Vol. 1 Edición 8 - Abril 2023

IN SOLIDUM

Social

Violación de datos personales y responsabilidad en el ámbito jurídico ecuatoriano

WWW.INSOLIDUMABOGADOS.COM

Introducción

Por Mgtr. José Ramírez

Fuente: El Economista - La violación de datos personales por terceras personas recae sobre el responsable del tratamiento *(https://www-eleconomista-es.cdn.ampproject.org/c/s/www.eleconomista.es/legal/amp/12247718/la-violacion-de-datos-personales-por-terceras-personas-recae-sobre-el-responsable-del-tratamiento)*

En el presente artículo queremos basarnos en una reciente noticia publicada por El Economista, donde se aborda la problemática de la violación de datos personales y cómo la responsabilidad recae sobre el responsable del tratamiento de datos en el marco de la normativa europea, conforme se lee en la nota. La noticia resalta la importancia de garantizar la seguridad y privacidad de los datos personales, así como las consecuencias legales que pueden enfrentar las empresas y otro tipos de organizaciones en caso de una violación de datos.

La situación planteada en Europa indudablemente es preocupante, debido a que demuestra la vulnerabilidad de los datos personales frente a ciberataques y la necesidad imperiosa de tomar medidas y acciones adecuadas para protegerlos. Así también, pone de manifiesto la importancia de cumplir con las regulaciones y responsabilidades que recaen sobre todo tipo de organizaciones y responsables del tratamiento de datos.

En esta oportunidad me he atrevido a realizar un breve análisis comparativo entre la normativa europea y la ecuatoriana en

materia de protección de datos, específicamente en lo que respecta a las responsabilidades y obligaciones del responsable del tratamiento de datos personales conforme lo prevé nuestra Ley Orgánica de Protección de Datos, LOPD.

En nuestro país, la LOPD establece las obligaciones del responsable y encargado del tratamiento de datos personales en su Artículo 47. Entre las obligaciones más relevantes que he podido identificar incluyen el cumplimiento de los principios y derechos establecidos en la LOPD, la implementación de medidas administrativas, técnicas, físicas, organizativas y jurídicas apropiadas para garantizar y demostrar que el tratamiento de datos personales se ha realizado conforme a la normativa, y la notificación a la Autoridad de Protección de Datos Personales (que por cierto aún no se ha expedido el Reglamento General a la LOPD, ni se ha creado el organismo de control, mucho menos designado una autoridad de protección de datos) y al titular de los datos acerca de violaciones a las seguridades implementadas para el tratamiento de datos personales.

Por otro lado, el Artículo 49 de la LOPD describe las funciones del delegado de protección de datos personales, quien asesora al responsable y al encargado del tratamiento de datos personales, supervisa el cumplimiento de la normativa y coopera estrechamente con la Autoridad de Protección de Datos Personales.

Haciendo el ejercicio de comparar las regulaciones europeas y ecuatorianas en materia de protección de datos, se desprende que ambas legislaciones establecen responsabilidades claras para el responsable del tratamiento de datos personales en caso de violación de datos. Si bien existen diferencias en cuanto a los detalles específicos de cada normativa, la premisa básica es similar: el responsable del tratamiento de datos personales debe garantizar la seguridad y privacidad de los datos, así como actuar diligentemente en caso de incidentes.

Por lo tanto, es fundamental que las empresas ecuatorianas se aseguren de cumplir con las obligaciones establecidas en la LOPD y, en caso de un incidente de violación de datos, actúen de manera responsable y rápida para minimizar los riesgos y las consecuencias legales.

Adicionalmente, es importante mencionar que las empresas en Ecuador deben estar conscientes de las implicaciones legales que conlleva no cumplir con la Ley Orgánica de Protección de Datos (LOPD). En caso de no adoptar las medidas adecuadas para garantizar la seguridad y protección de los datos personales, las empresas pueden enfrentar sanciones económicas, daños a su reputación y posibles acciones legales por parte de los titulares de los datos.

