuevas tecnologías
- Información genética
- Datos de menores de edad
- Estudios Clínicos
- Investigación médica
- Embarazadas
- Programas de adherencia pacientes
- Pruebas médicas
- Reacciones Adversas

Workflow


Análisis preliminar
Analizar la necesidad de realizar una EIPD
Contexto
1
Describir el ciclo de vida de los datos
2
Analizar la necesidad y proporcionalidad del tratamiento
Gestión de riesgos
3
Identificar amenazas y riesgos
4
Evaluar los riesgos
5
Tratar los riesgos
Conclusión y validación
6
Plan de acción y conclusiones
Supervisión
Supervisar y revisar la implantación
Consulta y asesoramiento por parte del DPD
Revisar ante cambios en el tratamiento

FASE	Responsable del tratamiento	DPD	Encargado del tratamiento	Otras áreas relevantes (pe seguridad, riesgos, Asesoría Jurídica, ...)
1 Describir el ciclo de vida de los datos	R/A	C/I	C	C
2 Analizar la necesidad y proporcionalidad del tratamiento	R/A	C/I	C	C
3 Identificar amenazas y riesgos	R/A	C/I	C	-
4 Evaluar los riesgos	R/A	C/I	C	-
5 Tratar los riesgos	R/A	C/I	C	C
6 Plan de acción y conclusiones	R/A	C/I	C	C

Tipo de amenaza	Amenaza	¿Qué preguntas se pueden formular para identificar la amenaza?
 Acceso ilegítimo a los datos	▪ Perdidas de dispositivos móviles ▪ Fuga de información ▪ Acceso intencionado por parte de personal no autorizado ▪ Ataques intencionados (hacking, suplantación de identidad, etc.) ▪ Uso ilegítimo de datos personales	- ¿Los **dispositivos móviles y de almacenamiento** están cifrados? - ¿Existen **métodos para extraer la información** durante la operación de tratamiento? - ¿Está expuesta la información al **acceso por parte de terceros** no autorizados? ¿**Existe un mecanismo** para dar acceso a los datos únicamente al personal autorizado? - ¿La operación de tratamiento es susceptible de **ataques de hacking?** ¿es susceptible de **ataques de phishing** o de otros métodos de suplantación de identidad? - ¿Existe una adecuada gestión de la configuración de los **parámetros de seguridad** de los elementos (elementos de red, SO y BBDD) - ¿Existe una **base legitimadora** para la actividad de tratamiento? ¿las **finalidades de las actividades** de tratamiento son necesarias y proporcionales?
 Modificación no autorizada de los datos	▪ Ataque para la suplantación de identidad ▪ Errores en los procesos de recopilación y captura de información ▪ Modificación no autorizada de datos intencionada ▪ Uso ilegítimo de datos personales	- ¿Existen **credenciales o mecanismos de control** que limiten el acceso a personal no autorizado? ¿Se **revisa periódicamente la actividad** realizada por los usuarios cuando acceden a los sistemas? - **¿Existen** controles sobre la integridad de la información durante el proceso de captura de datos? ¿se **identifica adecuadamente al interesado** que proporciona los datos? - ¿Los **datos son modificables** únicamente por el personal autorizado? - ¿La actividad de tratamiento sobre los datos son acordes a las finalidades para las cuales existe una **base legitimadora?** ¿se puede realizar un perfilado o una operación de tratamiento que no esté alineada con las finalidades de la operación de tratamiento?
 Eliminación de los datos	▪ Corte de suministro eléctrico o fallos en servicios de comunicaciones ▪ Error humano o ataque intencionado que provoca borrado o pérdida de datos ▪ Desastres naturales	- ¿Un **fallo de suministro eléctrico** puede implicar la pérdida de datos? ¿Un fallo en los servicios de comunicaciones puede ocasionar una pérdida de datos? - ¿Los datos pueden ser **eliminados únicamente por el personal autorizado**? ¿Existen **copias de seguridad?** - ¿Están los sistemas que **almacenan datos en ubicaciones expuestas** a la posibilidad de que se produzca un desastre natural? ¿Existe **réplica de los datos** en diferentes ubicaciones?

