Plan de Protección de Datos Personales

(Plan de PDP, Área de PDP, Responsabilidad Proactiva y Demostrada, Canal ético, Compromiso Alta Dirección)

Introducción

El **objetivo** de esta herramienta está destinada a **brindar recursos y orientación a organizaciones para acompañarlos en la implementación de un Plan de Protección de Datos Personales**, buenas prácticas que se recomiendan implementar.

En esta sección, se reforzarán algunos aspectos fundamentales, así como las pautas principales para su desarrollo y ejecución.

Cabe resaltar que **este Plan promueve una cultura de privacidad en las organizaciones**, conteniendo una descripción de los estándares más altos en materia de protección de datos personales a nivel nacional.

En conexión con lo anterior, es conveniente aclarar que, el presente Plan da cuenta de los conceptos sentados tanto en la Ley Nacional vigente de Protección de Datos Personales Nro. 25.326, su normativa complementaria, como así también describe algunos conceptos receptados en el Proyecto de Ley remitido al Congreso de la Nación (Mensaje Nro. 87/2023).

Por último, se aclara que este documento sólo hará hincapié en conceptos y lineamientos principales de la regulación, siendo necesario que toda organización consulte en detalle la normativa, glosario e instructivos aplicables.

I. Conceptos preliminares *("¿Su organización trata datos personales? ¿Qué rol desempeña en el tratamiento de datos personales?")*

En primer lugar, **es importante comenzar definiendo algunos conceptos preliminares**.

No todos los datos son datos personales. Cuando hacemos alusión a **datos personales**, nos referimos a información que identifica a personas humanas o bien, información que pueda llegar a identificarlas. En otras palabras, un dato personal **consiste en todo dato que identifica directa o indirectamente a una persona por uno o varios elementos característicos de su identidad**, como por ejemplo su domicilio, profesión, teléfono, situación crediticia, otros.

En particular, una organización en el marco de los propósitos que hacen a su actividad puede ser que tenga que realizar tratamiento de los datos personales de sus empleados, proveedores, clientes/usuarios. Es por esto por lo que, en este contexto, podría **realizar tratamiento de múltiples categorías de datos personales**, tales como datos

identificatorios, características personales, datos académicos y/o profesionales, datos laborales, comerciales y financieros.

En este punto, es importante destacar que existe una categoría de datos que requieren una protección reforzada: los **datos sensibles**. Estos **son datos que están especialmente protegidos por la normativa porque hacen a la esfera íntima de la persona** y que su uso indebido puede implicar riesgos graves, ya que poseen potencialidad discriminatoria.

Algunos ejemplos de esta categoría de datos son aquellos que puedan revelar aspectos como origen étnico; creencias o convicciones religiosas, filosóficas y morales, afiliación sindical u opiniones políticas, salud, discapacidad, orientación sexual, identidad de género, datos genéticos o biométricos. Son considerados datos sensibles cuando puedan revelar datos adicionales cuyo uso pueda resultar, como hemos dicho, potencialmente discriminatorio para la persona y que estén dirigidos a identificarla de manera unívoca.

Por estas razones, **en el tratamiento de datos sensibles, se debe implementar una responsabilidad reforzada que implica**, por ejemplo, mayores niveles de seguridad, confidencialidad, restricciones de acceso, uso y circulación.

Ahora bien, **¿qué debe entenderse por tratamiento de datos personales?** Este refiere a cualquier operación que permita el procesamiento de datos personales, como por ejemplo si su organización recolecta, almacena y realiza cesiones de datos personales. Hacemos notar que este tratamiento puede ser automatizado, parcialmente automatizado o no automatizado.

Por su parte, **una base de datos es un conjunto de datos vinculados a personas determinadas o determinables** (cualquiera sea la forma, modalidad de creación, almacenamiento, organización, tipo de soporte, localización o acceso, centralizado, descentralizado o repartido de forma funcional o geográfica), **que puede consistir en un archivo, registro, fichero o banco de datos**.

Teniendo esto en claro, es conveniente pasar a determinar **el rol que desempeña una organización en el tratamiento que hace de estos datos personales**, para poder entender la responsabilidad que le cabe en materia de cumplimiento con la normativa de protección de datos personales.

