ALTIA

Technology for real growth

RFC2350

ALTIA | CSIRT

Date	Version
04/06/2026	01

INDEX

1 Document Information

1.1 Object

This document aims to describe the framework for action of the ALTIA Security Incident Response Team (hereinafter, ALTIA-CSIRT), including its organizational structure, scope of action, responsibilities, contact channels and services provided.

1.2 Distribution list for notifications

Changes to this document are not distributed via mailing list. Any specific questions or comments should be directed to the following email address:ciberseguridad@altia.es

1.3 Document Location

The latest version of the document is published at:

- Spanish: https://www.altiacompany.com/sites/default/files/2026-06/RFC2350-ES.pdf
- English: https://www.altiacompany.com/sites/default/files/2026-06/RFC2350-EN.pdf

2 Contact information

2.1 Identification data

- Team Name: ALTIA-CSIRT
- Address:
  - Campus Universitario de Vigo. Lagoas
  - Marcosende, 32. 36310 Vigo
- Time Zone: CET / CEST
- Phone number: +34 986 90 23 00
- Fax number: Does not exist
- Other comunications: Do not exist
- E-mail addresses:
  - Exchange of information related to incidents: incidentes.ciber@altia.es
  - General inquires: ciberseguridad@altia.es
  - Additional information about the service and contact channels: https://www.altiacompany.com/en/services/cybersecurity-solutions
- Public keys and information encryption:

  ALTIA-CSIRT uses the email address incidentes.ciber@altia.es for communications related to cybersecurity incident response.

  This address is protected with the PGP key: B22C AB5B B719 E3C4 BE98 2817 B038 5792 749D 5767.

  For administrative communications or inquiries, please use the address ciberseguridad@altia.es protected with the PGP key: 12CC 535A 21A5 2DFC 87C1 E934 CADE 6CE0 1FA6 7757.

GPG/PGP keys can be downloaded from https://www.altiacompany.com/en/services/cybersecurity-solutions (section "Contact Information"). Additionally, GPG/PGP keys are available on the RedIRIS key server and can be found on the public ring by searching for https://pgp.rediris.es/.

2.2 Team

The team is made up of personnel performing the following roles:

- **Information Security Alert Analysts (Level 1)**
- **Security Incident Response Specialists (Level 2)**
- **Experts in Specific Areas of Information Security (Level 3).CSIRT Manager**
- **Security**
- **Manager**

- **Hours of Operation:** The incident response team is available during the following hours:
  - Service inquiries: Office hours (8:00 a.m. - 6:30 p.m.)
  - Incidents: extended hours (24x7x365).

- **Community touchpoints:** ALTIA-CSIRT primarily communicates with the organizations it serves through the following means:
  - Ticketing tool.
  - Support email.
  - Contact phone number enabled for operational coordination.

3 Constitution

ALTIA-CSIRT is ALTIA's specialized team for managing and responding to cybersecurity incidents, integrated within the company's Cybersecurity unit. Its creation stems from the need to provide an organized, specialized, and traceable capability for the detection, analysis, coordination, and response to incidents that could affect its clients' assets, services, and operations.

The team operates in a context marked by the increasing exposure of organizations to cyber threats, the complexity of technological environments, and the need to guarantee the continuity, availability, integrity, confidentiality, authenticity, and traceability of information and services provided.

To this end, ALTIA-CSIRT has the technical capabilities, operating procedures, and specialized personnel to address the complete incident management cycle, from preparation and detection to containment, eradication, recovery, and coordination with third parties when necessary.

Furthermore, the team operates in accordance with all applicable contractual, regulatory, and legal obligations, including, where appropriate, the notification, coordination, and information handling requirements associated with security incident management.

ALTIA-CSIRT provides services to public and private entities that contract for monitoring, detection, and incident response capabilities, with a focus on reducing the operational and security impact of threats and cyber incidents.

Its operations are supported by qualified personnel, specialized tools, and defined procedures to provide a consistent, coordinated, and appropriate response tailored to each client's needs and the contracted service framework.

3.1 Mision

ALTIA-CSIRT's mission is to contribute to reducing the probability and impact of security incidents affecting its clients' systems, services, and information assets.

To achieve this, it provides incident detection, analysis, coordination, and response capabilities, as well as technical and operational support for containment, eradication, and recovery, depending on the scope of the contracted service.

Some of the sectors in which it provides services include:

- Services sector.

- Finance.
- Healthcare.
- Energy.
- Public administration.