Riesgos y amenazas

Catálogo de amenazas y posibles soluciones (Continuación)

Categorías Especiales de Datos	
Amenazas	**Soluciones**
Fallos o errores sistemáticos u ocasionales para recabar el consentimiento expreso cuando éste sea la causa que legitima su tratamiento o cesión.	■ Evitar el uso de datos especialmente protegidos salvo que resulte absolutamente necesario.
	■ Establecer procedimientos que garanticen la obtención del consentimiento expreso (y por escrito cuando sea necesario) y que permitan probar que se cuenta con él.
Asunción errónea de la existencia de una habilitación legal para el tratamiento o cesión de datos de categorías especiales.	■ Nombrar un Delegado de Protección de Datos o Data ProtectionOfficer (DPO) para contar con asesoramiento cualificado.
Disociación deficiente o reversible que permita la re-identificación de datos de categorías especiales en procesos de investigación que solo prevén utilizar datos anónimos.	■ Utilizar técnicas de disociación que garanticen el anonimato real de la información o, al menos, que el riesgo residual de re-identificación es mínimo.

Riesgos y amenazas

Deber de secreto	
Amenazas	**Soluciones**
Accesos no autorizados a datos personales.	■ Establecer mecanismos y procedimientos de concienciación sobre la obligación de guardar secreto sobre los datos personales que se conozcan en el ejercicio de las funciones profesionales.
	■ Establecer sanciones disciplinarias para quienes incumplan el deber de secreto y las políticas de confidencialidad de la organización.
	■ Establecer procedimientos que garanticen que se notifica formalmente a los trabajadores que acceden a datos personales de la obligación de guardar secreto sobre aquellos que conozcan en el ejercicio de sus funciones y de las consecuencias de su incumplimiento.
	■ Notificar que se dará traslado a las autoridades competentes de las violaciones de confidencialidad que puedan entrañar responsabilidades penales.
	■ Establecer procedimientos para garantizar la destrucción de soportes desechados que contengan datos personales.

¿Qué roles deben involucrarse en la realización?

RACI

- **Respo**
- **Accountable (A):** Responsable de que la tarea se realice, sin necesidad de ser el que la ejecute y responsable de rendir cuentas sobre su ejecución.
- **Consulted (C):** Figura que debe ser consultada para la realización de la tarea.
- **Informed (I):** Figura que debe ser informada sobre la realización de la tarea.

DPO

+

CISO

EIPD - PIA

Evaluación de impacto

1. ANÁLISIS DE LA NECESIDAD DE LA PIA

Checklist para comprobar si el tipo de tratamiento exige realizar una evaluación de impacto

2. ANÁLISIS DE RIESGOS

Análisis de los riesgos que el tratamiento puede generar

3. NECESIDAD Y PROPORCIONALIDAD

Evaluación de la necesidad y la proporcionalidad del tratamiento en relación a sus finalidades

4. MEDIDAS Y CONTROLES

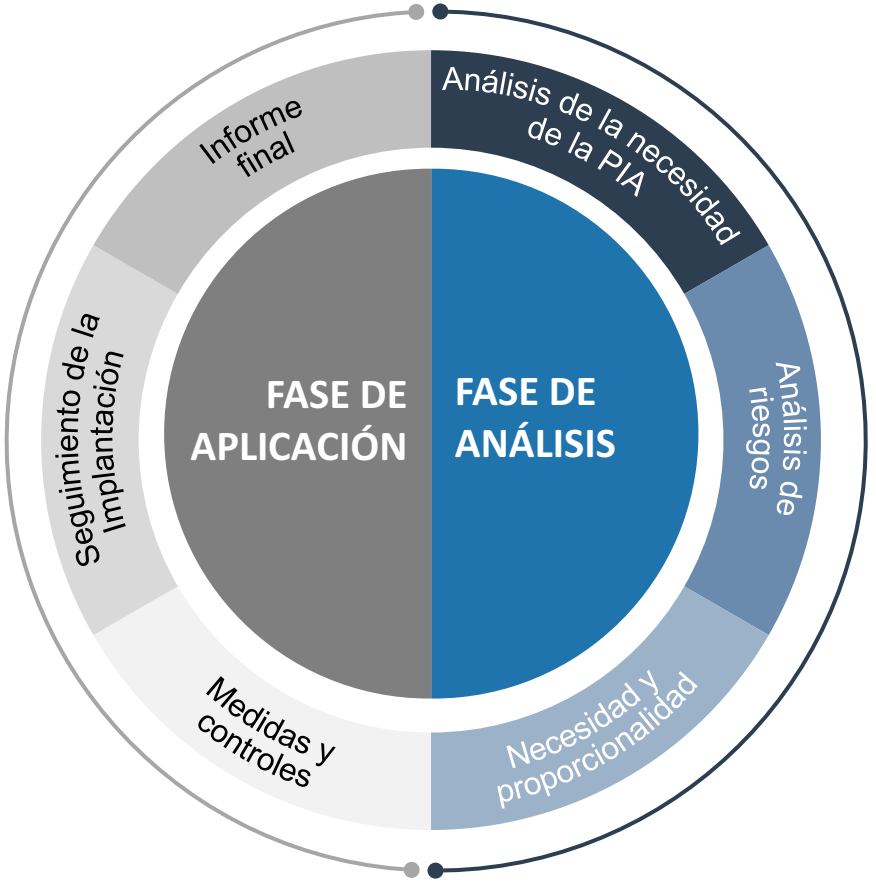
Medidas y controles orientados a mitigar los riesgos identificados en la fase de análisis

