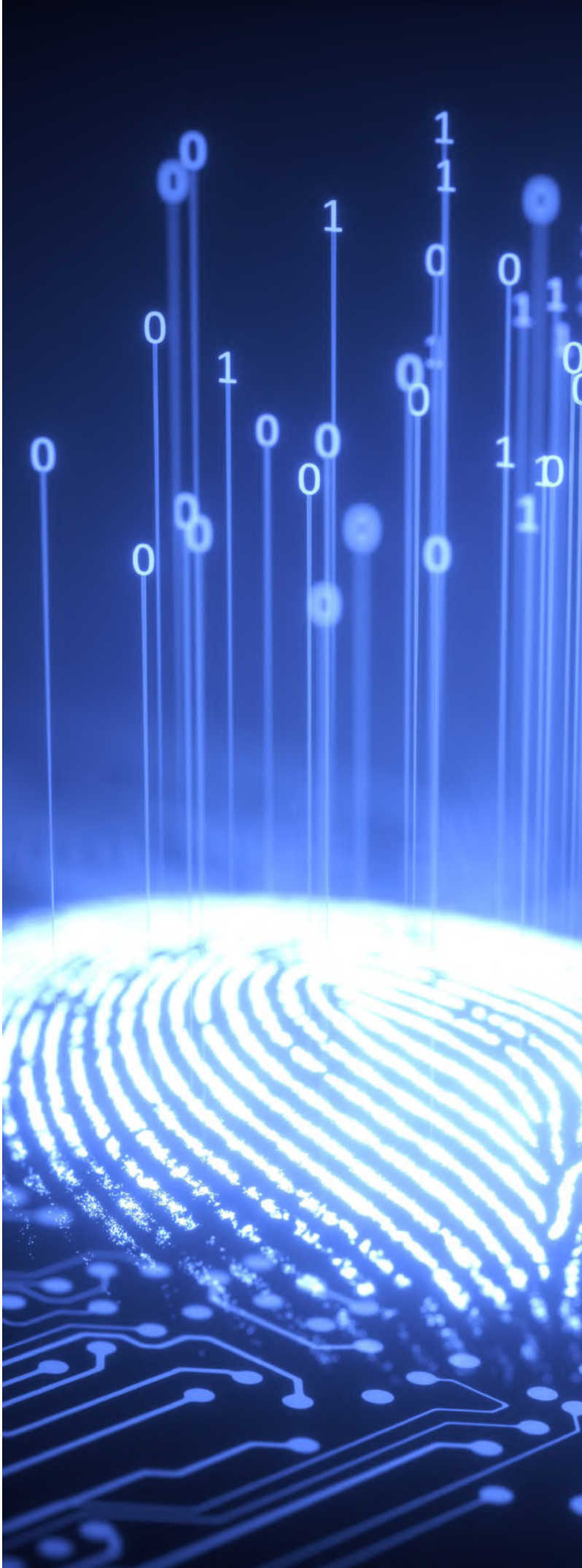
BDO 2022

¿CÓMO IMPLEMENTAR UN PROGRAMA DE PROTECCIÓN DE DATOS PERSONALES?

Contenido



Introducción

Millones de personas desconocen cómo se recopilan, utilizan o comparten sus datos personales en nuestra sociedad cada vez más digital. Como empresa, es más importante que nunca contar con un Programa de Protección de Datos Personales que permita proteger a los clientes, empleados y/o grupos de interés y cumplir con las regulaciones aplicables.

Durante la pandemia de Covid-19, la Autoridad Nacional de Protección de Datos Personales - ANPD en Perú ha impuesto **más de 9.5 millones de soles en multas.** Debido a esto, las organizaciones deben reforzar y centrar sus esfuerzos en la creación de un Programa Integral de Protección de Datos Personales, teniendo en cuenta que, una vez implementados los controles y lineamientos de la Ley de Protección de Datos Personales, estos requieren ser revisados y evaluados periódicamente.

Pero, en primer lugar, ¿qué es la Protección de Datos Personales?