Por otro lado, es esencial que las organizaciones ecuatorianas no solo cumplan con la normativa local, sino que también estén al tanto de las regulaciones internacionales en materia de protección de datos, especialmente si manejan información de ciudadanos extranjeros o realizan operaciones comerciales en otros países. De esta manera, podrán garantizar un nivel adecuado de protección de datos en todas sus operaciones y minimizar el riesgo de enfrentar problemas legales.

En conclusión, la ciberseguridad y la protección de datos personales son temas de gran relevancia tanto a nivel nacional como internacional. Las empresas en Ecuador deben prestar atención a las responsabilidades y obligaciones establecidas en la LOPD y otros marcos regulatorios, y adoptar medidas efectivas para garantizar la seguridad de los datos personales que manejan. Al hacerlo, estarán protegiendo no solo a sus clientes y

empleados, sino también a sus propias operaciones y reputación en el mercado.

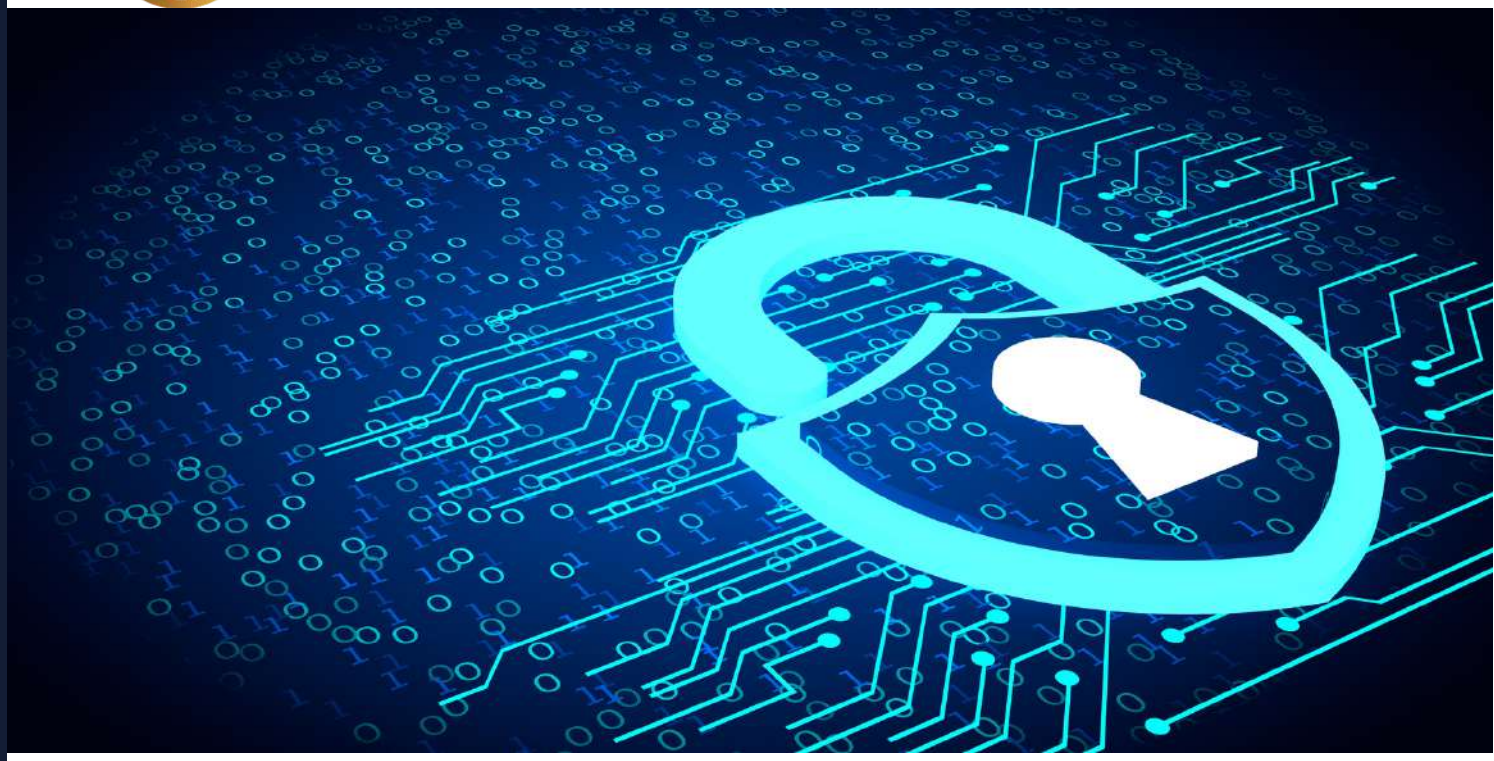
Tomando en cuenta los artículos 50 y 65 de la Ley Orgánica de Protección de Datos (LOPD), podemos destacar la importancia del papel del Delegado de Protección de Datos Personales en el marco legal ecuatoriano. Según el Artículo 50, el responsable y el encargado del tratamiento de datos personales deben garantizar la participación adecuada del delegado en todas las cuestiones relacionadas con la protección de datos personales, facilitar su acceso a los recursos necesarios y asegurar su capacitación y actualización en la materia. Además, el delegado debe mantener una relación directa con el más alto nivel ejecutivo y de decisión del responsable y encargado del tratamiento de datos, así como mantener la más estricta confidencialidad respecto a sus funciones.

