PLANTILLA P51 · NOTIFICACIONES Y COMUNICACIONES DE INCIDENTES

Notificaciones y comunicaciones de incidentes

Documenta la decisión de notificar o no cada régimen aplicable a un incidente de IA, prepara el contenido común de las notificaciones y las comunicaciones a afectados, empleados y clientes, y sigue sus plazos.

Fernando García Varela Versión 0.1 (borrador de trabajo) 19-09-2026 Borrador para revisión

EN ESTE DOCUMENTO

01 Instrucciones de uso

02 Identificación

03 Decisión de notificar o no

04 Contenido común de las notificaciones

05 Notificación de incidente grave (Reglamento de IA)

06 Notificación de violación de la seguridad de los datos personales (RGPD)

07 Notificaciones DORA y NIS2

08 Comunicación a personas afectadas

09 Comunicación interna y a clientes

10 Registro de notificaciones y comunicaciones

11 Criterios de calidad

12 Aprobación y verificación

13 Control de versiones

Aviso legal y exención de responsabilidad. SEVEN-G es un marco metodológico de referencia que se ofrece «tal cual» y con fines exclusivamente informativos. No constituye asesoramiento jurídico, regulatorio, financiero ni profesional, ni garantiza el cumplimiento de ninguna norma. Las referencias a regulación general (como el Reglamento Europeo de IA, el RGPD, DORA o NIS2), a normas técnicas y a regulación específica de cada sector o jurisdicción pueden ser incompletas, no aplicar a un caso concreto o quedar desactualizadas por cambios normativos, interpretaciones o criterios de las autoridades posteriores a su fecha de consulta. **Cada organización que use SEVEN-G es la única responsable de identificar la normativa que le aplica, verificar su vigencia y certificar su propio cumplimiento regulatorio**, con el asesoramiento cualificado que corresponda. Esta metodología es una ayuda genérica y gratuita, compartida con la comunidad para que nadie tenga que empezar desde cero; cada persona u organización puede y debe adaptarla a su propio uso. No debe entenderse que sus partes jurídicamente sensibles hayan sido revisadas por una asesoría jurídica: esas revisiones, para cada empresa o sector, son responsabilidad última de la empresa, el consultor o la organización que la use. Aunque se procura mantenerla al día, alguna norma puede haber cambiado sin que se recoja aquí. En la máxima medida permitida por la ley, el autor no asume responsabilidad alguna por los efectos de su aplicación en ninguna organización ni por su aplicabilidad completa. La metodología no otorga certificación de ningún tipo. El autor no asume responsabilidad alguna por el uso que se haga de este contenido ni por las decisiones que se adopten con él. Los datos, cifras, compañías y casos de los ejemplos son ficticios o ilustrativos.

Por qué importa. Un mismo incidente de IA puede activar a la vez el Reglamento de IA, el RGPD, DORA y NIS2, cada uno con su reloj, que empieza cuando se tiene constancia y no cuando termina el análisis. Omitir o retrasar una notificación obligatoria es una no conformidad crítica (01 §12), y no notificar sin dejar constancia del porqué es indefendible ante un supervisor. Esta plantilla obliga a valorar todos los regímenes en paralelo, a motivar por escrito la decisión de no notificar y a tener preparados los mensajes a personas afectadas, empleados y clientes antes de necesitarlos.

01

Instrucciones de uso

Aspecto	Indicación
Cuándo se usa	Los modelos de las secciones 5 a 9 se adaptan al sistema en la fase 5, junto con el plan de respuesta (P26), antes de G5. En cada incidente, la sección 3 se abre en el triaje y el registro de la sección 10 se mantiene hasta el informe final de cada régimen.
Quién la rellena	El responsable de riesgos de IA y cumplimiento valora los regímenes; el delegado de protección de datos, las brechas de datos personales; el coordinador del incidente aporta los hechos; comunicación corporativa redacta los mensajes.
Quién la verifica	Asesoría jurídica valida toda notificación y toda comunicación externa, y la decisión motivada de no notificar. En Enterprise, el auditor de IA revisa el registro en R6.
Quién decide o aprueba	Notifica quien la norma designa (proveedor, responsable del tratamiento, entidad financiera, entidad esencial o importante). Internamente firma la persona que el plan P26 designa; en S1, con conocimiento del patrocinador de IA y de la comisión delegada (37 §4.3).
Etapa, *gate* o momento	Preparación antes de G5 (G5.17). Uso en la fase 6 durante cada incidente. Revisión en R6 (R6.06), en el simulacro anual de S1 (37 §5) y en C4.
Herramienta	T08 · Registro de no conformidades e incidentes: relojes de notificación y alertas. Esta plantilla recoge el contenido que T08 no redacta.
Documento de referencia	Documento 37 §4.5 (fases 5 y 6) y §5 (regímenes, plazos y reglas); documento 34 (régimen aplicable a cada sistema); documento 36 (notificaciones de proveedores).

