Catalogo de servicios AndalucíaCERT

sedian Seguridad Digital de Andalucía

AndalucíaCERT

Misión

AndalucíaCERT es el instrumento de referencia para la **prevención, detección y respuesta a incidentes** y amenazas de seguridad digital en el ámbito de Andalucía.

Objetivos

1. Proporcionar la capacidad de detección y respuesta eficaz y coordinada ante incidentes de ciberseguridad a su grupo atendido
2. Asesorar a los organismos del grupo atendido sobre dudas y buenas prácticas en protección, detección y respuest
3. Establecer un modelo evolutivo a partir de la adaptación continua y ampliación de servicios para hacer frente a las amenazas cambiantes y nuevas necesidades del grupo atendido

Visión

Impulsar, junto con otras iniciativas de la ADA, un clima de confianza y seguridad que contribuya al **desarrollo de la economía y la sociedad digital enAndalucía**, así como el disponer de un ciberespacio abierto, seguro y protegido.

sedian Seguridad Digital de Andalucía

Servicios AndalucíaCERT

Servicios preventivos

Servicios enfocados a:

- **Fortalecimiento** de la infraestructura IT de los organismos
- Descubrimiento de **vulnerabilidades** y seguimiento del ciclo de vida de la remediación.
- Identificación de amenazas activas de forma **temprana**.

Servicios detectivos

Servicios enfocados a:

- Análisis de datos para la **identificación** de ataques.
- Obtención de información avanzada de los **atacantes**.
- Definición de **patrones** de actividad maliciosa.
- Defensa activa de los equipos finales de usuario.

Servicios reactivos

Servicios enfocados a:

- Definición de estrategias de **contención** ante incidentes.
- **Coordinación** de los esfuerzos del organismo con prestadores de servicios IT.
- Análisis avanzado de **amenazas**.
- **Entrenamiento** especializado en situaciones de crisis.

Servicios AndalucíaCERT

Servicios preventivos

- Escaneo de vulnerabilidades
- Auditoria de sistemas
- Seguimiento del ciclo de vida de vulnerabilidades
- Avisos de seguridad (Sistema de Alerta Temprana)
- Consulta en la configuración y despliegue de herramientas de forma segura
- Ciberejercicios y cibersimulaciones

Servicios detectivos

- Monitorización de eventos de seguridad
- Threat Hunting
- Threat Intelligence
- Spamtraps
- Honeypots
- Protección equipo final

Servicios reactivos

- Gestión de incidentes
- Análisis de malware
- Análisis forense

s

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Escaneo de vulnerabilidades

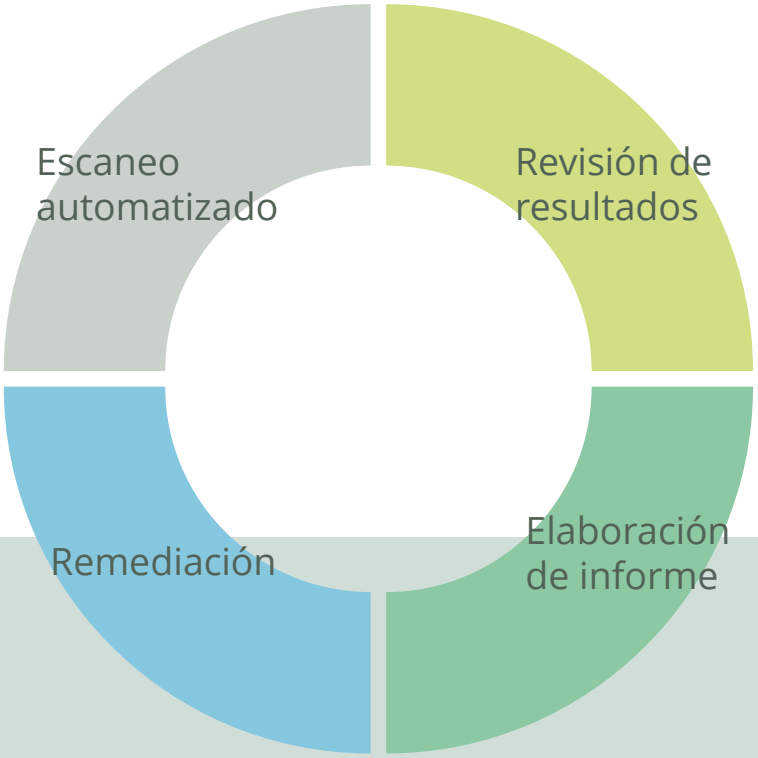
Tiene por finalidad la identificación de vulnerabilidades en aplicaciones publicadas en los organismos a través de un escaneo periódico desde la infraestructura de AndalucíaCERT.

