ALTIA

Technology for real growth

RFC2350

ALTIA | CSIRT

Fecha	Versión
04/06/2026	01

ÍNDICE

1 Información del documento

1.1 Objeto

Este documento tiene por objeto describir el marco de actuación del Equipo de Respuesta a Incidentes de Seguridad de ALTIA (en adelante, ALTIA-CSIRT), incluyendo su estructura organizativa, ámbito de actuación, responsabilidades, canales de contacto y servicios prestados.

1.2 Lista de distribución para notificaciones

Los cambios a este documento no se distribuyen por una lista de correo. Cualquier pregunta o comentario específico, por favor diríjase a la dirección de correo ciberseguridad@altia.es

1.3 Ubicación del documento

La última versión del documento se encuentra publicada en:

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

2 Información de contacto

2.1 Datos de identificación

- Nombre del Equipo: ALTIA-CSIRT
- Dirección:
  - Campus Universitario de Vigo. Lagoas
  - Marcosende, 32. 36310 Vigo
- Zona horaria: CET / CEST
- Número de Teléfono: +34 986 90 23 00.
- Número de Fax: No existente
- Otras Comunicaciones: No existente
- Direcciones de Correo Electrónico:
  - Intercambio de información relativa a incidentes: incidentes.ciber@altia.es
  - Consultas de carácter general: ciberseguridad@altia.es
  - Información adicional sobre el servicio y canales de contacto: https://www.altiacompany.com/es/servicios/cybersecurity-solutions
- Claves Públicas y cifrado de información:

  ALTIA-CSIRT utiliza la dirección incidentes.ciber@altia.es para comunicaciones relacionadas con la respuesta a incidentes de seguridad cibernética.

  Esta dirección está protegida con la clave PGP: B22C AB5B B719 E3C4 BE98 2817 B038 5792 749D 5767.

  Para comunicaciones administrativas o consultas, se utiliza la dirección ciberseguridad@altia.es protegida con la clave PGP: 12CC 535A 21A5 2DFC 87C1 E934 CADE 6CE0 1FA6 7757.

Las claves GPG/PGP se pueden descargar de https://www.altiacompany.com/es/servicios/cybersecurity-solutions (sección "Información de contacto"). A mayores, las claves GPG/PGP están disponibles en el servidor de claves de RedIRIS y pueden encontrarse en el anillo público mediante búsqueda en https://pgp.rediris.es/.

2.2 El equipo

El equipo se encuentra constituido por personal desempeñando los siguientes perfiles:

- **Analistas de alertas de seguridad de la información (Nivel 1)**
- **Especialistas en respuesta a incidentes de seguridad (Nivel 2)**
- **Expertos en ámbitos específicos de la seguridad de la información (Nivel 3).**
- **CSIRT Manager**
- **Security**
- **Manager**

- **Horario de Atención:** El equipo de respuesta a incidentes está disponible en los siguientes horarios:
  - Consultas sobre servicios: Horario de oficina (8.00h-18.30h)
  - Incidentes: horario extendido (24x7x365).

- **Puntos de contacto para la comunidad**: ALTIA-CSIRT se comunica principalmente con las organizaciones a las que presta servicio a través de los siguientes medios:
  - Herramienta de *ticketing*.
  - Correo electrónico de soporte.
  - Teléfono de contacto habilitado para la coordinación operativa.

3 Constitución

ALTIA-CSIRT es el equipo especializado de ALTIA para la gestión y respuesta ante incidentes de ciberseguridad, integrado en la unidad de Ciberseguridad de la compañía. Su creación responde a la necesidad de proporcionar una capacidad organizada, especializada y trazable para la detección, análisis, coordinación y respuesta ante incidentes que puedan afectar a los activos, servicios y operaciones de sus clientes.

El equipo desarrolla su actividad en un contexto marcado por la creciente exposición de las organizaciones a amenazas cibernéticas, la complejidad de los entornos tecnológicos y la necesidad de garantizar la continuidad, disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad de la información y de los servicios prestados.

Para ello, ALTIA-CSIRT cuenta con capacidades técnicas, procedimientos de actuación y personal especializado que permiten abordar el ciclo completo de gestión de incidentes, desde la preparación y detección hasta la contención, erradicación, recuperación y coordinación con terceros cuando resulte necesario.

