PLANTILLA P42 · INFORME TRIMESTRAL DE SEGUNDA LÍNEA

Informe trimestral de segunda línea

Informa cada trimestre a la comisión delegada, o al comité que la sustituya, de los riesgos de la cartera, los incidentes, las no conformidades, las excepciones, la conciliación del inventario y los cambios regulatorios, con las decisiones que se le piden.

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 Mensaje principal y decisiones solicitadas

04 Riesgos de la cartera

05 Incidentes

06 No conformidades

07 Excepciones vigentes

08 Conciliación trimestral del inventario

09 Cambios regulatorios

10 Condiciones vencidas, aceptaciones caducadas y desacuerdos

11 Propuestas de decisión

12 Criterios de calidad

13 Aprobación y verificación

14 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. La comisión delegada supervisa la eficacia del control sobre la IA, pero solo puede hacerlo con una visión de conjunto que ningún caso de uso ofrece por separado: riesgos que se concentran en un proveedor o un modelo, incidentes que se repiten, no conformidades vencidas, excepciones que se eternizan, sistemas que aparecen fuera del inventario o normas que cambian. Este informe es la pieza de la segunda línea en C4 (30 §6.3) y convierte esa visión en decisiones concretas para la comisión.

01

Instrucciones de uso

Aspecto	Indicación
Cuándo se usa	Una vez por trimestre, antes de la sesión de la comisión delegada (C4), con la misma fecha de corte que el paquete del consejo (60 §7.2). Se adelanta un informe parcial si hay un incidente S1 o una no conformidad crítica.
Quién la rellena	El coordinador de segunda línea para la IA (responde y realiza, 30 §6.3), con los responsables de riesgos de IA, seguridad, protección de datos y cumplimiento; la oficina de IA aporta los datos de T01, T02, T06, T08, T09 y T21.
Quién la verifica	La tercera línea es consultada (30 §6.3); el comité de IA la conoce antes de su envío y puede añadir su posición, sin modificar el contenido.
Quién decide o aprueba	La comisión delegada supervisa y decide sobre las propuestas de la sección 11.
Etapa del ciclo corporativo	Supervisión (trimestral). El cuarto trimestre alimenta C5. (C4)
Herramienta	T06 (riesgos), T08 (incidentes y no conformidades), T02 (inventario), T09 (proveedores), T21 (uso corporativo), T01 (excepciones y condiciones) y T18 (decisiones).
Documento de referencia	30 §3.2 y §6.3; 32 §9; 33 §10–12; 34 §10.3; 37 §9; 60 §4.5–4.6.

Reglas de cumplimentación:

- Lenguaje de negocio: qué puede pasar, a quién afecta, qué se hace y qué decisión se pide; no listados técnicos sin priorizar (33 §12).
- Escalas de la especificación común §5.1 (riesgo), §5.5 (severidad S1–S4) y 01 §12 (no conformidades menor, mayor y crítica).
- Se distinguen siempre **hechos confirmados** de **valoraciones en curso** (37 §9).
- Los cambios regulatorios llevan fecha de consulta; el informe no constituye asesoramiento jurídico.

02

Identificación

Campo	Contenido	Guía
Periodo		AAAA-Tn.
Fecha de corte de los datos		
Destinatario		[Comisión de Auditoría / Riesgos / Tecnología] o consejo si no existe comisión.
Sesión en que se presenta		Referencia del acta (P39).
Elaborado por		Coordinador de segunda línea para la IA.
Versión		

03

Mensaje principal y decisiones solicitadas

Campo	Contenido	Guía
Mensaje principal		Tres líneas con el formato de respuesta: «Sí» · «Sí, con una condición: …» · «Todavía no, porque falta …» · «No, porque …». Responde a «¿está la IA dentro del apetito de riesgo?».
Cambios desde el trimestre anterior		

Campo	Contenido	Guía
Decisiones solicitadas		Lista con código DEC y una línea; si no hay, se dice expresamente.
(ejemplo ilustrativo) **Mensaje principal**	Sí, con una condición: que se apruebe el plan de salida del proveedor principal de modelos, del que depende el 62 % del valor validado.	