La Protección de Datos Personales tiene como objetivo garantizar y proteger el derecho fundamental de toda persona de tener el control de aquellos datos que se puedan utilizar para identificarla. Para proteger los datos personales, las organizaciones disponen de un conjunto de medidas jurídicas, organizativas y técnicas orientadas a salvaguardar los datos de carácter personal.

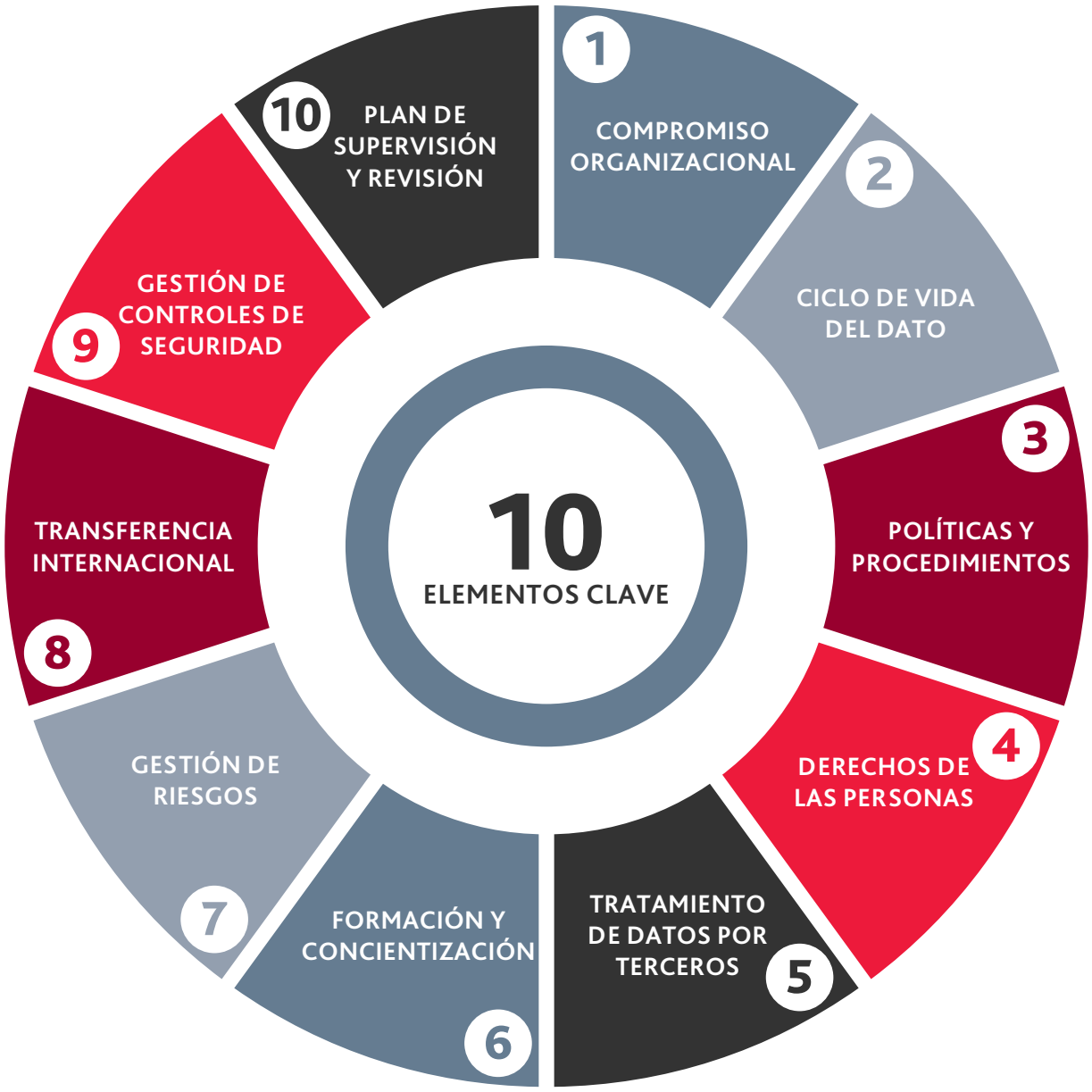
Para ello, establece reglas, requisitos y obligaciones que deberán cumplir las organizaciones al recopilar, registrar, almacenar, conservar, transferir y utilizar datos personales. Asimismo, deberán poner en marcha procedimientos para atender los derechos de las personas naturales.