5. VERIFICACIÓN DEL EFECTO

Seguimiento de la implantación de las medidas y los controles

6. INFORME FINAL

Comprobación del efecto mitigador de las medidas y de su eficacia



PIA - Fase 01

Identificación del proyecto o tratamiento evaluado

Nombre del tratamiento	Selección de personal
Breve descripción	Tratamiento de los datos de los candidatos a un puesto de trabajo con el fin de identificar a los candidatos más idóneos en función del perfil y las competencias requeridas.
Responsable del proyecto	Nombre del responsable
Empresas que participan en el tratamiento	Lista de empresas
Encargados del tratamiento	Lista de encargados del tratamiento
Interesados	Candidatos a un puesto de trabajo de la empresa
Finalidades	1. Realizar el proceso de selección 2. Obtener información del candidato 3. Obtener información de las personas de referencia 4. Obtener información de las redes sociales 5. Realizar pruebas psicotécnicas 6. Elaborar un perfil de personalidad del candidato 7. Evaluar a los candidatos 8. Seleccionar al candidato más idóneo

PIA - Fase 01

Identificación del proyecto o tratamiento evaluado

Nombre del tratamiento	Selección de personal
Breve descripción	Tratamiento de los datos de los candidatos a un puesto de trabajo con el fin de identificar a los candidatos más idóneos en función del perfil y las competencias requeridas.
Responsable del proyecto	Nombre del responsable
Empresas que participan en el tratamiento	Lista de empresas
Encargados del tratamiento	Lista de encargados del tratamiento
Interesados	Candidatos a un puesto de trabajo de la empresa
Finalidades	1. Realizar el proceso de selección 2. Obtener información del candidato 3. Obtener información de las personas de referencia 4. Obtener información de las redes sociales 5. Realizar pruebas psicotécnicas 6. Elaborar un perfil de personalidad del candidato 7. Evaluar a los candidatos 8. Seleccionar al candidato más idóneo

PIA - Fase 01

Análisis de la necesidad de llevar a cabo la evaluación

#	Punto a analizar
01	Tratamiento de datos de carácter personal
02	Evaluación sistemática y amplia de aspectos personales relativa a personas físicas
03	Se pueden determinar hábitos, comportamientos, preferencias, gustos, intereses, etc. de personas físicas
04	Una de las finalidades del tratamiento es elaborar perfiles personales o predecir comportamientos
05	Se toman decisiones con efectos jurídicos para las personas afectadas
06	Se toman decisiones que pueden afectar o perjudicar de alguna manera a las personas afectadas
07	Tratamiento de datos a gran escala
08	Tratamiento de categorías especiales de datos
09	Monitorización mediante videovigilancia
10	Se pueden relacionar diferentes fuentes u orígenes de datos personales, de manera que se incremente la capacidad de análisis de la información
11	Nuevas soluciones tecnológicas
12	Nuevas soluciones organizativas
13	Se pueden utilizar tecnologías que se pueden percibir como especialmente intrusivas para la privacidad
14	Se pueden utilizar metodologías que se pueden percibir como especialmente intrusivas para la privacidad
15	Datos de menores de 13 años
16	Datos de personas en situación de vulnerabilidad
17	Transferencias a países fuera de la UE