Aspecto	Indicación
Lite frente a Enterprise	La valoración de todos los regímenes y la decisión motivada de no notificar son obligatorias en ambas. Lite puede omitir los campos marcados **(Enterprise)**.

Reglas de cumplimentación:

- **Los formularios oficiales prevalecen.** Cuando una autoridad publica un formulario, una plantilla o un canal propio, se usa ese y esta plantilla solo sirve para preparar el contenido. Para el art. 73 del Reglamento de IA existe el Proyecto de orientaciones y plantilla sobre notificación de incidentes graves de la Comisión (34 §3.3); DORA tiene formularios en su normativa de desarrollo, y las autoridades de control y los CSIRT tienen sus propios canales. Esta plantilla no reproduce ni sustituye ninguno.
- Los plazos se toman del documento 37 §5 y se confirman con asesoría jurídica en el momento del incidente; esta plantilla no fija plazos propios.
- El reloj de cada régimen empieza en la fecha y hora de detección registrada en T08 o en el momento que la norma indique; nunca al terminar el análisis.
- Si la norma lo prevé, es preferible una notificación inicial incompleta en plazo a una completa fuera de plazo.
- Toda comunicación externa distingue hechos confirmados de valoraciones en curso y no especula sobre causas.
- Un incidente de IA que es también una brecha o un incidente de seguridad se gestiona **una sola vez**, con un único coordinador (37 §1).

Esta plantilla no constituye asesoramiento jurídico (fecha de consulta de referencia del marco: septiembre de 2026).

02

Identificación

Campo	Contenido	Guía
Incidente		INC-AAAA-NNN (P27, T08).
Sistema e caso de uso		SIA-AAAA-NNN · IA-AAAA-NNN.
Severidad actual		S1 · S2 · S3 · S4 (37 §4.2).
Fecha y hora de detección		Inicio de los relojes.

Campo	Contenido	Guía
Papel de la compañía respecto al sistema		Proveedor · Responsable del despliegue · Ambos (P11, documento 34).
Papel respecto a los datos personales		Responsable del tratamiento · Encargado · No aplica.
Sujeta a DORA · a NIS2		Sí · No · Por determinar (P26 §2).
Coordinador del incidente		
Responsable de la valoración regulatoria		Responsable de riesgos de IA y cumplimiento.

03

Decisión de notificar o no

Una fila por régimen. Se valora **en paralelo a la contención**. Cuando la respuesta es No, la motivación es obligatoria.

Régimen	¿Aplica? (Sí · No · Por determinar)	Criterio valorado	Decisión (Notificar · No notificar · Pendiente)	Motivación	Decide	Valida jurídico	Fecha y hora
Reglamento de IA, art. 73 (incidente grave de sistema de alto riesgo)		¿Incidente grave según el art. 3.49? ¿Sistema de alto riesgo? ¿Papel de la compañía?					
Reglamento de IA, art. 26.5 (información del responsable del despliegue al proveedor)		¿La compañía despliega un sistema de alto riesgo de un tercero?					

Régimen	¿Aplica? (Sí · No · Por determinar)	Criterio valorado	Decisión (Notificar · No notificar · Pendiente)	Motivación	Decide	Valida jurídico	Fecha y hora
RGPD, art. 33 (autoridad de control)		¿Brecha de datos personales? ¿Es improbable que suponga un riesgo para los derechos y libertades?					
RGPD, art. 34 (interesados)		¿Es probable un alto riesgo para las personas?					
DORA, art. 19		¿Incidente grave relacionado con las TIC según sus criterios de clasificación?					
NIS2, art. 23		¿Incidente significativo según la transposición nacional?					
Regulación sectorial		Supervisor sectorial o esquema de seguridad del sector público (P02).					
Obligaciones contractuales		Contratos con clientes o proveedores.					
***(ejemplo ilustrativo)* RGPD, art. 33**	Sí	Datos de contacto de 40 clientes visibles para otro cliente durante 20 minutos	Notificar	Riesgo no improbable: datos identificativos expuestos a un tercero no autorizado	Delegado de protección de datos	Sí	12-11-2026 18:30

3.1 Decisión motivada de no notificar

Una por cada régimen valorado como No notificar. Se conserva aunque el incidente se cierre sin consecuencias.