Elementos clave de un Programa de Protección de Datos Personales

La privacidad de datos es el conjunto de estrategias y procesos que se centran en cómo se recopilan, procesan, almacenan, comparten, retienen y destruyen los datos personales, mientras que la protección de datos se centra en asegurar la disponibilidad e integridad de los datos y protegerlos del acceso no autorizado.

Un Programa de Protección de Datos Personales considera lineamientos para fortalecer la privacidad y la protección de datos personales, minimizando el riesgo de que su organización pueda enfrentar sanciones y/o multas de entidades reguladoras, quejas de los clientes y daño reputacional, al no haber implementado de manera eficaz controles mínimos de seguridad.

Un Programa Integral de Protección de Datos debe contar con los siguientes elementos:



COMPROMISO ORGANIZACIONAL

El compromiso organizacional solo se puede tangibilizar si los ejecutivos son conscientes de la importancia de atender la privacidad de datos en su organización. A partir de ello, es importante iniciar con la definición de los responsables o líderes a cargo del cumplimiento de la protección de los datos personales en la organización y asignar funciones y/o actividades específicas para ejecutar de forma sistemática el Programa de Protección de Datos Personales, cumpliendo con los principios, deberes y obligaciones en materia de protección de datos. Para ello, es importante considerar que las personas asignadas como roles responsables cuenten con el conocimiento sobre la cadena de valor de la organización y el impacto del uso de los datos personales en la misma, además de aspectos técnicos y jurídicos.

CICLO DE VIDA DEL DATO

Contar con el control integral de la recopilación, tratamiento y almacenamiento de datos en medios físicos o digitales, a fin de conocer qué datos personales almacenan y cómo los utilizan, considerando la finalidad de su recolección. Por este motivo, se requiere contar con un inventario de los datos personales que administra la organización considerando elementos como: el volumen de datos, categoría de datos, transferencia nacional y/o internacional, tiempo de conservación e identificación de múltiples localizaciones; que ayuden a elaborar un reporte adecuado para las entidades reguladoras. Este inventario es útil para demostrar la gobernabilidad sobre los datos personales.

POLÍTICAS Y PROCEDIMIENTOS

La Política de Protección de Datos Personales debe reflejar el compromiso de la organización con el cumplimiento normativo. Los procedimientos de protección de datos deben proporcionar los lineamientos generales de la organización para el tratamiento de datos personales, desde su recopilación, tratamiento, almacenamiento, transferencia y eliminación, y considerar las actividades a ser ejecutadas por los roles previamente definidos. Procedimientos como la gestión de incidentes, gestión de accesos, gestión de respaldos de datos, entre otros; necesitan ser revisados para asegurar la privacidad y protección de la información personal.

DERECHOS DE LAS PERSONAS

Las personas cuentan con cuatro (4) derechos fundamentales: Acceso, Rectificación, Cancelación u Oposición (conocidos como Derechos ARCO). Estos derechos permiten a las personas obtener información sobre sus propios datos y cómo son utilizados por las organizaciones. Establecer un canal de atención de los Derechos ARCO permite garantizar el pleno y efectivo ejercicio de los mismos por parte de las personas, contemplando los plazos establecidos de acuerdo a las disposiciones de la normativa vigente.

TRATAMIENTO DE DATOS POR TERCEROS

En las relaciones contractuales celebradas, en virtud de las cuales se realiza tratamiento de datos personales por parte de terceros (proveedores y/o contratistas), se deben definir cláusulas robustas de confidencialidad y manejo de la información personal por parte de los terceros. Todos los terceros, deben aceptar y cumplir los lineamientos que la organización disponga como parte del servicio brindado. De igual manera, garantizar el cumplimiento de la normativa de protección de datos personales.

