



# Cuenta regresiva y oportunidades emergentes: El rol del abogado ante el nuevo reglamento de protección de datos personales

**Ilustre Colegio de Abogados de Arequipa**  
**12 de marzo de 2025**

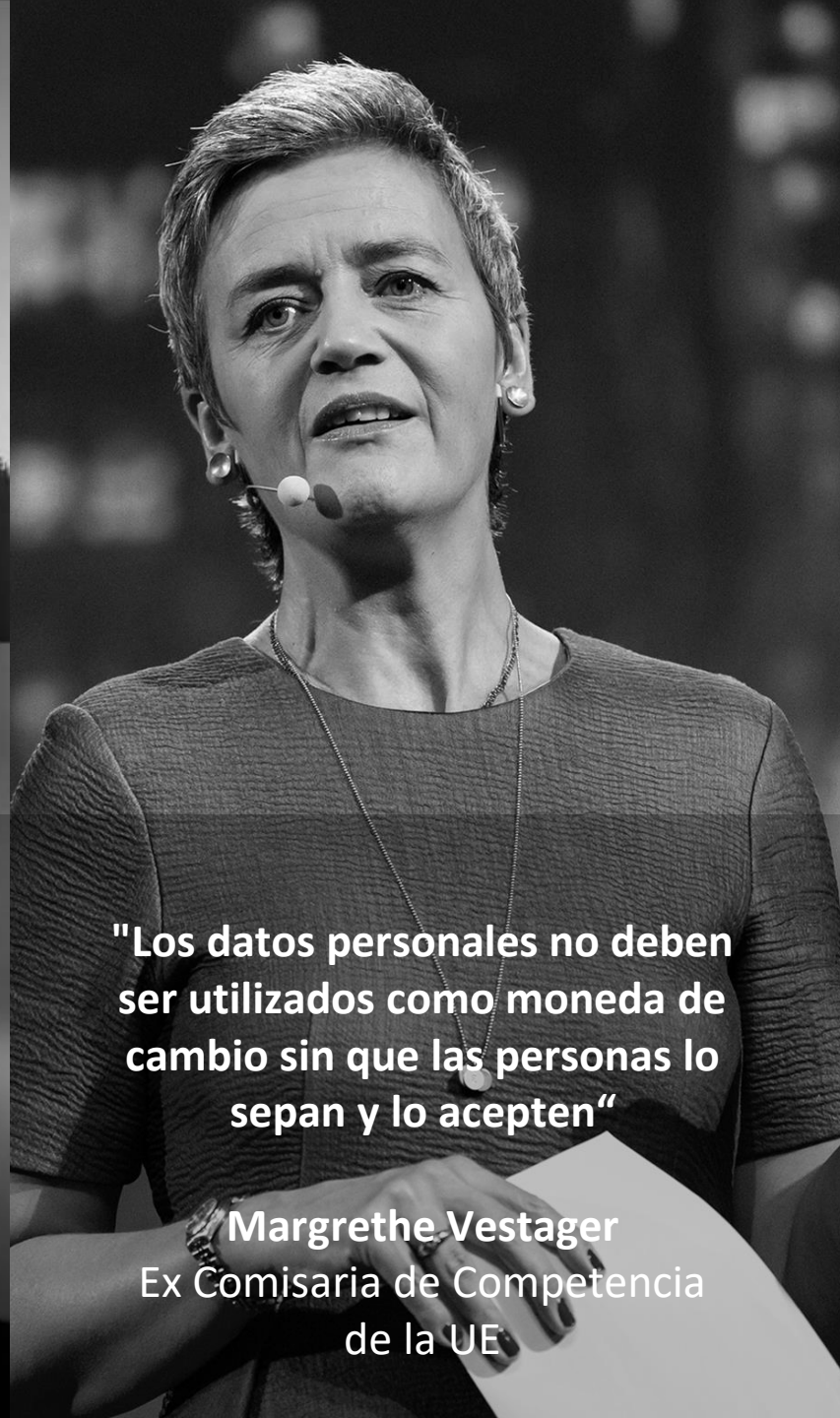
**Suárez & Asociados S.A.C.**  
**RUC 20601063345**  
Calle Los Geranios 104 – Segundo Piso  
Urb. Selva Alegre – Cercado, Arequipa.

