



RODRÍGUEZ ANGOBALDO
ABOGADOS

RODRÍGUEZ
HEREDIA
ABANTO
JIMÉNEZ
VARSI

INCIDENTE DE SEGURIDAD



¿Qué es un “incidente de seguridad” de datos personales en Perú?

En el marco peruano, un incidente de seguridad de datos personales es toda vulneración de seguridad que provoque la destrucción, pérdida o alteración ilícita de datos personales, o su comunicación/exposición no autorizada.

En el sector salud, este concepto es especialmente relevante porque se tratan datos personales relacionados con la salud (física o mental) incluyendo información derivada de un acto médico, discapacidad, entre otros supuestos que afectan la intimidad.

Un incidente de seguridad puede implicar algo más que el acceso por terceros ajenos a la organización a información personal, pues también se puede producir por el acceso no autorizado realizado por un miembro de la propia organización, el acceso autorizado cuando implique un tratamiento adicional o un exceso de sus funciones.





Obligaciones del titular / responsable frente a un incidente:

1) Notificar a la Autoridad Nacional de Protección de Datos Personales (ANPD).

El Reglamento exige notificar a la ANPD como máximo dentro de las 48 horas desde que se toma conocimiento/constancia del incidente. Si la notificación se retrasa, se deberá incluir una justificación por dicho retraso, acompañada del sustento probatorio correspondiente.

La notificación debe incluir, como mínimo, la naturaleza del incidente, tipos y volumen aproximado de datos/titulares afectados, un punto de contacto (Oficial de Datos Personales u otro), posibles consecuencias y medidas adoptadas o propuestas para remediar/mitigar.

Nota: el propio Reglamento tipifica como infracción grave no comunicar a la ANPD un incidente cuando correspondía hacerlo.



2) Comunicar al titular del dato dentro de las 48 horas si hay afectación de otros derechos

Si el incidente afecta al titular de los datos personales, el responsable debe comunicarlo al afectado dentro de las 48 horas, en lenguaje claro y accesible, incluyendo las medidas adoptadas para mitigar efectos del incidente.

Si no se produjo esta afectación y el incidente fue totalmente superado por las medidas adoptadas, la obligación de comunicar al titular no resulta exigible.

3) Notificar al Centro Nacional de Seguridad Digital (CNSD)

Cuando el incidente se desarrolla en y/o mediante el entorno digital, la notificación se deberá realizar, además, al Centro Nacional de Seguridad Digital, para su incorporación al Registro Nacional de Incidentes de Seguridad Digital.





4) Documentar el incidente

El responsable debe documentar el incidente de manera detallada, incluyendo los hechos relacionados, los efectos del incidente y las medidas que se han adoptado para mitigar o remediar la situación.

Y si hay encargados (proveedores que tratan datos por cuenta del responsable), estos deben informar de forma inmediata al titular /responsable cuando tomen conocimiento del incidente.

Medidas y garantías: cumplimiento “antes” del incidente

En Perú, el enfoque no se agota en reaccionar: el Reglamento desarrolla exigencias de medidas de seguridad en tratamiento digital (controles de acceso, autenticación, gestión de privilegios, trazabilidad y conservación de registros, entre otros).

Asimismo, exige que el responsable cuente con un Documento de Seguridad formal, actualizado y con fecha cierta, que incluya procedimientos de accesos/privilegios, políticas internas e inventario de datos/sistemas (incluyendo si se trata de datos sensibles), pudiendo tomarse como referencia estándares como ISO/IEC 27001.



Rol del Oficial de Datos Personales (ODP)

El Reglamento prevé la designación de un Oficial de Datos Personales en supuestos como tratamientos de grandes volúmenes, datos sensibles o actividades principales que comprendan tratamiento de datos sensibles.

Entre sus funciones mínimas están: informar y asesorar, verificar cumplimiento, cooperar con la Autoridad y actuar como punto de contacto con la ANPD.

Cómo debemos afrontar un incidente de seguridad:

0–4 horas

- Activar comité de crisis (Legal/Compliance + Tecnologías de la Información/Seguridad + Operaciones + Comunicaciones).
- Contener el incidente sin destruir evidencia (preservar logs, accesos, respaldos relevantes; cadena de custodia interna).
- Identificar si hay encargados involucrados y exigir reporte inmediato.



4–12 horas

- Clasificar datos comprometidos y estimar alcance (titulares/tipos/volumen).
- Evaluar si se encuentran en supuestos de notificación obligatoria a ANPD.
- Preparar borradores de notificación con el contenido mínimo exigido.

12–24 horas

- Tomar decisión formal de notificación y plan de comunicaciones, considerando el estándar de 48 horas.
- Si fue “entorno digital”, coordinar también reporte a CNSD.
- Abrir expediente interno de documentación del incidente (hechos/efectos/medidas).



RODRÍGUEZ ANGOBALDO
ABOGADOS

RODRÍGUEZ
HEREDIA
ABANTO
JIMÉNEZ
VARSI

Para mayor información, contactar:



Diego Arce
Asociado Sénior
darce@er.com.pe



Alejandra Flores
Asociada
aflores@er.com.pe

