MANUAL INTERNO DE PROTECCIÓN DE DATOS PERSONALES DE APEX TRADING S.A.S S.A.S.

CONTENIDO

1. INTRODUCCIÓN

Publicis Groupe es una organización con presencia global, que ha implementado dentro de su sistema de gobernanza global un marco integral de políticas y procedimientos para el cumplimiento de la protección de datos personales, alineado con estándares internacionales como el Reglamento General de Protección de datos (GDPR).

APEX TRADING S.A.S., empresa legalmente constituida e identificada con el NIT No. 901.106.368 de Bogotá D.C., con domicilio principal en la Carrera 13 No 89-59 , Piso 5 en Bogotá D.C. forma parte de la unidad de negocio de **Publicis Groupe**, y se adhieren al cumplimiento del marco integral de políticas y procedimientos globales adoptados por la compañía.

Sin perjuicio de lo anterior, se adopta el siguiente **Manual Interno de Protección de Datos Personales**, (en adelante "**EL MANUAL**"), como una medida para robustecer y evidenciar el cumplimiento con la Ley 1581 de 2012 y demás normas que la complementen, adicionen o modifiquen.

2. DEFINICIONES

Responsable del Tratamiento: Se refiere a la persona natural o jurídica, que por sí misma o en asocio con otros, decide sobre las bases de datos y/o el Tratamiento de los datos.

Encargado del Tratamiento: Persona natural o jurídica, pública o privada, que por sí misma o en asocio con otros, realice el Tratamiento de datos personales por cuenta del Responsable del Tratamiento.

Dato personal: Cualquier información que pueda vincularse o asociarse a una o varias personas naturales determinadas o determinables

Algunos ejemplos de datos personales pueden ser, pero sin limitarse:

a. Identificadores personales como el nombre o el alias, el nombre de la cuenta, la dirección, la dirección de correo electrónico y el teléfono, la dirección IP, los códigos de identificación de dispositivos, y otros identificadores en línea como los identificadores de publicidad y de

cookies, los perfiles de redes sociales, el número de fidelización, el identificador probabilístico y otros identificadores personales únicos.

b. Actividad de Internet como el abandono del carro de compras/del navegador, información de la red o del navegador, el comportamiento de navegación, el historial de búsqueda (clics, visualizaciones, «me gusta», comentarios, elementos compartidos, interacciones), los datos recopilados a través de las tecnologías de seguimiento de dispositivos, los historiales y las tendencias de compra y los productos o servicios considerados.

c. Información de geolocalización como latitud/longitud, radio o señal de seguimiento de localización (interiores y exteriores).

d. Inferencias y datos de perfil como preferencias, características, tendencias, comportamientos, actitudes, habilidades, inferencias efectuadas sobre un individuo y puntuaciones asignadas a individuos.

e. Registros del cliente como firma, características físicas o descripciones, número de póliza de seguro, datos académicos (nivel de estudios), datos de empleo e historial laboral, número de cuenta bancaria, número de tarjeta de crédito y débito, información financiera, información médica e información de seguro de salud.

Dato sensible: Es aquel afecta la intimidad del Titular y cuyo uso indebido puede generar discriminación, como aquellos datos que revelan el origen racial o étnico, la orientación política, las convicciones filosóficas, pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promueva intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición, así como los datos relativos a la salud, a la vida sexual, y los datos biométricos.

Dato Privado: Datos que por su naturaleza íntima o reservada solo son relevantes para el Titular.

Dato Público: Es el dato que no es semiprivado, privado o sensible. Son considerados datos públicos, entre otros, los datos relativos al estado civil de las personas, a su profesión u oficio y a su calidad de comerciante o de servidor público. Por su naturaleza, los datos públicos pueden estar contenidos, entre otros, en registros públicos, documentos públicos, gacetas y boletines oficiales y sentencias judiciales debidamente ejecutoriadas que no estén sometidas a reserva.

Dato Semiprivado: Es aquel que no tiene naturaleza íntima, reservada, ni pública y cuyo conocimiento o divulgación puede interesar no sólo a su Titular, sino a cierto sector o grupo de personas o a la sociedad en general como, por ejemplo, el dato referente al cumplimiento e incumplimiento de las obligaciones financieras o los datos relativos a las relaciones con las entidades de la seguridad social.

Subencargados: Se refiere a aquellas personas naturales o jurídicas que son contratados por para tratar los datos personales en nombre de un cliente. Algunos ejemplos de subencargados son los proveedores de personal, los proveedores de servicios de hosting, los centros de datos, los ISP y otros proveedores de servicios de infraestructura similares. Los subencargados son proveedores, pero no todos los proveedores son subencargados.

Autorización: Es el consentimiento previo, expreso e informado del Titular de los datos personales para llevar a cabo el Tratamiento por parte del Responsable.

Tratamiento: Cualquier operación o conjunto de operaciones sobre datos personales, tales como la recolección, almacenamiento, uso, circulación o supresión.

Titular: Persona natural cuyos datos personales son objeto de Tratamiento.

Acreditación: Es la forma como los Titulares, sus representantes legales o terceros confirman la identidad, presentando el documento idóneo para tal fin (cédula, cédula de extranjería, tarjeta de identidad, pasaporte).

Base de datos: Es un conjunto organizado de datos personales almacenados y estructurados en un archivo digital o físico, con el fin de ser utilizados o tratados con un propósito legítimo.

Causahabiente: Persona que ha sucedido a otra por causa del fallecimiento de esta (heredero).

Habeas Data: Es el derecho constitucional que tienen los Titulares de autorizar o no la recolección de sus Datos Personales, así como conocer la finalidad o el uso que se le dará a los datos, y a conocer, actualizar y rectificar los datos personales contenidos Base de Datos.

PTI: Se refiere a la Política de Tratamiento de Datos Personales adoptada por **APEX** disponible Politicade-TratamientoColombiaFinal_APEXNV2025.pdf.

Incidente de Seguridad: La violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información contenida en una base de datos administrada por el Responsable o el Encargado del Tratamiento.

PQR's: Abreviatura de consultas, peticiones, quejas y reclamos.

Queja: Manifestación de inconformidad a través de los canales de comunicación que **APEX** ha dispuesto para tal fin.

Reclamo: Solicitud del titular del dato o las personas autorizadas por éste o por la ley para corregir, actualizar o suprimir sus datos personales o cuando adviertan que existe un presunto incumplimiento del régimen de protección de datos, según el artículo 15 de la Ley 1581 de 2012.

Petición: Requerimientos relacionados con el tratamiento de los datos personales a través de los canales de comunicación que **APEX** ha dispuesto para tal fin.