[administracion@suarezsociados.pe](mailto:administracion@suarezsociados.pe)  
[www.suarezsociados.pe](http://www.suarezsociados.pe)  
+51 54 294063  
+51 958958184



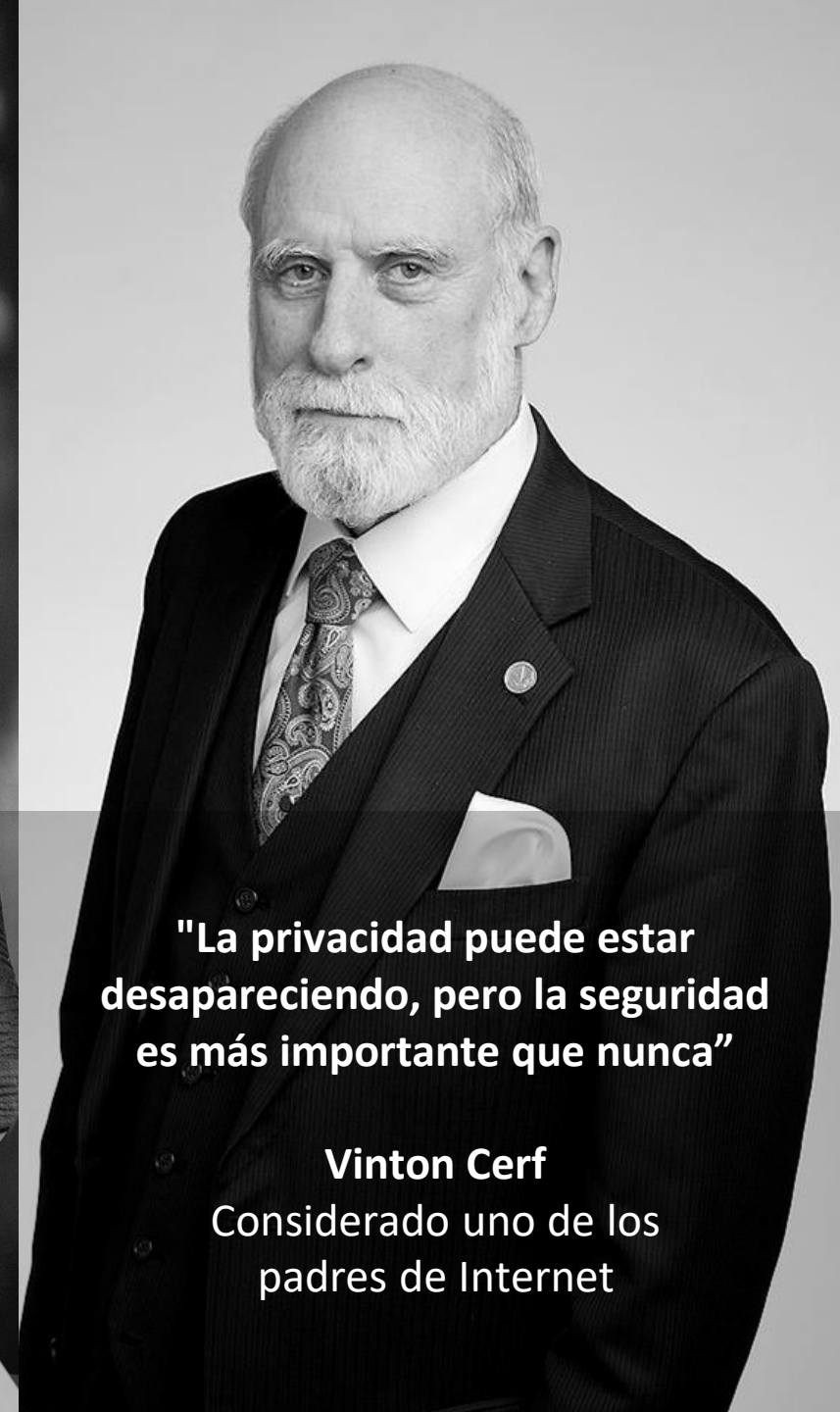
**“Cuando un servicio en línea es gratuito, tú no eres el cliente, sino el producto”**

