redeia

Incident management and resilience

All cybersecurity management frameworks and national and international regulations in this area place special emphasis on the proper **management of security incidents**, as a **resilience measure that guarantees the continuity of services** that essential operators provide to society.

At Redeia, we consider **our suppliers essential partners** in ensuring the protection of information systems linked to our supply chain. Therefore, effective security incident management is a key element in our ongoing collaboration with them.

To strengthen security, Redeia has developed the Technical Specification for Cyber Incident Notification for its suppliers. This document establishes:

- The obligations regarding the communication of any cyber incident that may affect Redeia.
- The **available channels** and the i**nformation** that must be provided.
- The **maximum timeframes** for notification after detection by the provider.

When applicable, this technical specification will form part of the contractual documentation for tenders.

Acting promptly is key

When an information security or information systems incident occurs, **acting at the right time is crucial**, as it allows the deployment of measures to **contain it, prevent its spread, and reduce its impact**.

For this reason, when a supplier becomes aware of having suffered a cyber incident, it must **immediately report it** to Redeia, **providing the best available information at that time** (incident classification, impact assessment, etc.).

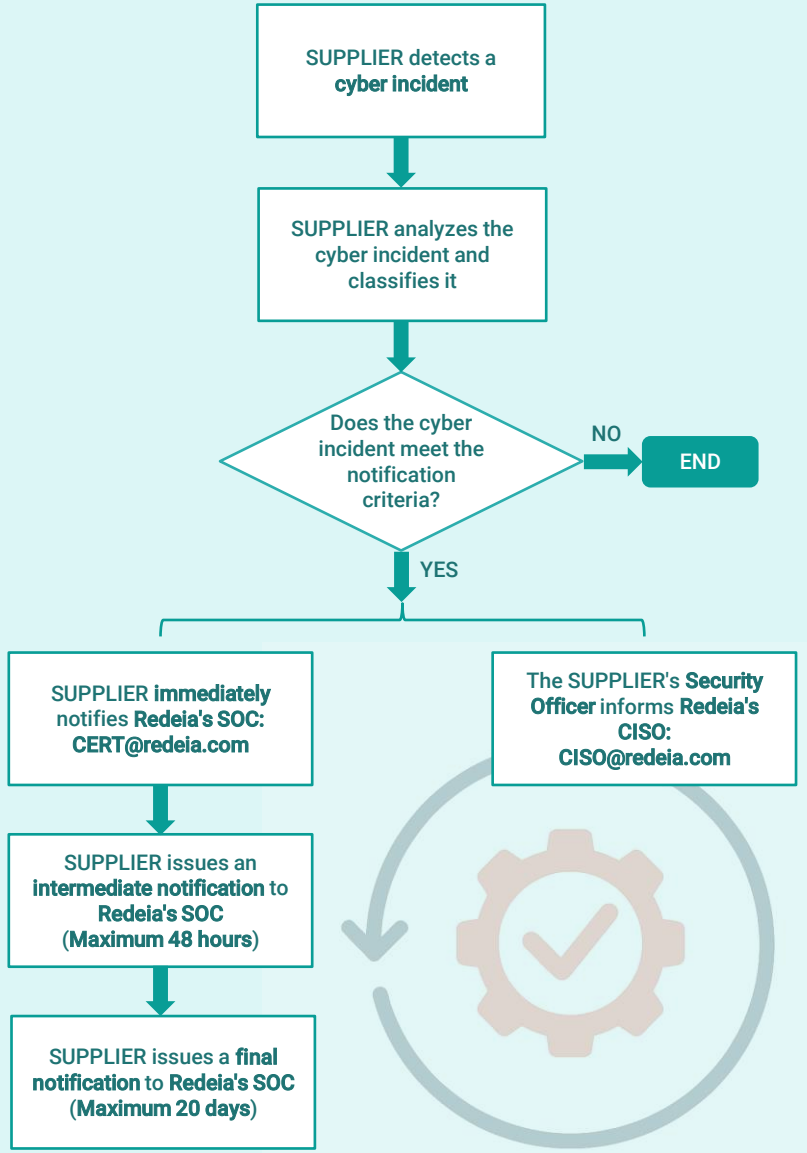
Point of contact

The established **24/7 point of contact** for notifications to Redeia is its **Security Operations Center (SOC)**:

SOC Redeia
CERT@redeia.com

The notification process

This flowchart shows the main milestones in the **cyber incident notification process** for our suppliers:



You can consult the Technical Specification R-EM001 **Cyber Incident Notification for Redeia suppliers** in the **Suppliers** section of **www.redeia.com**