Asimismo, el equipo opera teniendo en cuenta las obligaciones contractuales, regulatorias y normativas aplicables en cada caso, incluyendo, cuando corresponda, los requisitos de notificación, coordinación y tratamiento de la información asociados a la gestión de incidentes de seguridad.

ALTIA-CSIRT presta servicio a entidades públicas y privadas que contratan capacidades de monitorización, detección y respuesta ante incidentes, con un enfoque orientado a reducir el impacto operativo y de seguridad derivado de amenazas y ciberincidentes.

Su actividad se apoya en personal cualificado, herramientas especializadas y procedimientos definidos para proporcionar una respuesta consistente, coordinada y adecuada a las necesidades de cada cliente y al marco de servicio contratado.

3.1 Misión

ALTIA-CSIRT tiene como misión contribuir a la reducción de la probabilidad y el impacto de los incidentes de seguridad que afecten a los sistemas, servicios y activos de información de sus clientes.

Para ello, proporciona capacidades de detección, análisis, coordinación y respuesta ante incidentes, así como apoyo técnico y operativo para la contención, erradicación y recuperación, en función del alcance del servicio contratado.

Algunos de los sectores en los que presta servicios son:

- Sector servicios.
- Finanzas.
- Salud.
- Energía.
- Administraciones públicas.

Su actuación combina capacidades preventivas, de monitorización y de respuesta, con el objetivo de anticipar amenazas, mejorar la capacidad de detección temprana, contener incidentes con rapidez y favorecer la recuperación de la actividad afectada en el menor plazo posible.

- Mayor conocimiento en tiempo real de su situación de seguridad cibernética.
- Prevenir posibles amenazas y reducir la exposición a ellas.
- Identificar incidentes de manera temprana y contenerlos rápidamente.
- Gestionar eficientemente los incidentes de seguridad y minimizar su impacto.
- Recuperar la actividad en el menor plazo posible.

Para lograr su objetivo, el ALTIA-CSIRT ofrece un catálogo de servicios, con profesionales altamente cualificados y con experiencia en seguridad de la información, que están capacitados para brindar los servicios ofrecidos y así, detectar, investigar y responder a cualquier incidente de seguridad de manera adecuada. Tenemos los procedimientos y herramientas necesarios y adecuados para brindar los servicios ofrecidos.

Realizamos una monitorización continua, centralizando la **visibilidad** de la actividad y las posibles amenazas de todos los activos o servicios de una organización, reduciendo significativamente el tiempo de detección de posibles incidentes e identificando qué amenazas requieren intervención inmediata y cuáles son falsos positivos.

También realizamos tareas **proactivas y preventivas** para mejorar la seguridad de nuestros clientes. Intercambiamos información técnica sobre incidentes con otros CSIRTs para mejorar la respuesta conjunta ante ellos.

Es importante que una organización tenga estándares de calidad y cumplimiento y se asegure de seguirlos en todas sus actividades. Para ello, el ALTIA-CSIRT:

- Disponemos de políticas y procesos necesarios para garantizar que se cumpla con las leyes y regulaciones aplicables a los servicios prestados.

- Aplicamos las mejores prácticas reconocidas en el sector, tomando como referencia para su constitución y operativa, siguiendo las directrices de la RFC2350 (Expectativas para la respuesta a incidentes de seguridad informática), disponible en https://datatracker.ietf.org/doc/html/rfc2350.

Cumplimos con las mejores prácticas (ISO 20.000, ISO 27.001 y ENS Nivel Alto) que auditan periódicamente certificadores independientes.

3.2 Circunscripción

ALTIA-CSIRT presta servicios a empresas y organismos públicos o privados que formalicen la contratación correspondiente con ALTIA. El alcance efectivo de los servicios, activos cubiertos, horarios, niveles de soporte, canales de coordinación y condiciones de intercambio de información se definirá en cada relación contractual o acuerdo aplicable.

3.3 Autoridad

ALTIA-CSIRT se integra en la estructura organizativa de ALTIA y actúa bajo la dirección del responsable de los servicios de ciberseguridad. En el ejercicio de sus funciones, el equipo está facultado para analizar incidentes, coordinar actuaciones de respuesta, emitir recomendaciones técnicas y operar los servicios contratados dentro del marco organizativo, contractual y normativo aplicable.