**Tim Cook**  
CEO Apple



**“Los datos personales no deben ser utilizados como moneda de cambio sin que las personas lo sepan y lo acepten”**

**Margrethe Vestager**  
Ex Comisaria de Competencia  
de la UE



**“La privacidad puede estar desapareciendo, pero la seguridad es más importante que nunca”**

**Vinton Cerf**  
Considerado uno de los  
padres de Internet

# Objetivos de hoy

1. Explicar los cambios y oportunidades del nuevo Reglamento de Protección de Datos Personales.
2. Analizar el impacto en empresas y el rol clave de los abogados en este proceso.
3. Ofrecer estrategias para que los profesionales del derecho se adapten y aprovechen esta transformación.



¿Qué es la  
**protección de datos personales?**



# Derecho fundamental a la protección de datos personales

## La Constitución Política del Perú

Reconoce el derecho que tiene toda persona a que los servicios informáticos, computarizados o no, públicos o privados, no suministren informaciones que afecten la intimidad personal y familiar.

**Es el derecho que tenemos todos a controlar nuestra información personal**



# Ejemplos de algunos datos personales

Nombre

Apellidos

Placa del carro

Número de teléfono

Fecha de nacimiento

Dirección del domicilio

Dirección de correo electrónico

Pueden ser recogidos en bancos de datos:

- De administración pública
- De administración privada



Voz

Fotografía

Huella digital



## La huella de la oreja como método de identificación. Club Ciencias Forenses.

OCTUBRE 27, 2024 - RAFAEL LOPEZ PEREZ - 6 MINS READ

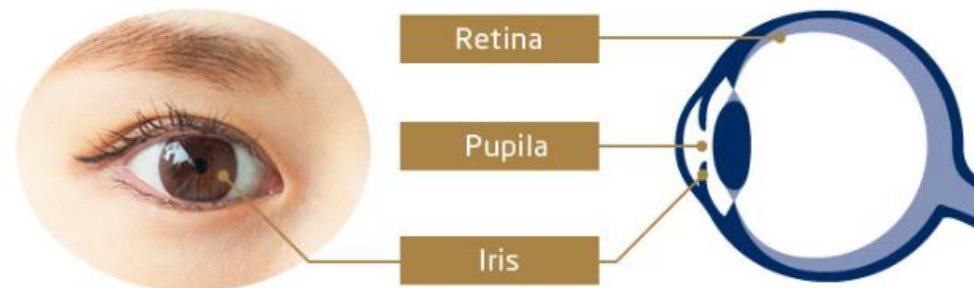


27/2/24 - JUSTICIA

## El iris, ¿el dato biométrico de moda?

*Se trata de una información muy sensible, unívoca y que se mantiene inalterable a lo largo del tiempo*

*Siguen las dudas en torno al rigor de la custodia de estos datos, la anonimización de la información y el interés comercial del proyecto*



# Obligaciones

## Consentimiento

Todos los datos que forman parte de un banco de datos **deben contar con el consentimiento del titular del dato personal**. Los consentimientos deben estar **guardados en un lugar accesible y seguro** para poder atender fiscalizaciones.

## Registro

**Los bancos de datos deben ser registrados** ante la Autoridad Nacional de Protección de Datos Personales indicando los datos que almacena, responsable, ubicación física, forma de obtención y medidas de seguridad implementadas para su protección.