Las organizaciones que comparten datos personales con terceros deben comunicarlo a las personas y, asimismo, pueden realizar revisiones (auditorías) del cumplimiento de las disposiciones realizadas por el tercero.

FORMACIÓN Y CONCIENTIZACIÓN

Entrenamientos y desarrollo de programas para crear conciencia en materia de protección de datos personales dirigidos a todo el personal de la organización para incluir anualmente actividades de capacitación sobre la Ley. Dicho esfuerzo busca poder crear una cultura organizacional de respeto hacia la privacidad de los datos personales, contemplando la segmentación de talleres según los grupos objetivos determinados, los cuales pueden ser los siguientes:

- Capacitación sobre las responsabilidades de los diversos actores (líderes a cargo) determinados en el Programa de Protección de Datos Personales.
- Capacitación en temas técnicos orientados al personal de las áreas de tecnología.
- Capacitación dirigida a todo el personal que maneja o realiza tratamiento de datos personales por el desempeño de sus funciones, entre otros.

GESTIÓN DE RIESGOS

De acuerdo al tipo de tratamiento que realice la organización, se debe definir una matriz de riesgos que identifique y mida los riesgos asociados al tratamiento de datos personales en la organización. El análisis de riesgos debe estar orientado en lo siguiente:

a. **Riesgo de protección de la información:** Acceso no autorizado a los datos personales, modificación o alteración intencionada de datos personales, pérdida o fuga de información
b. **Riesgos asociados al cumplimiento:** Ausencia de procedimientos para el ejercicio de los derechos de las personas naturales, tratamiento ilícito de datos personales, tratamiento desproporcional de información personal, entre otros.

TRANSFERENCIA INTERNACIONAL

Es importante que las organizaciones identifiquen cuáles son las transferencias internacionales que esté realizando de los datos personales bajo su responsabilidad, dado que según las normativas en materia de protección de datos personales, toda organización está obligada a reportar los destinatarios de las transferencias internacionales de datos y asegurar la protección de los mismos durante su transferencia.

Actualmente, el uso de tecnologías de vanguardia (cloud computing) se da como parte de la ejecución de una relación contractual que puede conllevar a la transmisión internacional de datos personales, por tanto, se aplican los mismos criterios establecidos para el tratamiento de datos por terceros a nivel nacional. Adicional a ello, se revisa que el país cuente con un nivel adecuado de protección de datos personales, en los términos que rigen la transferencia de datos personales. Asimismo, es importante tener identificadas de manera clara todas las transferencias internacionales de datos que realice la compañía, a fin de ser reportados ante la Autoridad Nacional de Protección de Datos Personales.

Las nuevas tecnologías requieren reforzar los controles técnicos durante la transferencia para velar por la privacidad y protección de los datos, asimismo, también, valerse de cláusulas contractuales u otros instrumentos jurídicos en los que se establezcan las obligaciones determinadas para la protección de los mismos.

GESTIÓN DE CONTROLES DE SEGURIDAD

Un Programa de Protección de Datos Personales se basa en la implementación de controles de seguridad. Esto incluye controles organizacionales, tales como: políticas, capacitación y concientización, planes de respuesta a incidentes y políticas de contraseñas, controles técnicos: tales como cifrado, anonimización, registro, autenticación multifactor y detección de vulnerabilidades, y controles jurídicos, tales como: cláusulas de consentimiento para el tratamiento de datos personales, autorización de uso de imagen y acuerdos de confidencialidad celebrados con terceros y personal de la organización.

PLAN DE SUPERVISIÓN Y REVISIÓN

El monitoreo del cumplimiento del Programa de Protección de Datos Personales se realiza a través de una auditoría anual (medida recomendada) basada en la revisión del cumplimiento de la protección de los datos personales, contemplando la generación de material de trabajo, informes de auditoría, hallazgos identificados e iniciativas o planes de acción a seguir por parte de la organización.

