

Guía de Evaluación de Impacto en la Protección de Datos.

Capítulo 1. Contextualización

1.1 El derecho a la privacidad y la protección de datos personales.

La protección de datos personales es un derecho humano, tuitivo no de los datos en sí, sino de las personas. Toda interpretación con respecto a los objetivos perseguidos en este documento debe partir de esa premisa fundamental.

Desde un punto de vista instrumental y en un escenario global de tráfico constante de información, la protección de datos personales cumple dos funciones. Por un lado, regula la capacidad que tienen las personas para conocer, editar, gestionar o eliminar datos sobre ellas mismas. Por otro, mediante un conjunto de reglas específicas y principios generales, establece límites para el uso de datos por parte de entidades públicas y privadas.

La interceptación de telecomunicaciones, el monitoreo desproporcionado de los espacios públicos a través de sistemas de videovigilancia, la recolección o publicación de datos personales sin el consentimiento de sus titulares, así como el tratamiento automatizado de información a través de algoritmos o inteligencia artificial representan algunos de los problemas que intenta resolver y de los que se ocupa activamente esta rama del derecho.

Observando con preocupación estos fenómenos de las décadas recientes y con el fin de mitigar los riesgos que entrañan, las Autoridades de Control de la República Oriental del Uruguay y de la República Argentina han decidido cooperar para diseñar un mecanismo de carácter preventivo que busca minimizar los potenciales daños a la privacidad: la Evaluación de Impacto en la Protección de Datos (EIPD).

El objetivo de esta herramienta es que, desde una etapa temprana, las prácticas y proyectos que puedan afectar los derechos de las personas, a través del tratamiento de sus datos personales, sean evaluados por los responsables de tratamiento y constituidos conforme a ciertos estándares restrictivos de seguridad y de integridad.

Para ello, las Autoridades de Control han seguido las más modernas legislaciones y guías en la materia, con particular atención a los Estados miembro de la Unión Europea y a los Estados parte del Convenio 108 para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personales -tratado internacional que tanto Argentina como Uruguay han suscrito y ratificado.

En este documento se explicará con más detalle en qué consiste este mecanismo, cuáles son sus etapas y sus implicancias posibles en las diversas prácticas que involucran el tratamiento de datos personales.

A esos efectos, resulta pertinente dar cuenta de algunos conceptos básicos en la materia en orden a facilitar la lectura del presente documento.

1.2 Conceptos fundamentales y ejemplos

Archivo, registro, base o banco de datos: indistintamente, designan al conjunto organizado de datos personales que sean objeto de tratamiento o procesamiento, electrónico o no, cualquiera que fuere la modalidad de su formación, almacenamiento, organización o acceso.

Autoridad de Control de Protección de Datos Personales: órgano administrativo de control cuya función es garantizar la protección de los datos personales. Cuenta con amplias facultades y tiene la potestad de iniciar inspecciones de oficio y aplicar sanciones. En la Argentina, la autoridad de control es la Agencia de Acceso a la Información Pública (AAIP). En el Uruguay, la autoridad de control es la Unidad Reguladora y de Control de Datos Personales (URCDP).

Cesión o comunicación de datos personales: toda revelación o envío de datos a una persona distinta del titular de los datos personales.

Dato personal: información de cualquier tipo referida a personas humanas o jurídicas determinadas o determinables.

Dato sensible: dato personal que revela origen racial y étnico, opiniones políticas, convicciones religiosas, filosóficas o morales, afiliación sindical o cuestiones relativas a la salud o a la vida sexual, como así también todo otro dato cuya utilización pueda producir discriminaciones arbitrarias.

Delegado de Protección de Datos Personales: persona designada o contratada por el responsable, con experiencia y conocimiento probados en la materia, al efecto de asesorar en la formulación, diseño y aplicación de políticas de protección de datos personales.

Disociación de datos: operación que permite que la información obtenida no pueda asociarse a persona determinada o determinable.

Encargado del tratamiento: persona física o jurídica, pública o privada, que sola o en conjunto con otros trate datos personales por cuenta del responsable del tratamiento.

Principio de finalidad: los datos personales que se recojan a los efectos de su tratamiento deben ser ciertos, adecuados, pertinentes y no excesivos en relación con el ámbito y finalidad para los que se hubieren obtenido. Los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención.

Principio de legalidad: la recolección de datos no puede hacerse por medios desleales, fraudulentos o en forma contraria a las disposiciones de la ley.

Principio de minimización: los datos deben ser destruidos cuando hayan dejado de ser necesarios o pertinentes a los fines para los cuales hubiesen sido recolectados.

Principio de seguridad y confidencialidad de los datos: el responsable o usuario de la base de datos debe adoptar las medidas que resultaren necesarias para garantizar la seguridad y confidencialidad de los datos personales. Dichas medidas tendrán por objeto evitar su adulteración, pérdida, consulta o tratamiento no autorizado, así como detectar desviaciones de información, intencionales o no, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

Privacidad por diseño: un enfoque que considera que la protección de la privacidad debe estar integrada con el sistema, aplicación o dispositivo desde su diseño. Desde esta perspectiva, la protección de los datos personales no debe ser analizada a posteriori, como si se tratara de un anexo, sino que debe estar presente en todas las etapas del proceso.

