redeia

Especificación técnica

Título:	Datos de control:			
Notificación de ciberincidentes para proveedores de Redeia	Código:	Código corporativo:	Edición:	Cancela:
	EM001	**R–EM001**	**1 / 28.10.25**	
	Gestión de la norma:			
	Responsabilidad:	Aprobación:	Control y difusión:	
	Dirección Corporativa de Transformación y Recursos	**Dirección Corporativa de Transformación y Recursos**	**Dirección de Auditoría Interna y Control de Riesgo**	
	Firma:	Firma:	Firma y fecha: 30.10.2025	

Índice

Introducción 2
Objeto 2
Aplicabilidad 2
Obligaciones del proveedor 3
Taxonomía de ciberincidentes 3
Umbrales de notificación 4
Proceso, plazos y canales de comunicación 5
Anexo 1. Definiciones 8
Anexo 2. Contenido de las notificaciones 9
Anexo 3. Normativa aplicable 10
Histórico de modificaciones 11

Título:	Datos de control:			
Notificación de ciberincidentes para proveedores de Redeia	Código:	Código corporativo:	Edición:	Cancela:
	EM001	**R–EM001**	**1 / 28.10.25**	

Introducción

La sofisticación de los ciberataques experimentados por los sistemas eléctricos y de las telecomunicaciones durante los últimos años ha aumentado significativamente y el ciberriesgo se ha convertido en una amenaza clave para los negocios de Redeia. La contención de este en particular y del riesgo operacional, con carácter general, debe constituir una parte esencial del marco de gestión de los riesgos adoptado por los proveedores de Redeia.

Objeto

El objeto de esta especificación técnica es establecer un marco de referencia y un procedimiento pautado para la comunicación de ciberincidentes que puedan sufrir los proveedores de Redeia y que puedan suponer algún impacto en los procesos de negocio de Redeia.

La notificación de ciberincidentes a Redeia objeto de esta especificación técnica será de obligado cumplimiento para sus proveedores (dentro de los criterios de aplicabilidad y umbrales de notificación indicados en esta especificación), independientemente de las obligaciones legales que les correspondan en materia de comunicación de ciberincidentes a las autoridades u organismos competentes según la normativa vigente.

Este procedimiento se encuentra alineado con la normativa española y de la Unión Europea en esta materia y es de obligado cumplimiento para algunos de los negocios de Redeia por su condición de operador de servicios esenciales y de infraestructuras críticas.

Esta especificación técnica formará parte de la documentación contractual en los procesos de licitación junto con otra documentación de aplicación como las Condiciones Generales de Contratación y la cláusula de ciberseguridad de Redeia, entre otras.

Aplicabilidad

Esta especificación técnica es de aplicación para los proveedores de bienes y servicios de Redeia que puedan encuadrarse en alguna de las siguientes actividades:

- Provean de infraestructura tecnológica a Redeia en cualquier modalidad: PaaS, IaaS, SaaS.
- Precisen para la realización del suministro del uso o la conexión previamente autorizada a cualquier sistema de información de Redeia, sus dispositivos o sus redes de telecomunicaciones.
- Suministren equipamiento tecnológico, aplicaciones informáticas, o sistemas de información, de la operación o de las comunicaciones.

- Realicen desarrollo de software para Redeia.
- Presten servicios, administren o mantengan sistemas de información o infraestructura tecnológica de Redeia.
- En el contexto del suministro, realicen algún tipo de tratamiento (elaboración, modificación, almacenamiento temporal o permanente) de información no pública de Redeia.

Obligaciones del proveedor

Esta especificación técnica proporciona a los responsables de ciberseguridad y a los equipos de respuesta ante incidentes de los proveedores las directrices para el cumplimiento de las obligaciones de reporte de incidentes de ciberseguridad que puedan tener relación con Redeia.

Los proveedores de Redeia deberán notificar aquellos eventos categorizados como **ciberincidentes**, según la definición del **Anexo 1. Definiciones**, que abarcan tanto eventos internos como externos de naturaleza maliciosa o accidental. El proveedor analizará el ciberincidente para clasificarlo empleando la clasificación descrita en el apartado ¡Error! La autoreferencia al marcador no es válida.. Este análisis debe evaluar los efectos negativos de la amenaza en la continuidad de los servicios prestados a Redeia, el impacto sobre su infraestructura tecnológica, sistemas de información o de la operación, redes de telecomunicaciones o sobre la información no pública de Redeia.

El proveedor informará sobre los ciberincidentes que puedan impactar potencialmente a los sistemas de Tecnologías de la Información y de las Comunicaciones utilizados para prestar sus servicios, incluso si no han causado un efecto adverso real, siguiendo los criterios que se enumeran en el apartado **Umbrales de notificación**.