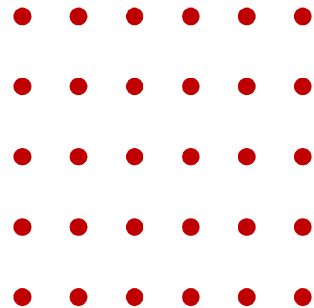
## Seguridad

Las empresas titulares de bancos de datos **deben establecer todas las medidas de seguridad técnicas, legales y organizativas requeridas para garantizar la seguridad y evitar la alteración, pérdida, tratamiento o acceso no autorizado** a sus bancos de datos personales.



# Consentimiento

Para el tratamiento de los datos personales se requiere el consentimiento **expreso, previo, libre e informado** del titular del dato personal.



Expreso e inequívoco



Previo



Libre



Informado

# Consentimiento



## Informado

Se debe comunicar clara, expresa e indubitablemente, con lenguaje sencillo:

✓	La identidad y domicilio o dirección del titular del banco de datos personales.
✓	La finalidad del tratamiento a las que sus datos serán sometidos.
✓	La identidad de los destinatarios.
✓	La existencia del banco de datos en el que almacenarán, cuando corresponda.
✓	El carácter obligatorio o facultativo de sus respuestas al cuestionario, cuando corresponda.
✓	Las consecuencias de proporcionar sus datos y de su negativa a hacerlo
✓	La transferencia nacional e internacional de datos que se efectúen, cuando corresponda.



## Política de Privacidad

1. Identidad y domicilio
2. ¿Para qué recopilamos tus datos?
3. ¿Qué datos recopilamos?
4. ¿Con quién compartimos tus datos?
5. ¿Durante cuánto tiempo conservamos tus datos?
6. Tu información está segura con nosotros
7. ¿Sabes cuáles son tus derechos en relación a tus datos?
8. Modificaciones de esta Política de Privacidad



# Sujetos

## Titular de datos personales

Persona natural a quien corresponde los datos personales.



## Encargado del banco de datos personales

Toda persona natural, persona jurídica de derecho privado o entidad pública que sola o actuando conjuntamente con otra realiza el tratamiento de los datos personales por encargo del titular del banco de datos personales.



## Titular del banco de datos personales

Cualquier persona natural, persona jurídica de derecho privado o entidad pública que determina la finalidad y contenido del banco de datos personales, el tratamiento de estos y las medidas de seguridad



# Derechos ARCO



A

**Acceso** Toda persona tiene derecho a obtener la información que sobre sí mismo sea objeto de tratamiento en bancos de datos personales, la forma en que fueron recopilados, y las razones de ello, así como las transferencias realizadas o que se realizarán.

R

**Rectificación:** Es el derecho por el cual el titular de los datos personales puede solicitar la modificación de sus datos, que no sean exactos, erróneos o falsos.

C

**Cancelación** El titular de los datos personales podrá solicitar la supresión o cancelación de sus datos cuando éstos hayan dejado de ser necesarios para la finalidad para la cual hayan sido recopilados, hubiere vencido el plazo o se haya revocado el consentimiento.