SIC: Superintendencia de Industria y Comercio.

Transferencia: Tiene lugar cuando el Responsable y/o Encargado del Tratamiento de datos personales, ubicado en Colombia, envía la información o los datos personales a un receptor, que puede estar dentro o fuera del país, que a su vez es Responsable del Tratamiento.

Transmisión: Es el tratamiento de Datos Personales que implica la comunicación de estos dentro o fuera de Colombia, cuando tenga por objeto la realización de un tratamiento por el Encargado por cuenta del Responsable.

OPD: Corresponde a la abreviatura para el Oficial de Protección de Datos, un funcionario de **APEX** encargado de vigilar, controlar y promover la aplicación de la **PTI**, así como apoyar y coordinar el desarrollo de las distintas actividades y procedimientos internos para el cumplimiento de las disposiciones corporativas y normativas en materia de protección de datos personales.

3. OBJETIVO

EL MANUAL tiene como objetivo establecer los lineamientos básicos en materia de protección de datos en Colombia, alineado con las políticas y procedimientos globales que hacen parte de la gobernanza de **Publicis Groupe**.

APEX está alineadas y deben cumplir con el sistema de gobernanza global de **Publicis Groupe**, el cual incluye las siguientes políticas internas:

3.1 POLÍTICAS DE LA OFICINA GLOBAL DE PROTECCIÓN DE DATOS

Política de protección de datos de Publicis	Número
(1) Política global de protección de datos	POL-GDPO-151
(2) Política de gestión de datos	POL-GDPO-152
(3) Política de solicitudes de la autoridad pública	POL-GDPO-153
(4) Política de solicitudes individuales	POL-GDPO-154
(5) Política de evaluación y mitigación de riesgos	POL-GDPO-155
(6) Política de protección desde el diseño y protección por defecto	POL-GDPO-156
(7) Resumen de la política de protección de datos de Publicis	POL-GDPO-451

3.2 POLÍTICAS DE LA OFICINA GLOBAL DE SEGURIDAD

Política	Número
Política de seguridad de la Información	POL-GSO-101
Política de control de acceso	POL-GSO-102
Política de seguridad de redes	POL-GSO-103
Política de seguridad en la nube	POL-GSO-104

Política de uso aceptable	POL-GSO-105
Política de Uso de Dispositivos Móviles I	POL-GSO-106
Política de respuesta a incidentes	POL-GSO-107
Estándares para la clasificación, etiquetado y manejo de la información	STD-GSO-706

Los objetivos definidos que se establecen para la protección de datos personales en Colombia son los siguientes:

(i) Adoptar procesos de atención y respuesta oportuna a las PQR's de los Titulares en Colombia respecto al tratamiento de sus datos personales;

(ii) Implementar medidas apropiadas y efectivas para cumplir con las obligaciones establecidas en la Ley 1581 de 2012 y demás normas que lo modifiquen, complementen o adicionen;

(iii) Gestionar y evitar pérdida económicas, reputacionales, operacionales o de cualquier otra índole por concepto de sanciones o multas impuestas con ocasión a una infracción al Régimen General de Protección de Datos; y

(iv) Colaborar con las autoridades locales e internacionales para la protección de datos personales.

4. ALCANCE DEL MANUAL

EL MANUAL será aplicable a todos los datos personales registrados en Bases de Datos de **APEX** que sean objeto de tratamiento y deberá ser aplicado por todos los empleados, contratistas, consultores, trabajadores, independientes y demás miembros **de APEX** están obligados a adherirse a **El MANUAL** y a todas las políticas incorporadas en la Oficina Global de Privacidad de Datos ("**GDPO**").

Cualquier tercero que trate datos recolectados por **APEX** en calidad de Responsable o Encargado, está obligado a cumplir con las disposiciones de **EL MANUAL**, o cuando menos, a cumplir con los principios de Protección de Datos Personales contenidos en la Ley 1581 de 2012, y demás normas que lo modifiquen, complementen o adicionen.

En caso de que surjan dudas o inquietudes relacionadas con la aplicación de **EL MANUAL**, podrá dirigirse a la **GDPO** al siguiente correo electrónico: privacyofficer@publicisgroupe.com.

5. PRINCIPIOS APLICABLES EN COLOMBIA

En Colombia, el tratamiento de datos personales se regirá por los principios establecidos en el artículo 4 de la Ley 1581 de 2012, y demás normas que la complementen, adicionen o modifiquen:

5.1 Principios relacionados con la recolección de datos personales

Principio de libertad: El Tratamiento sólo puede ejercerse con el consentimiento, previo, expreso e informado del Titular. Los datos personales no podrán ser obtenidos o divulgados sin previa autorización, o en ausencia de mandato legal o judicial que releve el consentimiento

Se deberá informar al Titular de manera clara, suficiente y previa acerca de la finalidad por la cual se tratará la información suministrada, por lo tanto, no podrá recolectarse datos sin la clara especificación acerca de la finalidad.

El principio de libertad debe observarse tanto para el caso de datos que se recolectan a través de formatos como los que hacen parte de los anexos o documentos que se entregan a los Titulares de los datos.

Principio de limitación de la recolección: Sólo deben recolectarse los Datos personales que sean estrictamente necesarios para el cumplimiento de las finalidades del tratamiento, de tal forma que se encuentra prohibido el registro y divulgación de datos que no guarden estrecha relación con el objetivo del tratamiento. En consecuencia, debe hacerse todo lo razonablemente posible para limitar el procesamiento de Datos personales al mínimo necesario. Es decir, los datos deberán ser: (i) adecuados, (ii) pertinentes y (iii) acordes con las finalidades para las cuales fueron previstos.

Los Datos personales, salvo la información pública, no podrán ser accesibles por Internet o por otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido sólo a los Titulares o los usuarios autorizados conforme a la ley aplicable.

5.2 Principios relacionados con el uso de datos personales

Principio de finalidad: El Tratamiento debe obedecer a una finalidad legítima de acuerdo con la Constitución y la Ley, la cual debe ser informada al Titular. Solo se recopilan Datos Personales para fines específicos.

Principio de temporalidad: Los datos personales se conservarán únicamente por el tiempo razonable y necesario para cumplir la finalidad del tratamiento y las exigencias legales o instrucciones de las autoridades de vigilancia y control u otras autoridades competentes. Los datos serán conservados cuando ello sea necesario para el cumplimiento de una obligación legal o contractual. Para determinar el término del Tratamiento se considerarán las normas aplicables a cada finalidad y los aspectos administrativos, contables, fiscales, jurídicos e históricos de la información.