En caso de subcontratación, el proveedor es responsable de hacer extensiva la responsabilidad de esta especificación técnica en toda su cadena de subcontratación.

Una vez recibida notificación de ciberincidente por parte de un proveedor y analizado su posible impacto, Redeia tomará las medidas que considere necesarias para mitigar los riesgos sobre sus activos, lo que podrá afectar a los procesos previamente establecidos con el proveedor para la ejecución de sus contratos y/o al estado de calificación del proveedor.

Taxonomía de ciberincidentes

Con la finalidad de que las unidades de Redeia implicadas en dar posible respuesta al ciberincidente dispongan de información útil para analizar y evaluar su alcance, el proveedor empleará en los informes de notificación la clasificación / taxonomía de los ciberincidentes definida en la **normativa vigente sobre esta materia**, que se indica en el **Anexo 3. Normativa aplicable**.

Dependiendo del ciberincidente, el proveedor debe asignar una o más de las categorías en el informe de notificación, tal y como se detalla en el apartado **Proceso, plazos y canales de comunicación**. Las categorías que componen la taxonomía no son excluyentes y, en consecuencia, en el informe de notificación deberán indicarse todas las clasificaciones aplicables.

Como información complementaria, en todo caso deberá indicarse si el ciberincidente responde a alguna de las siguientes naturalezas:

- Afecta a la confidencialidad, integridad, disponibilidad o privacidad de la información de Redeia.
- Afecta a la infraestructura tecnológica del proveedor de manera que resulten afectados los servicios prestados por el proveedor a Redeia.
- Casos de ransomware o compromiso del servicio de correo electrónico.
- Compromiso, manipulación o alteración de productos tecnológicos que el proveedor o su cadena de valor haya suministrado a Redeia.

Umbrales de notificación

El ciberincidente debe ser notificado si se cumple alguno de estos criterios:

- El ciberincidente puede dañar significativamente la reputación de Redeia si aparece en medios de comunicación o redes sociales.
- El ciberincidente ha implicado la destrucción, robo o divulgación de información no pública de Redeia.
- El proveedor considerará relevante un ciberincidente si requiere internamente en su compañía escalado a un comité de gestión para decisiones ejecutivas u operativas.
- El ciberincidente ha supuesto o es probable que suponga el incumplimiento de obligaciones legales o regulatorias.
- El ciberincidente ha llevado a la activación de los planes de continuidad del negocio o de contingencia tecnológica del proveedor.
- El ciberincidente se ha notificado al CERT/CSIRT nacional o autonómico, o a las Fuerzas y Cuerpos de Seguridad del Estado.
- La infraestructura tecnológica, los sistemas de información, operación o redes de comunicaciones de Redeia pueden verse afectados: si hay un riesgo significativo de afección sistémica, el ciberincidente es relevante, incluso si el proveedor lo ha contenido adecuadamente.

Si se identifican varios ciberincidentes vinculados, el proveedor puede decidir agruparlos en una única notificación o gestionarlos por separado. El análisis de relevancia debe mantenerse a lo largo de todo el ciclo

de vida del ciberincidente, dado que un evento inicialmente insignificante puede evolucionar y necesitar ser notificado.

Proceso, plazos y canales de comunicación

El proceso de notificación se divide en tres etapas, cada una con un contenido progresivamente detallado: **notificaciones inicial, intermedia y final**.

La información requerida para cada una de las notificaciones se incluye en el **Anexo 2. Contenido de las notificaciones** de este documento.

- La **notificación inicial** es la comunicación que informa y alerta sobre un incidente. Incluye datos generales para ofrecer una visión inicial del ciberincidente y confirmar el contacto dentro del proveedor para futuras comunicaciones. Es crucial que esta notificación se produzca **sin dilación indebida**, con la finalidad de que los equipos operativos de Redeia puedan tomar las medidas necesarias para evitar la propagación del incidente.
- La **notificación intermedia** es una comunicación mediante la que se actualizarán los datos disponibles en ese momento relativos al incidente comunicado y actuaciones mitigatorias realizadas.
- La **notificación final** es una comunicación de cierre del incidente, mediante la que se amplían y confirman los datos definitivos relativos al incidente comunicado.

Los plazos para notificar se cuentan desde el momento en que el ciberincidente es detectado por el proveedor y se considera significativo, es decir, desde que se cumple alguno de los criterios establecidos en el apartado **Umbrales de notificación**.

Estas notificaciones se deberán realizar según la siguiente ventana temporal de reporte:

Notificación inicial	Notificación intermedia	Notificación final
Inmediata	**Máximo 48 horas**	**20 días**

En caso de incumplimiento de los plazos máximos de notificación, Redeia se reserva la potestad de considerar medidas adicionales en relación con el proveedor.