Its operation combines preventative, monitoring and response capabilities, with the aim of anticipating threats, improving early detection capabilities, containing incidents quickly and facilitating the recovery of affected activity in the shortest possible time.

- Greater real-time awareness of your cybersecurity situation.
- Prevent potential threats and reduce exposure to them.
- Identify incidents early and contain them quickly.
- Manage security incidents efficiently and minimize their impact.
- Restore operations as quickly as possible.

To achieve its objective, ALTIA-CSIRT offers a catalog of services, with highly qualified and experienced information security professionals trained to provide the services offered and thus detect, investigate, and respond appropriately to any security incident. We have the necessary and appropriate procedures and tools to provide the services offered.

We perform continuous monitoring, centralizing **visibility** of activity and potential threats across all of an organization's assets and services, significantly reducing the time to detect potential incidents and identifying which threats require immediate intervention and which are false positives.

We also carry out **proactive and preventative** tasks to improve our clients' security. We exchange technical information about incidents with other CSIRTs to improve our joint response.

It is important for an organization to have quality and compliance standards and ensure that they are followed in all its activities. To this end, ALTIA-CSIRT:

- We have the necessary policies and processes in place to ensure compliance with all applicable laws and regulations governing the services we provide.
- We apply recognized best practices in the industry, using RFC 2350 (Expectations for Computer Security Incident Response), available at https://datatracker.ietf.org/doc/html/rfc2350, as a reference for our structure and operations.

We comply with best practices (ISO 20000, ISO 27001 and ENS High Level) which are periodically audited by independent certifiers.

3.2 Constituency

ALTIA-CSIRT provides services to companies and public or private organizations that formalize the corresponding contract with ALTIA. The actual scope of services, assets covered, hours, support levels, coordination channels, and information exchange conditions will be defined in each applicable contractual relationship or agreement.

3.3 Authority

ALTIA-CSIRT is integrated into ALTIA's organizational structure and operates under the direction of the head of cybersecurity services. In carrying out its functions, the team is authorized to analyze incidents, coordinate response actions, issue technical recommendations, and operate contracted services within the applicable organizational, contractual, and regulatory framework.

3.4 Responsability

ALTIA-CSIRT is responsible for providing the incident detection, analysis, coordination, and response services included in its catalog and contracted by each client. Its services encompass, among other functions, the technical and operational management of the incident, issuing recommendations, coordinating with designated contacts, and supporting containment, eradication, and recovery activities.

Any actions involving changes to the client's assets, systems, or services will be carried out in accordance with the agreed-upon scope, the corresponding authorizations, and the procedures defined with each organization. ALTIA-CSIRT will also promote cybersecurity best practices and coordinated communication throughout the incident management process.

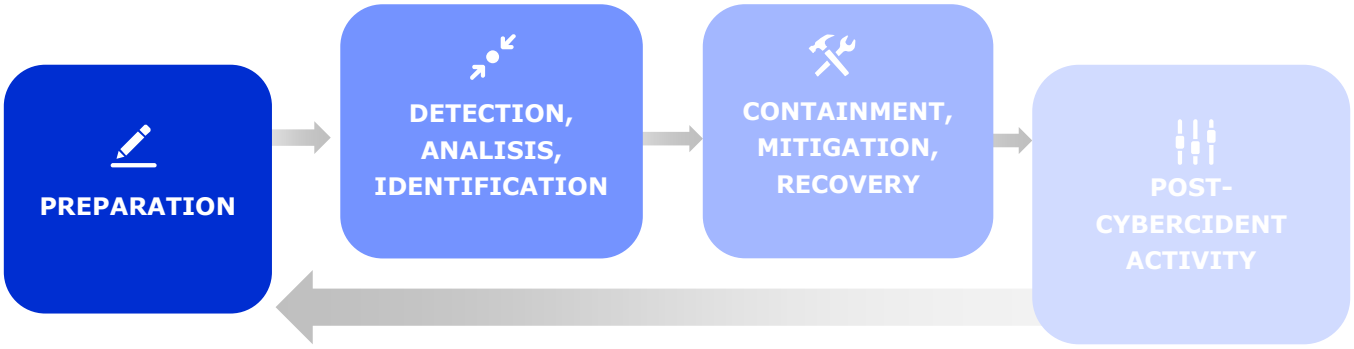
4 Policies

4.1 Type of incidents and level of support

ALTIA-CSIRT provides services for the detection, analysis, investigation, and response to security incidents and threats that may affect the information security dimensions of its clients' systems and processes: confidentiality, integrity, availability, authenticity, and traceability.