Cabe recordar que, **el responsable de tratamiento es la persona u organización que define para qué y cómo se van a tratar los datos**, la finalidad y otras cuestiones vinculadas con el tratamiento de los datos personales. Mientras que **el encargado de tratamiento** suele ser un tercero externo a la organización, **que únicamente actúa por cuenta del responsable del tratamiento**.

Es necesario resaltar **que la relación entre ambos, es decir las obligaciones del encargado del tratamiento con respecto al responsable, deberán ser especificadas**

mediante un contrato[1]. Corresponde al encargado de tratamiento, obligaciones como aplicar seguridad a los datos, devolverlos o destruirlos cuando acabe el servicio, entre otros.

En síntesis, en relación con todos los conceptos tratados en esta sección, se debe tener presente que, si su organización es responsable de tratamiento y posee bases que contienen datos personales que permitan obtener información sobre personas, es recomendable que implemente un Plan de Protección de Datos Personales. Esto a fines de implementar esto como buena práctica que le será de suma utilidad para demostrar el cumplimiento de sus obligaciones ante la Agencia de Acceso de Información Pública (AAIP), autoridad nacional de control en materia de privacidad y protección de datos personales.

II. Registro de Bases de Datos Personales

Siguiendo con los conceptos definidos en el apartado anterior**, los archivos y bases de datos que permitan obtener información sobre las personas deben estar inscriptos en el Registro Nacional de Bases de Datos**, conforme al artículo 21 de la Ley 25.326. Incumplir con esta obligación puede ocasionar sanciones.

Al respecto se resalta que, las bases de datos de uso exclusivamente personal están exceptuadas de la obligación de inscripción, por ejemplo: direcciones de amistades en computadoras personales, agendas, etc. En la misma línea, cabe mencionar que existen diversos tipos de bases de datos dentro del ámbito privado que pueden ser fácilmente identificables, a saber:

- *Base de datos de clientes*: con esta base de datos se llevan a cabo diversas cesiones de datos personales como la emisión de facturación, se realizan retenciones y liquidaciones a AFIP, IIBB, se puede informar morosidad.
- *Base de datos de proveedores*: se desarrollan diversas cesiones de datos personales como las retenciones de tributos, emisión de recibos, informaciones a las cámaras, en suma, una serie de cesiones de información que exceden el uso personal de la base.
- *Base de datos de personal:* se producen cesiones de información cuando se liquidan cargas sociales a ANSES, impuesto a las ganancias a AFIP, se transfiere información al banco para depositar el sueldo, a la ART (implica cesión de datos

[1] Los contratos previstos deben estipular el objeto, alcance, contenido, duración, naturaleza y finalidad del tratamiento de datos, el tipo de datos personales, las categorías de los datos, el cumplimiento del deber de confidencialidad y demás obligaciones y responsabilidades del Responsable y del Encargado de tratamiento.

sensibles, art. 7º, Ley Nro. 25.326), al sindicato si el empleado se encuentra afiliado (implica cesión de datos sensibles, art. 7º, Ley Nro. 25.326).

La inscripción del responsable es requisito previo para registrar una base de datos personal. Para inscribir a una persona física o jurídica como responsable de bases de datos personales, deberá acceder con su clave fiscal de la AFIP o bien, apoderar a una persona física en la plataforma Trámites a Distancia (TAD). Por ejemplo, la AAIP se encuentra registrada como responsable de las bases de datos personales que administra.

Para contar con mayores detalles sobre cómo avanzar con este trámite, es posible consultar los instructivos que se acompañan a la presente herramienta sobre responsables y bases de datos.

En este mismo orden de cosas, hay que mencionar a las **bases de extranjeros**. Dentro de la AAIP **se habilitó el Registro de Responsables de Bases de Datos Personales que no se encuentren establecidos en el territorio de la República Argentina**. Si se desea realizar esta inscripción, podrá encontrar un formulario web en la página de la AAIP para que las empresas y organizaciones extranjeras que procesan bases de datos personales de argentinos en carácter de responsables de tratamiento, procedan a inscribirse al mencionado registro. El mencionado formulario reviste el carácter de Declaración Jurada y que exige brindar información del Responsable Extranjero. Asimismo, la registración requiere determinar un autorizado o apoderado para la realización del trámite, y acreditar dicha personería, además de brindar sus datos de contacto a los fines del registro del Responsable. Posterior al envío de la información requerida, la AAIP caratúla la solicitud mediante el sistema de Gestión Documental Electrónica (GDE) y notifica al interesado del número de expediente a través del cual se comenzará a tramitar su inscripción.