Privacidad por defecto: enfoque que exige que, por defecto, solo sean objeto de tratamiento aquellos datos personales que sean necesarios para cada una de las finalidades específicas del tratamiento.

Responsable de la base de datos o del tratamiento: persona física o jurídica, pública o privada, propietaria de la base de datos o que decida sobre la finalidad, contenido y uso del tratamiento.

Riesgo a los derechos de las personas: daño probable que puede producirse como resultado de una operación de tratamiento de datos y que afecta algún derecho del titular de los datos.

Titular de los datos: persona cuyos datos sean objeto de un tratamiento incluido dentro del ámbito de acción de la ley.

Transferencia internacional: cesión o comunicación de datos que tiene como destinatario un responsable de tratamiento ubicado en el extranjero.

Tratamiento de datos personales: operaciones y procedimientos sistemáticos, electrónicos o no, que permitan la recolección, conservación, ordenación, almacenamiento, modificación, relacionamiento, evaluación, bloqueo, destrucción y, en general, todo procesamiento de datos personales, así como también su cesión a terceros a través de comunicaciones, consultas, interconexiones o transferencias.

1.3 ¿Qué es una Evaluación de Impacto en la Protección de Datos (EIPD)?

Una Evaluación de Impacto en la Protección de Datos (EIPD) es un proceso que las organizaciones deben efectuar para identificar y tratar los riesgos que puedan producir sus actividades habituales, sus nuevos proyectos o sus políticas corporativas cuando involucran el tratamiento de datos personales. Ello considerando que el tratamiento de datos personales puede provocar impactos en 06 los derechos de las personas que deben ser de algún modo identificados, gestionados, minimizados o eliminados para cumplir con la normativa vigente.

Si bien se ha incorporado recientemente como una obligación expresa en las legislaciones de Latinoamérica y Europa, la EIPD resulta desde hace tiempo una buena práctica reconocida por normas técnicas internacionales. Su objetivo es reforzar los principios en materia de protección de datos personales y orientar al responsable a los efectos de su cumplimiento, en especial cuando la complejidad del proyecto o actividad bajo análisis exige un examen más detallado.

Para que este proceso resulte exitoso, es necesario involucrar a las personas que integran la organización, a consultores expertos e incluso a los sectores o grupos de titulares de datos que posiblemente puedan ser afectados. Es notorio que la EIPD ayuda a resolver potenciales problemas en materia de protección de datos, sobre todo, al principio del desarrollo de un proyecto o actividad, posibilitando la integración de mecanismos de privacidad por diseño y por defecto desde una etapa temprana.

Debe aclararse que la EIPD no está concebida únicamente para las grandes organizaciones que producen un impacto ostensible en la comunidad, sino también para las startups de tecnología y otras pequeñas empresas que, por la especificidad de sus emprendimientos, generen o puedan generar en el futuro un impacto en los datos personales de la ciudadanía.

Los riesgos que sean identificados en el proceso deben evaluarse tanto en una dimensión individual como en una dimensión comunitaria. Hay operaciones de tratamiento de datos que, consideradas individualmente, no lucen relevantes, pero que en el agregado podrían suponer un riesgo significativo para derechos y garantías fundamentales de las personas. Es evidente que no pueden preverse todos los efectos posibles de un proyecto, cualquiera este sea, pero se deben empeñar los mejores esfuerzos para computar la mayor cantidad de riesgos en la EIPD, a fin de que ésta pueda ser considerada completa y válida.

En este sentido, la EIPD busca conocer, de manera acabada, la relación específica que existe entre la organización y los titulares de datos. Así es que se deben tener en cuenta, entre otras cosas:

- Las expectativas razonables de privacidad que tienen las personas involucradas.
- La influencia que tiene la actividad de la organización en la sociedad.
- Cómo y por qué la organización toma ciertas decisiones, cuáles son sus objetivos.

En todos los casos, la EIPD es un proceso que genera valor para la organización que la lleva adelante.

En el caso de los organismos públicos, permite establecer lazos de confianza con la ciudadanía. En el caso de las empresas privadas, evita potenciales costos reputacionales y fideliza a los clientes o consumidores. Por otra parte, la EIPD no es necesariamente un proceso complejo e injustificadamente oneroso, ni debe ser, tampoco, idéntico para todas las organizaciones. La evaluación de un proyecto de una pequeña empresa es distinta de la evaluación de las actividades habituales o de las políticas corporativas de un grupo económico entero, pero esto no significa que se prescinda de rigor 07 en los reportes que resulten de la evaluación en el primer caso, sino que, dentro de ciertos parámetros, la EIPD es adaptable a cada caso particular.

Por último, y como se verá con más atención en el capítulo que sigue, el proceso de elaboración de la EIPD presupone distintas fases:

VA IMAGEN

Capítulo 2. Metodología para la EIPD

Sin importar cuál sea la metodología aplicada a la EIPD, ésta debe asegurar la homogeneidad y comparabilidad de los resultados, mediante un proceso sistemático y repetible, garantizando así la objetividad del proceso.

2.1 Determinación de participantes y documentación de los procesos de elaboración de la EIPD

El objetivo de esta fase 1 es determinar los participantes del Análisis Preliminar y la EIPD, y definir los procesos para la documentación.