Esta revisión puede realizarse a través de una auditoría interna como también, por una auditoría externa por parte de empresas especializadas en brindar asesoramiento y sostenibilidad al Programa de Protección de Datos Personales.

Tecnologías clave para la Protección de Datos Personales

La protección de datos se debe respaldar en tecnología. Teniendo en cuenta las tecnologías de vanguardia emergentes, las organizaciones pueden adoptar nuevas soluciones tecnológicas que les permitan asegurar la protección de los datos personales bajo su responsabilidad.

A continuación, se mencionan las tecnologías clave que permiten proteger los datos personales:

Gestión integral de accesos

Solución integral que sincroniza la administración de contraseñas, cuentas, privilegios de acceso y dispositivos.

Clasificación de documentos

Identificación automática de información confidencial usando inteligencia artificial.

Anonimización automatizada

Procedimiento tecnológico que elimina la posibilidad de identificar a la persona natural propietaria de los datos.

Sala de datos virtual

Permite almacenar y compartir información confidencial de forma segura agregando un sello de agua de seguridad.

Protección de Datos Personales en canales digitales

Durante los años 2020 y 2021, en el contexto de la pandemia de COVID-19, la Autoridad Nacional de Protección de Datos Personales (ANPD) **fiscalizó a 640 empresas, imponiendo multas por más de 9.5 millones de soles.**

A continuación, presentamos un breve resumen de infracciones relacionadas al incumplimiento de los elementos clave de la protección de datos personales:

INSCRIPCIÓN DEL BANCO DE DATOS PERSONALES	**S/ 11,000**	Una entidad del sector salud fue sancionada por no haber registrado el banco de datos personales de los usuarios de su página web.
DECLARACIÓN DEL FLUJO TRANSFRONTERIZO	**S/ 4,400**	Una entidad del sector salud fue sancionada por no haber comunicado que los datos personales recopilados a través de su página web estaban alojados en el exterior del país (Estados Unidos).
CONSENTIMIENTO INFORMADO	**S/ 79,200**	Una empresa de telecomunicaciones fue sancionada por utilizar los datos personales de sus clientes para una finalidad distinta para la que fueron recopilados.
DERECHOS ARCO	**S/ 52,800**	Una institución educativa fue sancionada por no informar a los titulares de datos personales de forma detallada, sencilla, expresa e inequívoca sobre el uso que se realizará de su información personal.
IMPLEMENTACIÓN DE MEDIDAS DE SEGURIDAD	**S/ 176,000**	Una entidad financiera fue sancionada por no implementar las medidas de seguridad necesarias para el resguardo de los datos personales de sus clientes.

PRINCIPALES CONDUCTAS REVISADAS A TRAVÉS DE MEDIOS DIGITALES

La ANPD es la encargada de velar por la protección de los datos personales y, debido a la pandemia de Covid-19 y el trabajo remoto, ha venido revisando las conductas adoptadas en materia de protección de datos por las instituciones a través de canales digitales, tales como:

Página web

Los usuarios de una página web pueden ser asociados a identificadores en línea (cookies), que permiten identificarlo mientras navega por la web. Para ello, se debe contar con la publicación de una Política de Cookies y solicitar su consentimiento.

Redes sociales

Mediante las redes sociales utilizadas por la organización se pueden publicar imágenes de personas naturales. Para ello, se debe contar con el consentimiento del uso de imagen de dichas personas de acuerdo a las disposiciones del Artículo 18 de la Ley.

Aplicativo móvil

Cuando las personas ingresan a un aplicativo móvil (app) y se crean un usuario utilizando sus datos personales, se debe habilitar una Política de Privacidad y una opción (check box) para que la persona pueda brindar su consentimiento previo e informado.

Chatbot

Los chatbots están programados para interpretar y responder preguntas utilizando Inteligencia Artificial, por lo cual pueden tener acceso a información personal, para ello se debe informar sobre la Política de Privacidad y solicitar el consentimiento del usuario.

