

NOTA INFORMATIVA

ECIJA
GPA

Nueva Norma Técnica de Notificación de Vulneraciones de Seguridad de Datos Personales





*La Superintendencia de Protección de Datos Personales expidió la Resolución N° SPDP-SPD-2026-0040-R, que regula el **proceso de notificación de brechas de seguridad por parte de responsables y encargados del tratamiento.***



Plazos obligatorios

Dos plazos que no se pueden incumplir.

Los encargados del tratamiento deben notificar al responsable en un máximo de **2 días**. Los responsables, a su vez, deben notificar a la SPDP en un término de **5 días** desde que reciben la comunicación.

La ausencia de notificación —tanto a la SPDP como a los titulares— constituye una **infracción grave** conforme a la LOPDP.



Clasificación de vulneraciones

Tres tipos, tres niveles de gravedad.

Tipo	Temporal	Permanente	Irreversible
Integridad	Se puede recuperar y restaurar	No es posible recuperar la integridad	Sin posibilidad técnica de restablecimiento
Disponibilidad	Se puede restablecer el acceso	No es posible recuperar los datos	Sin posibilidad técnica de recuperación
Confidencialidad	—	Esencialmente permanente: los datos pueden usarse o publicarse en cualquier momento	Datos que el titular no puede cambiar, especialmente sensibles

Un mismo incidente puede ocasionar vulneraciones de más de un tipo.



Cómo y dónde notificar

Canal único: el SISPD.

Toda notificación a la SPDP debe realizarse a través del **Sistema Nacional de Registro de Datos Personales en servicios.spdp.gob.ec**. Solo excepcionalmente, si el sistema no está disponible, se podrán usar otros canales oficiales, previa convalidación de la SPDP. >



El sistema AlxSPDP —basado en inteligencia artificial con intervención humana— asigna trazabilidad, genera métricas y estima niveles de riesgo para cada notificación recibida..



Notificación a titulares

Informar con claridad y por los canales correctos.

La notificación a los titulares debe incluir, como mínimo: la naturaleza de la vulneración, la fecha de detección, las medidas adoptadas y las recomendaciones. El lenguaje debe ser claro, accesible y sencillo.



Se usarán los canales habituales del responsable: **página web, correo electrónico o comunicación directa**. Solo cuando no exista un canal preestablecido se requerirá publicación en un medio de difusión masiva.

.



Lo que viene

Plazos para prepararse.

La SPDP publicará en su portal web los **modelos de riesgo y las ontologías de IA del sistema AIXSPDP** dentro de los 6 meses siguientes a la entrada en vigencia de la norma.



Los responsables y encargados deben revisar desde ahora sus protocolos internos de respuesta a incidentes, asegurar el acceso al SISPD y capacitar a sus equipos para cumplir los plazos y requisitos de esta nueva regulación.





Contacto

Área de TMT, Ciberseguridad, Privacidad y Protección de
Datos de ECIJA GPA

Info.ecuador@ecija.com

T [+\(593-2\) 2986528](tel:+59322986528)

Av. 12 de Octubre, N26-97 y Lincoln,
Ed. Torre 1492, 170516. Piso 10 Oficina 1005
Quito, Ecuador.