Un aspecto fundamental a tener en cuenta en todos los casos es la determinación en forma anticipada de los participantes en la EIPD, del proceso de registro de las actividades y de los formatos de informes, conclusiones y planes de tratamiento.

Un conjunto mínimo de personas de distintas áreas de la organización deberá participar en el análisis preliminar, sin perjuicio de la necesidad de agregar otros participantes en caso de que, a partir de dicho análisis o de alguna prescripción de la normativa vigente, resulte necesario realizar efectivamente la EIPD.

En cuanto a la determinación de las personas que participarán en una EIPD en general, es indispensable que la organización realice una serie de consultas internas y externas, que deberán ser documentadas.

a. Consultas internas

La participación integral de la organización en la EIPD es fundamental para que ésta conduzca a buenos resultados. Es más probable que los riesgos permanezcan sin tratarse si la EIPD no involucra conversaciones y discusiones internas entre las distintas personas y equipos que forman la organización. Este proceso de conversaciones puede incluir intercambios informales en persona o vía correo electrónico, reuniones de trabajo, así como mecanismos de evaluación y aprobación de los directores de la empresa o principales funcionarios del organismo, si se tratara de una entidad pública.

Dependiendo del proyecto o de la actividad analizada en la EIPD, los participantes y el grado de participación de cada uno de ellos puede variar. Es evidente que no es lo mismo diseñar una aplicación de mensajería instantánea que montar un foro digital o recolectar datos de acceso público para enviar publicidad por medio de un correo automatizado. Cada una de estas operaciones es particular y las características de la organización habrán de hacer de cada EIPD un proceso distinto.

3. Como se verá luego, la realización del análisis preliminar resulta fundamental en todos los casos a efectos de determinar la necesidad de una EIPD, pero puede ser obviada en caso de que la normativa vigente establezca la obligación de realizarla para determinados tratamientos.

En ese sentido, es recomendable que se forme un equipo especializado y multidisciplinario destinado a coordinar las distintas etapas de la EIPD. Ese equipo puede ser estable o designado de manera ad hoc de acuerdo a las necesidades de la organización. Cuando la organización es pequeña, puede no resultar necesario.

También es posible contratar a un consultor experto, ajeno a la organización, para que coordine y organice el equipo de EIPD.

De forma tentativa y tomando como modelo a la gran organización, se establecerá una lista con los potenciales participantes del equipo de EIPD. Esta lista no es exhaustiva, sino que pretende exponer cómo distintas partes de una organización podrían involucrarse en este proceso:

- **Funcionales:** es fundamental contar con la participación de las personas que efectivamente conocen el negocio del responsable o encargado en su caso, son aquellos que poseen información de los alcances y las razones para la definición de los procesos que se llevan adelante en la organización.
- **Delegado de protección de datos:** si existe en la organización un delegado de protección de datos, es recomendable que integre o incluso lidere el equipo de EIPD. El delegado de protección de datos es un especialista en la materia que conoce la legislación específica y está familiarizado con los procesos de EIPD.
- **Ingenieros, desarrolladores, comunicadores y diseñadores:** aquellos que están desarrollando un producto –sea este un objeto material, una pieza de software o un aviso publicitario– deben considerar cómo ese producto puede llegar a impactar en la privacidad y otros derechos de las personas.
- **Especialistas en seguridad informática:** están capacitados para aconsejar medidas de seguridad, así como para detectar riesgos potenciales en el proyecto bajo análisis.
- **Proveedores de servicios informatizados y otros encargados de tratamiento:** si la actividad o proyecto involucra algún tercero contratado en calidad de encargado del tratamiento de datos, es recomendable que sea incluido en las consultas internas.
- **Gobernanza corporativa y compliance:** profesionales o funcionarios que se ocupan del análisis y la gestión de riesgos podrían integrar la protección de datos personales y, por lo tanto, la EIPD en su esfera de trabajo. Alternativamente, un miembro del equipo de compliance podría integrar el equipo de EIPD.
- **Investigadores, analistas y estadísticos:** la información producida o relevada por un proyecto podría llegar a utilizarse para analizar el comportamiento de los consumidores o con algún otro propósito estadístico. Cuando sea relevante, consultar a los investigadores puede resultar útil para aplicar

salvaguardas tales como la disociación de los datos.

- **Directorio o principales funcionarios del organismo:** es conveniente que aquellos que tienen mayor responsabilidad en la organización participen en el proyecto, supervisándolo y aprobando el reporte final.

b. Consultas externas

Las consultas externas involucran a las personas que potencialmente podrían ser afectadas por el proyecto, a expertos del sector privado y eventualmente a la autoridad de control en materia de protección de datos.

La opinión de aquellos que podrían ser perjudicados por el proyecto es un elemento de gran importancia en la EIPD. En primer lugar, porque permite a la organización entender más acabadamente las preocupaciones de la ciudadanía. En segundo lugar, porque es una práctica de transparencia que visibiliza y concientiza a las personas afectadas sobre cómo su información podría ser utilizada por las empresas o por el Estado. Los expertos y la autoridad de control, por su parte, tienen un rol de apoyo y pueden asesorar a la organización sobre los posibles riesgos involucrados en el proyecto bajo análisis.