¿Cómo afrontar con éxito un proceso de fiscalización de la Ley de Protección de Datos Personales?

DESIGNACIÓN DEL RESPONSABLE DE ATENDER A LA AUTORIDAD DURANTE EL PROCESO DE FISCALIZACIÓN

Definir al encargado, calificado según sus competencias, para acompañar a la Autoridad.

ATENCIÓN A LA AUTORIDAD EN COMPAÑÍA DE UN REPRESENTANTE DEL ÁREA LEGAL

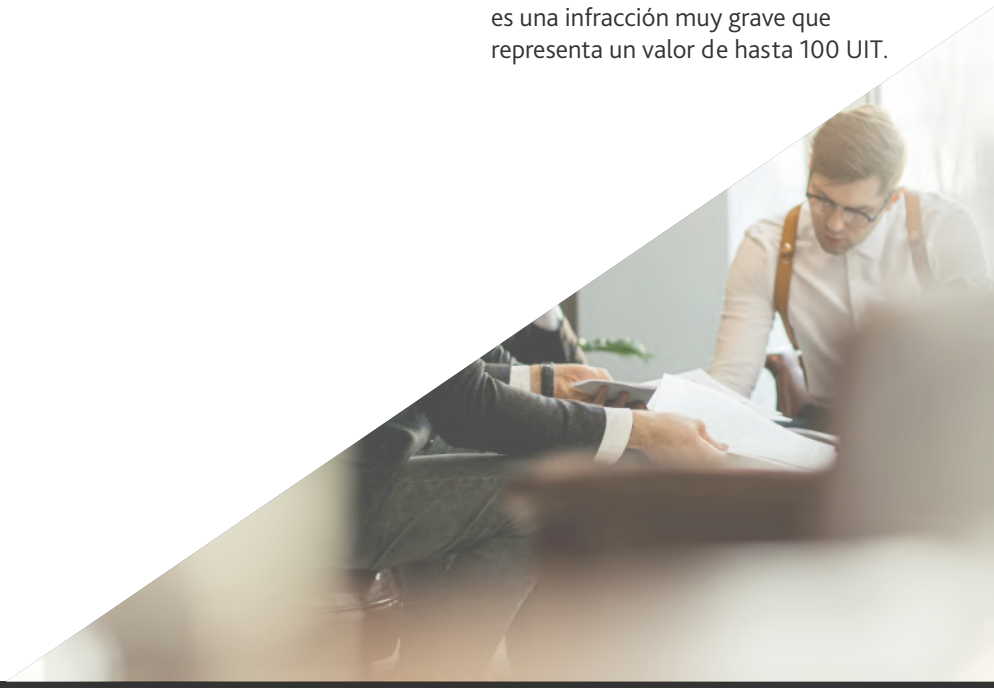
La participación del Áreal Legal puede evitar contingencias dado que cumple el rol de mediador y defensor de la protección de datos.

ASESORÍA DE ESPECIALISTAS EN PROTECCIÓN DE DATOS PERSONALES

La guía de un consultor contribuye a implementar las medidas correctivas y realizar un análisis organizacional de la protección de datos.