PIA - Fase 01

Análisis de la necesidad de llevar a cabo la evaluación

Conclusiones sobre la necesidad de realizar la evaluación

La conclusión del análisis previo puede ser que la empresa debe realizar una evaluación de impacto en relación al tratamiento analizado, por razones como las siguientes, en el caso del tratamiento de ejemplo:

1. Se utilizan datos de naturaleza especial.
2. Se realiza un análisis sistemático de la personalidad de los candidatos.
3. Se combinan datos de diversas bases de datos con el fin de elaborar perfiles.
4. Se toman decisiones en procesos en los que compiten varios candidatos.
5. Se toman decisiones que pueden impedir que el candidato acceda a un contrato de trabajo.
6. Se toman decisiones que pueden producir efectos jurídicos sobre los interesados.
7. Existe el riesgo de que los datos y perfiles obtenidos se utilicen para decisiones discriminatorias.

Por ello se ha considerado necesario, en este caso, realizar la evaluación de impacto.

PIA - Fase 02

Descripción sistemática de las operaciones de tratamiento

Ciclo de vida de los datos

El informe de la evaluación de impacto contendrá una descripción sistemática de las operaciones de tratamiento como la del siguiente ejemplo, en la que se representará el ciclo de vida de los datos y se explicará las acciones que se vana a desarrollar en cada fase:

1. Entrada de datos.
2. Registro y clasificación.
3. Acceso a los datos.
4. Análisis de los datos.
5. Combinación de los datos con otras bases de datos.
6. Elaboración de perfiles.
7. Modificación de los datos.
8. Toma de decisiones.
9. Transmisión de datos.
10. Bloqueo o supresión.

PIA - Fase 02

Descripción sistemática de las operaciones de tratamiento

Canales de entrada de datos

#	Fuente	Canal de entrada	Formato
01	El propio interesado	Correo electrónico	CV en formato PDF
02	El propio interesado	Formulario web de la empresa	CV en formato PDF
03	El propio interesado	Mostrador de recepción	CV en formato papel
04	El propio interesado	Entrega en mano	CV en formato papel
05	Familiar del interesado	Correo electrónico	CV en formato PDF
06	Familiar del interesado	Entrega en mano	CV en formato papel
07	Terceros	Varios canales	Varios formatos
08	Referencias	Llamada telefónica	Campo en la aplicación
09	Redes sociales	Captura de datos	Campo en la aplicación
10	Tratamientos anteriores	Bases de datos de la empresa	Campo en la aplicación
11	Captura automatizada	IP, cookies, logs, geoetiquetas	Campo en la aplicación
12	Cálculos	Cálculos de la aplicación	Campo en la aplicación
13	Datos disociados	Singularización	Campo en la aplicación

PIA - Fase 02

Descripción sistemática de las operaciones de tratamiento

Medios de tratamiento

La descripción sistemática de las operaciones de tratamiento contendrá una descripción los medios de tratamiento, como la de la siguiente tabla de ejemplo:

Medio	Descripción
Servidor	Tipo de servidor
Localización del servidor	Localidad
Ordenadores de sobremesa	Descripción
Ordenadores portátiles	Descripción
Tablets	Descripción
Smartphones	Descripción
Accesos remotos	Descripción
Web	Formulario web
Correo electrónico	Envío de CV
Aplicaciones	Aplicación de selección de personal Aplicación de pruebas psicotécnicas
Bases de datos	Base de datos de candidatos Base de datos de CV Base de datos de cuestionarios
Nuevas soluciones tecnológicas	No se utilizan nuevas soluciones tecnológicas
Nuevas soluciones organizativas	No se utilizan nuevas soluciones organizativas

PIA - Fase 02

Descripción sistemática de las operaciones de tratamiento

Modelo de datos

La descripción sistemática de las operaciones de tratamiento contendrá una descripción del modelo de datos, como la de la siguiente tabla de ejemplo:

Categoría de datos	Datos	Riesgo
Datos identificativos	Nombre Apellidos Edad	Bajo
Datos de contacto	Domicilio Mail Teléfono fijo Teléfono móvil	Medio
Datos académicos	Titulación Universidad Formación de postgrado	Medio
Datos económicos	Perfil salarial	Medio
Datos relativos a la personalidad	Perfil del candidato	Alto
Resultados de las pruebas psicotécnicas	Coeficiente intelectual	Alto
Datos de salud	Alergias Minusvalías	Alto
Opiniones de los evaluadores	Sí	Alto
Opiniones de antiguos empleadores	Sí	Alto
Datos obtenidos en redes sociales	Sí	Alto
Conclusiones sobre la idoneidad del candidato	Sí	Alto