Las consultas pueden ser formales o informales, pero se sugiere que sean plasmadas en un documento que identifique con claridad a los consultados. Asimismo, se reconoce que el momento y la naturaleza de la consulta puede ser relevante si el proyecto es de carácter reservado. Una organización puede no querer revelar sus planes a terceros por razones comerciales, marcarias, publicitarias o de seguridad. En tales casos, en la EIPD deberá acreditarse y justificar cuáles fueron las razones que limitaron las consultas externas.

De acuerdo a la magnitud de los riesgos involucrados, dependerá la extensión y la sofisticación de la consulta. Una organización puede ya tener mecanismos de consulta, tales como focus groups o sistemas de feedback o retroalimentación de usuarios en plataformas online. También puede organizar activamente paneles o eventos de discusión que integren a la ciudadanía. Cuando sea posible, es conveniente emplear las herramientas de consulta ya disponibles para comprender las expectativas de los titulares de datos desde distintas perspectivas.

Este proceso debe llevarse a cabo de modo que tenga valor dentro del proyecto y no sea meramente accesorio. La organización debe ser clara respecto de qué aspectos del proyecto estarían dispuestos a modificar y qué aspectos quisieran, por el contrario, preservar. En tal sentido, puede ser eficiente consultar sobre aspectos específicos y no sobre la totalidad del proyecto o actividad. En todos los casos, resulta indispensable presentar a los consultados preguntas y opciones de respuesta que sean realistas, de modo tal que el framing de la consulta no sea tendencioso.

2.2 Análisis del marco normativo aplicable

El objetivo de esta fase 2 es analizar la normativa aplicable al tratamiento realizado para comprender su aplicación a las distintas etapas de dicho tratamiento.

Toda EIPD supone, además, conocer los presupuestos habilitantes para un tratamiento lícito y que, por tanto, cumple con la normativa vigente. Debe recordarse que la EIPD es una herramienta que orienta al responsable para cumplir de manera acabada con las normas locales en materia de 11 protección de datos, en particular, cuando la complejidad del proyecto o actividad de la organización impide una aplicación simple de la legislación local.

Así pues, resulta necesario identificar cuáles son las normas que deben aplicar tanto en forma previa, al efectuar el análisis preliminar que se verá, como luego, al momento de realizar la EIPD, si del análisis surge la necesidad efectiva. En ese caso, corresponde evaluar si existen normas sectoriales que además le sean aplicables al caso concreto.

A continuación, se listan de manera sintética los principales aspectos de las legislaciones uruguaya y argentina que el responsable debe tener en consideración durante toda EIPD:

1. Licitud del tratamiento

- Identificar cuál es la norma o base legal que autoriza el tratamiento.
- Determinar cuál es la fuente de obtención de los datos.
- Definir si existen otros derechos involucrados además de la protección de datos que justifiquen el tratamiento.

2. Comunicación o cesión de datos personales

- Definir el cumplimiento del principio de previo consentimiento informado o aplicabilidad de alguna de las excepciones legalmente dispuestas.
- Identificar la forma de resguardar los consentimientos y de acreditarlos si fuese necesario.
- Identificar los procesos de revocación de consentimiento.
- Conocer la base legal para realizar la comunicación o cesión de datos.

3. Transferencias internacionales

- Identificar si se realizan transferencias y los territorios o jurisdicciones a las que se realiza.
- Determinar la causal que legitima las transferencias.
- Identificar los tipos de datos transmitidos.
- Identificar si es necesario o si se cuenta con autorización del órgano de control.
- Para el caso de que existan encargados de tratamientos, verificar si se requiere realizar transferencias internacionales.

4. Veracidad y proporcionalidad de los datos

- Identificar que solamente se traten los datos necesarios para la finalidad del tratamiento.
- Evaluar la pertinencia de recabar datos con fines históricos, científicos o estadísticos.
- Definir si existen mecanismos de actualización de datos.
- Identificar cuál es el procedimiento para eliminar los datos una vez agotada la finalidad.
- Analizar la necesidad de mantener los datos bloqueados y en ese caso definir los procedimientos de disociación.

5. Datos con regímenes especiales de protección

- Determinar si se tratan datos dentro de alguna de las categorías especialmente protegidas.
- Si se tratan datos sensibles, indicar si se cuenta con el consentimiento por expreso y por escrito.

6. Principio de reserva o confidencialidad

- Determinar la necesidad de formar al personal en protección de datos y, en especial, en el deber de debida reserva o confidencialidad.
- Elaborar procesos de reacción ante eventuales infracciones a la reserva o confidencialidad.

7. Tratamiento de datos personales

- Definir medidas para recabar consentimientos, especialmente de representantes de menores de edad o personas incapaces.
- Definir si es necesario trabajar con encargados de tratamiento.
- Evaluar la necesidad de contar con documentación que acredite las relaciones entre responsables y

encargados, y eventualmente, sub encargados (tratamiento de los datos, medidas de seguridad, eliminación de la información).

8. Ejercicio de derechos

- Adoptar las medidas necesarias para dar cumplimiento al ejercicio de derechos en los plazos establecidos normativamente.
- Asegurar formas de acreditar la identidad de los titulares de datos.
- Definir procesos para el ejercicio de derechos ante encargados y sub encargados.
- Definir especialmente procesos para dar respuesta al ejercicio del derecho de impugnación de valoraciones personales.

9. Seguridad

- Revisar las medidas de seguridad adoptadas.
- Realizar el análisis de riesgos.