III. Plan de protección de datos personales (PDP) *("¿La organización tiene un plan de protección de datos personales? ¿La política de privacidad informa los derechos que tienen los titulares de los datos?" "Responsabilidad Proactiva y Demostrada")*

Un plan de protección de datos personales es una perspectiva integral de resguardo a la privacidad. Éste incluye todas las medidas técnicas y organizacionales adoptadas por la organización para garantizar el derecho de las personas/clientes/usuarios a la protección de sus datos personales, que incluye hasta la protección de los datos personales de los propios integrantes de la empresa.

Ahora bien, la primera pregunta que una organización debe hacerse para confeccionar un Plan de protección de datos personales es **¿con qué finalidad uso los datos que recolecto, proceso y, en su caso, conservo?** Para este propósito, es clave que se

identifiquen las bases de datos, los flujos de la información, como así también, finalidades asociadas y las bases legales para cada tratamiento de datos que se realice.

¿De qué modo se encuentran legitimada la organización para realizar el tratamiento de datos personas? Las bases legitimadoras de tratamiento son básicamente las razones que hacen que el tratamiento que lleva a cabo la organización sea legítimo. Por tanto, el tratamiento de datos personales solo puede realizarse si se cumple al menos una de las siguientes bases legales:

A. **El consentimiento otorgado por el Titular del dato para uno o varios fines específicos.** Este **debe ser previo a la recolección** de datos, **debe ser expreso** (la persona debe exteriorizar su voluntad con una clara acción positiva), **debe ser libre** (la persona debe tener la opción de negarse a otorgar su consentimiento), **debe ser específico** (el titular debe otorgar su consentimiento para cada finalidad) **y debe ser inequívoco** (no debe prestar dudas sobre el alcance de la autorización prestada);
B. Que el tratamiento sea necesario para el cumplimiento de una obligación legal de la organización (obligaciones previstas por ley, como por ejemplo obligaciones impositivas, fiscales, laborales, otras);
C. Que sea necesario para la ejecución de un contrato o bien, para la aplicación de medidas precontractuales (estos datos son recabados, requeridos o proporcionados para permitir el normal desenvolvimiento de las relaciones allí acordadas). Por ejemplo, el caso de un usuario que contrató un servicio y la empresa sin el procesamiento de su información personal, no podría prestarlo
D. Que sea necesario para salvaguardar la vida de la persona Titular de los datos o de terceros, siempre que sobre dichos intereses no prevalezcan los intereses o los derechos de la persona Titular de los datos;
E. O bien, que sea necesario para la satisfacción del interés legítimo del Responsable de tratamiento, siempre que sobre dicho interés no prevalezcan los intereses o los derechos de la persona Titular de los datos (se deberá fundamentar la existencia de un interés legítimo que justifique la necesidad del tratamiento de datos personales realizándose un análisis detallado, previo y documentado, que incluya el contexto y las circunstancias en las que se llevará a cabo el tratamiento y el nivel de riesgo que implica).

En este punto, es importante señalar que conforme la Ley Nro. 25.326 el tratamiento de datos personales por parte de una organización es considerado ilícito cuando el titular no hubiere prestado su consentimiento, excepto en los siguientes supuestos:

A. Los datos se obtengan de fuentes de acceso público e irrestricto (art. 5, inc. 2 a, Ley 25.326), información cuya consulta puede ser realizada en principio por cualquier persona. Algunos ejemplos de fuentes de acceso público son: diarios, boletines oficiales y medios de comunicación.
B. Se trate de listados cuyos datos se limiten a los datos contenidos en el art. 5 inc. 2 c de la Ley 25.326 (datos que se limitan a nombre, documento nacional de identidad, identificación tributaria o previsional, ocupación, fecha de nacimiento y domicilio).
C. Se trate de las operaciones que realicen las entidades financieras y de las informaciones que reciban de sus clientes conforme las disposiciones del artículo 39 de la Ley 21.526 (datos derivados de operaciones que realizan entidades financieras).