PIA - Fase 02

Descripción sistemática de las operaciones de tratamiento

Categorías especiales de datos

La descripción sistemática de las operaciones de tratamiento contendrá una relación de las categorías especiales que se han identificado en el tratamiento evaluado, como la de la siguiente tabla de ejemplo:

#	Categoría especial de datos	Participan en el tratamiento
01	Origen étnico o racial	Si
02	Opiniones políticas	No
03	Convicciones religiosas o filosóficas	No
04	Afiliación sindical	Si
05	Datos genéticos	No
06	Datos biométricos identificativos	No
07	Datos relativos a la salud	Si
08	Datos relativos a la vida sexual	No
09	Datos relativos a la orientación sexual	No
10	Datos relativos a condenas e infracciones penales	No

PIA - Fase 02

Descripción sistemática de las operaciones de tratamiento

Flujo de datos - Local e internacional

La descripción sistemática de las operaciones de tratamiento contendrá una relación de los flujos de datos que se han identificado en el tratamiento evaluado, como la de la siguiente tabla de ejemplo:

#	Remitente	Destinatario	Datos transferidos
01			
02			
03			
04			
05			
06			
07			
08			
09			
10			

PIA - Fase 02

Descripción sistemática de las operaciones de tratamiento

Fines del tratamiento

La descripción sistemática de las operaciones de tratamiento contendrá una relación de los fines del tratamiento, como la de la siguiente tabla de ejemplo:

#	Fin	Riesgo
01	Iniciar el proceso de selección	Bajo
02	Obtener información del candidato	Medio
03	Obtener información de las personas identificadas como referencia	Medio
04	Obtener información de las redes sociales	Alto
05	Realizar pruebas psicotécnicas	Alto
06	Elaborar un perfil de personalidad del candidato	Alto
07	Evaluar a los candidatos	Alto
08	Seleccionar al candidato más idóneo	Alto

PIA - Fase 02

Descripción sistemática de las operaciones de tratamiento

Base de legitimación

#	Base	Descripción
01	Consentimiento	El interesado ha dado su consentimiento inequívoco
02	Contrato	Ejecución de un contrato
03	Base legal	Obligación legal
04	Interés legítimo	La empresa tiene el interés legítimo de seleccionar a su personal y contratar a las personas más apropiadas para cada puesto de trabajo con el fin de evitar que una selección defectuosa pueda provocar daños a clientes y a terceros.

PIA - Fase 02

Descripción sistemática de las operaciones de tratamiento

Interés legítimo

La descripción sistemática de las operaciones de tratamiento contendrá una relación de los intereses legítimos perseguidos por el responsable del tratamiento, como la de la siguiente tabla de ejemplo:

#	Interés legítimo	Riesgo
01	Seleccionar a las personas que formarán parte de la plantilla de la empresa	Medio
02	Contratar a las personas más apropiadas para cada puesto de trabajo	Medio
03	Evitar que una selección defectuosa pueda provocar daños a clientes	Alto
04	Prevenir incumplimientos y delitos	Alto

NOTA IMPORTANTE: Al intentar determinar los intereses legítimos del responsable del tratamiento aparecen fines adicionales del tratamiento que deben ser identificados y evaluados, debido al impacto que pueden tener en materia de protección de datos y de compliance. Algunos controles pueden generar datos no previstos en el modelo de datos que pueden llegar a ser innecesarios, excesivos o desproporcionados. Por ejemplo, solicitar los antecedentes penales para puestos de trabajo que no los exigen.