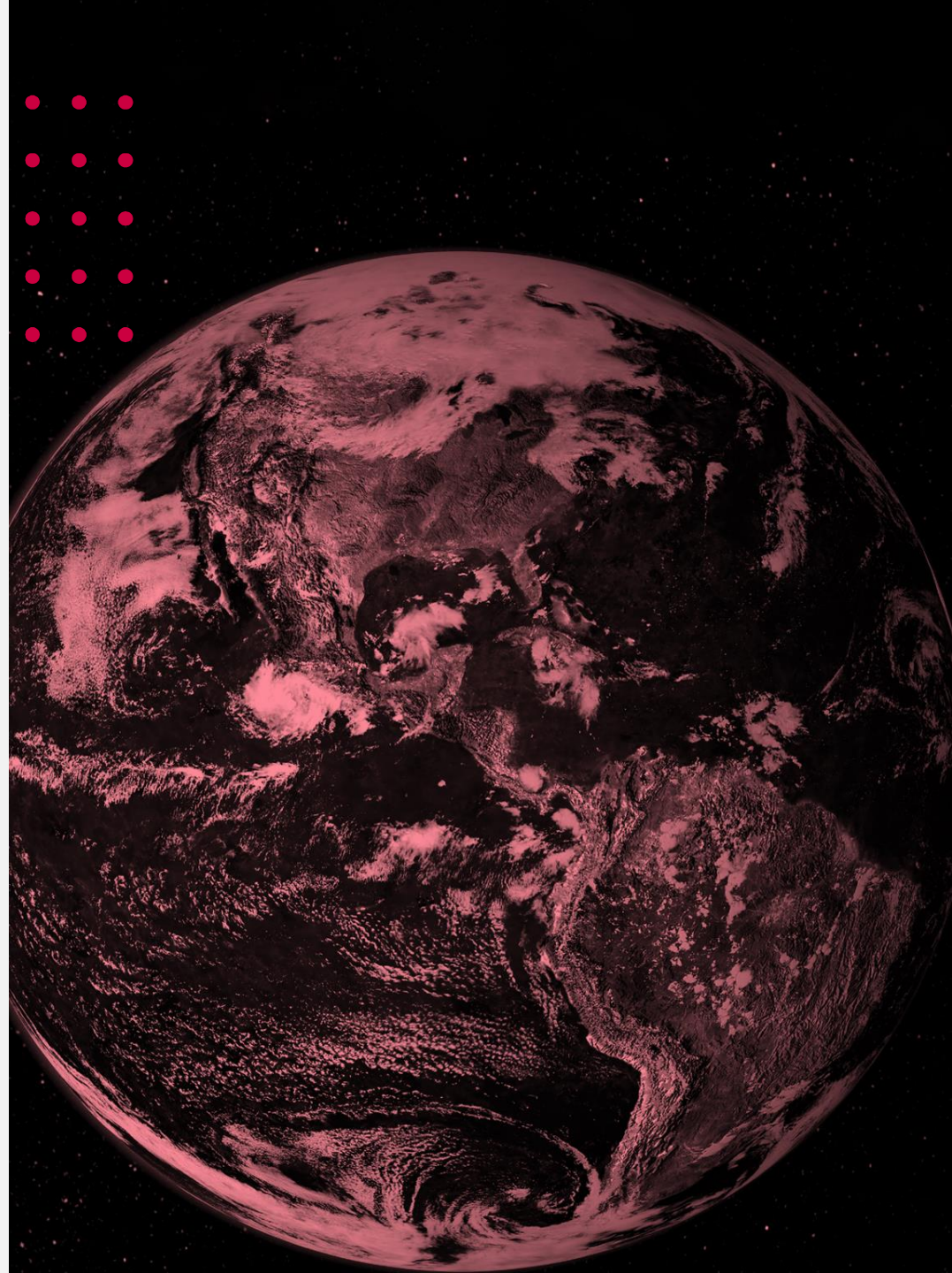
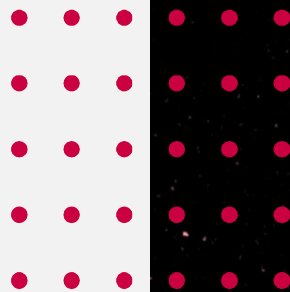
O

**Oposición** Toda persona tiene derecho a oponerse, por un motivo legítimo y fundado, a figurar en un banco de datos personales o al tratamiento de sus datos personales, siempre que por una Ley no se disponga lo contrario.