En el Artículo 52, se señala que los responsables y encargados de tratamiento de datos personales pueden adherirse voluntariamente a códigos de conducta, certificaciones, sellos y marcas de protección, y cláusulas tipo. Aunque estas iniciativas de autorregulación no eximen a las empresas de cumplir con las disposiciones de la LOPD, pueden ser un complemento útil para demostrar su compromiso con la protección de datos personales.

Por último, el Artículo 65 establece que, en caso de incumplimiento de las disposiciones de la LOPD o transgresión a los derechos y principios que componen el derecho a la protección de datos personales, la Autoridad de Protección de Datos Personales puede dictar medidas correctivas. Estas medidas pueden incluir la eliminación de los datos y la imposición de medidas técnicas, jurídicas,

organizativas o administrativas para garantizar un tratamiento adecuado de los datos personales.

La LOPD define un marco legal sólido para garantizar la protección de datos personales en Ecuador y establece responsabilidades y obligaciones específicas para los responsables y encargados del tratamiento de datos. La adopción de medidas de autorregulación y la designación de un Delegado de Protección de Datos Personales, así como la implementación de las medidas correctivas requeridas en caso de incumplimiento, son aspectos clave para garantizar el cumplimiento de la normativa y proteger los derechos de los titulares de datos personales en el país.



Análisis de las sanciones previstas en la LOPD

Las leyes de protección de datos buscan garantizar la privacidad y seguridad de los datos personales de los ciudadanos quienes son dueños de sus datos personales, y por lo tanto la Ley garantiza y defiende el uso adecuado que se le dan a sus datos. En este sentido, es importante que las personas conozcan las sanciones que pueden enfrentar en caso de incumplimiento para efectos de defender sus derechos. En consecuencia de esto, me he permitido presentar una explicación más amigable de las sanciones por incumplimiento de la ley de protección de datos en tres categorías: infracciones leves, graves y sanciones correspondientes.

Infracciones leves del Responsable de protección de datos incluyen:

- No atender adecuadamente las solicitudes o quejas de los titulares de datos.
- No proteger adecuadamente los datos desde el diseño y por defecto.
- No contar con políticas de protección de datos adecuadas.
- Elegir un encargado del tratamiento de datos personales sin garantías suficientes.
- No cumplir con las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.
- Infracciones graves del Responsable de protección de datos incluyen:
- No implementar medidas para garantizar un tratamiento de datos personales conforme a la ley.
- Utilizar datos personales con fines distintos a los declarados.