5.3 Principios relacionados con la calidad de la información

Principio de veracidad o calidad: La información sujeta a Tratamiento debe ser veraz, completa, exacta, actualizada, comprobable y comprensible. Se prohíbe el Tratamiento de datos parciales, incompletos, fraccionados o que induzcan a error.

En caso de que el Titular solicite o **APEX** determine que los datos deben ser actualizados, rectificados o suprimidos, **APEX** cuenta con las medidas necesarias para hacerlo, garantizando que la información recopilada sea precisa y suficiente.

5.4 Principios relacionados con la protección, el acceso y circulación de datos personales

Principio de seguridad: Cada trabajador, colaborador, proveedor o cliente de **APEX** que tenga acceso a datos personales debe cumplir con las medidas técnicas, humanas y administrativas que se establezcan para otorgar seguridad a los datos personales evitando su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento.

Principio de transparencia: En el Tratamiento debe garantizarse el derecho del Titular de obtener del Responsable del Tratamiento o del Encargado en cualquier momento y sin restricciones, información acerca de la existencia de datos que le conciernan.

Principio de acceso y circulación restringida: El Tratamiento debe estar sujeto a los límites de la naturaleza del dato, de las disposiciones en materia de protección de datos.

Solo se permitirá el acceso a los datos personales a las siguientes personas: (i) al Titular del dato; (ii) las personas autorizadas por el titular del dato; y (iii) a las personas que por mandato legal u orden judicial sean autorizados para conocer la información.

Los datos personales, salvo que sea información pública, no pueden estar disponibles en Internet u otros medios de divulgación o comunicación masiva, salvo que el acceso sea técnicamente controlable para brindar un conocimiento restringido solo a los Titulares o terceros autorizados.

Principio de confidencialidad: Todas las personas que intervengan en el Tratamiento de datos personales que no tengan la naturaleza de públicos están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el Tratamiento, pudiendo sólo realizar suministro o comunicación de datos personales cuando ello corresponda al desarrollo de las actividades autorizadas en la ley.

6. POLÍTICA DE TRATAMIENTO DE DATOS PERSONALES

Sin perjuicio de la Política Global de Protección de Datos adoptada por **Publicis Groupe**, **APEX** ha adoptado una **PTI** aplicable en Colombia, que podrá ser consultada en su sitio web y que establece: 1. Los datos de Identificación y contacto en su calidad de Responsable, 2. El tratamiento y las finalidades a las cuales se someterán los Datos Personales recolectados, 3. Los derechos que le asisten a los Titulares, 4. Los mecanismos para garantizar la seguridad de la Información recolectada y, 5. El procedimiento por medio del cual el Titular puede ejercer sus derechos.

En caso de que se modifique o actualice la **PTI**, dicha modificación debe ser comunicada oportunamente a los Titulares empleando mecanismos eficientes como, por ejemplo, un aviso en la página web que sea visible para los Titulares, o un correo electrónico enviado a la dirección registrada en las Bases de Datos de **APEX**, antes de que entren en vigor y se implementen los cambios.

Para consultar la **PTI** puede visitar el siguiente enlacePoliticade-TratamientoColombiaFinal_APEXNV2025.pdf o solicitarla a través del correo electrónico privacyofficer@publicisgroupe.com.

7. RESPONSABILIDADES DE AQUELLOS QUE ADMINISTRAN DATOS PERSONALES

Personas responsables:

Todos los empleados, contratistas, consultores, trabajadores, independientes y demás miembros de **APEX** deberán cumplir con las siguientes obligaciones, sin perjuicio de las adicionales que estén incluidas en las políticas globales:

a. Usar los datos únicamente para las finalidades autorizadas por el Titular o por la Ley, deberá seguir las instrucciones de la *Política de Gestión de Datos*;

b. Mantener la confidencialidad de la información que contenga datos personales a las que pueda acceder con ocasión de sus funciones, siguiendo las instrucciones de la *Política de Gestión de Datos*;

c. Informar al Titular acerca del tratamiento que se dará a sus datos personales;

d. Garantizar que el Titular tenga acceso a los datos personales;

e. Cumplir con los procedimientos y canales definidos para el ejercicio de los derechos de los Titulares;

f. Informar cualquier incidente de seguridad que ponga en riesgo la seguridad, confidencialidad e integridad de los Datos Personales, siguiendo las instrucciones de las *Políticas de la oficina global de seguridad*; y

g. Abstenerse de transferir o divulgar los datos personales a personas no autorizadas.

La **GDPO** asignada para Colombia cumplirá con las siguientes funciones, de acuerdo con la *Guía Oficial de Protección de Datos Personales* de la SIC y demás políticas internas:

a. Monitorear y hacer seguimiento a la normatividad en materia de protección de datos personales y hacer las recomendaciones necesarias;

b. Atender con el apoyo de los demás trabajadores de **APEX** las solicitudes, consultas y reclamos de los Titulares respecto al tratamiento de datos personales que se canalicen a través de los canales habilitados para tal fin;

c. Servir de enlace y coordinación con las demás áreas de **APEX**, con los Titulares de los datos personales y las autoridades nacionales;

d. Impulsar una cultura de protección de Datos personales;

e. Registrar las bases de datos de **APEX** en el Registro Nacional de Base de Datos y actualizar el reporte atendiendo a las instrucciones que emita la SIC;

f. Revisar los contratos de transferencias internacionales de Datos Personales que se suscriban con otros Responsables del Tratamiento, ubicados o no en territorio colombiano;

g. Revisar los contenidos de los contratos de transmisión internacional de datos personales que se suscriban con Encargados del tratamiento, ubicados o no en territorio colombiano;

h. Realizar entrenamiento y capacitaciones en protección de datos personales a los empleados y nuevos colaboradores de **APEX** que, por las condiciones de sus contratos, tengan acceso a datos personales;

i. Integrar las políticas globales de protección de datos dentro de las actividades de las demás áreas de **APEX**;

j. Velar por la implementación de auditorías internas o externas para verificar el cumplimiento de las políticas globales en materia de datos personales;

k. Valorar los incidentes de seguridad de la información relacionados con datos personales, a fin de establecer las medidas correctivas;

l. Realizar el reporte de incidentes de seguridad que comprometan datos personales ante la **SIC**; y

m. Las demás funciones propias del cargo que se establezcan en las políticas globales de **Publicis Groupe**.

Para mayor información, se podrá consultar la *Política Global de Protección de Datos*, en la cual encontrará la asignación de responsabilidades.