# Transferencia de datos personales

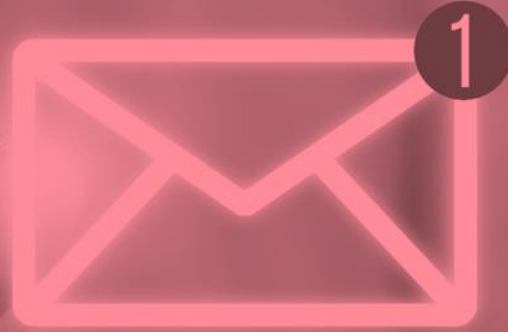
- Cualquier transmisión de datos personales, a nivel nacional o internacional, a otra persona distinta al titular de dichos datos.
- Para poderlas llevar a cabo, se requiere contar con el consentimiento, así como su declaración ante la Autoridad.

**Flujo transfronterizo de datos personales:** Transferencia de datos personales fuera del territorio nacional. El país destinatario debe mantener niveles de protección adecuados.





# Mailing



¿Solicitaste consentimiento?

¿Compraste una base de datos?

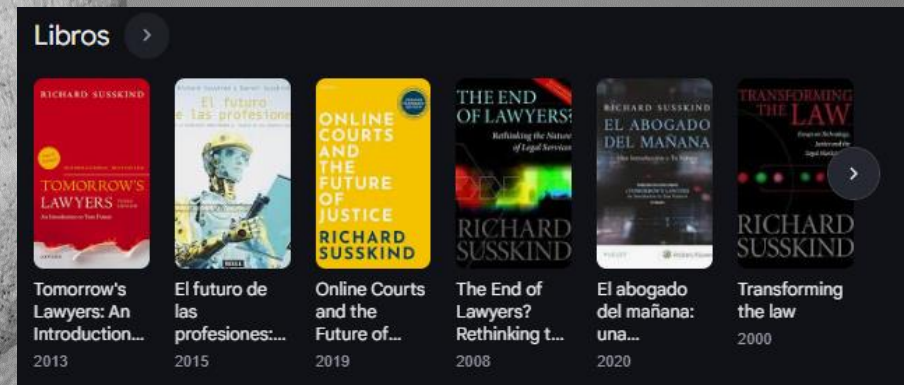
¿Informaste a los titulares de la base de datos?



- Lo que se protege es el dato personal.
- El dato personal protegido corresponde a las personas naturales.
- El banco de datos se protege en tanto continente o fuente de datos personales.
- El **centro de gravedad** de la PDP **está en el tratamiento**, no en la existencia de un banco de datos.



"Un abogado que solo ve el caso y no el contexto, es un riesgo para su cliente."  
*Richard Susskind*



## Crecimiento del comercio digital y servicios en línea

El comercio digital y los servicios en línea han experimentado un notable crecimiento en los últimos años.

Por ejemplo, MercadoLibre, una de las principales plataformas de comercio electrónico en América Latina, anunció una inversión de 3.400 millones de dólares en México para 2025, incrementando en un 40% respecto al año anterior. Esta inversión busca fortalecer su ecosistema tecnológico y financiero, así como crear 10.000 nuevos empleos en el país.

## Expansión de la inteligencia artificial y tecnologías de big data

La inteligencia artificial y el big data han crecido significativamente. Empresas como Palantir han visto un aumento del 500% en sus acciones desde enero de 2024, consolidando su liderazgo en sectores clave.

En España, la adopción de IA en pequeñas empresas ha aumentado al 11,8% y en microempresas al 4,6%, reflejando una tendencia en alza.

## Incremento de incidentes de ciberseguridad y filtraciones de datos

Los incidentes de ciberseguridad aumentaron un 24% en España en 2023, afectando a ciudadanos y empresas debido a la creciente sofisticación de los ciberataques.

Además, mafias del cibercrimen han reclutado a más de 250.000 personas en Asia para realizar estafas en línea bajo condiciones de esclavitud.

