redeia

El valor de lo esencial

Seguridad en la cadena de suministro

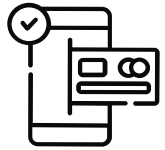
Gestión de ciberincidentes con proveedores

Diciembre, 2025

Información general sobre el desarrollo del evento

Grabación del evento.

Duración: 1 hora.



Dudas a través del chat de Teams.

Encuesta satisfacción - Ronda de dudas y preguntas
(al final de la sesión).

Índice

redeia

1. Motivaciones, contexto, modelo gestión del riesgo y controles

Motivaciones

Continuidad de los servicios esenciales que Redeia presta a la sociedad

Los proveedores son actores fundamentales en la prestación de los servicios y en la gestión eficaz de los incidentes de seguridad

La digitalización de los negocios ha transformado el perfil de las amenazas y los riesgos deben ser gestionados

La seguridad de los activos de Redeia es una labor compartida con sus proveedores

Contexto de seguridad

Digitalización y conectividad. **Aumento de la superficie de exposición** de las tecnologías de la información y de la operación.

Infraestructuras y entidades críticas: objetivo de atacantes con diferentes motivaciones.

Amenaza creciente: **aumento de los ataques a las cadenas de suministro** de las organizaciones (30% de las brechas de seguridad), RaaS, utilización de la IA como vector de ataque.

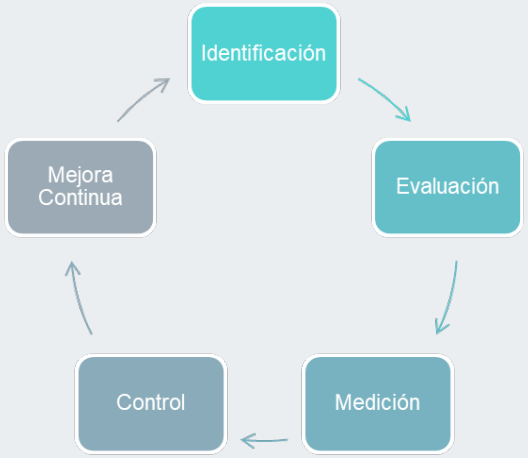
Entorno regulatorio: NIS2 y CER
Foco específico en la gestión de la seguridad en la cadena de suministro. Cumplimiento y debida diligencia.

Resiliencia y continuidad de los servicios: clave en la gestión de los riesgos en la cadena de suministro

Modelo gestión del riesgo y controles

Modelo integral de riesgos para proveedores: Establece un **marco estructurado** para identificar, evaluar, monitorizar y controlar los **riesgos asociados a la gestión de los proveedores de Redeia**, con el **fin último** de poder **actuar para su mitigación**, aportando información de valor para la **toma de decisiones** en los procesos relativos a la cadena de suministro.

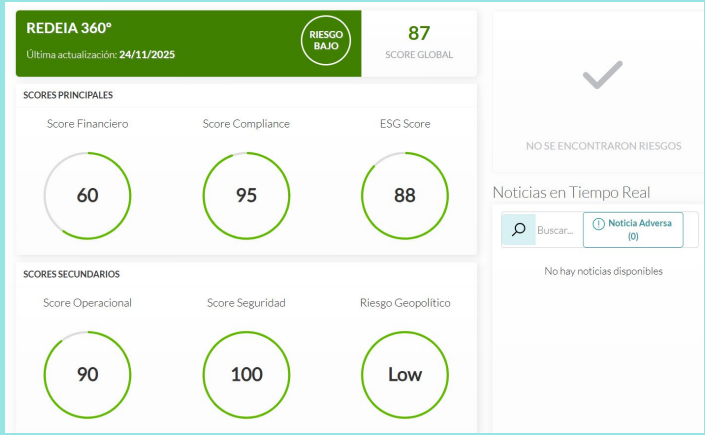
Ámbitos monitorizados: estado empresarial, estados financieros, posicionamiento en sostenibilidad (ESG, Cumplimiento, Seguridad), ubicación geográfica y operación del proveedor con Redeia.