- Ceder o comunicar datos personales sin cumplir con los requisitos y procedimientos establecidos.
- No utilizar metodologías de análisis y gestión de riesgos adaptadas.
- No realizar evaluaciones de impacto cuando sean necesarias.
- No implementar medidas para prevenir y controlar riesgos y vulneraciones a la seguridad de datos personales.
- No notificar vulneraciones a la seguridad y protección de datos personales.
- No mantener actualizado el Registro Nacional de protección de datos personales.
- No designar al delegado de protección de datos personales cuando corresponda.
- No permitir auditorías o inspecciones por parte del auditor acreditado.

Infracciones leves del Encargado de protección de datos incluyen:

- No colaborar con el responsable del tratamiento de datos personales en atender solicitudes de titulares.
- No facilitar información sobre el cumplimiento de las obligaciones establecidas en la ley.
- No permitir o contribuir a auditorías o inspecciones por parte del responsable del tratamiento de datos personales.
- No cumplir con las medidas correctivas dispuestas por la Autoridad de Protección de Datos Personales.
- Infracciones graves del Encargado de protección de datos incluyen:
- Realizar tratamientos de datos personales sin observar los principios y derechos establecidos en la ley.
- No tratar datos personales conforme al contrato con el responsable del tratamiento de datos personales.

- No suscribir contratos con cláusulas de confidencialidad y tratamiento adecuado de datos personales.
- No implementar mecanismos para mantener la confidencialidad, integridad, disponibilidad y resiliencia de los datos personales.
- No implementar medidas preventivas y correctivas en la seguridad de los datos personales.
- No suprimir los datos personales transferidos o comunicados al responsable del tratamiento de datos personales.
- Comunicar datos personales sin cumplir con los requisitos y procedimientos establecidos.
- No notificar al responsable del tratamiento de datos personales sobre vulneraciones de seguridad.

Sanciones por infracciones leves:

- Multas de 1 a 10 salario básico unificado

Forma más adecuada de implementar un sistema de tratamiento de datos personales

Llegando a este punto del artículo, he considerado que es importante conocer los mecanismos más adecuados para garantizar el cumplimiento de la LOPD en cualquier tipo de organización, empezando por designar a un responsable de protección de datos, conocido como DPO (por sus siglas en inglés, Data Protection Officer). El DPO debe poseer un conocimiento adecuado en la normativa de protección de datos y será el encargado de supervisar y asegurar el cumplimiento de la LOPD dentro de la organización.

Para iniciar el proceso de protección de datos, es indispensable llevar a cabo un análisis preliminar de riesgos. Este análisis consiste en identificar y evaluar los riesgos asociados con el tratamiento de datos personales en la organización. El objetivo de esta actividad es comprender las posibles amenazas y vulnerabilidades, lo que permite adoptar medidas de seguridad adecuadas para proteger los datos personales.

Una vez que se hayan identificado los riesgos, es esencial implementar medidas de seguridad técnicas y organizativas para garantizar la confidencialidad, integridad y disponibilidad de la información. Este tipo de medidas pueden incluir la encriptación de datos, la implementación de sistemas de autenticación de usuarios y la creación de políticas internas que regulen el acceso a los datos personales.

Además, con igual importancia se debe elaborar un registro de actividades de

tratamiento de datos personales. Este registro debe documentar todas las actividades de tratamiento llevadas a cabo por la organización, incluyendo la finalidad del tratamiento, las categorías de datos personales involucrados y los destinatarios a los que se comunican los datos.

Una parte esencial para dar cumplimiento a la LOPD es establecer políticas de privacidad claras y transparentes. Estas políticas deben ser informadas a las personas sobre cómo se tratan sus datos personales, cuáles son sus derechos en relación con sus datos y cómo pueden ejercer estos derechos. Para garantizar una comunicación efectiva, las políticas de privacidad deben ser fácilmente accesibles y comprensibles para cualquier persona.