Campo	Contenido	Guía
Régimen		
Hechos considerados		Qué se sabía en el momento de decidir, con fecha y hora.
Criterio normativo aplicado		Por qué no se cumple el umbral (por ejemplo, no es un sistema de alto riesgo; es improbable que la brecha suponga un riesgo; no se alcanzan los criterios de clasificación).
Incertidumbres		Qué no se sabe todavía y qué haría cambiar la decisión.
Revisión prevista		Cuándo se revisa la decisión si aparecen hechos nuevos.
Decide · valida		Rol, nombre, fecha; validación de asesoría jurídica y, en brechas, del delegado de protección de datos.

04

Contenido común de las notificaciones

Base para rellenar cualquier formulario oficial. Cada régimen pide un subconjunto y su propio formato.

Campo	Contenido	Guía
Entidad notificante y contacto		Razón social, persona de contacto, delegado de protección de datos si aplica.
Referencia interna		INC-AAAA-NNN.
Fechas y horas		Inicio estimado, detección, clasificación, contención.
Sistema afectado		Nombre, versión, proveedor, finalidad, papel de la compañía.
Descripción del incidente		Qué ha ocurrido, en lenguaje claro.
Personas y datos afectados		Número y categorías, aproximados si no se conocen con exactitud. *Sin dato* si se desconoce.

Campo	Contenido	Guía
Consecuencias probables		Por eje de impacto (33 §4.2).
Vínculo causal con el sistema		Establecido · Probabilidad razonable · En análisis (relevante para el art. 73).
Medidas adoptadas y previstas		Contención, mitigación para las personas, corrección.
Efecto transfronterizo		Estados miembros afectados.
Evidencias conservadas		Registros, versiones y configuraciones preservados antes de modificar el sistema (37 §4.5; art. 73.6 para proveedores de alto riesgo).
Naturaleza del informe		Inicial · Intermedio · Final · Complemento de un informe incompleto.

05

Notificación de incidente grave (Reglamento de IA)

Campo	Contenido	Guía
¿Quién notifica?		Proveedor del sistema de alto riesgo. Si la compañía es responsable del despliegue, informa **inmediatamente** primero al proveedor y después al importador o distribuidor y a las autoridades de vigilancia del mercado (art. 26.5).
Destinatario		Autoridad de vigilancia del mercado del Estado miembro donde se produjo; la Oficina Europea de IA para los sistemas de su competencia (37 §5).
Supuesto de plazo		General: no más de 15 días · Infracción generalizada o alteración grave e irreversible de infraestructuras críticas: 2 días · Fallecimiento: 10 días. Desde que se tiene conocimiento.
Fecha y hora en que se tiene conocimiento		
Fecha límite calculada		Confirmada por asesoría jurídica.
Informe inicial incompleto		Sí · No. Qué falta y cuándo se completará.
Régimen limitado por notificación sectorial equivalente		Sí · No, con justificación (art. 73.9 y 73.10).

Campo	Contenido	Guía
Formulario usado		Plantilla oficial vigente o canal de la autoridad; versión y fecha.
Aplicabilidad temporal		Las obligaciones de los sistemas de alto riesgo del anexo III se aplican desde el 2 de diciembre de 2027; hasta entonces, el criterio de incidente grave es el umbral interno de S1 y la valoración se documenta (37 §5).