The security incidents it manages are based on the guidelines established by the Spanish National Cryptologic Center (CCN-CERT), following the *CCN-STIC-817 Cyber Incident Management Security Guide*, within the framework of the National Security Framework. These incidents are classified according to their type and severity, and response times are determined accordingly. Security incident preparedness consists of all tasks focused on establishing the foundation for having the capacity to respond appropriately to any security incident that may occur. Therefore, it is an initial phase that is independent of the occurrence of any security incident and is subject to a continuous improvement process that allows for maintaining optimized security incident response capabilities.

The cybersecurity incident management lifecycle will fundamentally follow these stages:



Cyber Incident Response Lifecycle

The level of support provided in each case will depend on the contractual agreement with each ALTIA CSIRT client.

The level of interaction during incident management, the channels to be used, the information that may or may not be shared with other parties such as other CSIRTs, and the level of protection to be applied will be defined in the contract with each client, or even at the time of incident detection if necessary, always respecting the laws and regulations governing these communications.

4.2 Cooperation, interaction and dissemination of information

ALTIA-CSIRT handles the information managed within the framework of its services according to the principles of need-to-know, confidentiality, and appropriate protection, in accordance with its internal policies, incident management procedures, and applicable contractual and regulatory obligations.

When necessary for the proper management of an incident, ALTIA-CSIRT may maintain cooperation and coordination mechanisms with other response teams, competent authorities, technology providers, or other relevant parties, always respecting applicable legal, contractual, and confidentiality restrictions.

Currently, ALTIA's CSIRT is a member of the Cybersecurity NODE that AMTEGA (Axencia para a Modernización Tecnolóxica de Galicia) has created within the Cybersecurity initiative of the Xunta de Galicia, is a member of the National Network of SOCs sponsored by the CCN-CERT (https://rns.ccn-cert.cni.es/) Gold category and is in the process of joining the Forum of Incident Response Teams and Security (FIRST, https://www.first.org/).

4.3 Communication and authentication

The available means of communication with ALTIA-CSIRT are as follows:Email encrypted with dedicated public keys.

- Website: https://soporte.altia.es

5 Services provided

The main services provided by ALTIA-CSIRT are summarized below. Each of these aligns with the functions and service areas defined within FIRST's CSIRT services framework[1].

- **Security event monitoring and correlation service (SIEM as a Service):** provides continuous monitoring, event correlation, anomaly detection, alert generation and contextual information to support early identification of security incidents.
  - In this service, a specialized operations team works on the continuous review and analysis of security alerts, relying on defined procedures, technical expertise, and threat intelligence sources to identify potential incidents, rule out false positives, confirm relevant events, and notify the client according to the agreed-upon protocol.
  - Additionally, a service for defining and adjusting use cases can be included, aimed at creating and maintaining specific correlation rules for detecting threats relevant to each environment.
    - FIRST CSIRT Framework- Service Area: Information Security Event Management: Monitoring and detection
    - FIRST CSIRT Framework- *Service* Area: Information Security Event Management: Event analysis
- **Incident Response Service:** This complements monitoring capabilities through detailed technical analysis and advanced investigation of cyber incidents. Depending on the situation, it may utilize forensic analysis, malware analysis, or other specialized techniques, and provides support for incident containment, eradication, recovery, and coordination.
  - FIRST CSIRT Framework- Service Area: Information Security Incident Management: Information security incident report acceptance
  - FIRST CSIRT Framework- Service Area: Information Security Incident Management: Information security incident analysis
  - FIRST CSIRT Framework- Service Area: Information Security Incident Management: Mitigation and recovery
  - FIRST CSIRT Framework- Service Area: Information Security Incident Management: Information security incident coordination

6 Incident Reporting Methods

Incident reporting can be done through:

- **Dedicated mailbox**: incidentes.ciber@altia.es
- **Ticketing tool**: Incident reporting tool[1] https://soporte.altia.es
- **Telephone numbers provided during the customer onboarding process** or in support of specific incidents.

[1] Accessible portal for ALTIA services customers.

7 Disclaimer

ALTIA-CSIRT takes reasonable measures to ensure the quality and accuracy of the information, notifications, alerts, and reports it issues as part of its services. However, this information is provided based on the data available at any given time and the concurrent operational context. Therefore, ALTIA-CSIRT assumes no responsibility for unintentional errors or omissions, nor for damages resulting from the misuse of the information contained in this document or provided as part of its services.

ALTIA

www.altiacompany.com

LinkedIn X YouTube Instagram

Technology for real growth