8. PROCEDIMIENTO INTERNO EN MATERIA DE DATOS PERSONALES Y CICLO DE VIDA DEL DATO

8.1 Para la recolección y el almacenamiento de Datos Personales

La recolección de Datos Personales se hará por los medios dispuestos por **APEX** con la autorización expresa, previa e informada de los Titulares.

Cuando se recolecten Datos Personales se debe determinar qué tipo de información se está recolectando, toda vez que hay casos en los cuales no se requiere la autorización del Titular para recolectar los datos:

(i) Datos personales públicos (por ejemplo, datos relacionados con el Registro Mercantil de una empresa);

(ii) Datos personales recolectados por un mandato legal, como ocurre en temas tributarios, pólizas de seguro, entre otros;

(iii) Datos requeridos para una urgencia médica o sanitaria;

(iv) Datos requeridos para fines estadísticos, históricos o científicos; y

(v) Datos requeridos por una entidad pública, administrativa o judicial en ejercicio de sus funciones.

Si se recolectan datos personales en situaciones distintas a las descritas anteriormente, se requiere la autorización del Titular en los términos descritos por la ley.

En todo caso, se debe tener en cuenta lo siguiente para la recolección y almacenamiento de Datos Personales:

1. Respecto de cada Base de datos, el área o unidad de negocio que la administre deberá: (i) definir las finalidades de tratamiento a las cuales estarían sometidos los Datos personales; (ii) identificar si existen formatos o mecanismos de autorización de tratamiento de información de **APEX** y solicitar a la **GDPO** concepto sobre la viabilidad del Tratamiento de la base para dichas finalidades.
2. Una vez definidas las finalidades, el área correspondiente debe utilizar un formato o mecanismo de autorización avalado por la **GDPO** para obtener y almacenar la autorización para el tratamiento de datos personales de los titulares.
3. Se determinará el medio de conservación de los Datos personales tratados, entendiendo que esta podrá ser en medios físicos o electrónicos, y deberá conservar la autorización o copia de cada autorización otorgada por los Titulares.
4. En todo caso, el medio de conservación deberá contar con medidas adecuadas de seguridad para proteger los Datos personales, conforme a las políticas de la **GDPO**.

8.2 Autorización de Titular

El tratamiento de Datos Personales requiere del consentimiento libre, previo, expreso e informado por el Titular. Asimismo, **APEX** en su condición de Responsables del Tratamiento, han dispuesto mecanismos para obtener la autorización de los Titulares.

La autorización puede constar en cualquier mecanismo que permita su posterior consulta, como lo son: 1. Por escrito, 2. De forma oral y/o 3. Mediante conductas inequívocas del Titular que permitan concluir de forma razonable que ha otorgado su autorización, en ningún caso el silencio podrá asimilarse a una conducta inequívoca.

Para esto, **APEX** han adoptado formularios para obtener la autorización del Titular dependiendo de la finalidad.

8.3 Conservación de la prueba de la Autorización

Las áreas y unidades de negocio de **APEX** que recolecten datos personales deben asegurarse de siempre obtener la correspondiente Autorización del Titular y conservar una prueba de esta, la cual debe ser objeto de consulta posterior. La prueba de la Autorización otorgada debe ser conservada con medidas adecuadas de seguridad.

En el caso de pruebas físicas de Autorización, se podrá implementar un archivo físico que permita conservarlas garantizando las condiciones de seguridad adecuadas. En el caso de pruebas digitales de Autorización, se deben cumplir los lineamientos establecidos por la **SIC**.

8.4 Conservación y eliminación de los datos

Los datos personales y Bases de datos en las que se registre la información tendrán una vigencia igual al tiempo en que se mantenga y utilice la información para las finalidades descritas en las **PTI** y las autorizaciones del Titular. Una vez se cumplan las finalidades para las cuales fueron recolectados los datos, y siempre que no exista un deber legal o contractual de conservar la información, los datos serán eliminados de las Bases de datos.

En todo caso, los datos personales proporcionados se conservarán mientras se mantenga la relación contractual con el Titular de la información y serán resguardados durante el tiempo requerido según la finalidad del Tratamiento y en cumplimiento de los deberes legales o contractuales.

Para mayor información se podrá consultar la *Política de Gestión de Datos*. Así mismo, en el Anexo No. 2 de este Manual se define el protocolo de eliminación de datos personales.

9. DERECHOS DE LOS TITULARES

En Colombia, los Titulares tienen los siguientes derechos, de acuerdo con lo establecido en el artículo 8 de la Ley 1581 de 2012:

a. A conocer, actualizar, rectificar sus datos personales frente a los responsables o encargados sobre datos parciales, inexactos, incompletos, fraccionados, que induzcan a error, o aquellos cuyo tratamiento esté expresamente prohibido o no haya sido autorizado;

b. Solicitar prueba de la autorización otorgada al Responsable del Tratamiento salvo cuando esté dentro de las excepciones del artículo 10 de la Ley 1581 de 2012;

c. Ser informado por el Responsable o Encargado del tratamiento, previa solicitud, respecto del uso que se ha dado a sus datos personales;

d. Presentar ante la Superintendencia de Industria y Comercio quejas por infracciones a lo dispuesto en la Ley 1581 de 2012 y las demás normas que la modifiquen, adicionen o complementen;

e. Revocar la autorización y/o solicitar la supresión del dato en el momento en que así lo desee, siempre y cuando no exista un deber legal o contractual de permanecer en la base de datos; y

f. Acceder de forma gratuita a sus datos personales que hayan sido objeto del Tratamiento.

10. ATENCIÓN DE PETICIONES, CONSULTAS Y RECLAMOS

Para efectos de que los Titulares puedan ejercer cualquiera de sus derechos **APEX** han dispuesto una **Unidad de Privacidad**, llamada **GDPO** para Colombia, la cual se encargará de atender los reclamos y cualquier consulta de los Titulares en atención a sus derechos a través de los siguientes canales:

Correo electrónico: privacyofficer@publicisgroupe.com
Dirección Física: Carrera 13 No. 89-59, Piso 5, Bogotá.

Sin perjuicio de los canales enunciados, cuando se recibe una solicitud o reclamo de un Titular, la **GDPO** deberá seguir los pasos indicados en la *Política de solicitudes individuales*.

Consultas de información

Los titulares o las personas legitimadas para el efecto podrán consultar la información personal del Titular que repose en cualquier Base de Datos de **APEX**. Para efectos de la atención de las consultas se seguirá el siguiente procedimiento:

1. La recepción de la solicitud efectuada por cualquiera de los canales habilitados para tal propósito deberá contener el nombre completo del Titular, así como el tipo y número de identificación. Lo anterior con el fin de constatar que quien está presentando la consulta es efectivamente el Titular de la información y garantizar su derecho a la intimidad y confidencialidad. No serán atendidas solicitudes anónimas.

