Módulo Evaluación de riesgo

Introducción

Tal como se trató en el módulo "Plan de protección de datos personales", las actividades de tratamiento llevadas a cabo en una organización pueden implicar riesgos para los derechos y libertades de las personas.

En este contexto**, es importante que los responsables de tratamiento identifiquen -desde instancias tempranas- los posibles riesgos de afectación a derechos de personas en las prácticas y proyectos que llevan adelante en sus actividades habituales**, de acuerdo con la naturaleza, contexto, el alcance y los fines de cada tratamiento de datos de los que es responsable.

Una vez representado el ciclo de vida de los datos, debe iniciarse la gestión de riesgos. Por lo que, resulta importante que se evalúen los riesgos que un tratamiento de datos personales podría implicar.

A este fin, es recomendable que las organizaciones lleven adelante una evaluación de impacto, con el objeto de gestionar los potenciales riesgos, posibilitando la **integración de mecanismos de privacidad por diseño y por defecto desde una etapa temprana.**

Es dable destacar que oportunamente, la Agencia de Acceso a la Información Pública Argentina (AAIP) y la Unidad Reguladora y de Control de Datos Personales de Uruguay, publicaron una **Guía "Evaluación de Impacto en la Protección de Datos",** con conceptos fundamentales y ejemplos para orientar a los responsables de tratamiento de datos personales.

Se hace notar que, por cuestiones de extensión, el presente documento sólo repasará brevemente algunos de los principales aspectos de la mentada Guía, recomendándose a las organizaciones su consulta pormenorizada.

Metodología para la Evaluación de Impacto

Un aspecto relevante a tener en cuenta en todos los casos es la determinación en forma anticipada de los **participantes** en la Evaluación de Impacto, **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 Evaluación de impacto.**

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

Esta etapa supone, además, analizar la **normativa aplicable** al tratamiento realizado para comprender su aplicación a las distintas etapas de dicho tratamiento y si del análisis surge su cumplimiento efectivo.

Ejemplo de análisis preliminar -normativa aplicable

Un tratamiento que puede conllevar riesgos para los titulares de datos, es la realización de **transferencias de datos personales fuera del territorio nacional -incluidas las transferencias ulteriores-** que no garanticen una protección de la privacidad equivalente a la proporcionada por nuestro país. Lo anterior, por ejemplo, en cuanto al ejercicio de derechos de las personas, obligaciones a cargo, principios aplicables, entre otros.

Por tanto, una primera pregunta que su organización debe hacerse es **¿realizo transferencias internacionales de datos personales?** En caso **afirmativo**, una segunda pregunta a realizarse es **¿bajo qué mecanismos se realizan estas transferencias?**

En este punto es importante destacar que, en la actualidad, por regla general, las transferencias internacionales de datos personales de cualquier tipo a países u organismos internacionales o supranacionales, se encuentran prohibidas. No obstante, existen 3 (tres) mecanismos que bajo ciertas condiciones habilita el flujo transfronterizo de datos personales:

1. **Mediante una decisión de adecuación**: si su organización realiza transferencia de datos personales, debe tener en cuenta si el país destino proporciona niveles de protección adecuados.

¿Cuáles son los países considerados adecuados actualmente por la AAIP? Los países enumerados en la Disposición Nro. 60. Es decir que, si su organización realiza una transferencia a alguno de los países allí listados, la transferencia se encuentra habilitada.

2. A través de mecanismos que permitan ofrecer garantías adecuadas mediante normas de autorregulación o cláusulas contractuales:

Las organizaciones que deseen realizar transferencias internacionales de datos personales **a países sin legislación adecuada**, deberán implementar normas de autorregulación o cláusulas contractuales, que brinden una protección similar a la normativa nacional de protección de datos personales.

En este sentido, una organización deberá adoptar los modelos de Cláusulas contractuales para la cesión y/o prestación de servicios dispuestos por la AAIP mediante Disposición Nro. 60.

Mientras que, las empresas que conforman un mismo grupo económico deberán seguir los lineamientos y contenidos básicos de normas corporativas vinculantes, determinados en la Resolución Nro. 159.

3. Mediante excepciones habilitantes:

a) Que la persona Titular de los datos haya otorgado su consentimiento;

b) Que la transferencia sea necesaria para la ejecución de un contrato entre la persona Titular de los datos y el Responsable de tratamiento o para la ejecución de medidas precontractuales adoptadas a solicitud de la persona Titular de los datos;

c) Que la transferencia sea necesaria:

I) Por razones de interés público;

II) Para el reconocimiento, ejercicio o defensa de un derecho en un proceso judicial;

III) Para proteger la vida de la persona Titular de los datos o de otras personas, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos de la persona Titular de los datos y esta se encontrara imposibilitada de otorgar su consentimiento por sí o por sus representantes

Por último, es fundamental que se implementen medidas para garantizar cabalmente los derechos de los Titulares de datos y se responda frente a eventuales vulneraciones.