PIA - Fase 03

Evaluación de la necesidad y la proporcionalidad

Puntos de la evaluación de la necesidad y la proporcionalidad

Para realizar la evaluación de la necesidad y la proporcionalidad se pueden tener en cuenta las cuestiones planteadas en la siguiente tabla de ejemplo:

#	Cuestión analizada	Resultado del análisis
01	¿Los objetivos y las finalidades del tratamiento están definidos de tal manera que permita valorar si las operaciones del tratamiento son necesarias para conseguir dichos fines?	
02	¿Pueden conseguirse estos fines por otros medios, es decir, sin tratar datos personales?	
03	¿Pueden conseguirse los mismos fines tratando menos datos, es decir, eliminado algunos de los datos que aparecen en el modelo de datos?	
04	¿Puede reducirse cuantitativamente el universo de personas físicas afectadas por el tratamiento?	
05	¿Puede reducirse cualitativamente el universo de personas físicas afectadas por el tratamiento?	
06	¿Pueden utilizarse tecnologías, procedimientos o medios de tratamiento menos invasivos?	
07	¿Las operaciones de tratamiento a realizar son idóneas para los fines perseguidos?	
08	¿Los datos recogidos se pueden utilizar de manera incompatible con la finalidad para la cual se recogieron?	
09	¿Los datos que se ha previsto tratar son adecuados, pertinentes y limitados a lo que es necesario en relación con las finalidades, en el sentido de que no son excesivos?	

PIA - Fase 04

Análisis de riesgos

Riesgos que afectan a los principios relativos al tratamiento

Para realizar la evaluación de los riesgos que afectan a los principios relativos al tratamiento se pueden tener en cuenta los riesgos planteados en la siguiente tabla de ejemplo:

#	Riesgo	Probabilidad	Impacto
01	Consentimiento defectuoso, insuficiente o inexistente		
02	Consentimiento obtenido de forma tácita antes del 25/05/18		
03	Interés legítimo sobrevalorado		
04	Base jurídica mal interpretada		
05	Finalidades imprecisas, excesivas o ilegítimas		
06	Cambio de finalidad que no figura en la información facilitada		
07	Cambio de finalidad que invalida el consentimiento inicial		
08	Cambio de finalidad que invalida una evaluación de impacto anterior		
09	Datos inadecuados, no pertinentes, excesivos o innecesarios		
10	Datos inexactos o no actualizados		
11	Plazos de conservación excesivos		
12	Tratamiento desleal o poco transparente		
13	Operaciones de tratamiento desproporcionadas		
14	Datos de categoría especial sin consentimiento expreso		
15	Datos biométricos aplicados a finalidades que no lo necesitan		
16	Información incompleta sobre las finalidades del tratamiento		

PIA - Fase 04

Análisis de riesgos

Riesgos que afectan a los derechos y libertades del interesado

Para realizar la evaluación de los riesgos para los derechos y las libertades de los interesados se pueden tener en cuenta los riesgos planteados en la siguiente tabla de ejemplo:

#	Riesgo	Probabilidad	Impacto
01	Discriminación por razón de los datos obtenidos o inferidos		
02	Vulneración del derecho a la imagen, la intimidad o el honor		
03	Vulneración del libre desarrollo de la personalidad		
04	Rechazo social		
05	Daño económico		
06	Efectos jurídicos perjudiciales para el interesado		
07	Perjuicio laboral		
08	Intromisión en la intimidad y el secreto de las comunicaciones		
09	Infracción de su derecho a la protección de los datos personales		
10	Información incompleta sobre las finalidades del tratamiento		
11	Falta de respuesta a su solicitud de ejercicio de derechos		
12	Respuesta fuera de plazo a su solicitud de ejercicio de derechos		
13	Identificación insuficiente de la persona que ejercita un derecho		
14	Decisiones exclusivamente automatizadas		
15	Divulgación de categorías especiales de datos personales		
16	Creación o utilización de perfiles de personalidad		
17	Perfiles o pruebas que permitan conocer problemas de salud		
18	Tratamiento incorrecto de datos de niños		
19	Tratamiento incorrecto de datos de colectivos vulnerables		
20	Tratamiento incorrecto de datos a gran escala		