El proceso se realiza en función de las necesidades del organismo, que determina en el momento de la solicitud si requiere un escaneo **puntual** o **periódico**.

El servicio parte de las **herramientas automáticas** de análisis de AndalucíaCERT y se enriquece con la **revisión de un experto** del Centro antes de remitir el entregable.

El organismo recibe un correo electrónico con **resumen de resultados**, un **informe de resultados ejecutivo** y un **informe de resultados técnico** para cada servicio escaneado, así como las recomendaciones de remediación aplicables.

El servicio puede ser solicitado a través de un **formulario firmado** por cada servicio a escanear. Dicho formulario debe ser remitido a AndalucíaCERT a través de correo electrónico.



sedian Seguridad Digital de Andalucía

Requiere suscripción

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Auditoria de sistemas

Tiene como objetivo **identificar, enumerar y describir** las diversas **vulnerabilidades** que pudieran presentarse en un determinado servicio de los organismos del grupo atendido.

La auditoria se realiza a medida y bajo petición del organismo que la solicite y puede ser de diferentes **tipos:**

Identifica aspectos vulnerables de servicios publicados.

Utiliza técnicas de hacking para buscar una intrusión.

Identifica vulnerabilidades en el código fuente de una aplicación.

El organismo que realiza la petición recibe un **informe de auditoria** en función del tipo de auditoria solicitado.

El servicio puede ser solicitado a través de los responsables del propio servicio o a la dirección de **correo electrónico** de AndalucíaCERT. Su ejecución debe ser objeto de aprobación por la USTIC-C.

sedian Seguridad Digital de Andalucía

Requiere suscripción

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Seguimiento del ciclo de vida de vulnerabilidades

Este servicio persigue incrementar la capacidad de **vigilancia** y simplificar al organismo la gestión de la **superficie de exposición** a las diferentes vulnerabilidades identificadas.

El servicio se apoya en la publicación de una instancia de **ANA** (herramienta para la Automatización y Normalización de Auditorías del CCN-CERT) para el seguimiento de vulnerabilidades.

El organismo solicitante cuenta con un perfil disponible en la instancia de ANA para la **explotación y seguimiento de vulnerabilidades** de manera autónoma.

El organismo puede albergar las vulnerabilidades identificadas por sus medios, mientras que AndalucíaCERT se encargará de almacenar todas aquellas vulnerabilidades obtenidas del organismo a través de **otros servicios proactivos**.

El servicio puede ser solicitado a través del **correo electrónico** de AndalucíaCERT o de forma directa a través de los responsables del Centro.

sedian Seguridad Digital de Andalucía

Requiere suscripción

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Avisos de seguridad (Sistema de Alerta Temprana)

El servicio pretende dar a conocer dentro del grupo atendido de AndalucíaCERT novedades relevantes para la protección de éstos, con especial relevancia en el entorno de **amenazas y vulnerabilidades** aplicables.

El equipo de expertos de AndalucíaCERT realiza un **análisis diario** de la información publicada en las más relevantes fuentes de información, extrayendo aquella que sea de aplicación y genere valor para el grupo atendido.

A partir de la información filtrada y contrastada, y se llevan a cabo publicaciones y envíos con un contenido **elaborado a medida** para los organismos del grupo atendido.