En cuanto a las finalidades de tratamiento, se subraya que, los datos objeto de tratamiento no pueden ser utilizados para finalidades distintas o incompatibles con aquellas que motivaron su obtención (**principio finalidad**) o en caso de existir nuevas finalidades, se debe contar con bases legales en relación con estos nuevos propósitos.

Los datos deben ser limitados a lo necesario en relación con los fines para los que fueron recolectados (**principio de minimización**). Del mismo modo, el tratamiento debe acotarse sobre la base de criterios expresos de **proporcionalidad y razonabilidad**.

En relación con lo anterior, otra pregunta relevante es **¿por cuánto tiempo se conservan los datos?** Los datos no deben ser mantenidos más allá del tiempo necesario para la finalidad del tratamiento, salvo que exista una obligación legal para conservarlos por más tiempo. El plazo de caducidad debe estar determinado. Se debe proceder a una eliminación adecuada, segura y permanente (**principio de conservación**)

Otro aspecto central en un Plan de Protección de Datos es preguntarse si el Responsable y, en su caso, el Encargado de **tratamiento ¿implementan medidas de seguridad y confidencialidad?** (**principio de seguridad**). A tal efecto, **el Responsable y el Encargado de tratamiento deben adoptar las medidas técnicas, organizativas** y de cualquier otra naturaleza que resulten apropiadas **para garantizar la seguridad y confidencialidad de los datos personales, para evitar su adulteración, pérdida, uso, consulta o tratamiento no autorizado, y que permitan detectar desviaciones**, intencionales o no, de información, ya sea que los riesgos provengan de la acción humana o del medio técnico utilizado.

En tal sentido, **se deben adoptar las medidas de seguridad aplicables a los datos personales que trate** y considerar distintos factores como, por ejemplo, el riesgo inherente por el tipo de dato personal; el carácter sensible de los datos personales tratados; las posibles consecuencias de un incidente de seguridad para las personas Titulares de los datos, entre otros.

Algunos ejemplos de medidas técnicas y organizativas que las empresas y entidades deben implementar son: robustos sistemas de seguridad de la información, cifrado de datos, auditorías periódicas, copias de seguridad, políticas de seguridad, actualizaciones de software. También, la implementación de Sistemas de autenticación, control de acceso, establecimiento de políticas de privacidad y confidencialidad, entre otras.

Se hace notar que, **ante la ocurrencia de un incidente de seguridad, se recomienda que el responsable de tratamiento lo notifique a la AAIP, dentro de las SETENTA Y DOS (72) horas de haber tomado conocimiento de aquel e informar a la persona Titular** de los datos sobre el incidente ocurrido, en un lenguaje claro y sencillo.

Para dar cumplimiento a estas cuestiones, es importante que la organización posea manuales o políticas internas de procedimiento que indiquen el correcto tratamiento de datos personales, como así también por ejemplo se lleven a cabo convenios específicos

de confidencialidad con el personal que accede al contenido de las bases de datos de tratamiento de su organización.

Por último, es menester destacar muy especialmente dos principios incorporados en el Proyecto de Ley como: **el principio de preeminencia y el de Responsabilidad Proactiva y Demostrada.** El primero refiere a que, en caso de duda sobre la interpretación y la aplicación de la Ley, prevalecerá la más favorable a la persona Titular de los datos personales.

Mientras que, el **Principio de Responsabilidad Proactiva y Demostrada** trata sobre la diligencia del Responsable al aplicar las medidas técnicas y organizativas para garantizar que el tratamiento que lleva a cabo es conforme a la normativa aplicable y se encuentre en capacidad de demostrarlo. **Este principio exige una actitud diligente y proactiva por parte de las organizaciones frente a todos los tratamientos de datos personales llevados a cabo diariamente.** La debida diligencia es entendida como como un proceso continuo, orientado a identificar, prevenir, rendir cuentas y mitigar los impactos adversos que se pudieran ocasionar.

