

NOTIFICACIÓN DE VIOLACIÓN DE SEGURIDAD (NVS)

1. Tipo de notificación	
Notificación completa (todos los campos son obligatorios)	
Notificación inicial (todos los campos son obligatorios)	
Notificación complementaria o de modificación de la NVS núm. (rellenar solo los campos en los que se introduzcan cambios)	
2. Responsable del tratamiento	
Tipo de entidad	
Generalidad de Cataluña	Administración local
Otras personas jurídico-públicas	Otras entidades
Nombre del organismo o entidad	CIF
Dirección	Código postal
Población	
Nombre y apellidos de la persona que realiza la notificación	
Cargo	
3. Delegado de protección de datos (DPD) (u otro punto de contacto)	
Nombre y apellidos	
Cargo	
Teléfono	Dirección electrónica
4. Encargado de tratamiento (solo si está implicado en el incidente)	
No procede	
Nombre del organismo o entidad	CIF
Dirección	

5. Información sobre la violación de seguridad

5.1. Circunstancias temporales de la VS

Fecha y hora del incidente (si no se conoce con exactitud, indicar la aproximada):

Fecha y hora de constatación de la VS (momento en que el responsable ha tenido conocimiento de la VS):

Si la notificación se realiza pasadas 72 horas desde su constatación, justificación de la demora.

Motivo:

No procede

5.2. Naturaleza de la VS (pueden marcarse diferentes opciones)

Violación de la confidencialidad (se ha producido una revelación no autorizada o accidental de los datos personales a terceros, o han accedido a ellos personas no autorizadas):

Violación de la integridad (se ha producido una alteración no autorizada o accidental de los datos personales):

Violación de la disponibilidad (se ha producido una pérdida de acceso o destrucción de los datos personales, accidental o no autorizada):

5.3. Descripción del incidente

Descripción o resumen de las circunstancias de la VS. Indicar la causa posible, la ubicación física y el soporte de almacenamiento de la información.

5.4. Categoría o tipología de datos personales afectados (pueden marcarse diferentes opciones y, después, precisar lo que corresponda)

Estado civil (ej.: nombre, sexo, fecha de nacimiento, edad, etc.):

Datos de contacto (ej.: dirección postal o electrónica, números de teléfono móvil o fijo, etc.):

Datos de identificación o de acceso vinculados a la prestación del servicio del responsable del tratamiento (ej.: código identificativo, contraseña, número de cliente o paciente, etc.):

Otros datos identificativos (DNI/NIF/NIE/pasaporte, etc.):

Datos académicos:

Datos relativos a infracciones administrativas:

Datos relativos a información financiera o económica (ej.: ingresos, número de tarjeta de crédito, cuenta bancaria, etc.):

Categorías especiales de datos personales (origen étnico o racial, opiniones políticas, convicciones religiosas o filosóficas o afiliación sindical, y datos genéticos, biométricos, relativos a la salud, relativos a la vida sexual o las orientaciones sexuales de una persona física):

Datos relativos a condenas e infracciones penales:

Datos específicamente vinculados a la prestación de un servicio por Internet o al uso que los empleados hacen de Internet (ej.: datos de localización o de conexión, relativos al historial de navegación en Internet, mensajes de correo electrónico, etc.):

Otros datos personales. Hay que precisarlos:

Aun no se han determinado:

5.4.1. Número de registros de datos personales afectados (o de categoría de datos afectados) (si no se conoce este dato, indicar un número mínimo y máximo aproximado)

5.5. Colectivo y/o tipología de las personas afectadas (pueden marcarse diferentes opciones)

Trabajadores propios

Ciudadanos

Alumnos

Estudiantes

Pacientes

Clientes

Menores de edad

Personas especialmente vulnerables

Aun no se ha determinado

Otros

5.5.1. Número de personas afectadas (si no se conoce este dato, indicar un número mínimo y máximo aproximado)

5.6. Posibles consecuencias de la VS de los datos para las personas afectadas

Pérdida de control sobre los datos (ej.: difusión no deseada de una imagen en Internet, pérdida de control de información publicada a las redes sociales, etc.)

Restricción de derechos (ej.: la pérdida de datos imposibilita la prestación del servicio al afectado)

Utilización de los datos con finalidades ilegítimas (ej.: usurpación o suplantación de identidad, fraude, uso para contactar o localizar a las personas afectadas, amenazas, etc.)