Documentación Contractual

- Condiciones Generales de Contratación TI
- Anexo Ciberseguridad
- ET Notificación de ciberincidentes para proveedores (R-EM001)
- Contrato de encargado de tratamiento de datos personales

Herramienta Global de Gestión de Riesgos proveedor en el Portal de Aprovisionamientos



redeia

2. Caso práctico - Gestión de ciberincidentes

Encuesta. Procedimiento de gestión de incidentes

Seleccione la opción que considera que se ajusta más a la realidad de su compañía:

- **1.** No dispone de ningún documento normativo interno que regule la gestión de ciberincidentes.
- **2.** Se dispone de un procedimiento de gestión de ciberincidentes en el que se establecen roles y responsabilidades, medidas de respuesta y recuperación, tiempos máximos y notificación a autoridades y clientes.
- **3.** Se dispone de un protocolo interno para la gestión de ciberincidentes orientado a la continuidad de las operaciones de la compañía.
- **4.** Se dispone de un procedimiento de gestión de ciberincidentes en el que se definen las alternativas de continuidad, los tiempos máximos de recuperación y el cumplimiento de obligaciones legales.
- **5.** Lo desconozco.

Caso práctico

El proveedor xYz tiene un contrato de prestación de servicios con Redeia por el que elabora información confidencial de Redeia que almacena en su infraestructura tecnológica. Para la prestación del servicio, también dispone de conexión a sistemas de información de Redeia mediante cuentas de usuario.

Sus sistemas de monitorización detectan una actividad inusual en el tráfico de red en una de sus sedes. Tras investigación inicial, se descubre que ha sufrido un ataque de ransomware y que:

- se ha cifrado información de varios servidores.
- se ha producido exfiltración de información.

Un día después, los delincuentes comunican la autoría del ataque y reclaman un rescate para obtener las claves de cifrado y para no revelar la información exfiltrada (doble extorsión) y proporcionan una muestra de esta información.

Durante el avance de la investigación se descubre que ha sido exfiltrada información propiedad de Redeia sujeta a regulación y que está expuesta en la DarkWeb.

Pregunta 1. Respuesta inicial

¿Cuál de estas opciones considera que sería la respuesta inicial más idónea ante el ciberincidente?

- **1.** Lo prioritario es la recuperación de los servicios. Se activará el procedimiento de recuperación de los sistemas afectados por el incidente y una vez recuperado, se realizará un análisis forense y en caso de obligación legal, se notificará a las autoridades.
- **2.** Activación de medidas de contención. Se almacenarán los registros de los sistemas que permitan analizar el incidente. Se activarán los mecanismos de recuperación de los sistemas. En paralelo, se realizará una notificación inicial a autoridades (si fuera preciso) y clientes afectados con la mejor información posible sobre el tipo del incidente y una valoración inicial del alcance.
- **3.** Desconexión de todos los sistemas para evitar la propagación y contratación de una empresa externa especializada en la investigación forense del incidente. Se detendrán las operaciones hasta disponer de toda la información sobre el incidente. Se restaurarán las últimas copias de seguridad para arrancar los servidores afectados. Una vez superado el incidente, se realizará una comunicación pública (web, redes sociales) sobre el ataque sufrido y la vuelta a la normalidad de las operaciones.

Pregunta 2. Recuperación y cierre del incidente

¿Cuál de estas opciones considera que sería más idónea en lo que se refiere a aplicación de medidas de recuperación y cierre del incidente?

- **1.** Se prioriza la recuperación de los sistemas. En paralelo, se investiga el incidente para clasificarlo y determinar alcance. Si la información exfiltrada está sujeta a algún tipo de regulación, se realizará una notificación inicial a las autoridades. Una vez analizado el vector de ataque y posibles vulnerabilidades, se aplicarán medidas de seguridad adicionales. Una vez superada la crisis, se informará a los clientes de la vuelta a la normalidad de los servicios.
- **2.** Debe evitarse en todo momento el daño reputacional que pueda afectar a su compañía. La comunicación externa se realizará una vez subsanado el incidente y recuperada la normalidad de las operaciones. Ante solicitudes de los clientes, se limitará la información a la mínima imprescindible, indicando que se está priorizando la recuperación de los servicios.
- **3.** Se activan los procedimientos de continuidad de negocio relativos a los sistemas afectados. Se acuerdan con los clientes afectados las alternativas de continuidad y los plazos de recuperación previstos. En paralelo, se investiga el incidente para clasificarlo y determinar alcance. Si la información exfiltrada está sujeta a algún tipo de regulación, se realizará una notificación inicial a las autoridades y a los clientes responsables de esta. Como cierre del incidente, se proporcionará a los clientes un informe indicando los análisis de seguridad realizados en la infraestructura y las medidas de seguridad adicionales implantadas para subsanar las posibles vulnerabilidades detectadas.