06

Notificación de violación de la seguridad de los datos personales (RGPD)

Campo	Contenido	Guía
Autoridad de control competente		En España, la Agencia Española de Protección de Datos , salvo tratamientos transfronterizos con otra autoridad principal.
Fecha y hora en que se tiene constancia		
Fecha límite de 72 horas		Si se notifica después, motivos del retraso.
Contenido		Naturaleza de la violación; categorías y número aproximado de interesados y de registros; contacto del delegado de protección de datos; consecuencias probables; medidas adoptadas o propuestas, incluidas las de mitigación. Si no se dispone de toda la información, se facilita por fases.
Encargado del tratamiento implicado		Fecha en que notificó a la compañía.
Documentación interna de la brecha		Todas las brechas se documentan, se notifiquen o no.

07

Notificaciones DORA y NIS2

Solo por remisión: se usan los formularios y canales oficiales. Esta tabla sigue las fases y los plazos de 37 §5.

Régimen	Fase	Plazo de referencia (37 §5)	Fecha límite	Enviada (fecha y hora)	Referencia de la autoridad
DORA	Notificación inicial	4 horas desde la clasificación como grave y no más de 24 horas desde que se tiene conocimiento			
DORA	Informe intermedio	72 horas desde la notificación inicial			
DORA	Informe final	Un mes después del último informe intermedio			
DORA	Información a clientes	Cuando el incidente afecta a sus intereses financieros			
NIS2	Alerta temprana	24 horas			
NIS2	Notificación del incidente	72 horas			
NIS2	Informe final	Un mes después de la notificación			

Para las entidades financieras, DORA actúa como norma sectorial respecto de NIS2 en la notificación de incidentes; el régimen se confirma en el documento 34.

08

Comunicación a personas afectadas

Obligatoria cuando el RGPD la exige (probable alto riesgo para las personas) y recomendable cuando el incidente afecta a sus decisiones o intereses aunque ninguna norma la exija **(Enterprise)**.

Elemento del mensaje	Contenido	Guía
Qué ha ocurrido		Lenguaje claro y sencillo, sin tecnicismos.
Qué datos o decisiones les afectan		
Consecuencias posibles		Sin minimizar ni alarmar.
Qué ha hecho la compañía		Contención y corrección.

Elemento del mensaje	Contenido	Guía
Qué pueden hacer ellos		Medidas de protección recomendadas; revisión humana de decisiones afectadas.
Contacto		Delegado de protección de datos o punto de contacto específico.
Canal y fecha de envío		

(ejemplo ilustrativo) «El 12 de noviembre, durante unos 20 minutos, un error en nuestro asistente de consultas mostró su nombre y su teléfono a otro cliente. Hemos corregido el fallo y el asistente funciona con controles adicionales. No se vieron datos bancarios ni contraseñas. Si recibe llamadas inesperadas en nombre de la compañía, no facilite datos y contacte con nuestro delegado de protección de datos en el canal habitual.»

09

Comunicación interna y a clientes

Destinatario	Momento	Contenido mínimo	Autor	Valida	Enviada
Comité de IA	S1: 4 horas · S2: 24 horas (37 §4.3)	Qué ha ocurrido, a quién afecta, qué se ha contenido, notificaciones hechas o en plazo, decisiones que pueden requerirse	Coordinador	Responsable de riesgos de IA	
Comisión delegada del consejo	S1: 24 horas	Igual que el anterior, con hechos confirmados separados de valoraciones (37 §9)	Patrocinador de IA	Comité de IA	
Empleados que usan o supervisan el sistema	Al contener	Qué cambia en su trabajo, proceso alternativo, a quién consultar	Responsable de producto de IA	Comunicación	
Clientes afectados (no personas físicas) (Enterprise)	Según contrato o cuando proceda	Hechos, efecto en el servicio, medidas, contacto	Comunicación	Jurídico	
Proveedores implicados	Al triaje	Hechos, solicitud de información y de conservación de evidencias (36 §6)	Responsable técnico de IA	Jurídico	

Destinatario	Momento	Contenido mínimo	Autor	Valida	Enviada
Comunicación pública (Enterprise)	Solo si procede	Mensaje único coordinado	Comunicación	Jurídico y patrocinador	

10

Registro de notificaciones y comunicaciones

Una fila por envío. Las filas se identifican con el código del incidente y un número de orden (INC-AAAA-NNN · N*nn*).