   En caso de que quien presente la consulta sea una persona distinta al Titular, deberá acreditar la calidad en la que actúa.

2. El sistema generará automáticamente un número de radicado para aquellas consultas realizadas. En caso de que la solicitud haya sido presentada ante la Superintendencia de Industria y Comercio, la **GDPO** será la que radique la solicitud con el fin de obtener el número de radicado, el cual será entregado al Titular para su posterior seguimiento.
3. En cualquier caso, independientemente del mecanismo implementado para la atención de las solicitudes, las mismas serán atendidas en un término máximo de diez (10) días hábiles contados a partir de la fecha de su recibo. Cuando no fuere posible atender la consulta dentro de dicho término, se informará al interesado antes del vencimiento de los 10 días, expresando los motivos de la demora y señalando la fecha en que se atenderá su consulta, la cual en ningún caso podrá superar los cinco (5) días hábiles siguientes al vencimiento el primer plazo.
4. Una vez se cuente con la respuesta esta deberá ser remitida al medio indicado por el titular en su solicitud. En caso de que el solicitante no lo indique, se dará respuesta por el medio que se considere más adecuado.
5. Se deberá dejar constancia y prueba de la respuesta dada al solicitante.

Reclamos, solicitudes y peticiones de actualización y/o rectificación.

El Titular, sus Causahabientes o los terceros autorizados por el Titular o la ley que consideren que la información contenida en una Base de datos debe ser objeto de corrección, actualización o supresión, o cuando adviertan el presunto incumplimiento de cualquiera de los deberes contenidos en la ley o en la **PTI**, podrán presentar un reclamo ante **APEX** mediante los canales habilitados, el cual será tramitado bajo las siguientes reglas:

1. El titular debe presentar el reclamo mediante los canales de comunicación indicados en este capítulo.

2. El reclamo, solicitud y/o petición debe contener el nombre del Titular, su identificación, la descripción de los hechos que dan lugar a su reclamo, solicitud y/o petición, dirección de notificación y los anexos. No serán atendidos reclamos de carácter anónimo.
3. El término máximo para atender el reclamo, solicitud y/o petición será de quince (15) días hábiles contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atenderlo dentro de dicho término, se informará al interesado los motivos de la demora y la fecha en que se atenderá, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.
4. Para efectos de atender la solicitud, el equipo encargado de dar respuesta podrá solicitar ayuda del área y/o unidad de negocio que administre la base de datos en la que reposan los datos del titular o cualquier otra área de la compañía que estime necesario.
5. Una vez se cuente con la respuesta esta deberá ser remitida al medio indicado por el titular en su solicitud. En caso de que el solicitante no lo indique, se dará respuesta por el medio que se considere más adecuado.
6. Se deberá dejar constancia y prueba de la respuesta dada al solicitante.

Peticiones de supresión de datos o revocatoria de autorización.

El Titular tiene derecho a solicitar a **APEX** la supresión (eliminación) de sus datos personales

Esta supresión implica la eliminación total o parcial de la información de acuerdo con lo solicitado por el Titular en los registros, archivos, Bases de Datos o Tratamientos realizados por **APEX**. Por lo anterior, será necesario que el Titular al momento de elevar la solicitud de revocatoria del consentimiento a **APEX** indique en ésta si la revocación que pretende realizar es total o parcial. En la segunda hipótesis se deberá indicar con cual tratamiento el Titular no está conforme. Sin embargo, este derecho del titular no es absoluto y, en consecuencia, **APEX** podrá negar el ejercicio de este cuando:

(i) El titular tenga un deber legal o contractual de permanecer en la base de datos.

(ii) La eliminación de datos obstaculice actuaciones judiciales o administrativas vinculadas a obligaciones fiscales, la investigación y persecución de delitos o la actualización de sanciones administrativas.

(iii) Los datos sean necesarios para proteger los intereses jurídicamente tutelados del titular, para realizar una acción en función del interés público o para cumplir con una obligación legalmente adquirida por el Titular.

Además de las reglas previstas para la atención de Reclamos, ante la solicitud de supresión o revocatoria de la autorización deberá, por su cuenta o con apoyo de otras áreas de la compañía:

(i) Determinar el estado actual de los datos del titular.

(ii) Al momento de recibir la solicitud ordenar la suspensión temporal del uso de los datos mientras se resuelva la solicitud.

(iii) Si determina que la solicitud es procedente deberá ordenar a las áreas o unidades de negocio de **APEX** pertinentes que realicen la supresión o eliminación de los datos de conformidad con el protocolo previsto en Anexo No. 2 de este documento, y seguir las reglas allí previstas.

(iv) En todos los casos se conservará prueba de la actualización o rectificación pertinente en las bases de datos de **APEX**.

(v) Se deberá dejar constancia y prueba de la respuesta dada al solicitante.

Sin perjuicio de los procedimientos enunciados, cuando se recibe una solicitud o reclamo de un Titular, la **GDPO** deberá seguir los pasos indicados en la *Política de solicitudes individuales*.

11. PROCEDIMIENTO PARA EL EJERCICIO DEL DERECHO DE HABEAS DATA

En cumplimiento de las normas sobre protección de datos personales, **APEX** presenta el procedimiento y requisitos mínimos para el ejercicio de los derechos de los titulares, sin perjuicio de las políticas globales adoptadas por **Publicis Groupe** a las cuales se adhiere **APEX**:

Para la radicación y atención de las solicitudes se debe verificar que estas tengan la siguiente información:

(i) Nombre completo y apellidos;

(ii) Datos de contacto (Dirección física y/o electrónica y teléfonos de contacto);

(iii) Medios para recibir respuesta a la solicitud;

(iv) Motivo(s)/hecho(s) que dan lugar a la solicitud con una breve descripción del derecho que el solicitante desea ejercer (conocer, actualizar, rectificar, solicitar prueba de la autorización otorgada, revocarla, suprimir, acceder a la información); y

(v) Firma (si aplica) y número de identificación.

El término máximo previsto por la ley para resolver la reclamación es de quince (15) días hábiles en el caso de los reclamos, y diez (10) días hábiles en el caso de las consultas, contados a partir del día siguiente a la fecha de su recibo. Cuando no fuere posible atender el reclamo dentro de dicho término, **APEX** informará al interesado los motivos de la demora y la fecha en que se atenderá su reclamo, la cual en ningún caso podrá superar los ocho (8) días hábiles siguientes al vencimiento del primer término.