10. Cumplimiento de obligaciones formales

- Determinar las bases de datos existentes y la necesidad de su inscripción.
- Designar cuando sea necesario un Delegado de Protección de Datos.
- Determinar contenido y ubicación de las políticas de privacidad.

2.3 Análisis preliminar

El objetivo de esta fase 3 es realizar un análisis previo de varios factores que inciden en la necesidad de efectuar posteriormente una EIPD, Puede obviarse cuando la EIPD se impone obligatoriamente por la normativa vigente.

Hay algunos factores que deben evaluarse para conocer la conveniencia de realizar o no una EIPD.

Cuando uno o varios de estos factores concurren, se puede inferir que el proyecto o actividad bajo análisis entraña riesgos significativos para los derechos de las personas. En tales casos, el responsable del tratamiento debe realizar una EIPD a los fines de cumplir con la normativa vigente.

No hay puntajes asignados a cada factor, se apela a la razonabilidad y a la responsabilidad proactiva del equipo de la EIPD, el que debe evaluar si las características del proyecto o la actividad de la organización ameritan la realización de este procedimiento preventivo. Una vez ponderados estos factores, la organización deberá elaborar un informe en el que explique y argumente si existe o no una necesidad de realizar la EIPD.

Para facilitarle este proceso al responsable, se sugieren a continuación una serie de preguntas que lo ayudarán en esta primera etapa inicial.

Tabla

2.4 Contexto del tratamiento

El objetivo de esta fase 4, y primera fase efectiva de la EIPD, es analizar todas las instancias de tratamiento que se va a realizar desde la perspectiva de la protección de datos personales.

2.4.1 Representar las etapas del ciclo de vida de los datos

Una vez identificada la necesidad de realizar una EIPD, resulta necesario mapear las distintas etapas del ciclo de vida de los datos, ya sea respecto del proyecto en curso o de las actividades habituales de la organización. El ciclo de vida de los datos personales puede definirse como el proceso que identifica las instancias asociadas a su tratamiento, desde la recolección hasta la supresión.

Es fundamental que las entidades describan cómo recolectan, almacenan, utilizan y finalmente eliminan la información en su poder. Deben explicar qué datos personales tratan, para qué y qué personas tienen acceso autorizado al flujo de información. Este es un presupuesto necesario para toda EIPD. Solo es posible realizar una adecuada gestión de riesgos si la organización entiende exhaustivamente cómo procesa o procesará datos personales. Ignorar qué información se tiene y para qué se usa, en sí, puede entrañar un riesgo significativo a los derechos de las personas.

El flujo de información puede ser representado en el formato que resulte más adecuado para la organización (un diagrama de flujo, un cuadro sinóptico, uno o varios listados) y es conveniente que la representación gráfica acompañe un informe escrito. A todo evento, es de notar que la identificación del ciclo de vida se orienta al cumplimiento de las normas en materia de protección de datos, sin perjuicio de que la EIPD pueda ser de utilidad en la consideración de otros aspectos de la vida de los datos, como en la materia de seguridad de la información.

Así pues, en términos generales, pueden identificarse las siguientes etapas en el ciclo de vida de los datos:

AGREGAR IMAGEN

Recolección

La recolección de los datos implica toda actividad de captura de datos de persona determinada o determinable para destinar a actividades de tratamiento. Esa captura de información puede provenir del propio titular de los datos o de terceros que realicen cesiones o comunicaciones.

En lo que refiere a la recolección de la información, debemos:

1. Determinar los tipos de datos recolectados con relación a la finalidad prevista.

Preguntas vinculadas: ¿Estoy recolectando estrictamente los datos que necesito en función de mi finalidad? ¿Existen finalidades conexas y compatibles que requieran de otro tipo de datos? ¿Estoy ofreciendo opciones al titular de datos para comunicar un tipo de datos personales y no otros?

2. Considerar la información provista a los titulares de los datos previo a su recolección.

Preguntas vinculadas: ¿Se informó debidamente a los titulares de los alcances de la información que se recolectará? ¿La información es clara y completa? ¿Determiné los mecanismos de ejercicio de los derechos?

3. Detallar las fuentes de los datos obtenidos.

Preguntas vinculadas: ¿Obtengo la información directamente de los titulares? En caso contrario, ¿mis fuentes son fuentes públicas de acceso irrestricto? ¿Obtengo la información de cesiones o comunicaciones, en cumplimiento de la ley local?

4. Especificar los mecanismos y personas involucradas en la recolección.

Preguntas vinculadas: ¿Por qué medios se realiza la recolección de datos? ¿Se realiza por algún mecanismo automatizado? ¿Qué empleados de la organización o eventual personal tercerizado están involucrados en el proceso de recolección?

Categorización

La categorización implica toda actividad de clasificación de la información, incorporándola en distintas categorías definidas por el tipo de dato y su finalidad. También refiere a la determinación de los potenciales vínculos de los datos capturados con otros datos, preexistentes o no, a efectos de obtener inferencias.

Distintas categorías de datos pueden ser objeto de distintas medidas de seguridad, de acuerdo a su naturaleza. En cuanto a los datos sensibles, estos deben ser tratados siempre con estricta reserva y bajo severas medidas

de seguridad.