Los avisos de seguridad se realizan mediante publicación en **web,** listas de distribución de **correo electrónico** y publicaciones en la red social **Twitter** .

sedian Seguridad Digital de Andalucía

Servicio base

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Consulta en la configuración y despliegue de herramientas de forma segura

AndalucíaCERT como centro de referencia en Andalucía en cuanto a la **prevención, detección y respuesta** a incidentes y amenazas de **seguridad** dispone de un servicio de tratamiento de consultas y asesoramiento experto en cuanto a la ciberseguridad para su grupo atendido.

Particularmente se ofrece resolución de consultas en materia de:

- Seguridad en **la configuración y despliegue de herramientas**, sin llegar a suplir el soporte que pueda dar el integrador o fabricante.
- **Indicadores de compromiso** de amenazas.
- **Medidas de protección genéricas** frente a malware.
- **Información sobre los servicios** de AndalucíaCERT.
- **Información sobre herramientas** y servicios del CCN-CERT.

El servicio puede ser solicitado a través del **correo electrónico** para cuestiones generales del CERT.

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Ciberjercicios y cibersimulaciones

El propósito de la ejecución de ciberejercicios es aumentar el nivel de madurez de los organismos en términos de **eficacia y eficiencia** ante la existencia de un ciberincidente.

Los ciberejercicios son el único método efectivo que permite poner a prueba la capacidad de respuesta en un entorno controlado.

Roleplay

- Persigue entrenar y evaluar la **toma de decisiones** por parte del comité de crisis ante la existencia de un incidente de alta prioridad.
- Se basa en casos reales de grandes incidentes.

Dada su planificación y diseño se controla con detalle el impacto en la organización y loas aspectos a ser medidos.

Simulación

- Persigue entrenar y evaluar la **capacidad técnica** de análisis de un ciberincidente.
- Se basa en la determinación de un entorno comprometido hasta la formulación del análisis de acciones del atacante.

La participación en ciberejercicios se puede formular a través del **envío de solicitud** a por correo electrónico.

Requiere suscripción

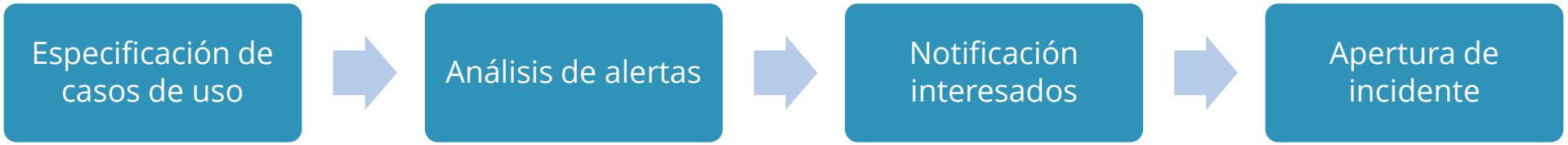
Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Monitorización de eventos de seguridad

Este servicio consiste en la **identificación de actividad maliciosa** a través de la aplicación de un conjunto de reglas de correlación y casos de uso a los eventos de actividad enviados por determinados dispositivos de los organismos al servidor central de correlación de AndalucíaCERT.

Habitualmente estos sistemas son **dispositivos perimetrales** como cortafuegos o sistemas de prevención y detección de intrusiones como elementos de red, que concentran información relevante de la actividad en una organización.



Los casos de uso elaborados se alinean con las técnicas y tácticas utilizadas por los atacantes, lo que permite identificar su presencia a través de **patrones de comportamiento**.

El análisis de alertas llevado a cabo por los expertos de AndalucíaCERT **verifica la existencia de un incidente** de forma manual, lo que genera una **notificación a los interesados** a través de los medios disponibles y mueve el caso al servicio especializado de Gestión de Incidentes.

El servicio puede ser solicitado mediante **formulario de adhesión** firmado y remitido por correo electrónico.

sedian Seguridad Digital de Andalucía

Servicio base

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Threat Hunting

Este servicio consiste en la adquisición, procesamiento y análisis de tráfico y datos, de forma continua para **detectar anomalías, usos indebidos y amenazas persistentes avanzadas**.

</carmen>
ccn-cert

Permite **detectar** mecanismos de **infección** y descubrir amenazas en la fase de persistencia gracias a la identificación de **movimientos externos y laterales**.