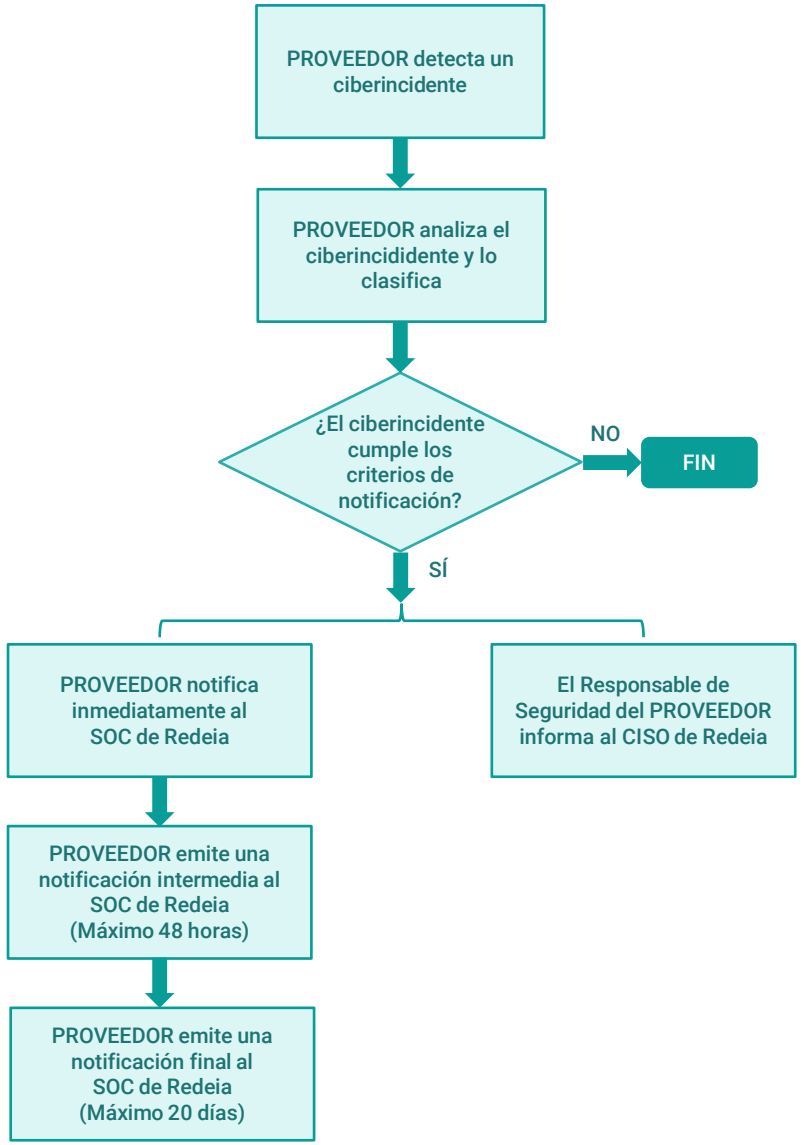
Gestión de ciberincidentes

La **Especificación Técnica E-RM001** establece las obligaciones de los proveedores de Redeia en cuanto a notificación de ciberincidentes.
En esta se definen la clasificación de ciberincidentes, criterios de notificación, canales, información necesaria y plazos máximos.
[Instrucción nacional de notificación y gestión de ciberincidentes]

Los **tiempos de notificación** son la clave para la adecuada **contención** del ciberincidente. Permite a los equipos operativos en ciberseguridad de Redeia desplegar las **medidas para evitar su propagación o reducir el impacto**.

Contacto operativo único: el **canal de notificación** 24 x 7 es el **SOC de Redeia: CERT@redeia.com**

Colaboración y coordinación con nuestros proveedores, poniendo el foco en la recuperación y **continuidad de los servicios** y en el **cumplimiento de obligaciones legales**



https://www.redeia.com/es/conocenos/proveedores

redeia

3. Encuesta de satisfacción - dudas y preguntas

Encuesta satisfacción

- Encuesta de opinión después del evento

Dudas y preguntas

- Micrófonos silenciados.
- Necesario levantar la mano.
- Preguntas claras y concisas