Preguntas vinculadas: ¿Cuáles son los tipos o categorías de datos que estoy tratando? ¿Estoy tratando datos sensibles o datos relativos a antecedentes penales o contravencionales? ¿Poseo sistemas, programas o aplicaciones que relacionan múltiples datos en mi poder? ¿La categorización de los datos es manual o procede por mecanismos automáticos? ¿Quiénes intervienen en la categorización o tienen acceso a los datos ya categorizados?

Tratamiento

Tratamiento en sentido estricto hace referencia a todo tipo de gestión sobre los datos, incluyendo su almacenamiento y aplicación en sistemas de la empresa u organización, dentro de finalidades determinadas. También incluye las actividades de actualización, rectificación y disociación de la información.

En lo que refiere al almacenamiento de los datos, éste opera en relación con las categorías definidas en la etapa anterior. El tipo de dato marca las medidas de seguridad que corresponde adoptar y la eficacia de los sistemas que se pongan en práctica.

Preguntas vinculadas: ¿Implemento distintas medidas de seguridad para las diferentes categorías de datos? ¿El almacenamiento lo realizo en servidores locales o en la nube? ¿Almaceno varias copias de la información y, en ese caso, las tengo identificadas a efectos de correcciones y supresiones? ¿Puse en práctica algún sistema de contraseñas o una política de acceso a la información de los miembros de mi organización? ¿Cuento con un mecanismo sencillo y estudiado para habilitar el acceso a su información en caso de solicitudes de los titulares de los datos? ¿Y para rectificar, actualizar o suprimir la información en el plazo correspondiente? ¿Realizo operaciones de disociación de los datos? ¿Quiénes intervienen en las operaciones de tratamiento?

Por otra parte, tal como se indicó antes, el tratamiento de la información puede aplicarse para obtener mediante inferencias nueva información, en la medida en que ello sea acorde a la finalidad declarada por el responsable.

Preguntas vinculadas: ¿Cuál es la finalidad del tratamiento de datos previsto en el proyecto o en la actividad de la organización? ¿Establezco vínculos entre los datos que cuento para obtener información adicional? ¿Esa información generada también se vincula a los fines de mi organización? ¿Cómo almaceno la información resultante?

Comunicación o cesión y transferencias internacionales

La comunicación o cesión refiere a toda revelación o envío de datos personales a personas distintas del titular, en el marco de las hipótesis expresamente previstas por las normas. Por su parte, la transferencia internacional es aquella cesión o comunicación que tiene como destinatario un responsable de tratamiento ubicado en el extranjero.

Sin perjuicio de la discusión sobre los alcances de los conceptos de comunicación o cesión y de transferencia internacional, en oportunidades puede ser necesario enviar los datos a terceros a efectos de que realicen operaciones de tratamiento, que pueden abarcar desde el mero almacenamiento hasta una actividad de cobranza de morosos, entre otros servicios. En particular, la contratación de servicios en la nube es una actividad cada vez más frecuente y que involucra, en numerosas oportunidades, la ejecución de transferencias internacionales. También es posible que un responsable de tratamiento quiera vender o compartir su información con empresas asociadas o del mismo rubro, lo que es perfectamente lícito en la medida en que se cumpla con la normativa local.

A los fines de garantizar la protección de los datos, es importante contar con contratos o normas corporativas vinculantes que instrumenten salvaguardas y que delimiten las responsabilidades de los contratantes. Cuando la comunicación o cesión se produce por otras hipótesis distintas del consentimiento del titular, es importante tener presente las bases legales que lo habilitan. Es relevante determinar la legitimación del destinatario de la información, el alcance de las obligaciones, el tipo de información a comunicar o ceder, el destino de la información y los mecanismos para la eliminación de la información una vez que el contrato se cumpla.

Preguntas vinculadas: ¿Se realizan cesiones o transferencias internacionales? ¿Existe una clara delimitación de las obligaciones de una y otra parte del contrato? ¿Se define la finalidad para la cual se entregan los datos? ¿Se han determinado los tipos de datos que se enviarán a efectos de no remitir más que los necesarios para cumplir con el contrato? ¿Solicité la autorización previa de la autoridad de control o corroboré estar dentro de alguna de las bases legales que habilitan las transferencias internacionales de datos?

Eliminación

El hecho de que se conserve la información no significa que ésta deba permanecer en poder del responsable o encargado de forma indefinida. Salvo excepciones, una vez cumplida la finalidad para la que se obtuvo la información, corresponde proceder a su supresión. Asimismo, no se considera válida aquella finalidad que

justifica la conservación de datos personales a perpetuidad o por lapsos desproporcionados de tiempo. Por esta razón, el responsable debe proceder a eliminar la información de manera periódica, en plazos cuya razonabilidad ha de determinarse conforme a la naturaleza de los datos y la finalidad del tratamiento.

A este respecto, es fundamental tener en cuenta las habilitaciones especiales o previsiones específicas de la ley local que justifican la conservación, así como las excepciones al derecho de supresión. Asimismo, debe recordarse que la eliminación supone algo más que la mera eliminación del archivo, pues también requiere de una constatación de dicha eliminación, comprobando que no hayan quedado rastros de los datos en el sistema.