DOCUMENTACIÓN E INFORMACIÓN FIDEDIGNA

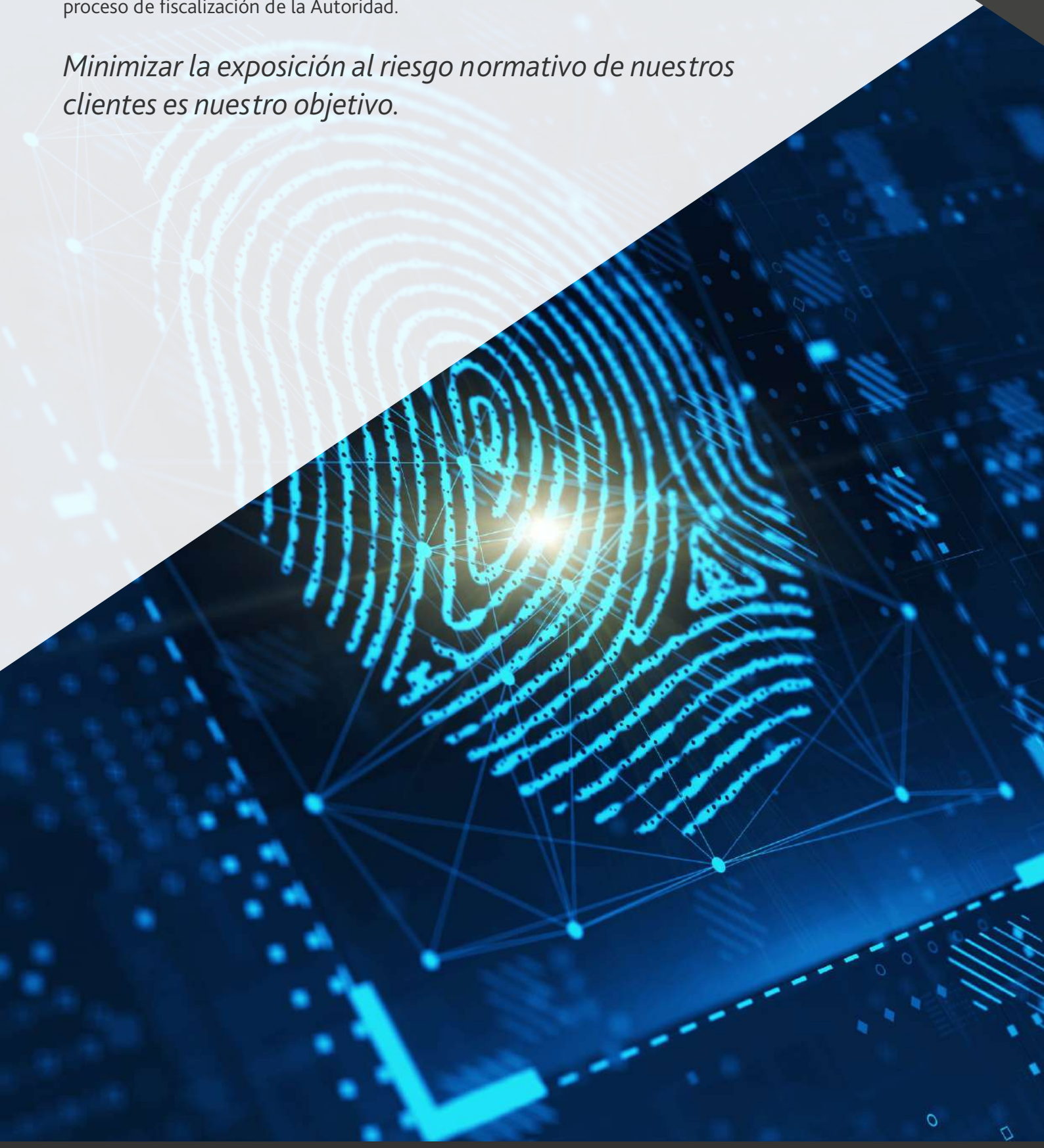
Suministrar documentos e información falsa a la Autoridad es una infracción muy grave que representa un valor de hasta 100 UIT.



Cómo agrega valor BDO

BDO Perú cuenta con experiencia asesorando a corporaciones, empresas e instituciones en el proceso de adecuación a la Ley de Protección de Datos Personales, realizando auditorías periódicas a la norma para darle sostenibilidad y asesorando en el proceso de fiscalización de la Autoridad.

Minimizar la exposición al riesgo normativo de nuestros clientes es nuestro objetivo.



PARA MAYOR INFORMACIÓN:

VICTOR VERA TUDELA
Socio de Consultoría de Negocios
vveratudela@bdo.com.pe

www.bdo.com.pe

AUDITORÍA | TAX & LEGAL | CONSULTORÍA DE NEGOCIOS | BSO