PLANTILLA P26 · PLAN DE RESPUESTA A INCIDENTES

Plan de respuesta a incidentes

Prepara la respuesta a los incidentes de un sistema de IA: qué se considera incidente, cómo se clasifica su severidad, quién actúa, cómo se contiene y qué notificaciones deben comprobarse.

Fernando García Varela Versión 0.1 (borrador de trabajo) 16-09-2026 Borrador para revisión

EN ESTE DOCUMENTO

01 Instrucciones de uso

02 Identificación

03 Qué se considera incidente de este sistema

04 Severidad

05 Roles durante el incidente

06 Fases de respuesta

07 Acciones de contención preparadas

08 Notificaciones regulatorias y contractuales a verificar

09 Escalado interno

10 Simulacros

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.

01

Instrucciones de uso

Aspecto	Indicación
Cuándo se usa	Se prepara en la fase 5 (requisito previo de la firma P23) y se aprueba al inicio de la fase 6. Se revisa tras cada incidente S1 o S2 y en cada R6.
Quién la rellena	Responsable de operación de IA, con seguridad de la información, protección de datos y el responsable de riesgos de IA.

Aspecto	Indicación
Quién la verifica	Oficina de IA en Lite; auditor de IA en Enterprise.
En qué *gate* se revisa	G5 (existencia y adecuación) y R6 (vigencia y resultado de simulacros).
Lite frente a Enterprise	Lite puede omitir los campos marcados **(Enterprise)**. La comprobación de notificaciones regulatorias (bloque 8) no se omite nunca.
Herramienta	T08 Registro de no conformidades e incidentes.
Relación	P17 Supervisión humana · P18 Seguridad e interruptor de parada · P19 Reversión · P24 Manual de operación · P25 Alertas · P27 Registro de incidentes y cambios · documentos 35, 37 (No conformidades e incidentes) y 52.

Reglas:

- Los **criterios de severidad, los plazos de notificación y el proceso completo** están en el documento 37. Este plan los aplica al sistema concreto; no fija plazos regulatorios propios.
- Este plan se integra en el proceso general de gestión de incidentes de la compañía (seguridad, continuidad, protección de datos); no crea un circuito paralelo.
- Un incidente grave no notificado cuando procedía es una no conformidad **crítica** (01 §12).
- Ante la duda sobre la severidad, se clasifica en el nivel superior y se revisa después.

Esta plantilla no constituye asesoramiento jurídico. Las obligaciones de notificación y sus plazos deben verificarse con asesoría jurídica en el momento del incidente (fecha de consulta de referencia del marco: septiembre de 2026).

02

Identificación

Campo	Contenido	Guía
Código del caso de uso		IA-AAAA-NNN (T01).
Sistema(s) de IA		Identificador en el inventario (T02).
Clasificación regulatoria		Prohibido · Alto riesgo · Obligaciones de transparencia · Riesgo mínimo · Fuera de ámbito · Pendiente de clasificar.

Campo	Contenido	Guía
Papel de la compañía respecto al sistema		Proveedor · Responsable del despliegue · Ambos · Por determinar. Condiciona las obligaciones de notificación (documento 34).
¿Sujeta a DORA ?		Sí · No · Por determinar.
¿Sujeta a NIS2 (según transposición nacional)?		Sí · No · Por determinar.
¿Trata datos personales?		Sí · No.
Intensidad		Lite · Enterprise.
Versión del documento		
Autor		Rol y nombre.
Fecha		DD-MM-AAAA.
Estado del documento		Borrador · Presentado para verificación · Verificado · Aprobado · Sustituido.

03

Qué se considera incidente de este sistema

Tipo de incidente: Degradación del rendimiento · Resultado erróneo con impacto · Resultado discriminatorio o sesgado · Fuga de información · Acción no autorizada de un agente · Inyección de instrucciones o manipulación · Indisponibilidad · Incumplimiento regulatorio · Uso indebido del sistema · Incidente de un proveedor.

Tipo	¿Aplica a este sistema? (Sí · No)	Ejemplo concreto para este sistema	Detección prevista (alerta de P25 u otra vía)
Acción no autorizada de un agente *(ejemplo ilustrativo)*	Sí	El agente emite un reembolso por encima del límite	AL-02

04

Severidad

Escala común del marco: **S1 Crítica · S2 Alta · S3 Media · S4 Baja**. Los criterios completos están en el documento 37 y prevalecen sobre esta orientación.

Severidad	Orientación	Ejemplo para este sistema
S1 Crítica	Incluye cualquier posible incidente grave según el Reglamento Europeo de IA y los incidentes graves de DORA o NIS2 cuando apliquen.	
S2 Alta	Impacto relevante sobre personas, clientes, operación o cumplimiento, contenido o acotado.	
S3 Media	Impacto limitado, sin efecto relevante sobre personas ni obligaciones de notificación.	
S4 Baja	Sin impacto apreciable; anomalía que conviene registrar.	

05

Roles durante el incidente

Rol	Titular	Sustituto	Se activa en	Responsabilidad
Coordinador del incidente			S1–S4	Dirige la respuesta y decide la contención. Normalmente, responsable de operación de IA.
Responsable técnico			S1–S3	Diagnóstico, contención técnica y reversión.
Seguridad de la información			Incidentes de seguridad y agentes	Análisis de ataque y preservación de evidencias.
Protección de datos			Si hay datos personales	Valorar violación de seguridad de datos y derechos de afectados.
Responsable de riesgos de IA			S1–S2	Valorar obligaciones regulatorias y efecto en el registro de riesgos.
Comunicación (Enterprise)			S1–S2	Mensajes internos y externos coordinados.
Patrocinador de IA			S1–S2	Decisiones de negocio y escalado a órganos.