El objetivo se consigue a través del análisis de grandes volúmenes de información y la aplicación de procedimientos especializados para identificación de amenazas.

En caso de identificar una amenaza presente en la organización se lleva a cabo la **notificación** a los interesados y se traslada el caso al servicio especializado de **Gestión de Incidentes** para su tratamiento.

Este servicio se presta para todos aquellos organismos suscritos al servicio de **monitorización de eventos de seguridad.**

sedian Seguridad Digital de Andalucía

Servicio base

Servicios AndalucíaCERT

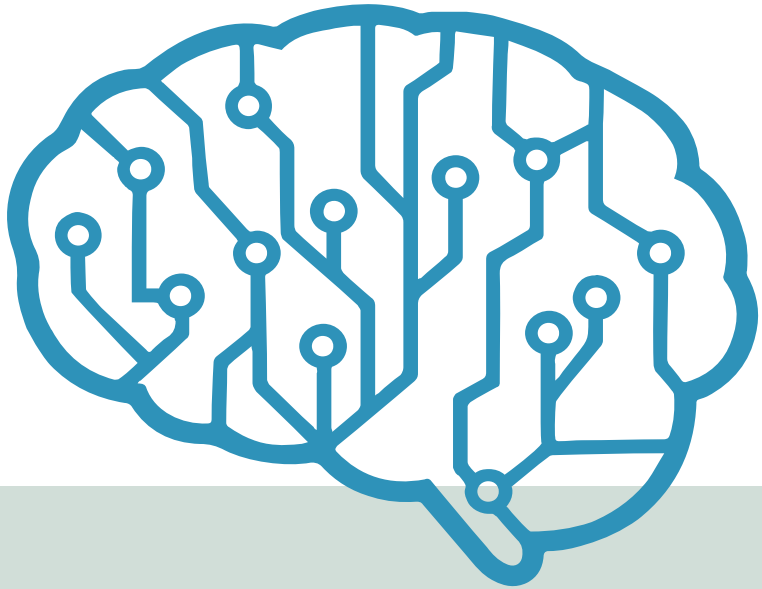
Servicios preventivos | Servicios detectivos | Servicios reactivos

Threat Intelligence

El objetivo de este servicio consiste en la **recopilación y correlación de indicadores de compromiso** sobre amenazas, artefactos y los actores que las operan, para su compartición con el grupo atendido y que puedan ser utilizadas en los procesos de protección y detección.

El servicio de threat intelligence recopila información accionable para su empleo por parte de los organismos, destacando:

- Hash: identificador único de muestras de malware
- URL: indicador de direcciones utilizadas por atacantes
- Filename: referencia a nombres utilizados por malware
- Subject: asunto de correos electrónicos con finalidad maliciosa
- IP: dirección empleada para desencadenar el ataque o para ejercer de Command & Control



Además de la compartición de IOCs para su utilización como **listas negras** se elaboran y comparten **reglas SNORT** para IDS.

El servicio puede ser solicitado mediante **formulario de solicitud firmado** y remitido por correo electrónico

Requiere suscripción

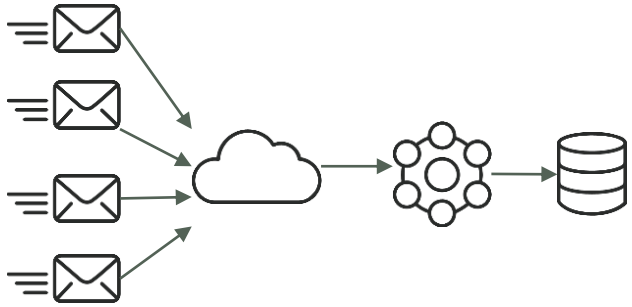
Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Spamtraps

El servicio se encarga de **detectar de forma temprana** campañas de spam a través de cuentas trampa de los organismos que son difundidas en diferentes sitios públicos de internet (foros, blogs, etcs...) donde serán indexados por bots y/o arañas.

La agregación de alertas ofrece una visión global de la evolución, comportamiento, tácticas y técnicas utilizadas a lo largo del tiempo por los atacantes.