Las medidas para el cumplimiento de la responsabilidad proactiva deben ser efectivas y proporcionales a las finalidades del tratamiento de datos, su contexto, el tipo y categoría de datos tratados, y en atención al riesgo que el referido tratamiento pueda acarrear sobre los derechos del Titular de los datos.

Algunos ejemplos de estas medidas son:

A. La adopción de procesos internos para llevar adelante de manera efectiva las medidas de responsabilidad;
B. La implementación de procedimientos para atender el ejercicio de los derechos por parte de las personas;
C. La realización de supervisiones o auditorías, internas o externas, para controlar el cumplimiento de las medidas adoptadas; y
D. La implementación de procedimientos de evaluación de impacto.

Se destaca que el responsable de tratamiento debe ser capaz de demostrar a la Autoridad de control de qué manera da cumplimiento efectivo a las obligaciones a su cargo, como así también, cómo mitiga los impactos adversos que se pudieran ocasionar en el marco de los tratamientos que lleva a cabo.

¿Cómo se puede demostrar cumplimiento a la autoridad de control?

Con evidencia, es decir con documentación respaldatoria que dé cuenta de los tratamientos en curso realizados por la organización, y el cumplimiento de sus obligaciones vinculadas. Tal como vimos en la primera sección, un ejemplo de cumplimiento de la relación responsable-encargado de tratamiento, podría ser

demostrada a la autoridad de aplicación a través de la formalización de un contrato entre las partes que detalle las obligaciones y deberes a su cargo.

Como se verá en las siguientes secciones**, la Responsabilidad Proactiva y Demostrada es un concepto que atraviesa de manera transversal a cada principio y obligación en materia de privacidad**, razón por la que, en los próximos puntos, se tratarán ejemplos adicionales.

Por último, se hace notar que, este Principio también se encuentra relacionado con la Privacidad por diseño y por defecto, así como la realización de una Evaluación de Impacto, conceptos se encuentran desarrollados en el "Módulo de gestión de riesgos", disponible para su consulta.

IV. Política de privacidad

Es importante destacar que, **el tratamiento de datos se considerará lícito** si se realiza conforme a lo establecido en la normativa, **se considerará leal** si el Responsable de tratamiento se abstiene de tratar los datos a través de medios engañosos o fraudulentos y **se considerará transparente** si la información vinculada al tratamiento de los datos es fácilmente accesible y utiliza un lenguaje sencillo y claro (**principio de licitud, lealtad y transparencia**).

¿Qué quiere decir esto en la práctica?

Que los responsables de tratamiento previo a recabar datos personales deberán dar cumplimiento al Deber de información y al Principio de licitud, lealtad y transparencia anterior, a través de una adecuada Política de Privacidad.

Asimismo, es importante tener presente que, en caso de que se realicen cambios sustanciales en el contenido de estas políticas, los Responsables y Encargados de tratamiento deben notificar y obtener una nueva autorización para el tratamiento de los datos.

En particular, **una Política de Privacidad es un documento legal que describe cómo una organización recolecta, procesa y maneja los datos del usuario o cliente titular de datos**. Esta Política **tiene por objeto informar a los titulares de datos, en forma expresa y clara** (lenguaje claro, sencillo e idioma nacional) y es importante que sea publicada en una sección visible de su sitio web. Respecto a la información contenida en la misma podemos señalar la que se detalla a continuación:

A. Nombre o razón social, domicilio y medios electrónicos del Responsable de tratamiento; en su caso, del Delegado de Protección de Datos y, en el supuesto de los Responsables o Encargados de tratamiento no establecidos en la REPÚBLICA ARGENTINA, los de su Representante en el territorio nacional;
B. Las categorías de datos personales que serán objeto del tratamiento;
C. Las finalidades que se persiguen con el tratamiento de los datos y las bases legales de este;
D. Los derechos de la persona Titular de los datos y los medios, procedimientos y persona o área responsable para su ejercicio;
E. Toda información sobre cesiones a otros Responsables o Encargados de tratamiento;
F. Información sobre las transferencias internacionales de datos, con inclusión de países de destino, identidad y datos de contacto del destinatario, posibles riesgos asociados a las transferencias y salvaguardas aplicables, categorías de datos involucradas, finalidad y mecanismos para ejercer sus derechos;
G. El carácter obligatorio o facultativo de proporcionar los datos personales y las consecuencias de proporcionarlos, o de la negativa a hacerlo, o de hacerlo en forma incompleta o defectuosa;
H. El derecho de la persona Titular de los datos a revocar el consentimiento;
I. El plazo durante el cual se conservarán los datos personales o, si esto no es posible, los criterios utilizados para determinar este plazo;
J. La existencia o no de decisiones automatizadas o semiautomatizadas, incluida la elaboración de perfiles;
K. El derecho a presentar una denuncia, a iniciar el trámite de protección de datos personales ante la AAIP detallándose sus datos de contacto (Av. Pte. Gral. Julio A. Roca 710, piso 5 - Ciudad Autónoma de Buenos Aires) y preferiblemente un enlace a su sitio web, o a ejercer la acción de hábeas data en caso de que el Responsable o el Encargado de tratamiento incumpla con la Ley.

Asimismo, se resaltar que el titular de datos tiene derecho a revocar su consentimiento.

V. Ejercicio de derechos *("Canal ético")*

De acuerdo con la normativa vigente, se deben garantizar los siguientes derechos a los titulares de datos:

Derecho de acceso. El Titular de los datos, previa acreditación de su identidad tiene el derecho a saber si se están tratando sus datos personales y, en tal caso, a solicitar información y obtener confirmación de ello. También le asiste el derecho de acceso a sus datos, así como a conocer cualquier información relacionada con las condiciones generales y específicas de su tratamiento.

Derecho de Actualización: El titular del dato tiene derecho a solicitar que sus datos sean actualizados si éstos se han visto modificados.

Derecho de rectificación. La persona Titular de los datos tiene el derecho a obtener del Responsable de tratamiento la rectificación de sus datos personales cuando estos resulten ser inexactos, falsos, erróneos, incompletos o desactualizados.

Derecho de Supresión. el Titular de los datos tiene derecho a solicitar la supresión de sus datos personales al Responsable de tratamiento cuando ya no sean necesarios para la finalidad o cuando el titular haya revocado su consentimiento.

Es importante destacar que, a su vez, **el Proyecto Actualización de la Ley adiciona los siguientes derechos**:

Derecho de oposición. La persona Titular de los datos puede oponerse al tratamiento, o una finalidad específica de este, si no ha prestado consentimiento. El Responsable de tratamiento debe dejar de tratar los datos personales objeto de oposición, salvo que existan motivos legítimos para el tratamiento que prevalezcan sobre los derechos de la persona Titular de los datos. Por ejemplo, el titular tiene derecho a no ser objeto de una decisión que le produzca efectos jurídicos perniciosos, lo afecte de forma negativa o tengan efectos discriminatorios, basada, única o parcialmente, en el tratamiento automatizado de datos, incluida la elaboración de perfiles e inferencias.

Derecho de Limitación. El Titular de datos tiene derecho a obtener del Responsable de tratamiento la limitación del tratamiento de los datos cuando se cumpla alguna de las condiciones siguientes:

A. Si la persona Titular de los datos impugna la exactitud de los datos personales, durante un plazo que permita al Responsable de tratamiento verificar la exactitud de estos;
B. Si el tratamiento es ilícito y la persona interesada se opone a la supresión de los datos personales y solicita en su lugar la limitación de su uso;
C. Si el Responsable de tratamiento ya no necesita los datos personales para los fines del tratamiento, pero la persona interesada los necesita para la formulación, el ejercicio o la defensa de sus derechos;
D. Si la persona interesada se ha opuesto al tratamiento, mientras se verifican si los motivos legítimos del Responsable de tratamiento prevalecen sobre los de la persona interesada.

Derecho de No inferencia. derecho a no ser objeto de una decisión perjudicial o efectos discriminatorios – derecho a solicitar la revisión por una persona humana

Derecho de Portabilidad. Si se tratan datos personales, mediante medios electrónicos o automatizados, el Titular de los datos tiene derecho a obtener una copia de los datos personales que hubiere proporcionado al Responsable de tratamiento o que sean objeto de tratamiento, en un formato que le permita su ulterior utilización por parte de otro Responsable de Tratamiento y también puede solicitar que sus datos se transfieran directamente de Responsable a Responsable de tratamiento si ello fuera técnicamente posible.