## Fortalecimiento de la regulación en protección de datos a nivel global:

GDPR en Europa (impacto extraterritorial)

Nuevas leyes en Latinoamérica (Brasil, Argentina, México, Chile)

Perú y la necesidad de adecuarse a los estándares internacionales.



# Principales cambios y novedades del nuevo reglamento





# Principales modificaciones

<b>Nuevos principios rectores:</b> Principio de transparencia y responsabilidad proactiva.	<b>Derecho de portabilidad:</b> como parte del derecho de acceso	<b>Tratamiento especial:</b> uso de datos con fines publicitarios
<b>Medidas de seguridad:</b> más estrictas y obligatorias	<b>Mayores inspecciones:</b> Fiscalizaciones remotas	<b>Regulación específica:</b> para el tratamiento de datos de menores de edad y datos sensibles.
<b>Nuevo responsable:</b> Oficial de Datos Personales		

Tipo de Empresa	Nuevas Obligaciones	Entrada en Vigencia	Infracción por Incumplimiento
<b>Empresas con ventas anuales:</b> - Superiores a 2,300 UIT - Entre 1,700 UIT y 2,300 UIT - Entre 150 UIT y 1,700 UIT - Hasta 150 UIT y microempresas	Designar un oficial de Datos Personales	<ul style="list-style-type: none"> <li>• 30 de noviembre de 2025 (grandes empresas)</li> <li>• 30 de noviembre de 2026 (medianas empresas)</li> <li>• 30 de noviembre de 2027 (pequeñas empresas)</li> <li>• 30 de noviembre de 2028 (microempresas)</li> </ul>	Infracción Leve (0.5 - 5 UIT)
	Notificación de incidentes de seguridad de datos personales (48 horas)	30 de marzo de 2025	Infracción Grave (5 - 50 UIT)
	Medidas de seguridad reforzadas con un Documento de Seguridad aprobado formalmente y de fecha cierta	30 de marzo de 2025	<ul style="list-style-type: none"> <li>• Datos personales no sensibles: Infracción Leve (0.5 - 5 UIT)</li> <li>• Datos sensibles: Infracción Grave (5 - 50 UIT)</li> </ul>
	Atender el derecho a la portabilidad de datos	30 de septiembre de 2025	<ul style="list-style-type: none"> <li>• Fuera de plazo: Infracción Leve (0.5 - 5 UIT)</li> <li>• No atender: Infracción Grave (5 - 50 UIT)</li> </ul>

# Retos y oportunidades para el abogado



Portada / Tribunales

## Protección de Datos multa con 4.000 euros a una abogada por enviar por WhatsApp sentencias con información personal

## Sanción de la AEPD a un despacho de abogados por publicar fotos de personas trabajadoras sin su consentimiento

Nota informativa escrita por el área de Protección de Datos de ECIJA Madrid.

**La Agencia Española de Protección de Datos considera que la participación de un trabajador en una sesión de fotos organizada y realizada por la empresa, así como la publicación de estas imágenes por el trabajador en su perfil de la red social LinkedIn, no supone de facto el consentimiento expreso para que estas imágenes sean publicadas por la empresa en su página web corporativa.**

## Legal

EN COLABORACIÓN CON

DATOS PERSONALES >

## De sentencias sin anonimizar a documentos en la basura: las infracciones sobre protección de datos de los abogados

El regulador ha sancionado a algunos letrados por dejar al descubierto información sensible de sus representados

# Oportunidades

El abogado ya no solo interviene en la gestión de conflictos, sino que ahora es **clave en la prevención, cumplimiento y adaptación de las empresas a las nuevas normativas.**

Se requiere un **perfil interdisciplinario** que combine conocimientos legales con un entendimiento técnico y estratégico.

# Asesor Legal en Privacidad y Cumplimiento Normativo

Las empresas necesitan adecuarse a los estándares de protección de datos, lo que implica un trabajo legal detallado para evitar sanciones y mejorar la confianza de sus clientes.