Para la integración en el servicio únicamente es necesario facilitar **una o varias direcciones de correo** electrónico con antispam deshabilitado. Una vez creadas las cuentas, se informará a AndalucíaCERT y se **redireccionará** todo el correo entrante a la cuenta que se indique.

La detección temprana de campañas maliciosas (phishing, malware, etc..) que se produzca por AndalucíaCERT generará una **notificación al organismo** con los detalles de la campaña. Asimismo se generará un **informe de volumetrías** en las cuentas del organismo que será remitido mensualmente.

La información proporcionada permite la **creación de reglas**, aplicadas al conjunto de datos enriquecidos y analizados para la generación de alertas personalizadas.

sedian Seguridad Digital de Andalucía

Requiere suscripción

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Honeypots

La creación de servicios simulados dentro de la red interna de un organismo es una forma muy efectiva de **atraer y detectar atacantes** presentes en la red interna. AndalucíaCERT pone a disposición las herramientas que permiten la creación de estos servicios trampa y lleva a cabo el análisis de las alertas que producen.

Se ofrece una **imagen virtualizada** pre-empaquetada que debe ser desplegada en un entorno compatible dentro de la red interna de la entidad. Los eventos generados se procesan en AndalucíaCERT para la generación de alertas y su posterior análisis. Los casos habitualmente capturados son más avanzados y han superado las anteriores barreras de seguridad

- **Escaneos**
- **Movimientos laterales**
- **Intento de exfiltración**
- **Protocolos poco comunes**

El servicio produce la **notificación** en caso de un incidente confirmado y la generación de un **informe de alertas y eventos** recibidos con carácter mensual.

El servicio puede ser solicitado mediante **formulario de solicitud firmado** y remitido por correo electrónico.

sedian Seguridad Digital de Andalucía

Requiere suscripción

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Protección de equipo final

El objetivo de este servicio consiste en proteger frente a determinadas **amenazas emergentes** los equipos de usuario de los organismos del grupo atendido.

La principal amenaza emergente a la que se enfrentan nuestras organizaciones actualmente es el ransomware. Para luchar frente a él se hace uso de la herramienta **microCLAUDIA** del CCN-CERT.

Se pone a disposición la herramienta para descarga lo que permite el despliegue de un conjunto de **vacunas** para muestras de ransomware conocidas.

Las alertas producidas por la herramienta, son revisadas y analizadas por los expertos del Centro para **evaluar un incidente en curso**.

El servicio puede ser solicitado mediante **formulario de solicitud firmado** y remitido por correo electrónico

sedian Seguridad Digital de Andalucía

Requiere suscripción

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Gestión de incidentes

Es el servicio sobre el que se organiza el CERT. Consiste en el **apoyo técnico y organizativo** que se ofrece a los organismos del grupo atendido ante situaciones indeseadas en el ámbito de ciberseguridad.

El servicio se presta en un formato continuo (24x7x365) de forma **remota**. Si bien, se dispone de la posibilidad de desplazamiento al lugar del incidente en los casos de especial relevancia.

La gestión de los casos se invoca tanto **internamente** a través de varios de los servicios de detección disponibles, como por parte de los organismos. En el caso de la invocación de los organismos se dispone de una a **cuenta de correo** y el **teléfono de contacto**.

Los expertos de AndalucíaCERT se coordinan con el organismo en el análisis de elementos disponibles para la recomendación de acciones a través del **ciclo de vida del incidente** (especialmente desde la Contención a las Lecciones Aprendidas) y el organismo recibe un informe mensual de actividad

El servicio puede ser solicitado a través de un **formulario firmado**, que ser remitido a través de correo electrónico o del portal de AndalucíaCERT.