Preguntas vinculadas: ¿Cuáles son los motivos para mantener la información almacenada una vez agotada la finalidad del tratamiento? ¿Existe alguna norma que me habilite a conservar esa información? En caso de que no corresponda la eliminación, ¿implementé procedimientos para bloquear o disociar los datos? ¿Qué mecanismos debo emplear para eliminar la información? ¿Contabilicé las copias y respaldos de seguridad que puedan existir para asegurar la eliminación completa?

2.5 Gestión de riesgos

El objetivo de esta fase 5 es realizar un análisis de riesgo en cada una de las etapas del contexto de tratamiento definidas en la etapa anterior, para una adecuada gestión de dichos riesgos.

Una vez representado el ciclo de vida de los datos, debe procederse a iniciar la gestión de riesgos.

La gestión de riesgos es el proceso mediante el cual se identifica, analiza y valora la probabilidad e impacto de las ocurrencias de amenazas que, mediante la explotación de alguna vulnerabilidad, puedan materializar un riesgo para los derechos de las personas. El objetivo es establecer cuáles son las hipótesis de riesgo para, luego, en una etapa posterior, definir el plan de tratamiento necesario para minimizar aquellos riesgos que no se consideren aceptables.

Dado que el objetivo de la EIPD es proteger los derechos de las personas, la gestión de riesgos es inseparable del cumplimiento de la normativa vigente. En efecto, la EIPD es una herramienta que orienta al responsable para cumplir de manera acabada con las normas locales en materia de protección de datos, en particular, cuando la complejidad del proyecto o actividad de la organización impide una aplicación simplificada de la legislación local.

Es menester aclarar que la protección de los datos personales no sólo es un fin en sí mismo, sino además un medio legal para proteger otros derechos fundamentales, tales como la igualdad, el honor, la integridad psicofísica e incluso la libertad de expresión. Así pues, la EIPD debe evaluar no solo aquellos riesgos derivados de operaciones de tratamiento que afectan al derecho de protección de datos, sino también a todas aquellas que, afectando los datos personales, al mismo tiempo menoscaban otras garantías y bienes jurídicos de las personas que son igualmente relevantes.

En todos los casos, es recomendable que la gestión de riesgos utilice como insumo los informes y/o representaciones gráficas y conceptuales que resultaron de las etapas anteriores. Tanto el análisis preliminar como el ciclo de vida pueden contribuir a identificar las amenazas y vulnerabilidades existentes en el proyecto o en la actividad de la organización y servir como una base que luego ha de ser profundizada.

Asimismo, se describirán las tres etapas que conforman la gestión de riesgos: identificación del riesgo (en base a la identificación de amenazas); evaluación del riesgo; y plan de tratamiento del riesgo.

2.5.1 Identificación del riesgo

El riesgo en el marco de una EIPD es el potencial de que una amenaza dada explote vulnerabilidades y, por lo tanto, afecte datos personales y produzca un perjuicio a los derechos de alguna persona. En otras palabras, es el daño probable que puede producirse como resultado de una operación de tratamiento de datos y que afecta algún derecho del titular de los datos.

2.5.2 Evaluación del riesgo

La fórmula más popular y aceptada para la evaluación de riesgos es:

AGREGAR IMAGEN

Donde la probabilidad se determina en base a las posibilidades que existen de que la amenaza se materialice; y el impacto se determina en base a los daños que se pueden producir si la amenaza se materializa. En este último caso, se ha considerado una valoración de los impactos desde la perspectiva material y moral, de forma de facilitar la comprensión de cada uno de los impactos propuestos.

La fórmula es una ponderación derivada de la relevancia asignada al impacto por sobre la probabilidad de su acaecimiento. Las escalas utilizadas para la medición de probabilidad de impacto pueden ser diseñadas por cada organización. Sin perjuicio de ello, a continuación, se brinda un ejemplo de escala.

AGREGAR TABLAS

La organización deberá calcular el riesgo inherente y el riesgo residual. El cálculo del riesgo inherente se realiza sin tener en cuenta los controles ya aplicados. Por el contrario, el riesgo residual se calcula teniendo en cuenta los controles actualmente implementados en la organización. Esta práctica, entre otras cosas, nos permitirá medir la eficacia de los controles actualmente implementados, permitiendo su evaluación o mejora para el tratamiento de los riesgos.

Aquellos riesgos residuales que den por encima de 7, o sea, que están en rojo, deberán desarrollar un plan de tratamiento de riesgos. Los que estén entre 3 y 6 deberán justificar, mediante indicadores, la eficacia de los controles existentes.

2.6 Plan de tratamiento de riesgos

El objetivo de esta fase 6 es realizar un adecuado plan de tratamiento de los riesgos determinados en la etapa anterior. Toda EIPD supone, además, conocer los presupuestos habilitantes para un tratamiento lícito y que, por tanto, cumple con la normativa vigente. Debe recordarse que la EIPD es una herramienta que orienta al responsable para cumplir de manera acabada con las normas locales en materia de protección de datos, en particular, cuando la complejidad del proyecto o actividad de la organización impide una aplicación simple de la legislación local.

En esta etapa, la organización debe planificar las acciones que llevará a cabo para mitigar o eliminar los riesgos que fueron identificados previamente. A este respecto, debe recordarse que no siempre es posible suprimir el impacto derivado del tratamiento de datos y que, muchas veces, la EIPD solo permitirá reducir dicho impacto a un nivel bajo. En otras ocasiones, dada la finalidad o la estructura del proyecto o actividad bajo análisis, la mitigación del riesgo puede resultar igualmente imposible, por lo que en tales instancias la organización deberá discontinuar su iniciativa.