Antes de tratar los datos personales, un aspecto de muchísima importancia es obtener el consentimiento libre, informado, específico e inequívoco de las personas, a menos que exista otra base legal que permita el tratamiento. En cuanto al consentimiento debe ser obtenido mediante un proceso claro y sencillo que garantice que las personas comprenden a qué están dando su consentimiento. El incumplimiento a esta disposición acarreará sanciones legales para la organización.

Asimismo, las organizaciones deben respetar y facilitar el ejercicio de los derechos de los interesados. Este es un aspecto de suma relevancia por cuanto hoy en día persisten organizaciones que almacenan cantidades gigantescas de datos de usuarios que no han brindado su consentimiento, y tienen todo el derecho de ejercer las acciones administrativas y legales para defender sus derechos. Estos derechos incluyen el acceso, la rectificación, la supresión, la limitación

del tratamiento, la portabilidad de los datos y la oposición. Es fundamental responder a las solicitudes de ejercicio de estos derechos en los plazos establecidos por la LOPD.

En caso de que se produzca una violación de la seguridad de los datos personales, la organización debe contar con procedimientos establecidos para la notificación de estas violaciones. La notificación debe realizarse a la Autoridad de Protección de Datos del Ecuador y, en ciertos casos, también a las personas afectadas.

Un aspecto esencial también es la capacitación de los empleados en materia de protección de datos personales, considerado otro aspecto clave para garantizar el cumplimiento de la LOPD. Los empleados deben estar informados sobre las políticas y procedimientos internos de la empresa en relación con la protección de datos, así como sobre sus responsabilidades en este ámbito.

Al mantener al personal debidamente informado se mitigarán posibles brechas de seguridad, en virtud de que la mayoría de los ciberdelitos tienen que ver con prácticas de ingeniería social, donde el aspecto humano es el más débil.

El monitoreo y la auditoría periódica de las prácticas de tratamiento de datos personales son esenciales para garantizar un cumplimiento continuo con la LOPD. Estas auditorías deben realizarse de manera regular y deben incluir la revisión de las medidas de seguridad, las políticas de privacidad y la evaluación de la efectividad de las acciones correctivas implementadas. Los resultados obtenidos de las auditorías deben ser documentados y utilizados para mejorar continuamente las prácticas de protección de datos de la empresa. Además,

las auditorías permitirán conocer las fortalezas y debilidades de las prácticas implementadas en las organizaciones.

La colaboración con terceros que traten datos personales en nombre de la organización, también conocidos como encargados del tratamiento, debe ser gestionada adecuadamente. Es imprescindible firmar acuerdos contractuales con estos terceros que incluyan cláusulas específicas sobre protección de datos y garantías adecuadas para asegurar que el tratamiento se realice conforme a la LOPD. Además, la organización debe supervisar el cumplimiento de la normativa por parte de estos terceros y tomar las medidas necesarias en caso de incumplimiento.