04

Riesgos de la cartera

4.1 Riesgos residuales Críticos y Altos

Riesgo (caso de uso · Rnn)	Riesgo tipo	Nivel inherente	Nivel residual	Responsable	Controles y eficacia	Aceptado por y vigencia	Próxima revisión
IA-AAAA-NNN · R01	RT-XXX-NN		Alto · Crítico				

4.2 Concentración

Factores de 33 §10.1 y 14 §9; umbrales aprobados en C2.

Factor	Situación del trimestre	Umbral de C2	¿Alerta? (Sí · No)	Medida propuesta
Proveedor de modelos				
Plataforma y nube				
Función crítica				
Datos				
Personas				
Esfera y ambición				

4.3 Correlación: escenarios de cartera

Valorados con la matriz de 33 §4: suma de impactos económicos de los sistemas afectados y peor impacto en los demás ejes (33 §10.2).

Escenario	Sistemas afectados	Impacto económico agregado	Peor impacto no económico	Nivel	Cambio frente al trimestre anterior
Indisponibilidad del principal proveedor de modelos					
Cambio de comportamiento de un modelo base común					
Vulnerabilidad en un componente común de agentes					
Reclasificación regulatoria de un tipo de uso					
Brecha en una base de conocimiento compartida					

4.4 Indicadores de riesgo clave

Umbrales aprobados en C2 (33 §11.2).

Indicador	Umbral	Valor	Trimestre anterior	Estado (Dentro · Fuera)
Residuales Críticos sin aprobación del consejo	0			
Residuales Altos aceptados	Sin crecimiento dos trimestres seguidos			
Aceptaciones caducadas	0			
Controles no probados (Alto o Crítico)	< 10 %			
Acciones de tratamiento vencidas	0 con más de 30 días			
Riesgos materializados sin riesgo previo	Tendencia a la baja			

Indicador	Umbral	Valor	Trimestre anterior	Estado (Dentro · Fuera)
Deriva fuera de umbral sin acción	0			
Éxito de inyección en la última campaña	Tendencia a la baja; 0 en acciones sensibles			
Agentes con permisos excesivos	0			
Concentración de proveedor	Según límite de C2			
Clasificación regulatoria vencida	0			
Uso no autorizado no regularizado	Tendencia a la baja			

Campo	Contenido
Cumplimiento del apetito de riesgo	Dentro · Fuera, con los límites superados.
Exposición a IA ofensiva (documento 35)	Indicadores principales y hechos del trimestre.

05

Incidentes

Contenido trimestral de 37 §9 y 60 §4.6.

Código	Sistema e caso de uso	Severidad	Tipo	Fecha	Estado	Notificaciones (régimen, plazo cumplido)	Lecciones y acciones
INC-AAAA-NNN		S1 · S2					

Agregado S3 y S4	Número	Tipología principal	Tiempo mediano de contención

Campo	Contenido
Notificaciones regulatorias del trimestre y cumplimiento de plazos	

Campo	Contenido
Incidentes de proveedores	
Lecciones sistémicas	

06

No conformidades

Código	Requisito incumplido	Tipo	Alcance	Estado	Plazo	¿Vencida?	Acción correctiva
NC-AAAA-NNN		Crítica · Mayor				Sí · No	

Críticas: siempre individualmente. Mayores: individualmente si están abiertas fuera de plazo; agregadas en el resto. Menores: solo el número.

Resumen	Críticas	Mayores	Menores
Abiertas			
Vencidas			
Cerradas en el trimestre			

07

Excepciones vigentes

Resumen del registro de P40 (30 §7.4).

Código	Tipo	Requisito afectado	Nivel de riesgo con medidas	Aprobada por	Caducidad	Estado
EXC-AAAA-NNN						Vigente · Vencida

08

Conciliación trimestral del inventario

Resultado de la conciliación de 32 §9, realizada por la oficina de IA.