Se debe tener presente que, para demostrar ante la AAIP que la transferencia internacional fue realizada de manera apropiada, **la carga de la prueba recaerá, en todos los casos, en la organización responsable de tratamiento en su carácter de exportadora.**

Evaluación de Impacto relativa a la protección de datos

En primer lugar, **es conveniente aclarar que la Ley Nacional de Protección de Datos Personales vigente Nro. 25.326 no contempla el concepto de Evaluación de Impacto, mientras que el Proyecto de Actualización de Ley lo incorpora explícitamente** y, en ciertos casos, establece su obligatoriedad.

En este punto es conveniente señalar que, oportunamente, la Agencia de Acceso a la Información Pública Argentina (AAIP) y la Unidad Reguladora y de Control de Datos Personales de Uruguay, publicaron la Guía "Evaluación de Impacto en la Protección de Datos". Si bien el presente documento tratará brevemente algunos de sus principales temas, se recomienda su consulta pormenorizada.

En esta línea, la realización de **una evaluación del impacto debe implementarse de manera previa** en el caso que, el Responsable de tratamiento prevea realizar algún tipo de tratamiento de datos que, por su naturaleza, alcance, contexto o finalidades, entrañe un alto riesgo de afectación a las personas Titulares de datos.

Los riesgos que sean identificados en el proceso deben evaluarse tanto en una dimensión individual como en una dimensión comunitaria. Se destaca en este punto que 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.

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.

Se aclara que **la Evaluación de impacto no está concebida únicamente para las grandes organizaciones** que producen un impacto ostensible en la comunidad, sino también para los startups de tecnología y otras pequeñas empresas que, por la especificidad de sus emprendimientos o por el volumen de datos que traten, generen o puedan generar en el futuro un impacto en los datos personales de la ciudadanía. En todos los casos, **la Evaluación es un proceso que genera valor para la organización que la lleva adelante.**

Esta evaluación es obligatoria según el Proyecto de Ley, sin perjuicio de otros que establezca la Autoridad de Aplicación, en los siguientes casos:

A. Evaluación sistemática y exhaustiva de aspectos personales de personas humanas que se base en un tratamiento de datos automatizado y semiautomatizado, como la elaboración de perfiles, y sobre cuya base se tomen decisiones que produzcan efectos jurídicos para las personas humanas o que las afecten significativamente;
B. Tratamiento de datos sensibles a gran escala, o de datos relativos a antecedentes penales y contravencionales;
C. Observación sistemática a gran escala de una zona de acceso público.

La evaluación debe incluir, como mínimo:

A. Una descripción sistemática de las operaciones de tratamiento de datos previstas y de los fines del tratamiento, incluyendo, cuando proceda, el interés legítimo perseguido por el Responsable de tratamiento;
B. Una evaluación de la necesidad y la proporcionalidad de las operaciones de tratamiento de datos con respecto a su finalidad;
C. Una evaluación de los riesgos para la protección de los datos personales de las personas
D. Las medidas previstas para afrontar los riesgos, incluidas garantías, medidas de seguridad y mecanismos que garanticen la protección de los datos personales, teniendo en cuenta los derechos e intereses legítimos de los Titulares de los datos y de otras personas que pudieran verse potencialmente afectadas.

Cuando una evaluación de impacto evidencie que el tratamiento entraña un alto riesgo, el Responsable de tratamiento debe informar de esta circunstancia a la Autoridad de Aplicación.

El informe debe incluir, como mínimo:

A. Las obligaciones respectivas del Responsable y Encargado de tratamiento, en particular en caso de tratamiento de datos dentro de un mismo Grupo económico;
B. Los fines y medios del tratamiento previsto;
C. Las medidas y garantías establecidas para minimizar los riesgos identificados y proteger los derechos de los Titulares de los datos;
D. En su caso, los datos de contacto del Delegado de Protección de Datos;
E. La evaluación de impacto relativa a la protección de datos;
F. Cualquier otra información que solicite la Autoridad de Aplicación.

El Responsable de tratamiento no podrá iniciar el tratamiento de datos hasta tanto la Autoridad de Aplicación se pronuncie sobre el informe.

Tal como se ha expuesto, la Evaluación es un proceso de identificación y minimización de riesgos, pero, al mismo tiempo, 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 lo requiera.

Es por eso por lo 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.

Protección de datos desde el diseño y por defecto

En cuanto a la **protección de datos desde el diseño**, se refiere a que es preciso que el responsable de tratamiento deba, desde el diseño y antes del tratamiento, prever y aplicar medidas tecnológicas y organizativas apropiadas para cumplir los principios y garantizar los derechos de las personas titulares de los datos establecidos en esta Ley.

Las medidas deben ser adoptadas teniendo en cuenta el estado de la tecnología, los costos de la implementación y la naturaleza, ámbito, contexto y fines del tratamiento de los datos, así como los riesgos que entraña el tratamiento para el derecho a la protección de los datos de sus titulares.