redeia

Gracias

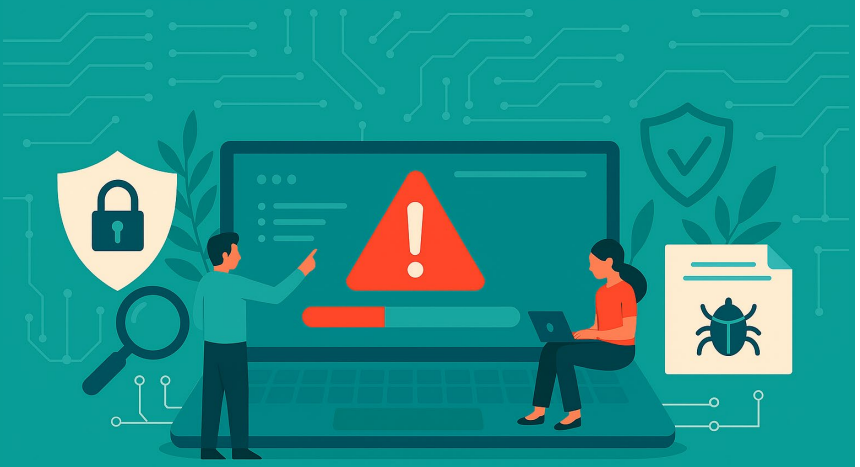
4. Anexos

redeia

Gestión de incidentes y resiliencia

Todos los marcos de gestión de ciberseguridad y las regulaciones nacionales e internacionales en esta materia ponen especial foco en la adecuada **gestión de los incidentes de seguridad**, como **medida de resiliencia que garantice la continuidad de los servicios** que los operadores esenciales prestan a la sociedad.

En Redeia, consideramos a **nuestros proveedores aliados esenciales** para garantizar la protección de los sistemas de información vinculados al suministro. Por ello, la gestión eficaz de los incidentes de seguridad constituye un elemento clave en la colaboración que mantenemos con ellos.



Para reforzar la seguridad, Redeia ha desarrollado la Especificación Técnica de Notificación de Ciberincidentes dirigida a sus proveedores. Este documento establece:

- Las obligaciones en la **comunicación** de cualquier ciberincidente que pueda afectar a Redeia.
- Los **canales** habilitados y la información que debe facilitarse.
- Los **plazos** máximos para la notificación desde su detección por parte del proveedor.

Cuando resulte de aplicación, esta especificación técnica formará parte de la documentación contractual de las licitaciones.

Actuar a tiempo es la clave

Cuando se produce un incidente de seguridad de la información o de los sistemas de información, **actuar en el momento oportuno es crucial**, ya que permite desplegar las medidas que permitan **contenerlo, evitar su propagación y reducir su impacto**.

Por este motivo, cuando un proveedor tenga constancia de haber sufrido un ciberincidente debe **comunicarlo de forma inmediata** a Redeia **aportando la mejor información disponible en ese momento** (clasificación del ciberincidente, evaluación de impacto, …).

Punto de contacto

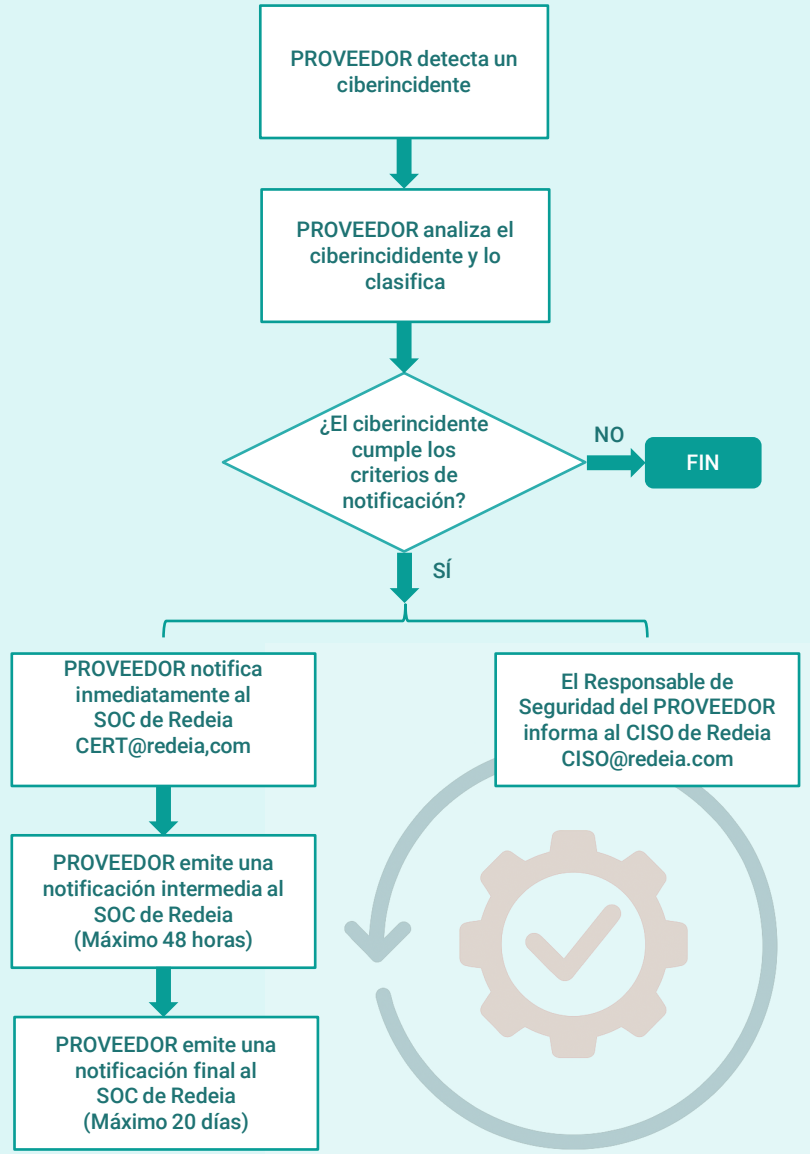
El **punto de contacto 24 x 7** establecido para las notificaciones a Redeia es su **Centro de Operaciones de Seguridad (SOC)** :