Una vez cumplidos los términos señalados por la Ley 1581 de 2012 y las demás normas que la reglamenten o complementen, el Titular al que se deniegue, total o parcialmente, el ejercicio de los derechos de acceso, actualización, rectificación, supresión y revocación podrá poner su caso en conocimiento de la SIC –Delegatura para la Protección de Datos Personales.

Cada vez que se ponga a disposición una herramienta nueva para facilitar el ejercicio de sus derechos por parte de los titulares de información o modifique las existentes, lo informará a través de su página web https://col-resources.com.co/

12. OFICIAL DE PROTECCIÓN DE DATOS PERSONALES EN COLOMBIA

Para efectos de cumplimiento con el Régimen de Protección de Datos Personales en Colombia, y como canal de contacto de autoridades, titulares y áreas internas, se ha designado **GDPO** como la **Unidad de Privacidad para Colombia**.

13. MEDIDAS DE SEGURIDAD

Para proteger las Bases de Datos, se adoptarán medidas de seguridad organizacionales y técnicas. Las medidas de seguridad aplicadas en el Tratamiento de las Bases de datos procurarán conservar la confidencialidad, integridad y disponibilidad de la información. Para el efecto se seguirán las medidas señaladas en las *Políticas de la Oficina Global de Seguridad*. Además de lo anterior, **APEX** podrá implementar, entre otras, los siguientes tipos de medidas organizacionales y técnicas:

(i) Protección de acceso a los datos mediante identificador único de usuario y contraseñas;

(ii) Aseguramiento del nivel de complejidad de las contraseñas de los usuarios;

(iii) Registro de actividades de la cuenta de usuario;

(iv) Procedimientos de recuperación y redundancia;

(v) Almacenamiento de las copias de respaldo;

(vi) Cifrado y protección por contraseña de los computadores desde los que se acceden a los datos;

(vii) Funciones y obligaciones del personal relacionados con seguridad de la información;

(viii) Medidas, normas, procedimientos, reglas y estándares encaminados a garantizar el nivel de seguridad exigido en la Ley 1581 de 2012;

(ix) Controles periódicos que se deban realizar para verificar el cumplimiento de lo dispuesto en el procedimiento de seguridad que se implemente;

(x) Medidas de seguridad serán adoptadas cuando un soporte o documento vaya a ser transportado, desechado o reutilizado;

14. INCIDENTES DE SEGURIDAD

Si se presenta un incidente de seguridad respecto de las Bases de Datos se deberán seguir las instrucciones de **EL MANUAL**, que se incluye como Anexo No. 1, así como las *Políticas de la Oficina Global de Seguridad.*

15. CONFIDENCIALIDAD DE LA INFORMACIÓN

Todas las áreas, empleados, colaboradores, contratistas, y demás terceros que puedan conocer datos personales almacenados en las Bases de datos de **APEX** están obligadas a garantizar la reserva de la información, inclusive después de finalizada su relación con alguna de las labores que comprende el tratamiento.

16. REGISTRO DE BASES DE DATOS

APEX debe efectuar la inscripción de las Bases de Datos ante el Registro Nacional de Bases de Datos de la Superintendencia de Industria y Comercio, de conformidad con lo estipulado en el Decreto 1074 de 2015.

De acuerdo con lo dispuesto en el Título V de la Circular Única de la Superintendencia de Industria y Comercio, los Responsables del tratamiento deberán realizar la actualización del Registro Nacional de Bases de Datos y novedades que se presenten, así:

1. Anualmente, entre el 2 de enero y el 31 de marzo.
2. Dentro de los quince (15) primeros días hábiles de los meses de febrero y agosto de cada año, a partir de la inscripción de la base de datos, se debe actualizar la información de los reclamos presentados por los Titulares.
3. Dentro de los primeros diez (10) días hábiles de cada mes, a partir de la inscripción de la base de datos, cuando se realicen cambios sustanciales en la información registrada.

Para efectos de lo anterior, se entenderán por cambios sustanciales los que se relacionan con lo siguiente:

1. La finalidad de la Base de Datos;
2. El Encargado del tratamiento;
3. La clasificación o tipos de Datos Personales almacenados en la Base de Datos;
4. Las medidas de seguridad de la información implementadas;
5. La Política de tratamiento de la información;
6. La transferencia y transmisión internacional de datos personales;
7. Los canales de atención al titular.

Las bases de Datos que se creen con posterioridad a la publicación de estos Manuales deberán inscribirse en el Registro Nacional de Bases de Datos dentro de los dos (2) meses siguientes, contados a partir de su creación.

17. PUBLICACIÓN, MODIFICACIONES Y VIGENCIA DEL MANUAL

El MANUAL podrá ser consultado por los trabajadores de **APEX** en cualquier momento.

EL MANUAL entra en vigencia a partir del 21 de noviembre 2025 y será revisado en caso de cambios normativos, actualizaciones de políticas internas o instrucciones impartidas por la Superintendencia de Industria y Comercio. Cualquier modificación que se realice se dará a conocer a través de comunicación dirigida a todos los trabajadores. En todo caso, las modificaciones serán implementadas dentro de los cinco (5) días hábiles siguientes a la fecha en que se haya dado a conocer la respectiva modificación a los Manuales, según lo aquí previsto.

Anexo No. 1. Protocolo de respuesta en el manejo de incidentes de seguridad de APEX

1. Objetivo del Protocolo. Este protocolo de respuesta en el manejo de incidentes de seguridad (en adelante "el protocolo" o "Protocolo de Manejo de Incidentes de Seguridad") busca facilitar que la Compañía pueda actuar de forma rápida, ordenada y eficaz ante cualquier incidente de seguridad que afecte la confidencialidad, disponibilidad e integridad de los datos personales bajo su protección. El presente protocolo incorpora roles, responsabilidades y acciones que deben ser desplegadas al interior de **APEX** para gestionar un incidente de seguridad[1]. Igualmente, debe seguirse la Política de Respuesta ante Incidentes del Grupo.

2. Definición de incidente de seguridad. Por "incidente de seguridad" se entiende "la violación de los códigos de seguridad o la pérdida, robo y/o acceso no autorizado de información de una base de datos administrada por el Responsable del Tratamiento o por su Encargado"[2].