PIA - Fase 04

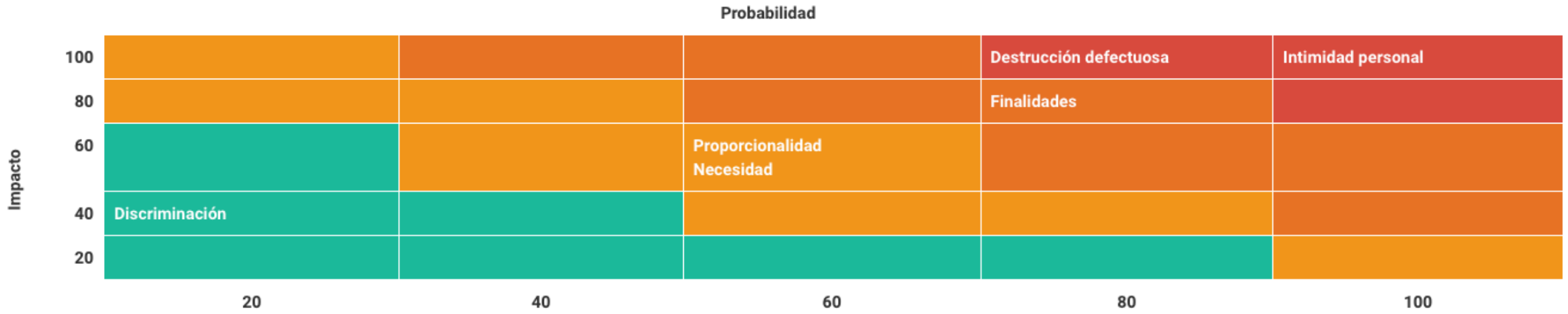
Análisis de riesgos

Riesgos que afectan a la seguridad de los datos

Para realizar la evaluación de los riesgos que afectan a la seguridad de los datos se pueden tener en cuenta los riesgos planteados en la siguiente tabla de ejemplo:

#	Riesgo	Probabilidad	Impacto
01	Medidas de seguridad insuficientes		
02	Medidas de seguridad obsoletas o no actualizadas		
03	Acceso no autorizado a datos personales por parte de terceros		
04	Divulgación de datos personales como resultado de un ciberataque		
05	Divulgación de datos personales de forma accidental		
06	Destrucción de datos personales como resultado de un ciberataque		
07	Destrucción de datos personales de forma accidental		
08	Secuestro, bloqueo o caída de los sistemas de información		
09	Incapacidad para detectar y gestionar incidentes de seguridad		
10	Brechas de seguridad no notificadas en tiempo y forma		
11	Identificación de un usuario causada por una disociación defectuosa		
12	Singularización causada por una disociación incompleta		
13	Control insuficiente de proveedores con acceso a datos y ET		

Mapa de Riesgos Inherentes La relación entre la Probabilidad y el Impacto económico de los distintos Grupos.

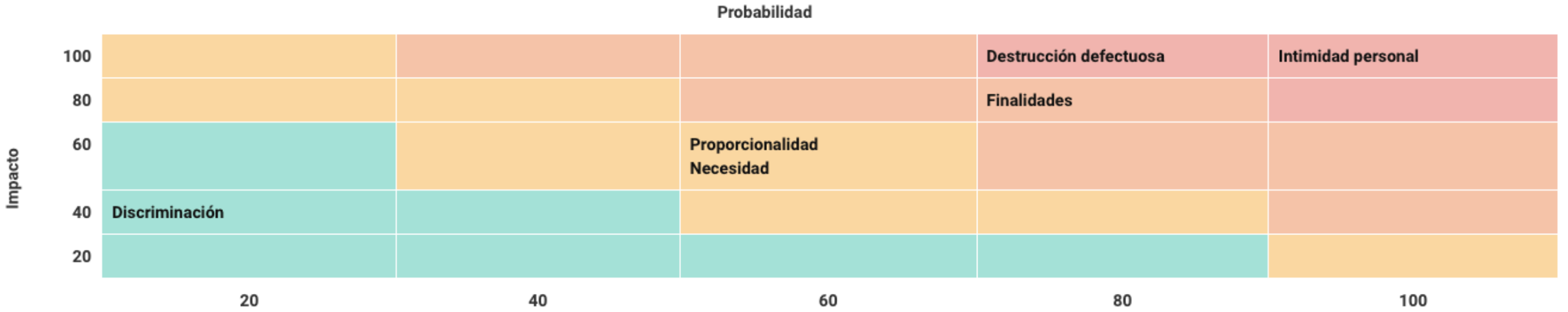


Identificador	Nombre	Probabilidad	Impacto	Riesgo Inherente
PIA001	Proporcionalidad	60	60	**60**
PIA002	Necesidad	60	60	**60**
PIA003	Intimidad personal	100	100	**100**
PIA004	Finalidades	80	80	**80**
PIA020	Destrucción defectuosa	80	100	**100**
PIA005	Discriminación	20	40	**20**

* Se muestran los valores más altos del Grupo

Mapa de Riesgos Residuales

Muestra la relación entre la Probabilidad y el Impacto económico de los distintos Grupos una vez considerados los Controles.