Pérdidas financieras

Reversión no autorizada de la seudonimización

Daño para la reputación

Discriminación

Pérdida de confidencialidad de los datos sujetos al secreto profesional

Perjuicio económico o social

Otros:

5.7. Medidas de protección técnicas y organizativas adoptadas o que se prevé adoptar para solucionar la VS, limitar sus riesgos y mitigar sus efectos adversos potenciales

Medidas técnicas y organizativas que se han implementado y que aseguran que el incidente se ha cerrado adecuadamente y que se han tomado las medidas para evitar que se vuelva a producir (describir las medidas).

Medidas técnicas y organizativas previstas (planificadas) para que finalice el incidente y no se vuelva a producir en el futuro. Especificar, de la forma más precisa posible, una previsión de la planificación.

Medidas técnicas y organizativas adoptadas o que se prevé adoptar para mitigar los posibles efectos negativos de la VS para los afectados.

Medidas recomendadas a las personas afectadas para mitigar sus efectos negativos potenciales.

No se ha previsto adoptar medidas (justificar el motivo).

6. Comunicación de la VS a las personas afectadas

6.1. ¿Se ha comunicado?

Se ha comunicado según lo indicado en los apartados 6.2, 6.3 y 6.4.

Está previsto realizar la comunicación en fecha:

No se comunicará. En este caso, hay que cumplimentar el apartado siguiente:

Explicar brevemente por qué no se considera necesario comunicar la VS a los afectados (hay que precisar alguna de las opciones y completar la respuesta).

El responsable del tratamiento ha adoptado medidas de protección técnicas y organizativas adecuadas y estas medidas se han aplicado a los datos personales afectados por la VS. Especificar las medidas.

El responsable del tratamiento ha tomado medidas inmediatamente después de la VS, para asegurar que el alto riesgo que supone para los derechos y libertades de las personas ya no es probable que se materialice. Especificar las medidas.

Contactar con las personas afectadas exige esfuerzos desproporcionados. Motivar esta circunstancia.

La comunicación puede afectar a las investigaciones que otras autoridades están llevando a cabo.

Otros. En este caso, indicar cuáles:

Es posible que se comunique, pero actualmente todavía no se ha decidido. Hay que tener en cuenta que, una vez decidido, se deberá informar nuevamente a la Autoridad.

6.2. Contenido de la comunicación entregada a las personas afectadas

Indicar el texto modelo de la comunicación y anexarla como fichero adjunto a esta notificación.

No procede

6.3. Sistema de comunicación utilizado

Información por correo postal

Información por correo electrónico

Otros medios. Indicar cuáles:

No procede

6.4. Número de personas afectadas a quienes se ha enviado o se prevé enviar la comunicación

No procede

7. Comunicación de la VS a otros organismos

Indicar si se ha comunicado o se ha previsto comunicar la VS a otros organismos (como fuerzas y cuerpos de seguridad, entidades competentes en seguridad de las redes y sistemas de información, etc.). Identificar dichos organismos:

No procede

8. VS que afectan a personas residentes en otras comunidades autónomas u otros países de la Unión Europea

VS que puede afectar a personas residentes en otras comunidades autónomas del Estado español u otros estados de la Unión Europea.

Notificación de la VS a otras autoridades de protección de datos. Identificar dichas autoridades:

No procede

Responsable del tratamiento	Dirección de la Autoridad Catalana de Protección de Datos C/ Rosselló, 214, esc. A, 1r 1a, 08008 Barcelona Tel. 93 552 78 00. Fax 93 552 78 30 apdcat@gencat.cat www.apdcat.cat
Delegado de protección de datos	dpd.apdcat@gencat.cat C/ Rosselló, 214, esc. A, 1r 1a, 08008 Barcelona Tel. 93 552 78 05
Finalidad del tratamiento	Analizar las circunstancias de la violación de seguridad notificada y los riesgos para los derechos y las libertades de las personas; ayudar al responsable a adoptar las medidas de protección; y, si procede, hacer recomendaciones o requerimientos.
Base jurídica	Ejercicio de un poder público.
Destinatarios	Los datos personales se podrán comunicar a otros organismos competentes en seguridad de las redes y sistemas de información, a las fuerzas y cuerpos de seguridad y a las autoridades de protección de datos de la Unión Europea.
Derechos de las personas	Puede acceder a sus datos, solicitar su rectificación o supresión, oponerse al tratamiento y solicitar su limitación, enviando una solicitud a la dirección de la APDCAT o mediante su sede electrónica (https://seu.apd.cat).
Plazo de conservación de los datos	4 años, desde la finalización del procedimiento iniciado a raíz de la notificación de la violación de seguridad.
Reclamación	Puede presentar una reclamación dirigida a la APDCAT, mediante la sede electrónica de la Autoridad (https://seu.apd.cat) o por medios no electrónicos.

Firma de la persona que realiza la NVS