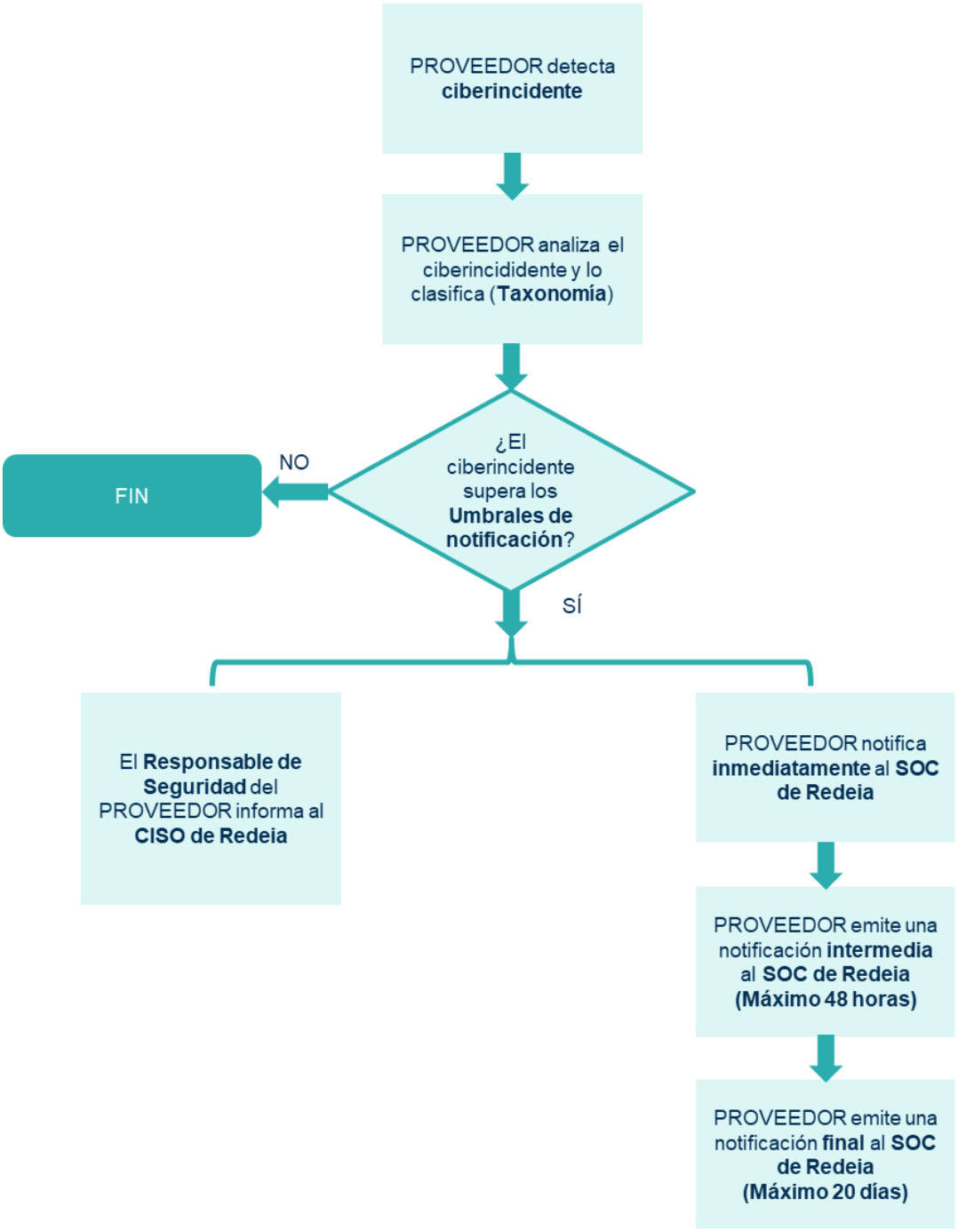
Título:	Datos de control:			
Notificación de ciberincidentes para proveedores de Redeia	Código:	Código corporativo:	Edición:	Cancela:
	EM001	**R–EM001**	**1 / 28.10.25**	

En cuanto al canal de comunicación para la notificación de los incidentes, se establece como canal único el **SOC (Security Operations Center)** de Redeia. Los incidentes deberán ser comunicados por correo y por teléfono en 24 x 7 x 365:

SOC Redeia
Teléfono: **+34 916 599 119 Ext. 2875**
Correo electrónico: **CERT@redeia.com**

Además de estas comunicaciones operativas, el responsable de Seguridad designado por el proveedor deberá comunicar toda la información relacionada con el incidente al Responsable de Seguridad de la Información (RSI / CISO) de Redeia, por correo electrónico al buzón **CISO@redeia.com.**

El diagrama de la siguiente página resume el proceso de notificación desde la detección de un ciberincidente.