Identificador	Nombre	Probabilidad	Impacto	Probabilidad Residual	Impacto Residual
PIA001	Proporcionalidad	60	60	60	60
PIA002	Necesidad	60	60	60	60
PIA003	Intimidad personal	100	100	100	100
PIA004	Finalidades	80	80	80	80
PIA020	Destrucción defectuosa	80	100	80	100
PIA005	Discriminación	20	40	20	40

* Se muestran los valores más altos del Grupo

PIA - Fase 04

Análisis de riesgos

Opinión de los interesados

Cuando proceda, se recabará la opinión de los interesados sobre:

1. La necesidad y la proporcionalidad de la información solicitada
2. Las finalidades informadas
3. Las referencias solicitadas
4. La naturaleza y el alcance de las actividades de tratamiento

PIA - Fase 05

Medidas preventivas y controles

Controles más significativos

En esta tabla se presenta una selección de los controles más significativos, destinados a mitigar la probabilidad y el impacto de los riesgos identificados:

#	Riesgo	Probabilidad	Impacto
01	Formación apropiada del personal		
02	Asignación clara de responsabilidades		
03	Anonimización y seudonimización		
04	Medidas de seguridad basadas en la ISO 27001		
05	Muestreos periódicos para comprobar el consentimiento inequívoco en todos los canales de entrada		
06	Comprobar periódicamente si existen otros canales de entrada de datos no identificados		
07	Comprobar periódicamente que la información suministrada a los interesados es completa		
08	Verificar periódicamente que los datos no se aplican a nuevas finalidades		
09	Comprobar periódicamente que los datos tratados son adecuados, pertinentes y limitados a los fines		
10	Simulaciones periódicas de solicitud de ejercicio de derechos		
11	Comprobar periódicamente si los datos tratados son exactos.		
12	Comprobar periódicamente si los datos son suprimidos o bloqueados una vez finalizado el plazo de conservación establecidos en la tabla de plazos de conservación.		
13	Realizar un control continuado de los proveedores con acceso a datos y de los ET		
14	Simulaciones periódicas de solicitud de ejercicio de derechos		
15	Obtención periódica de pruebas del cumplimiento con sellado de tiempo		

PIA - Fase 06

Fase final

Verificación y obtención de evidencias de la eficacia de los controles y de que consiguen mitigar los riesgos

Conclusiones finales de la evaluación de impacto sobre el riesgo que comporta el tratamiento

IMPLANTACIÓN DE LOS CONTROLES

ANÁLISIS DE LOS RIESGOS RESIDUALES

CONCLUSIONES FINALES

OPCIONES:

- ☐ Medidas de seguridad
- ☐ Medidas organizativas
- ☐ Medidas contractuales

OPCIONES:

- ☐ El riesgo residual es bajo
- ☐ El riesgo residual es medio
- ☐ El riesgo residual es alto

OPCIONES:

- ☐ Se puede realizar el tratamiento
- ☐ Se formulará una consulta previa
- ☐ No se puede realizar el tratamiento

Tratamiento en la nueva LOPD

Las evaluaciones de impacto en el anteproyecto de LOPD

Infracción grave

Artículo 73.t

El tratamiento de datos de carácter personal sin haber llevado a cabo la evaluación del impacto de las operaciones de tratamiento en la protección de datos personales en los supuestos en que la misma sea exigible.

En caso de que el laboratorio esté adherido a un Código de Conducta

4.4 ¿Qué ocurre cuando se está adherido a un código de conducta?

En el caso de que el responsable del tratamiento esté adherido a algún código de conducta (art. 40 y siguientes del RGPD) donde se incluya una metodología propia, se puede **utilizar la misma para la realización de las EIPD sin eximir de la obligación de realizar la EIPD si fuese de aplicación.**

Muchas gracias

D Diagonal 640 1C - 08017 Barcelona

W http://ribas.legal

B http://xribas.com

T 934940748 - 639108413

L Ribas y Asociados

Tw @xribas