3.4 Responsabilidad

ALTIA-CSIRT es responsable de la prestación de los servicios de detección, análisis, coordinación y respuesta ante incidentes incluidos en su catálogo y contratados por cada cliente. Su actuación comprende, entre otras funciones, la gestión técnica y operativa del incidente, la emisión de recomendaciones, la coordinación con los interlocutores designados y el apoyo a las actividades de contención, erradicación y recuperación.

Las actuaciones que impliquen cambios sobre activos, sistemas o servicios del cliente se realizarán conforme al alcance acordado, a las autorizaciones correspondientes y a los procedimientos definidos con cada organización. ALTIA-CSIRT promoverá, además, buenas prácticas de ciberseguridad y una comunicación coordinada durante la gestión de incidentes.

4 Políticas

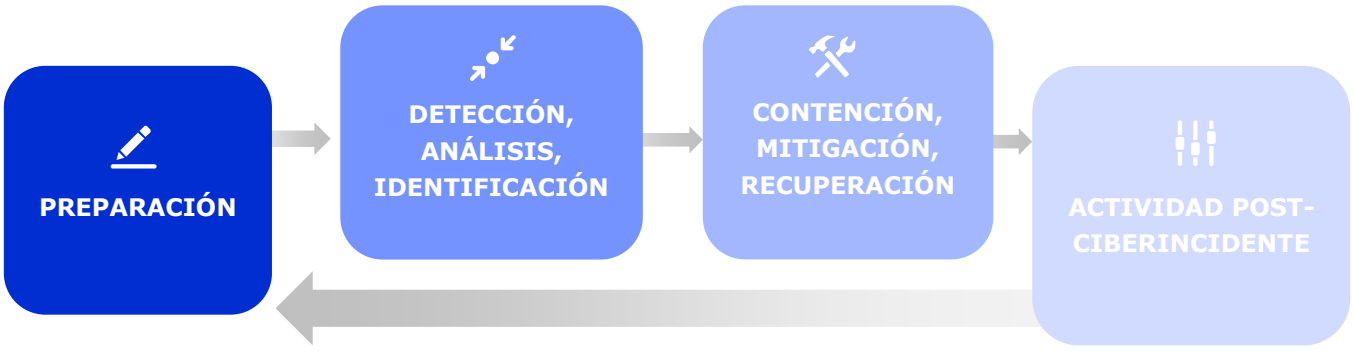
4.1 Tipo de incidentes y nivel de soporte

ALTIA-CSIRT presta servicios de detección, análisis, investigación y respuesta ante incidentes y amenazas de seguridad que puedan afectar a las dimensiones de seguridad de la información de los sistemas y procesos de sus clientes: confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad.

Los incidentes de seguridad que gestiona se basan en las pautas establecidas por el Centro Criptológico Nacional de España (CCN-CERT), siguiendo la Guía de *Seguridad de las CCN-STIC-817 Gestión de Ciberincidentes*, en el ámbito del Esquema Nacional de Seguridad. Estos incidentes se clasifican de acuerdo a su tipología y gravedad, y se determinan los plazos de respuesta en consecuencia.

La preparación para el tratamiento de incidentes de seguridad consta de todas aquellas tareas enfocadas a sentar las bases para disponer de la capacidad de responder adecuadamente a cualquier incidente de seguridad que se pueda producir. Por tanto, es una fase inicial que es independiente de la ocurrencia de cualquier incidente de seguridad, y que está sometida a un proceso de mejora continua que permita mantener optimizadas las capacidades de respuesta ante incidentes de seguridad.

El ciclo de vida de la gestión de incidentes de ciberseguridad seguirá fundamentalmente las siguientes etapas:



Ciclo de vida de la Respuesta a Ciberincidentes

El nivel de apoyo brindado en cada caso dependerá de lo acordado contractualmente con cada cliente del CSIRT de ALTIA.

El nivel de interacción durante el manejo del incidente, los canales a utilizar, la información que puede o no ser compartida con otros actores como otros CSIRTs, y el nivel de protección que debe ser aplicado se definirán en el contrato con cada cliente, o incluso en el momento de la detección del incidente si es necesario, siempre respetando las leyes y normativas que regulen estas comunicaciones.

