RFC2350

Altia | CSIRT

30/10/2024

ÍNDICE

1 Información del documento

1.1 Objeto

Este documento tiene como propósito describir el entorno en el que el Equipo de Respuesta a Incidentes de Seguridad Informática de Altia (en adelante denominado Altia-CSIRT) lleva a cabo sus actividades donde se destacará la estructura organizativa y los marcos institucionales del equipo Altia-CSIRT, así como la composición del equipo, sus objetivos y los servicios que ofrecen.

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.altia.es/es/cybersecurity-solutions/rfc2350.html
- Inglés: https://www.altia.es/en/cybersecurity-solutions/rfc2350.html

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
  - Otras direcciones de correo electrónico para contactar con el Altia: https://www.altia.es/es/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.altia.es/es/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:** El equipo de Altia-CSIRT se comunica principalmente con las organizaciones a las que brinda soporte a través de los siguientes medios:
  - Herramienta de *ticketing*.
  - Correo electrónico de soporte.
  - Teléfono de contacto directo.
  - Teléfono de contacto.

3 Constitución

En Altia llevamos revolucionando la tecnología desde hace casi 30 años (1994). Contamos con un crecimiento continuo gracias a una amplia propuesta de servicios, productos y enfoque **end-to-end**, combinados con la calidad, la pasión por la innovación y el compromiso como partner tecnológico de nuestros clientes. Creando valor, reimaginando todo.

Somos conscientes de que en los tiempos actuales las empresas se enfrentan a desafíos cada vez más complejos, incluyendo la necesidad de **digitalizar** cada vez más los procesos empresariales y adaptarse a las demandas de flexibilidad y disponibilidad de sus **usuarios** en cuanto al consumo de aplicaciones y servicios. Esto ha llevado a la eliminación del perímetro tradicional y a un aumento en la exposición a ataques, lo que requiere una atención especial a la seguridad.

La realidad actual de las organizaciones incluye el hecho de que los métodos y **ataques** utilizados son cada vez más complejos, automatizados y variados, lo que significa que los atacantes están cada vez más especializados y todos estamos más expuestos al cibercrimen. Al mismo tiempo, también existen dispositivos y soluciones de seguridad cada vez más avanzadas y diversas disponibles para protegerse contra estos ataques.

Además, es necesario cumplir con ciertas **obligaciones legales** en función del sector en el que se trabaje, como notificar incidentes o contar con un equipo de respuesta a incidentes de seguridad cibernética (CSIRT).

El CSIRT de Altia (en adelante “Altia-CSIRT”) está dentro de la unidad de Ciberseguridad de Altia; unidad que tiene como objetivo principal mejorar continuamente la ciberseguridad de nuestros clientes, desarrollando una amplia gama de servicios de seguridad de la información y ciberseguridad de manera integral y proactiva.

Con el objetivo de que nuestros clientes se sientan más seguros, desde Altia Ciberseguidad ayudamos a proteger la información clasificada y sensible, formamos a personal especializado, definimos e implementamos políticas y procedimientos de seguridad y, desarrollamos las tecnologías más adecuadas para este propósito.

3.1 Misión

El Altia-CSIRT tiene la misión de reducir la probabilidad y gravedad de los incidentes de seguridad que afectan a sus clientes, comprometiendo significativamente la seguridad y resiliencia de sus servicios de información e informaciones.

Lo hacemos proporcionando las herramientas y servicios necesarios para coordinar y responder de manera rápida y eficiente a las amenazas cibernéticas, en diferentes sectores en el territorio nacional e internacional.

Algunos de los sectores en los que presta servicios son:

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

Nuestro objetivo es mejorar nuestra ciberseguridad y la de nuestros clientes. Para lograrlo, empezamos por la prevención; buscamos **anticiparnos** a posibles amenazas y **reducir** la superficie de ataque. Continuamos tratando de **detectar** de forma temprana los incidentes y **contenerlos** rápidamente para **minimizar** su impacto. También nos esforzamos por **responder** eficazmente a cualquier incidente de seguridad y **recuperar** la actividad lo antes 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 ofrece servicios a empresas y organismos externos, ya sean públicos o privados, que decidan contratar sus servicios a Altia.

3.3 Autoridad

El Altia-CSIRT se encuentra dentro del Grupo Altia, bajo la autoridad del Gerente Proyectos y Servicios de Ciberseguridad (CSIRT Manager).

3.4 Responsabilidad

Nuestro equipo trabaja para mejorar la seguridad de la información de nuestros clientes y la ciberseguridad en general. Ofrecemos recomendaciones y avisos técnicos y operativos, así como servicios de modelado de amenazas, creación de casos de uso y gestión de los registros de información de seguridad a nuestros clientes.