3. Equipo de respuesta ante incidentes de seguridad (IRT). Ante un posible incidente de seguridad, se debe reportar ante la Oficina Global de Seguridad (GSO). Así mismo, se deberá consultar las *Política de respuesta a incidentes*. **APEX** cuenta con el equipo de IRT (Incident Response Team) a nivel global el cual es responsabilidad de la Oficina Global de Seguridad. El equipo IRT está conformado principalmente por la **GDPO** (para incidentes relacionados con datos personales), la Oficina Global de Seguridad, los dueños en el negocio del sistema impactado, lideres de la agencia, equipos de comunicaciones y com legales. Tenga en cuenta que los miembros del equipo IRT podrán variar en función de la naturaleza del incidente, la región/ubicación de los sistemas informáticos afectados, la gravedad del incidente y el riesgo percibido.

4. Identificación de los incidentes de seguridad. En caso de que cualquier empleado o colaborador de la Compañía detecte o sospeche la existencia de un incidente de seguridad que afecte o involucre Bases de Datos con información personal de **APEX**, deberá informarlo **inmediatamente** ante la Oficina Global de Seguridad (GSO), y éste se encargará de gestionar con el equipo **IRT**. Si un incidente está relacionado con información personal, debe consultarse al **GDPO** y/o al director de privacidad de los datos de **Publicis Groupe**, quienes aprobarán las acciones.

5. Documentar los hechos. Una vez definido si los hechos configuran un incidente de seguridad o no, se deberá preparar un acta en el cual se documente todos los aspectos relevantes de los incidentes de seguridad que ocurran, incluyendo el registro de lo siguiente

a. "Una descripción general de las circunstancias del incidente de seguridad (incluidas las Bases de Datos y las clases de datos -sensibles, privados, etc.- comprometidos)";
b. "Las categorías de Titulares de la información afectados";

---

[1] El protocolo se basa en las indicaciones provistas por la Superintendencia de Industria y Comercio (SIC) en su "Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales", publicada a finales de 2020, y en la Circular Única de la SIC.

[2] Sección 2.1, Capítulo Segundo, Título V, de la Circular Única de la SIC.

c. "La fecha y hora del incidente de seguridad y del descubrimiento del mismo";
d. "Las indagaciones preliminares e investigaciones realizadas por la organización";
e. "Las medidas correctivas" adoptadas;
f. "Los Responsables del manejo del incidente de seguridad";
g. "La prueba del reporte efectuado ante la SIC, así como la comunicación realizada a los Titulares de la información, si fue necesario";
h. "La evaluación del nivel de riesgo derivado del incidente de seguridad en los Titulares y los factores tenidos en cuenta";
i. "La inclusión de detalles personales, cuando deban establecerse".

Si el IRT concluye que los hechos informados no configuran un incidente de seguridad, se dejará constancia en el registro de las razones por las cuales se llegó a dicha conclusión.

6. Medidas para contener y mitigar los incidentes de seguridad e investigación inicial. El IRT definirá las medidas para contener y revertir el impacto que puede tener un incidente de seguridad y la gestión de dichas medidas se realizará de manera prioritaria. Para tal efecto, el IRT deberá realizar una investigación inicial sobre el evento u ocurrencia que le permita responder las siguientes preguntas respecto del incidente de seguridad:

- ¿Cómo se produjo el incidente?
- ¿Cuándo y dónde tuvo lugar?
- ¿Cuál fue la naturaleza y quién lo detectó?
- ¿Se continúa compartiendo o divulgando información personal sin autorización?
- ¿Quién tiene acceso a la información personal?
- ¿Qué se puede hacer para asegurar la información o detener el acceso, divulgación o disponibilidad no autorizada y reducir el riesgo de daños a los afectados?
- ¿Es un incidente de seguridad relacionado con datos personales que requiere la notificación a las personas tan pronto como sea posible?
- ¿Qué nivel de riesgo puede generar o generó el incidente?
- ¿Qué daños para las personas podrían resultar de un incidente de seguridad?

Durante esta etapa de investigación preliminar todos los empleados y colaboradores de la Compañía deben tener cuidado de no destruir la evidencia que pueda ser valiosa para:

- Establecer la causa del incidente de seguridad
- Identificar todos los riesgos generados a los Titulares de la información
- Responder los requerimientos de la SIC u otras autoridades

7. **Determinar la estrategia de comunicación a titulares (de ser necesario).** El IRT evaluará internamente los riesgos e impactos a los datos personales de los titulares asociados con el incidente de seguridad con el fin de definir si es necesario adelantar una estrategia de comunicación clara y precisa a los Titulares de la Información y los términos de dicha estrategia.

En el caso de que, previa evaluación interna, el IRT decida notificar a los titulares, la comunicación a los Titulares de la Información debe brindar la oportunidad para que ellos mismos puedan adoptar las

medidas necesarias para protegerse de las consecuencias de un incidente de seguridad. Por ejemplo, cambiar su nombre de usuario y contraseña etc.

Las comunicaciones deben ser suficientes, claras y precisas para permitir que los Titulares de la información comprendan la importancia del incidente y que tomen las medidas, si es posible, para reducir los riesgos que podría resultar de su ocurrencia. Es primordial no incluir información personal innecesaria en el aviso para evitar una posible divulgación no autorizada.

8. Reportar el incidente a la SIC (de ser necesario). El IRT evaluará internamente los riesgos e impactos asociados con el incidente de seguridad. En caso de que, previo a la evaluación interna, se determine que no existen riesgos en la administración de la información de los Titulares, el IRT podrá decidir si reporta o no dicho incidente ante la SIC.

Dentro de esa evaluación interna deberán tenerse en cuenta los siguientes factores que han sido indicados en las guías de la SIC:

- Determinar la naturaleza de los datos personales impactados (datos datos sensibles, semiprivados, públicos, entre otros); el volumen de los datos afectados; y el potencial riesgo de exposición.
- Precisar la categoría de los titulares de los datos personales (si se trató de datos de empleados, proveedores, clientes, u otro grupo); la cantidad de titulares afectados; e identificar si el riesgo fue potencial o real para los derechos de los titulares.
- Determinar y evaluar internamente el impacto en términos de confidencialidad, integridad y disponibilidad de los datos comprometidos.