4.2 Cooperación, interacción y divulgación de la información

ALTIA-CSIRT trata la información gestionada en el marco de sus servicios con criterios de necesidad de conocer, confidencialidad y protección adecuada, de acuerdo con sus políticas internas, los procedimientos de gestión de incidentes y las obligaciones contractuales y normativas aplicables.

Cuando resulte necesario para la correcta gestión de un incidente, ALTIA-CSIRT podrá mantener mecanismos de cooperación y coordinación con otros equipos de respuesta, organismos competentes, proveedores tecnológicos u otras partes relevantes, respetando en todo caso las restricciones legales, contractuales y de confidencialidad aplicables.

En la actualidad el CSIRT de ALTIA es miembro del NODO de Ciberseguridad que la AMTEGA (Axencia para a Modernización Tecnolóxica de Galicia) ha creado dentro de la iniciativa de Ciberseguridad de la Xunta de Galicia, es miembro de la Red Nacional de SOCs auspiciada por el CCN-CERT (https://rns.ccn-cert.cni.es/) categoría Gold y, está en proceso de adhesión al Foro de Equipos de Respuesta a Incidentes y Seguridad (FIRST, https://www.first.org/).

4.3 Comunicación y autenticación

Los medios disponibles para la comunicación con ALTIA-CSIRT son los siguientes:

- Correo electrónico cifrado con las claves públicas dedicadas para ello.
- Portal web: https://soporte.altia.es

5 Servicios proporcionados

A continuación, se describen de forma resumida los principales servicios prestados por ALTIA-CSIRT. Cada uno de ellos se alinea con funciones y áreas de servicio recogidas en el marco de servicios CSIRT de FIRST[1].

- **Servicio de monitorización y correlación de eventos de seguridad (SIEM as a Service):** proporciona supervisión continua, correlación de eventos, detección de anomalías, generación de alertas e información de contexto para apoyar la identificación temprana de incidentes de seguridad.
  - En este servicio, un equipo operativo especializado trabaja en la revisión y análisis continuos de alertas de seguridad, apoyándose en procedimientos definidos, experiencia técnica y fuentes de inteligencia de amenazas para identificar posibles incidentes, descartar falsos positivos, confirmar eventos relevantes y notificar al cliente conforme al protocolo acordado.
  - Adicionalmente, puede incluirse un servicio de definición y ajuste de **casos de uso**, orientado a crear y mantener reglas de correlación específicas para la detección de amenazas relevantes para cada entorno.
    - FIRST CSIRT Framework- Service Area: Information Security Event Management: Monitoring and detection
    - FIRST CSIRT Framework- *Service* Area: Information Security Event Management: Event analysis
- **Servicio de respuesta ante incidentes:** complementa las capacidades de monitorización mediante el análisis técnico detallado y la investigación avanzada de ciberincidentes. En función del caso, puede apoyarse en análisis forense, análisis de malware u otras técnicas especializadas, y proporciona apoyo para la contención, erradicación, recuperación y coordinación del incidente.
  - 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 Formas de notificación de incidentes

La notificación de incidentes puede realizarse mediante:

- **Buzón de correo específico**: incidentes.ciber@altia.es
- **Herramienta de ticketing**: Herramienta de notificación de incidentes[1] https://soporte.altia.es
- **Teléfonos proporcionados durante el proceso de adhesión de clientes** o en el apoyo a incidentes específicos.

[1] Portal accesible para clientes de los servicios de ALTIA.

7 Descargo de responsabilidad

ALTIA-CSIRT adopta medidas razonables para asegurar la calidad y exactitud de la información, notificaciones, alertas e informes que emite en el marco de sus servicios. No obstante, dicha información se facilita con base en los datos disponibles en cada momento y en el contexto operativo concurrente, por lo que ALTIA-CSIRT no asume responsabilidad por errores u omisiones no intencionados ni por los daños derivados del uso indebido de la información contenida en este documento o suministrada como parte de sus servicios.

ALTIA

www.altiacompany.com

LinkedIn X YouTube Instagram

Technology for real growth