Además, promovemos la cultura de ciberseguridad en todo lo que hacemos y comunicamos.

4 Políticas

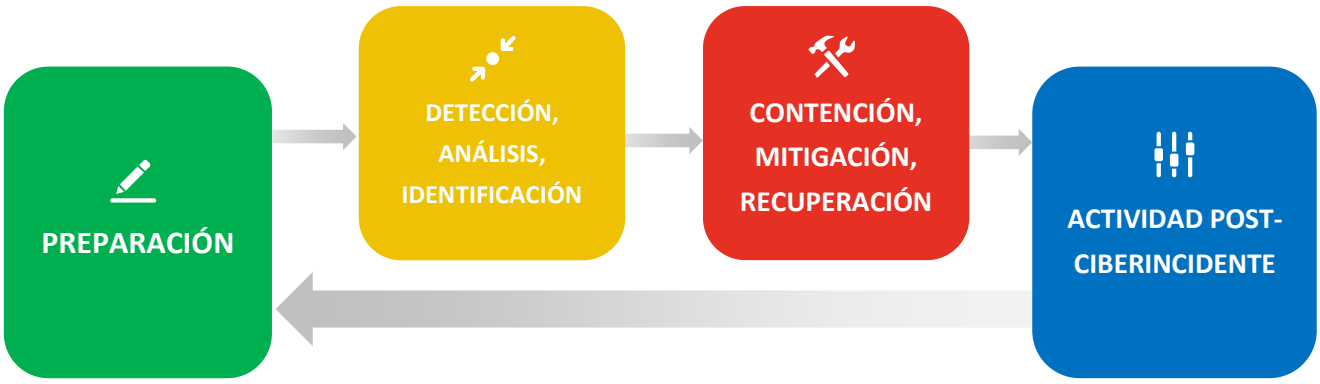
4.1 Tipo de Incidentes y nivel de soporte

El Altia-CSIRT presta el servicio de detectar, investigar y responder a amenazas de seguridad (TDIR) que puedan afectar a las dimensiones de la seguridad de la información (integridad, disponibilidad y confidencialidad, complementadas con autenticidad y trazabilidad) manejada por los sistemas y procesos de sus clientes.

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

El Altia-CSIRT trata la información con la máxima confidencialidad de acuerdo a sus políticas y procedimientos de gestión de incidentes, las políticas y normas internas y las normas de seguridad para proteger la información clasificada.

Es importante establecer acuerdos formales de colaboración con otros grupos de respuesta a incidentes y seguridad (CSIRTs).

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:

- Correo electrónico cifrado con las claves públicas dedicadas para ello.
- Portal web: https://soporte.altia.es
- Teléfonos proporcionados durante el proceso de adhesión o el apoyo a incidentes.

5 Servicios proporcionados

A continuación, detallaremos un poco más los servicios ofrecidos por Altia-CSIRT. Cada uno de los servicios están asociados a un servicio o función específica dentro del marco de servicios del FIRST[1]:

- **Security Event Monitoring and Correlation Service (SIEM as a Service):** proporcionamos supervisión en tiempo real, correlación de eventos, informes avanzados de alarmas detectadas y vistas personalizadas del estado de seguridad de los activos.
    - En el servicio de monitorización y correlación de eventos, ponemos a disposición un equipo operativo de técnicos que trabajan 24x7 en el análisis de potenciales análisis de potenciales incidentes y, apoyándose en su experiencia y conocimientos especializados y herramientas de inteligencia de ciberamenazas, llevando a cabo la actividad de detección de incidentes, descarte de detección de falsos incidentes, eliminación de falsos positivos, confirmación del incidente y notificación al cliente (en base a un protocolo previamente definido).

      Adicionalmente se incluye el servicio **"Use cases"** que permite crear reglas de correlación específicas para detectar posibles amenazas.
        - 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:** se añade a los dos servicios anteriores, un análisis detallado y una investigación avanzada de los ciberincidentes. Este análisis puede apoyarse en análisis de malware y/o forenses y, por lo general, ofrecerá una propuesta de resolución para su rápida contención o, en ocasiones, incluso una solución definitiva.
    - 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

[1] Ver FIRST CSIRT Services Framework versión 2.1 disponible en https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

- 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 [2] https://soporte.altia.es
- **Teléfonos proporcionados durante el proceso de adhesión de clientes** o en el apoyo a incidentes específicos.

[2] Portal accesible para clientes de los servicios de Altia.

7 Descargo de responsabilidad

El Equipo del Altia-CSIRT toma todas las precauciones en la preparación de información, notificaciones, alertas e informes, pero no asume ninguna responsabilidad por errores u omisiones, ni por daños resultantes del uso mal de la información contenida en este documento ni suministrada como parte de sus servicios.

altia.es