Fuente contrastada	Diferencias encontradas	Tratamiento	No conformidades abiertas
Registro de aplicaciones y arquitectura			
Contratos, compras y renovaciones			
Registro de proveedores de IA (T09) y registro de proveedores TIC (DORA , cuando aplique)			
Facturación de nube y consumo de APIs de modelos			
Repositorios de código y plataformas de datos			
Registro de actividades de tratamiento (RGPD)			
Navegación, prevención de fuga de datos y dispositivos			
Notas de gasto y tarjetas corporativas			
Notas de versión de proveedores			
Comunicaciones, encuestas y auditorías			

Campo	Contenido
Sistemas dados de alta por la conciliación	
Sistemas en producción sin *gate* detectados	Cada uno es no conformidad crítica (01 §12).

09

Cambios regulatorios

Registro de cambios del mapeo (34 §10.3).

Cambio	Fuente oficial y fecha de consulta	Casos de uso o sistemas afectados	Paso alcanzado (1–8 de 34 §10.3)	Aprobado por el comité (Sí · No · No requerido)	Acción pendiente

10

Condiciones vencidas, aceptaciones caducadas y desacuerdos

Tipo	Referencia	Órgano que la impuso	Fecha de vencimiento	Tratamiento
Condición de *gate* vencida	P29			Resultado pasa a Iterar (01 §7.4, regla 4).
Condición de decisión del consejo vencida	DEC-AAAA-NNN			Se informa al órgano (62 §10.3).
Aceptación de riesgo caducada	IA-AAAA-NNN · Rnn			El riesgo vuelve a bloquear el *gate*.
Desacuerdo con el comité de IA (E-13)				Propuesta de resolución.

11

Propuestas de decisión

Cada propuesta con la ficha de decisión de 60 §5.1.

Código	Qué se solicita	Tipo	Respuesta de la segunda línea	Opciones	Qué ocurre si no se decide
DEC-AAAA-NNN		Aprobar · Aceptar un riesgo · Tomar conocimiento · Encargar			

12

Criterios de calidad

#	Comprobación	Estado
1	Los riesgos Críticos y Altos, la concentración y los escenarios de cartera están actualizados (33 §10).	Cumple · No cumple · No aplica · Pendiente
2	Todos los indicadores de riesgo clave tienen valor y umbral aprobado en C2, o se declara «sin dato».	
3	Los incidentes S1 y S2 y las no conformidades críticas se informan individualmente (37 §9; 60 §4.6).	
4	Las excepciones vigentes coinciden con el registro de P40.	
5	La conciliación del inventario se hizo en el trimestre con todas las fuentes de 32 §9.	
6	Cada cambio regulatorio tiene fuente oficial y fecha de consulta.	
7	Las propuestas de decisión se pueden aprobar o rechazar tal como están escritas.	
8	Se distinguen hechos confirmados de valoraciones en curso.	

13

Aprobación y verificación

Función	Rol en SEVEN-G	Nombre y cargo	Fecha	Firma o referencia
Elabora	Coordinador de segunda línea para la IA			
Aporta datos	Oficina de IA			
Es consultada	Tercera línea			
Conoce y añade su posición	Comité de IA			

Función	Rol en SEVEN-G	Nombre y cargo	Fecha	Firma o referencia
Supervisa y decide	Comisión delegada			Sesión y acuerdo (P39)

Separación de funciones: la segunda línea informa con independencia de las áreas que patrocinan la cartera; el comité de IA puede añadir su posición, pero no modifica el informe.

14

Control de versiones

Documento cumplimentado

Versión	Fecha	Autor	Cambios

Plantilla

Versión	Fecha	Cambios
0.1	19-09-2026	Primera versión. Reúne la información trimestral de riesgos (33 §10–12), incidentes y no conformidades (37 §9), excepciones (30 §7.4), conciliación del inventario (32 §9) y cambios regulatorios (34 §10.3).

Fuentes externas citadas

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

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.e