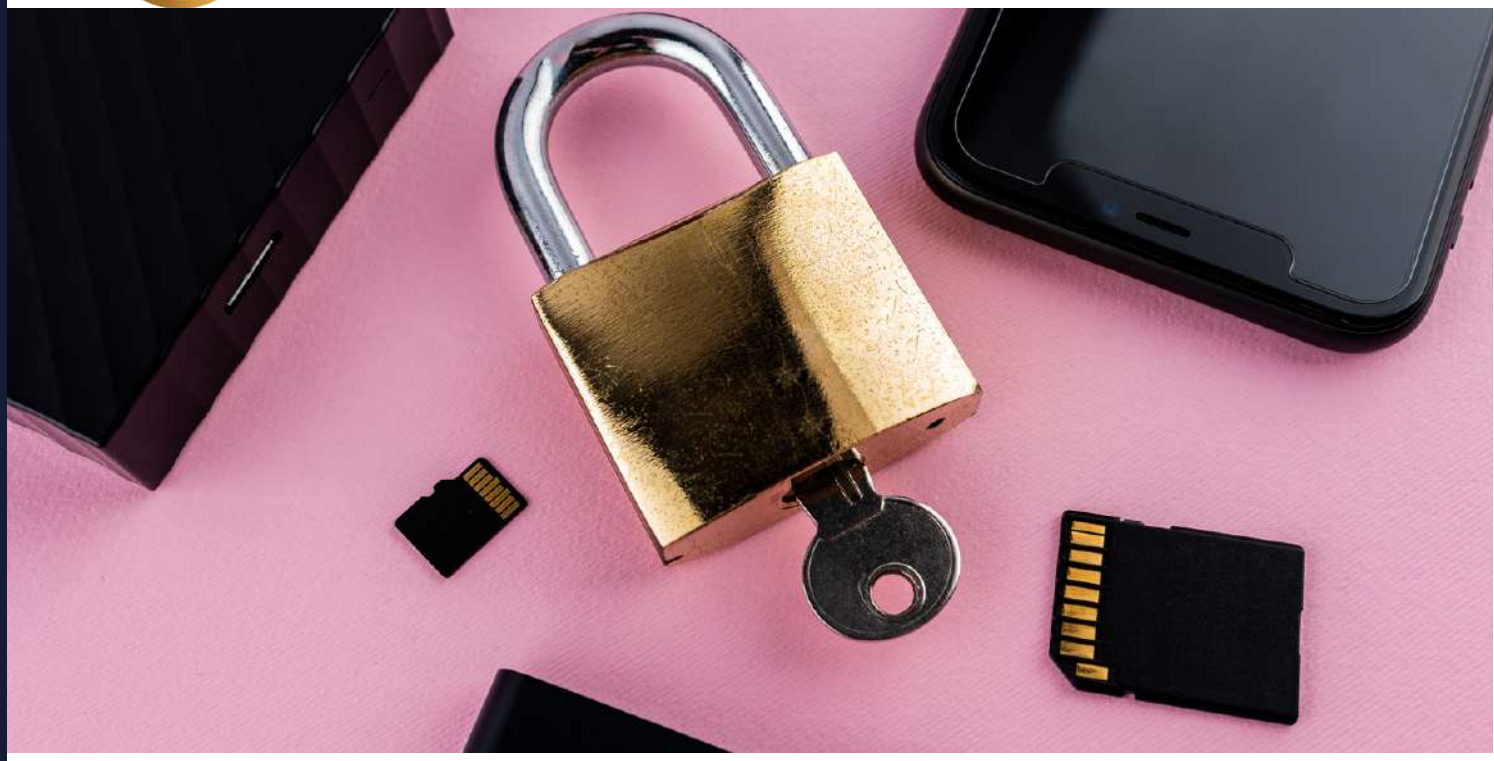
La gestión de las transferencias internacionales de datos personales es otro aspecto que debe ser abordado con especial atención. Cuando los datos personales sean transferidos a países fuera del Ecuador, la organización debe asegurarse de que se cumplen los requisitos establecidos por la LOPD en relación con las garantías y mecanismos adecuados para proteger los datos personales.

Así también, en caso de que la organización desarrolle nuevos productos, servicios o procesos que impliquen el tratamiento de datos personales, se sugiere aplicar el principio de protección de datos desde el diseño y por defecto, lo que quiere decir es integrar las consideraciones de protección de datos en todas las etapas de desarrollo y garantizar que la privacidad sea una prioridad desde el inicio del proyecto.

Es necesario también fomentar una cultura de protección de datos dentro de la organización, en la que todos los empleados,

desde la alta dirección hasta el personal operativo, comprendan la importancia de proteger los datos personales y se comprometan a cumplir con la LOPD. Lo cual estamos hablando de generar un cambio de nuestra visión y concepción para asimilar la importancia de cuidar y proteger los datos. En cuanto a la creación de una cultura de protección de datos, contribuirá a minimizar los riesgos y evitar posibles sanciones administrativas por incumplimiento de la normativa.