Nº	Régimen o destinatario	Tipo (inicial · intermedio · final · comunicación)	Reloj desde (fecha y hora)	Fecha límite	Enviada (fecha y hora)	¿En plazo?	Referencia de acuse	Responsable
N01								
N02								
***(ejemplo ilustrativo)* INC-2026-021 · N01**	RGPD · autoridad de control	Inicial	12-11-2026 17:10	15-11-2026 17:10	13-11-2026 11:40	Sí	Acuse de la sede electrónica	Delegado de protección de datos

Una notificación fuera de plazo o omitida abre una no conformidad crítica en P50, además de las que revele el incidente (37 §6).

11

Criterios de calidad

Criterios formales en el documento 21 (G5.17 y R6.06) y proceso en el documento 37.

#	Comprobación	Estado
1	Se han valorado todos los regímenes en paralelo a la contención, con fecha y hora.	Cumple · No cumple · No aplica · Pendiente

#	Comprobación	Estado
2	Cada decisión de no notificar está motivada, fechada y validada por asesoría jurídica.	
3	Los plazos se calculan desde el momento de conocimiento y están confirmados por asesoría jurídica.	
4	Se han usado los formularios o canales oficiales vigentes cuando existen.	
5	Las comunicaciones distinguen hechos confirmados de valoraciones en curso y han sido validadas.	
6	El registro permite demostrar para cada envío que se hizo en plazo.	
7	Los incumplimientos de plazo tienen no conformidad abierta en P50.	

12

Aprobación y verificación

Función	Rol en SEVEN-G	Nombre y cargo	Fecha	Firma o referencia
Valora los regímenes	Responsable de riesgos de IA y cumplimiento			
Valora las brechas y comunica a interesados	Delegado de protección de datos			
Aporta los hechos	Coordinador del incidente			
Redacta las comunicaciones	Comunicación corporativa			
Valida	Asesoría jurídica			
Revisa el registro en R6	Oficina de IA (Lite) · Auditor de IA (Enterprise)			

Separación de funciones: quien decide no notificar no valida su propia decisión; la validación la hace asesoría jurídica.

13

Control de versiones

Documento cumplimentado

Versión	Fecha	Autor	Cambios

Plantilla

Versión	Fecha	Cambios
0.1	19-09-2026	Primera versión. Decisión de notificar con decisión motivada de no notificar, contenido común, notificaciones del Reglamento de IA y del RGPD, remisión a DORA y NIS2, comunicaciones a afectados, internas y a clientes, y registro de plazos según 37 §5.

Fuentes externas citadas

Enlaces a la fuente oficial o primaria, comprobados antes de publicar. Verifique siempre la versión vigente en la fecha de uso.

Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas destinadas a garantizar un elevado nivel común de ciberseguridad en toda la Unión (Directiva SRI 2 / NIS2) · https://eur-lex.europa.eu/eli/dir/2022/2555/oj/spa · Parlamento Europeo y Consejo de la UE · 14-12-2022

Reglamento (UE) 2016/679 del Parlamento Europeo y del Consejo, de 27 de abril de 2016, relativo a la protección de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos y por el que se deroga la Directiva 95/46/CE (Reglamento general de protección de datos) · https://eur-lex.europa.eu/eli/reg/2016/679/oj/spa · Parlamento Europeo y Consejo de la UE · 27-04-2016

Reglamento (UE) 2022/2554 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, sobre la resiliencia operativa digital del sector financiero (DORA) · https://eur-lex.europa.eu/eli/reg/2022/2554/oj/spa · Parlamento Europeo y Consejo de la UE · 14-12-2022

Reglamento (UE) 2024/1689 del Parlamento Europeo y del Consejo, de 13 de junio de 2024, por el que se establecen normas armonizadas en materia de inteligencia artificial (Reglamento de

Inteligencia Artificial) · https://eur-lex.europa.eu/eli/reg/2024/1689/oj/spa · Parlamento Europeo y Consejo de la UE · 13-06-2024

Agencia Española de Protección de Datos (AEPD) · https://www.aepd.es/ · Agencia Española de Protección de Datos

Oficina Europea de IA (Comisión Europea) · https://digital-strategy.ec.europa.eu/es/policies/ai-office · Comisión Europea (DG CONNECT)

Proyecto de orientaciones y plantilla de notificación de incidentes graves de IA (art. 73 del Reglamento de IA) · https://digital-strategy.ec.europa.eu/es/consultations/ai-act-commission-issues-draft-guidance-and-reporting-template-serious-ai-incidents-and-seeks · Comisión Europea · 26-09-2025