En relación con **la protección de datos por defecto**, se entiende que se deben aplicar las medidas tecnológicas y organizativas apropiadas con miras a garantizar que, por defecto, solo sean objeto de tratamiento aquellos datos personales que sean necesarios para cada uno de los fines del tratamiento. Esta obligación se aplica a la cantidad, calidad y categoría de datos personales tratados, al alcance de su tratamiento, a su plazo de conservación y a su accesibilidad.

Tales medidas deben garantizar que, por defecto, los datos personales no sean accesibles, sin la intervención de la persona titular de los datos, a un número indeterminado de personas humanas.

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.

A continuación, 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.

1. Identificación del riesgo

El riesgo 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. Evaluación del riesgo

La fórmula más popular y aceptada para la evaluación de riesgos es: **Riesgos = Probabilidad x impacto.**

La probabilidad se determina en base a las posibilidades que existen de que la amenaza se materialice, por ejemplo, Baja, Media, Alta y Muy alta.

El impacto se determina en base a los daños que se pueden producir si la amenaza se materializa, pudiendo ser este Bajo, Medio, Alto y Crítico.

La valoración de los impactos puede realizarse desde la perspectiva material y moral.

Las escalas utilizadas para la medición de probabilidad de impacto pueden ser diseñadas por cada organización.

Por ejemplo, un impacto alto puede ser cuando los titulares de datos son afectados de manera significativa y solo podrían superar la situación con grandes dificultades.

Tal como fue definido en la Guía "Evaluación de Impacto en la Protección de Datos", algunos ejemplos de **impacto material Alto** son:

A. Adjudicación errónea del dinero del titular de datos a otra persona sin compensación.
B. Dificultades financieras a medio o largo plazo.
C. Pérdida de oportunidades únicas, no recurrentes.
D. Pérdida del trabajo.
E. Daño a la propiedad.
F. Pérdida financiera como resultado de un fraude.

Mientras que algunos ejemplos de **impacto moral Alto** son:

A. Daños psicológicos serios (depresión, paranoia, desarrollo de una fobia).
B. Sensación de invasión de la privacidad con daño irreversible.
C. Sensación de vulnerabilidad por tener que intervenir en un procedimiento judicial.
D. Sensación de violación de los derechos fundamentales (discriminación, libertad de expresión)
E. de expresión).
F. Sufrimiento de extorsiones
G. Cyberbullying y acoso.

En este punto, se resalta que, si se combina la probabilidad y el impacto, se obtendrá una **matriz de riesgos**, que dará cuenta de qué riesgos necesitan un tratamiento y una protección reforzada, cuáles se deben vigilar y cuales no presentan un riesgo significativo para la organización.

Con este semáforo podremos determinar qué riesgos necesitan, indiscutidamente, un tratamiento (rojo), cuales debemos vigilar (amarillo) y cuales no presentan un riesgo significativo para la organización (verde).

3. Plan de tratamiento de riesgos

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

En particular, se hace hincapié en que, 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.**

Por ejemplo, en todos los casos, el plan de tratamiento de riesgos debería detallar (al menos) para cada riesgo identificado:

A. Control a implementar, detallando las medidas a implementar
B. Responsable de su implementación
C. Plazo de implementación

Algunas de las medidas más frecuentes son:

A. Implementar períodos razonables de conservación de los datos y mecanismos seguros para la destrucción de información.
B. Implementar medidas adecuadas de seguridad de la información.

C. Capacitar al personal en materia de protección de datos y concientizarlo respecto de los riesgos involucrados en las operaciones de tratamiento.
D. Contratar un delegado de protección de datos que le dé seguimiento al proyecto o actividad bajo análisis.
E. Establecer pactos de confidencialidad con el personal que desalienten la difusión no autorizada de información.
F. Implementar técnicas de disociación de datos cuando sea posible.
G. Producir códigos de procedimiento que enseñen cómo compartir información dentro de la organización.
H. Desarrollar contratos de cesión de datos que esclarezcan qué información será compartida, cómo será compartida y con quiénes será compartida.
I. Instrumentando contratos de transferencia internacional con salvaguardas efectivas de protección de datos.

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

A. Control a implementar: detallando las medidas a implementar Responsable de su implementación
B. Plazo de implementación: Los riesgos y las soluciones deben quedar registradas en un informe.

Informe final

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.

Es por esto que se insta al responsable de tratamiento a realizar informes parciales en cada etapa del proceso para luego poder ser integrados en un informe final que describa las acciones previstas y los resultados alcanzados. En este sentido, es importante registrar y dar cuenta del proceso de la Evaluación de manera exhaustiva y auditable.

Ejecución del plan de acción

Por último, **es relevante que los resultados de la Evaluación se incorporen en la gestión del proyecto** o en la gestión habitual de las actividades de la organización que hayan sido objeto de análisis. 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 Evaluación de impacto realizada.