## Diseño de estrategias de cumplimiento normativo:

- Identificación de normativas aplicables (Perú, GDPR, regulaciones sectoriales).
- Evaluación de riesgos y planes de acción para la adaptación legal.

## Creación de políticas de privacidad y contratos de tratamiento de datos:

- Desarrollo de políticas claras y accesibles para clientes y empleados.
- Redacción de acuerdos de confidencialidad, cláusulas contractuales y términos de uso.
- Implementación de protocolos para la gestión de datos sensibles.





# Especialización en Litigios y Defensa Legal en Materia de Privacidad

El incumplimiento de las normativas de protección de datos puede derivar en sanciones administrativas y acciones legales, lo que genera una creciente demanda de abogados expertos en defensa de datos personales.

## **Representación en procedimientos sancionadores:**

- Defensa ante organismos de control por vulneraciones a la privacidad.
- Asesoría en la gestión de reclamaciones y cumplimiento de medidas correctivas.

## **Defensa ante reclamos de usuarios y filtraciones de datos:**

- Manejo de crisis y estrategias de mitigación legal ante fugas de información.
- Negociaciones con autoridades y partes afectadas para minimizar daños reputacionales.

# Emprendimiento en LegalTech y Soluciones de Privacidad

La digitalización del sector legal abre nuevas oportunidades para abogados que quieran innovar con herramientas tecnológicas que faciliten el cumplimiento de la normativa.

## **Creación de herramientas tecnológicas para la gestión del cumplimiento normativo:**

Desarrollo de plataformas para evaluar riesgos de privacidad en empresas.  
Software de automatización de documentos legales y políticas de privacidad.

## **Consultoría digital para startups y empresas en transformación digital:**

Servicios especializados en protección de datos en fintech, e-commerce y healthtech.  
Implementación de modelos de privacidad desde el diseño (Privacy by Design).

# Oficial de Protección de Datos (DPO):

Con la creciente exigencia de cumplimiento normativo en protección de datos, el Oficial de Protección de Datos (DPO - Data Protection Officer) se ha convertido en un puesto clave dentro de empresas y organizaciones. Este rol es obligatorio en ciertas instituciones y altamente recomendable en cualquier empresa que maneje información personal de clientes, empleados o terceros.

## Funciones clave:

- Garantizar el cumplimiento legal en protección de datos.
- Asesorar a la empresa y capacitar al personal.
- Supervisar la gestión de derechos ARCO (acceso, rectificación, cancelación y oposición).
- Realizar evaluaciones de impacto y gestionar riesgos.
- Actuar como enlace con autoridades regulatorias.

## ¿Por qué un abogado puede ser un excelente DPO?

- Conocimiento normativo y capacidad de interpretación legal.
- Habilidades de comunicación y negociación.
- Análisis de riesgos en tratamiento de datos personales.

- La protección de datos ya no es solo un requisito legal, **sino un diferencial competitivo.**
- El nuevo reglamento impone mayores responsabilidades, **pero también abre oportunidades para abogados especializados.**
- Las empresas necesitan **estrategias claras** para cumplir con la normativa y minimizar riesgos.
- **Llamado a la acción:** Es el momento ideal para especializarse y asesorar en este campo. La privacidad y protección de datos se consolidan como áreas de crecimiento en el derecho digital.
- Invitación a seguir investigando, formándose y participando en espacios de debate sobre estos cambios.



**“Sin seguridad se pierde  
la confianza en la innovación”**



**Nos encargamos de lo legal**

**Tú de hacer crecer tu negocio**



**Socios** no solo abogados

**Suárez & Asociados S.A.C.**  
RUC 20601063345

Calle Los Geranios 104 – Segundo Piso  
Urb. Selva Alegre – Cercado, Arequipa.

administracion@suarezasociados.pe

[www.suarezasociados.pe](http://www.suarezasociados.pe)

+51 54 294063  
+51 958958184