Cuando una organización está evaluando soluciones, debe considerar, en qué medida el impacto en los derechos de las personas es proporcional a los fines del proyecto y cómo podría alcanzar los mismos objetivos a través de medios menos riesgosos para los derechos de las personas. Hay muchas y muy diversas medidas que las organizaciones pueden tomar para reducir riesgos identificados en la EIPD. Algunas de las más frecuentes son:

- No recolectar o almacenar algún tipo de dato personal.
- No recolectar o almacenar datos sensibles.
- Monitorear o limitar la toma de decisiones automatizada cuando esta se funde en el tratamiento de datos personales.
- Otorgar al titular de datos la posibilidad de gestionar preferencias en la entrega de su información, permitiéndole entregar categorías de datos de manera discriminada.
- Implementar períodos razonables de conservación de los datos y mecanismos seguros para la destrucción de información.
- Implementar medidas adecuadas de seguridad de la información.
- Capacitar al personal en materia de protección de datos y concientizarlo respecto de los riesgos involucrados en las operaciones de tratamiento.
- Contratar un delegado de protección de datos que le dé seguimiento al proyecto o actividad bajo análisis.
- Establecer pactos de confidencialidad con el personal que desalienten la difusión no autorizada de información. Implementar técnicas de disociación de datos cuando sea posible.
- Producir códigos de procedimiento que enseñen cómo compartir información dentro de la organización.
- Diseñar sistemas que permitan el fácil acceso a la información por parte de los titulares de datos, así como plataformas que hagan más sencillo atender y contestar a los requerimientos de rectificación y supresión.
- Estableciendo una política de privacidad que informe exhaustivamente a los titulares de datos cómo se utilizará su información y a quién deben y pueden contactar en caso de algún reclamo.
- Vinculándose con encargados de tratamiento que garanticen la seguridad de la información e implementando contratos robustos tendientes a ese fin.
- Desarrollando contratos de cesión de datos que esclarezcan qué información será compartida, cómo será compartida y con quiénes será compartida.
- Instrumentando contratos de transferencia internacional con salvaguardas efectivas de protección de datos.

Más allá de los ejemplos anteriores, en la práctica de la gestión de riesgos se suele considerar que existen por lo menos tres maneras amplias de tratar los riesgos, que son las siguientes:

- Aceptando el riesgo: el riesgo se encuentra en un nivel aceptable o por razones justificadas se opta por asumirlo.
- Transfiriendo el riesgo: trasladar el riesgo a alguien más, por ejemplo, mediante la contratación de un seguro.
- Mitigando el riesgo: implementación de nuevos controles o mejoramiento de los existentes para llevar el riesgo a un valor aceptable. Estos controles podrán influir sobre la probabilidad de ocurrencia, o sobre el impacto que tiene el riesgo para la organización.

En todos los casos, el plan de tratamiento de riesgos deberá detallar (al menos) para cada riesgo identificado:

- Control a implementar, detallando las medidas a implementar
- Responsable de su implementación
- Plazo de implementación

Los riesgos y las soluciones deben quedar registradas en un informe. Tal informe debe reflejar cómo las medidas propuestas por la organización disminuyen o suprimen los riesgos detectados.

Cuando una organización acepta determinados riesgos, debe explicar por qué ha tomado esa decisión y qué impide llevar adelante alguna acción al respecto. ha llegado a dicha conclusión.

Capítulo 3. Etapas posteriores

a. Informe final

Tal como se ha expuesto hasta aquí, la EIPD es un proceso de identificación y minimización de riesgos. Pero, al mismo tiempo, la EIPD es un procedimiento que tiene como finalidad el cumplimiento de la normativa vigente en materia de protección de datos y que, en tal sentido, debe poder ser informado a la autoridad de control, en el caso de que esta la requiera o así lo disponga la normativa local. Es por eso que en cada etapa del proceso se insta al responsable a realizar informes parciales, que luego puedan ser integrados en un informe final que describa las acciones previstas y los resultados alcanzados.

Así pues, es importante registrar y dar cuenta del proceso de la EIPD de manera exhaustiva y auditable. A los fines de aumentar incluso más la transparencia de las actividades de tratamiento, se recomienda al responsable publicar el informe final en su plataforma online, si la tuviera, o a facilitarlo si algún ciudadano lo requiriese. Sin perjuicio de lo expuesto, se reconoce que esta es una buena práctica que puede encontrar sus limitaciones en la protección de intereses comerciales, de seguridad o marcarios.

b. Ejecución del plan de acción

Los resultados de la EIPD deben incorporarse en la gestión del proyecto o en la gestión habitual de las actividades de la organización que hayan sido objeto de análisis. Como es evidente, esto debe realizarse a través del establecimiento de objetivos y plazos razonables, así como de capacitaciones del personal involucrado. Las organizaciones deben supervisar la ejecución del plan de acción de modo que aseguren que las medidas previstas se estén implementando adecuadamente y tengan el efecto buscado. Si la actividad o proyecto en curso son modificados sustancialmente, puede ser necesario revisar la vigencia de la EIPD realizada.