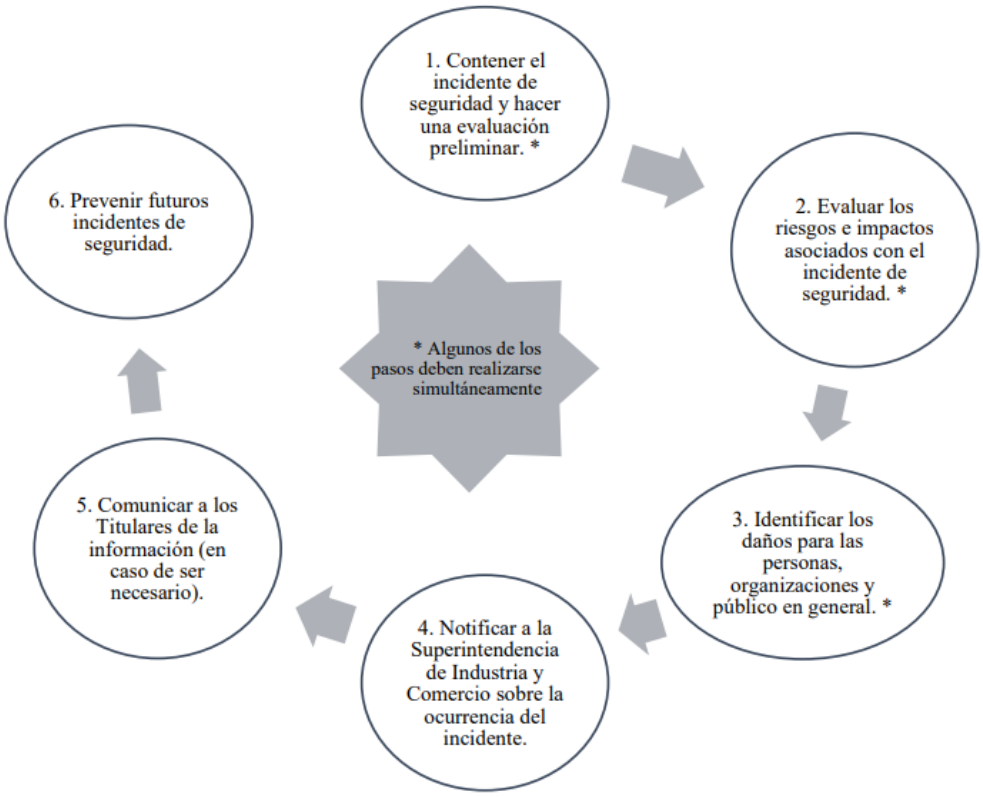
En caso de decidir reportar el incidente, el IRT preparará el reporte del incidente a la SIC y definirá cómo se presentará el reporte dentro de los quince (15) días hábiles siguientes al momento en que se haya detectado el incidente y se haya puesto en conocimiento

9. Hacer seguimiento a los hechos que dieron origen al incidente y monitorear las acciones implementadas para prevenir futuros incidentes de seguridad. El IRT se reunirá periódicamente para hacer seguimiento a los hechos que dieron origen al incidente y monitorear las acciones implementadas para prevenir futuros incidentes de seguridad. Una vez que se hayan tomado las medidas necesarias para mitigar los riesgos asociados con el incidente, el IRT debe ejecutar un plan de prevención para evitar futuros eventos que puedan afectar los datos personales que **APEX** ha tratado. El IRT también evaluará si se justifica ajustar el presente protocolo para incrementar su efectividad. La evaluación de cómo ocurrió el incidente de seguridad y el éxito de su gestión, puede ayudar a **APEX** a evaluar la efectividad del protocolo y a documentar las lecciones aprendidas para tenerlas presentes en futuras ocasiones.

Además de las medidas señaladas en la Política de Seguridad, algunas medidas que pueden contribuir para prevenir futuros incidentes de seguridad sugeridas por la SIC son:

- Reforzar los programas de capacitación y educación del personal.
- Identificar y mejorar los controles internos que no tuvieron el efecto esperado en la contención del incidente de seguridad.
- Identificar y eliminar malware o desactivar cuentas de usuarios vulnerables.
- Realizar un contraste con las medidas adoptadas para solucionar el incidente de seguridad en cuestión, y garantizar un análisis pormenorizado de las soluciones que pudieron haberse adoptado.
- Actualizar el antivirus de la organización.
- Analizar con el antivirus todo el sistema operativo, incluidas aquellas secciones que no se vieron afectadas.
- Garantizar que la estrategia adoptada encuentre un balance entre la continuidad del negocio y el riesgo intrínseco en los activos que se hayan visto afectados por el incidente de seguridad.
- Elaborar un informe final tendiente a recopilar la información, plazos de actuación y medidas adoptadas, de cara a una revisión por terceras personas.

10. Pasos para responder a un incidente de seguridad recomendados por la SIC. La siguiente figura resume los pasos que debe poner en marcha el Equipo ante la ocurrencia de un incidente de seguridad:



Fuente: SIC (2020), "*Guía para la gestión de incidentes de seguridad en el tratamiento de datos personales*"

Anexo No 2 - Protocolo de eliminación de los datos ante la solicitud de supresión, revocatoria de la autorización o agotamiento de la finalidad

Para hacer efectivos los derechos de supresión y revocatoria de la Autorización de Tratamiento, sin perjuicio del procedimiento señalado en **EL MANUAL** para la atención de solicitudes de los titulares, así como las Políticas Globales y directrices implementadas por **Publicis Groupe**, en esta sección se establecen guías para la adecuada eliminación de los datos personales en estos escenarios y cuando se agota la finalidad para los cuales fueron recolectados.

1. Cuando una solicitud de supresión de datos o revocatoria de autorización sea procedente, o siempre que se vaya a suprimir o eliminar datos personales de las Bases de datos de la Compañía, se debe realizar un "acta de supresión". No obstante, siempre se debe conservar la prueba de la Autorización de Tratamiento.

2. El acta de supresión deberá indicar las razones por las cuales se suprimieron los datos y la forma en que se eliminaron, y adjuntar a dicha acta la prueba de la Autorización y la solicitud de supresión y/o la orden de la SIC.

3. Dichas actas deben conservarse en un repositorio aparte al que solo pueda acceder el área encargada de la supresión, la **GDPO** y el área legal[3], por lo menos durante 5 años, contados a partir de la suscripción del acta, a menos de que la Ley disponga otro término de conservación. El repositorio puede ser digital o en físico, lo importante es que se conserve la prueba de la Autorización, y de la solicitud de supresión en los casos en que aplique, y se implementen las medidas de seguridad necesarias para poder responder en cualquier momento a una eventual solicitud de la SIC o del Titular.

[3] La creación de un repositorio de pruebas de autorización, por ejemplo, en los términos previstos en el protocolo de eliminación no implicará el deber de registrar una nueva base de datos en el RNBD de la SIC, en la medida en que el acta de destrucción de los datos y sus anexos serían un subconjunto de datos de la respectiva base de datos respecto de la cual se suprimió la información.