PROVEEDOR detecta **ciberincidente**
PROVEEDOR analiza el ciberincidiente y lo clasifica (**Taxonomía**)
¿El ciberincidente supera los **Umbrales de notificación**?
NO
FIN
SÍ
El **Responsable de Seguridad** del PROVEEDOR informa al **CISO de Redeia**
PROVEEDOR notifica **inmediatamente** al **SOC de Redeia**
PROVEEDOR emite una notificación **intermedia** al **SOC de Redeia (Máximo 48 horas)**
PROVEEDOR emite una notificación **final** al **SOC de Redeia (Máximo 20 días)**

Anexo 1. Definiciones

Cibermedio	Infraestructura para la interconexión e interacción entre personas, procesos, datos y sistemas de información
Ciberseguridad	Protección de la confidencialidad, integridad y disponibilidad de la información y sistemas de información en el cibermedio
Ciberevento	Cualquier acontecimiento observable en un sistema de información o en el cibermedio
Ciberincidente	Ciberevento que tenga efectos adversos reales en la seguridad de las redes y sistemas de información o que violen las políticas y/o procedimientos de seguridad de la organización, independientemente de que sean intencionados.
Ciberriesgo	La combinación de la probabilidad de ocurrencia de ciberincidentes y la materialización de sus consecuencias.
Ingeniería social	Se definen así a todas aquellas técnicas que buscan la revelación de información sensible de un objetivo, generalmente mediante el uso de métodos persuasivos y con ausencia de voluntad o conocimiento de la víctima

Anexo 2:	Datos de control:			
Contenido de las notificaciones	Código:	Código corporativo:	Edición:	Cancela:
	EM001	**R–EM001**	**1 / 28.10.25**	

Anexo 2. Contenido de las notificaciones

	Contenido
Asunto	Frase que describa de forma general el incidente. Este campo lo heredarán todas las notificaciones asociadas al incidente.
Proveedor	Identificación del proveedor que notifica
Servicio afectado	Identificación de los suministros (si aplica, identificando los números de pedidos de Redeia) y unidades de Redeia afectadas
Fecha y hora del incidente	Indicar con la mayor precisión posible cuándo ha ocurrido el ciberincidente
Fecha y hora de detección del incidente	Indicar con la mayor precisión posible cuándo se ha detectado el ciberincidente
Descripción	Describir lo sucedido con el mayor detalle del que se disponga
Recursos tecnológicos de Redeia afectados	Indicar toda la información técnica relevante sobre el número y tipo de activos afectados por el ciberincidente
Origen del incidente	Indicar la causa del incidente si se conoce
Taxonomía del incidente	Posible clasificación y tipo de ciberincidente en función de la taxonomía descrita.
Plan de acción y contramedidas para su mitigación y contención	Actuaciones realizadas hasta el momento en relación con el ciberincidente. Indicar el plan de acción seguido junto con las contramedidas implantadas, focalizando las acciones relacionadas con el suministro realizado a Redeia.
Adjuntos	Indicar la relación de documentos adjuntos que se aportan para ayudar a conocer la causa del problema o a su resolución (IOCs, capturas de pantalla, ficheros de registro de información, correos electrónicos, etc.).
Regulación relacionada con el incidente	Si resulta de aplicación (Ley de Protección de Infraestructuras Críticas, Reglamento General de Protección de Datos, Ley Orgánica de Protección de datos personales y garantía de los derechos digitales, Ley de Seguridad de las redes y sistemas de información y cualquier otra normativa aplicable en el momento del ciberincidente).
Ha requerido actuación de FCS	Sí / No
Contactos	Datos de contacto del proveedor para futuras comunicaciones

Anexo 3. Normativa aplicable

La **Instrucción nacional de notificación y gestión de ciberincidentes**, se encuentra en el **Real Decreto 43/2021**, de 26 de enero, por el que se desarrolla el **Real Decreto-ley 12/2018**, de 7 de septiembre, de **seguridad de las redes y sistemas de información**.

Datos de control:				
Histórico de modificaciones	Código:	Código corporativo:	Edición:	Cancela:
	EM001	**R–EM001**	**1 / 28.10.25**	

Histórico de modificaciones

Control de cambios del cuerpo

Afecta a:	Edición/Fecha:	Cancela a:	Control de cambios:
Cuerpo	1 / 28.10.25	N/A	• Primera edición del documento.

Control de cambios de anexos

Afecta a:	Edición/Fecha:	Cancela a:	Control de cambios:
Anexo 1	1 / 28.10.25	N/A	• Primera edición del documento.
Anexo 2	1 / 28.10.25	N/A	• Primera edición del documento.
Anexo 3	1 / 28.10.25	N/A	• Primera edición del documento.