SOC Redeia

CERT@redeia.com

El proceso de notificación

Este flujograma muestra los hitos principales del **proceso de notificación de un ciberincidente** para nuestros proveedores:



Puede consultar la Especificación técnica R-EM001 **Notificación de ciberincidentes para proveedores de Redeia** en el espacio **Proveedores** de **www.redeia.com**

Modelo de seguridad

Gobierno
Modelo de gestión de riesgos
Condiciones generales de contratación TI
Anexo de ciberseguridad
ET Notificación de ciberincidentes para proveedores (E-RM001)
Tratamiento de datos de carácter personal
Procedimientos internos de gestión de incidentes en terceros

Protección
Evaluación del riesgo en los diferentes tipos de suministro
Requerimientos de calificación de proveedores
Evaluación de proveedores en los requerimientos de seguridad que mitigan los riesgos
Scoring de cumplimiento de proveedores

Defensa
Seguimiento de proveedores adjudicatarios de contratos
Finalización de contratos (Devolución de información)

Resiliencia
Gestión de incidentes en la cadena de suministro
Gestión de la continuidad de negocio

Implantación del modelo de gestión. Recorrido

Redeia ha implantado un **modelo de seguridad propio** en la cadena de suministro en el **ámbito de la ciberseguridad, la seguridad de la información y la seguridad física.** Su objetivo es realizar una **gestión adecuada de los riesgos de seguridad asociados al aprovisionamiento de Redeia**.

2020

Desarrollo del modelo de gestión: evaluación del riesgo y catálogo de requerimientos de seguridad

2021

Prueba de implantación del modelo en 10 suministros de diferente nivel de riesgo inherente

Solicitud de información a proveedores sobre cumplimiento de requerimientos de seguridad

2022

Arranque del despliegue en suministros de nivel de riesgo Alto y Muy alto

Solicitud de información a proveedores sobre cumplimiento de requerimientos de seguridad

Foro proveedores
Divulgación del modelo de gestión de seguridad en la cadena de suministro

2023

Finalización del despliegue en suministros de nivel de riesgo **Alto y Muy alto**

Campaña de divulgación sobre **tratamiento de información no pública**

Solicitud de información a proveedores sobre cumplimiento de requerimientos de seguridad

Envío de **feedback** a proveedores sobre **resultados de la evaluación**

Publicación de resultados generales en la web

2024

Despliegue en suministros de nivel de riesgo **Moderado**
Primer ciclo completo de evaluación

Automatización de procesos de envío de feedback

Solicitud de información a proveedores sobre cumplimiento de requerimientos de seguridad

Envío de feedback a proveedores sobre resultados de la evaluación

Jornada en el Campus Redeia
Cibeserguridad industrial para proveedores con accesos a equipos y sistemas

2025

Integración del modelo de seguridad en la **herramienta de monitorización del riesgo de proveedores**

ET E-RM001 **Notificación de ciberincidentes para proveedores**

Divulgación de la ET Notificación de ciberincidentes en web

Foro proveedores
Gestión de ciberincidentes

redeia

El valor de lo esencial

red eléctrica reintel hispasat redinter elewit