La implementación de un correcto sistema de tratamiento de datos personales en las organizaciones requiere una combinación de medidas técnicas, organizativas y culturales que garanticen el cumplimiento de la LOPD. Con la adopción de un enfoque proactivo y la atención continua a la protección de datos personales, permitirá a las organizaciones evitar sanciones y fortalecer la confianza de sus clientes y usuarios en el manejo de su información personal.



Conclusiones y recomendaciones

A manera de conclusión, la protección de datos personales es un tema de creciente importancia en la era digital, y tanto las organizaciones como el público en general deben estar conscientes de sus derechos y responsabilidades en este ámbito. La LOPD en Ecuador establece un marco normativo que busca garantizar un tratamiento adecuado de los datos personales y proteger la privacidad de las personas.

Recomendaciones para el público en general:

- **Informarse**: Conocer sus derechos en relación con la protección de datos personales es de suma importancia y debemos ser más conscientes de ello. Además, hay que familiarizarse con la LOPD y las disposiciones que le son aplicables, como el derecho de acceso, rectificación, supresión y otros.
- **Responsabilidad**: Asegúrese de que sus datos personales sean tratados de manera responsable por las organizaciones con las que interactúa. Antes de proporcionar información personal, verifique las políticas de privacidad y las medidas de seguridad implementadas por las organizaciones. Finalmente, si alguien lo contacta y usted no ha brindado su consentimiento, asesórese con nuestros abogados especialistas para defender sus derechos.
- **Protección en línea**: Sea cauteloso al compartir información personal en línea y en redes sociales. Asegúrese de utilizar contraseñas seguras, proteger sus dispositivos con soluciones de seguridad y mantener sus aplicaciones y sistemas operativos actualizados.
-

- **Denunciar violaciones**: Si considera que sus datos personales han sido tratados de manera indebida o que sus derechos han sido violados, no dude en presentar una denuncia ante la Autoridad de Protección de Datos del Ecuador. Esta entidad tiene la facultad de investigar y, en su caso, sancionar a las empresas que incumplan con la LOPD.

- **Educación continua**: La protección de datos personales es un tema en constante evolución. Manténgase informado sobre las nuevas tendencias y desarrollos en esta área, así como sobre las mejores prácticas en seguridad y privacidad digital.

Siguiendo estas recomendaciones, el público en general podrá contribuir a crear una cultura de protección de datos personales y garantizar el respeto de sus derechos en esta materia. La responsabilidad compartida entre las empresas, las autoridades y los ciudadanos es fundamental para lograr un entorno digital seguro y respetuoso de la privacidad de todos.

En este contexto, si desea profundizar en la protección de datos personales y garantizar el cumplimiento de la LOPD en su empresa o actividad, nuestro estudio jurídico In Solidum Abogados es una opción confiable y experta en la materia. Contamos con abogados especialistas en protección de datos y prevención digital, quienes están altamente calificados para asesorarle en todos los aspectos relacionados con la protección de datos personales.

En In Solidum Abogados, nos comprometemos a defender sus derechos en caso de infracciones y a implementar sistemas adecuados de tratamiento de datos

personales para todo tipo de organizaciones, independientemente de su actividad económica. Nuestro equipo de profesionales se mantiene siempre actualizado en la legislación y las mejores prácticas en el ámbito de la protección de datos, lo que nos permite ofrecer un servicio integral y de calidad a nuestros clientes.

Le invitamos a contactarnos para recibir asesoría especializada y respaldar su confianza en nosotros, ya que conocemos la LOPD y estamos preparados para proteger y defender sus derechos en esta materia. No dude en ponerse en contacto con nuestras oficinas ubicadas en la ciudad de Quito, Ecuador, o bien, comuníquese con nosotros por teléfono o correo electrónico. Estamos a su disposición para brindarle la información y el apoyo necesario en la protección de datos personales y la prevención digital.

En Solidum Abogados: Su aliado en la protección de datos y prevención digital.

IN SOLIDUM
ABOGADOS