sedian Seguridad Digital de Andalucía

Servicio base

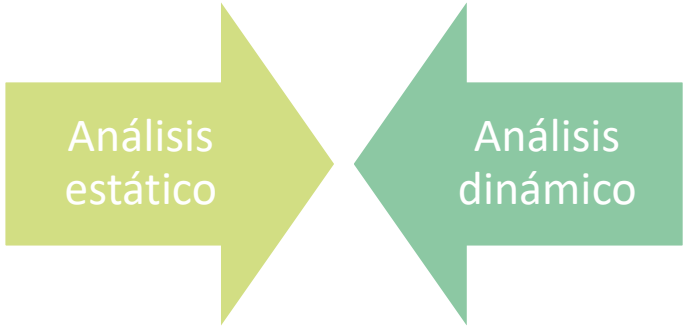
Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Análisis de malware

Este análisis es habitualmente invocado por el servicio de gestión de incidentes, si bien puede ser solicitado por los organismos cuando se requiera información detallada de una muestra de malware. Su finalidad consiste en conocer de forma detallada el **funcionamiento de la muestra** para llevar a cabo acciones de detección y poner en marcha reglas de protección.

Analiza la muestra sin ejecutarla a través de la extracción de su código binario y observación de características



Analiza la muestra ejecutándola en un entorno controlado y analizando los resultados que produce sobre dicho entorno.

El análisis de la muestra obtiene **elementos relevantes** de la misma como propósito, capacidad de propagación, conexión con Command & Control, vulnerabilidades explotadas, información recopilada o acciones llevadas a cabo sobre el sistema infectado.

El entregable del servicio es un **informe de análisis** que presenta las características identificativas de la muestra, así como los hallazgos en términos de operatividad.

El servicio puede solicitarse a través de la apertura de un ticket de incidente y remisión de la muestra de malware.

sedian Seguridad Digital de Andalucía

Servicio base

Servicios AndalucíaCERT

Servicios preventivos | Servicios detectivos | Servicios reactivos

Análisis forense

El servicio se encarga de llevar a cabo un **análisis profundo** sobre un activo implicado en un incidente con el objetivo de conocer los detalles técnicos del incidente para poder enfocar las acciones de contención y erradicación.

El conocimiento de aspectos como el vector de entrada o la fecha inicial de compromiso son la única forma de asentar de forma correcta las fases de erradicación y recuperación en **grandes incidentes**. De otra forma se corre el riesgo de restaurar un sistema ya infectado o erradicar sin eliminar la causa raíz que produjo el incidente.

1 Obtención evidencias

El análisis forense parte de la recopilación de evidencias, que se lleva a cabo durante la fase de **contención** de la gestión del incidente.

2 Informe técnico

El informe técnico trata de aclarar las **técnicas y tácticas** utilizadas por el atacante, la **debilidad** aprovechada para el ataque, las **fechas clave** de compromiso y acaba ofreciendo una serie de conclusiones y recomendaciones.

3 Informe pericial

En los casos que se requiera judicializar el incidente, se plantea la elaboración adicional de un informe pericial con la **metodología y planteamiento** que requiere esta casuística.

El servicio se debe invocar de forma explícita por el organismo a través de su solicitud en el marco de la gestión del incidente. Su ejecución debe ser objeto de aprobación por la USTIC-C.

sedian Seguridad Digital de Andalucía

Servicio base

Puntos de contacto

Correo electrónico

Se utilizarán las siguientes cuentas para contacto, con sus correspondientes claves PGP para cifrar el contenido:

- Reporte de incidentes:
  atencion.cert@juntadeancalucia.es

  Clave PGP ID: 0xE407E049
- Cuestiones de propósito general, contacto con representantes del CERT o suscripción a servicios:
  consultas.cert@juntadeandalucia.es

  Clave PGP ID : 0x93DF1055

Teléfono

El teléfono disponible de forma continua (24x7x265):
+34 955 060 974

Portales web

Se dispone de los siguientes sitios web para obtener información e interactuar con el CERT:

- Portal de servicios: https://andaluciacert.juntadeandalucia.es/
- RFC 2350: https://www.juntadeandalucia.es/export/drupaljda/RFC2350-AndaluciaCERT_20180706_0.txt

De cara a gestionar adecuadamente las pertinentes autorizaciones, salvo en el caso de reporte de incidentes, el resto de puntos de contacto deben ser empleados por el contacto designado para cada organismo.

sedian Seguridad Digital de Andalucía