Se resalta que, el Responsable de tratamiento debe responder y, en su caso, satisfacer los derechos de la persona Titular de los datos dentro de los DIEZ (10) días hábiles de haber sido intimado fehacientemente. Vencido el plazo sin que se satisfaga el pedido,

o si a juicio de la persona Titular de los datos la respuesta se estimara insuficiente, quedará expedito el trámite de protección de los datos personales ante la Autoridad de Aplicación.

En conexión con los derechos antes expuestos, es fundamental que los responsables habiliten canales de comunicación para que los titulares reclamen y ejerzan sus derechos en relación con la protección de datos personales.

A nivel interno en la organización, es deseable que existan procedimientos para que se canalicen estas consultas en tiempo y forma para dar cumplimiento a los plazos de ley. Asimismo, se resalta como buena práctica, en relación con el Principio de Responsabilidad Proactiva y Demostrada, que dichos procedimientos se encuentren documentados para el eventual supuesto que tenga que demostrarse ante la autoridad de aplicación que se ha obrado de manera diligente ante las solicitudes y/reclamos recepcionados.

VI. Área o persona encargada de la protección de datos personales

Para implementar el Plan de Protección de Datos Personal es fundamental que exista dentro de la organización un área o persona encargada de la protección de datos personales a la que se le asigne responsabilidad para dar cumplimiento a todos los deberes asociados a derechos de protección de datos y privacidad.

Se trata de una Persona u organización encargada de asesorar al Responsable o al Encargado de tratamiento sobre sus obligaciones legales en materia de protección de datos, de velar y supervisar el cumplimiento de la normativa de protección de datos personales, así como cooperar con la Autoridad de Aplicación como punto de contacto.

Se resalta que, para llevar adelante estas funciones dentro de una organización de manera adecuada, es recomendable que quien se desempeñe como responsable, reúna los requisitos de idoneidad, capacidad y conocimientos específicos para el ejercicio de sus funciones.

Es relevante mencionar que **dicha responsabilidad puede asignarse** de distintas maneras. Por ejemplo, **mediante la creación de un área de integridad/integridad sostenible o de privacidad /de protección de datos personales, o bien asignándole la responsabilidad a un área existente o a una persona en particular las funciones del Delegado de Protección de Datos (DPO).** Constituyendo un cuerpo colegiado o también es posible, mediante la contratación de un servicio especializado externo.

A tales fines, si la responsabilidad recae sobre un órgano colegiado, éste puede estar integrado por alguna persona de la Alta Dirección y si se le asignó la responsabilidad a una persona, ésta podría llevar sus funciones bajo la figura de Delegado de Protección de Datos Personales

Se hace notar que, el Responsable de tratamiento está obligado a respaldar al Delegado de Protección de Datos o al área designada en el desempeño de sus funciones, como así también a facilitarle los recursos necesarios para su desempeño y para el mantenimiento de sus conocimientos especializados y la actualización de estos.

El Delegado de Protección de Datos debe ejercer sus funciones de manera autónoma y libre de interferencias, sin recibir instrucciones, y solo debe responder ante el más alto nivel jerárquico de la organización, tampoco puede ser destituido ni sancionado por desempeñar sus funciones.

VII. Visión estratégica *("Compromiso de la Alta Dirección")*

Para implementar el Plan de Protección de Datos Personales de manera efectiva y eficiente, es esencial que exista compromiso de la Alta Dirección, esto es que se le otorgue importancia estratégica a la privacidad y protección de los datos personales de manera transversal a toda la organización.

Algunas medidas asociadas a estos fines son que, la Alta Dirección se encuentre involucrada en la definición el plan de protección de datos personales, que la política estratégica de la organización cuente con un capítulo de protección de datos personales y que participe de la planificación estratégica en materia de privacidad. Por último, también es relevante que el presupuesto de la organización prevea acciones y medidas asociadas a mejorar la gestión de la privacidad.