Rol	Titular	Sustituto	Se activa en	Responsabilidad
Registro del incidente			S1–S4	Cronología, decisiones y evidencias en P27.

06

Fases de respuesta

Los tiempos objetivo internos los fija la compañía; no sustituyen a los plazos regulatorios del documento 37.

Fase	Qué se hace	Responsable	Tiempo objetivo interno S1	Tiempo objetivo interno S2	Registro
Detección	Recibir alerta o aviso; abrir incidente	Guardia			P27
Clasificación	Tipo y severidad inicial	Coordinador			P27
Contención	Aplicar acciones del bloque 7	Coordinador y técnico			P27
Comprobación de notificaciones	Revisar bloque 8	Riesgos y protección de datos			P27
Resolución	Corregir la causa inmediata	Técnico			P27
Recuperación	Volver al funcionamiento normal con autorización	Coordinador			P27
Cierre y lecciones	Causa raíz, acciones correctivas, lecciones	Coordinador y riesgos			P27 · P12

07

Acciones de contención preparadas

Acción	Cuándo se aplica	Quién puede ejecutarla	Procedimiento
Interruptor de parada	Acción no autorizada, inyección con efecto, fuga en curso		P18 bloque 9
Reducir el nivel de autonomía	Degradación con riesgo de impacto		P19
Revertir a versión anterior	Fallo atribuible a un cambio reciente		P19
Desactivar una herramienta o permiso del agente	Abuso de una herramienta concreta		P18 bloque 5
Revocar credenciales	Compromiso de identidad		P18 bloque 4
Retirar o corregir contenido publicado	Contenido erróneo o inadecuado visible para terceros		
Preservar registros y evidencias	Siempre en S1 y S2		

08

Notificaciones regulatorias y contractuales a verificar

Casillas de comprobación. Para cada incidente se verifica si aplican; los plazos se toman del documento 37 y se confirman con asesoría jurídica. Esta tabla no afirma plazos.

☐	Notificación a verificar	Referencia	¿Aplica? (Sí · No · Por determinar)	Quién decide	Quién notifica	Plazo confirmado en documento 37 y fecha de verificación	Evidencia
☐	Incidente grave de un sistema de IA de alto riesgo	Reglamento Europeo de IA (obligaciones del proveedor y del responsable del despliegue; documento 34)					

☐	Notificación a verificar	Referencia	¿Aplica? (Sí · No · Por determinar)	Quién decide	Quién notifica	Plazo confirmado en documento 37 y fecha de verificación	Evidencia
☐	Información al proveedor del sistema de IA	Reglamento Europeo de IA y contrato (si la compañía es responsable del despliegue)					
☐	Violación de la seguridad de los datos personales a la autoridad de control	RGPD, artículo 33					
☐	Comunicación a los interesados	RGPD, artículo 34					
☐	Incidente grave relacionado con las TIC	DORA					
☐	Incidente significativo	NIS2 y transposición nacional					
☐	Notificaciones sectoriales	Regulación sectorial de la compañía					
☐	Obligaciones contractuales con clientes o proveedores	Contratos					
☐	Comunicación a personas afectadas no exigida por norma pero adecuada **(Enterprise)**	Política de la compañía					

Los modelos de notificación, la decisión motivada de no notificar y las comunicaciones están en P51.

09

Escalado interno

Severidad	A quién se informa	Plazo interno	Referencia
S1	Comité de IA y comisión delegada del consejo, además de los roles del bloque 5		Documento 37
S2	Comité de IA y patrocinador		Documento 37
S3	Responsable de producto de IA y oficina de IA		Documento 37
S4	Registro en P27		Documento 37

Si el incidente revela un incumplimiento del marco (control desactivado, cambio sin aprobar, gate omitido), se abre además una no conformidad con código NC-AAAA-NNN (P50, documento 37).

10

Simulacros

Fecha	Escenario	Participantes (roles)	Tiempo hasta contención	Resultado (Superado · Superado con observaciones · No superado)	Acciones de mejora
(ejemplo ilustrativo)	Documento con instrucciones ocultas provoca envío externo no autorizado	Guardia, seguridad, protección de datos, coordinador	35 minutos	Superado con observaciones	Protección de datos no tenía sustituto localizable; se designa

En Enterprise debería realizarse al menos un simulacro antes de G5 y repetirse con la periodicidad que fije la compañía.

11

Criterios de calidad

Criterios formales de G5 y R6 en el documento 21; proceso de incidentes en el documento 37.

#	Comprobación	Estado (Cumple · No cumple · No aplica · Pendiente)
1	Los tipos de incidente aplicables tienen ejemplo concreto y vía de detección.	
2	La severidad usa la escala S1–S4 y remite a los criterios del documento 37.	
3	Todos los roles tienen titular y sustituto.	
4	Las acciones de contención están preparadas y enlazadas con P18 y P19.	
5	Las notificaciones regulatorias están identificadas como casillas a verificar, sin plazos no confirmados.	
6	El escalado interno llega al comité de IA y a la comisión delegada en S1.	
7	Se ha realizado al menos un simulacro (Enterprise).	

12

Aprobación y verificación

Función	Rol	Nombre	Fecha	Firma o referencia
Autor	Responsable de operación de IA			
Revisión	Seguridad de la información			
Revisión	Protección de datos			
Conformidad	Responsable de riesgos de IA			
Verificador	Oficina de IA (Lite) · Auditor de IA (Enterprise)			

Separación de funciones: el verificador no forma parte del equipo que construye ni opera el sistema.

13

Control de versiones

Versión	Fecha	Cambios
0.1	16-09-2026	Primera versión de la plantilla.

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