

Nº y año del exped.
188_23-PIDS
Referencia

DENOMINACIÓN:

Acuerdo de 1 de marzo de 2023, del Consejo de Gobierno, por el que se toma conocimiento del Informe sobre el estado de la Ciberseguridad en la Administración de la Junta de Andalucía correspondiente al año 2022.

El artículo 1.d) del Decreto 152/2022, de 9 de agosto, por el que se establece la estructura orgánica de la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa le atribuye a ésta la competencia relativa a la estrategia digital, como marco común y unificado de referencia para la elaboración, desarrollo e implantación de un modelo digital en la Administración de la Junta de Andalucía y sus entidades instrumentales, que se oriente a la prestación de servicios públicos. Por su parte, el artículo 2.4.d) determina que la Agencia Digital de Andalucía está adscrita a la Consejería de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa, a través de la persona titular de la Consejería.

La Agencia Digital de Andalucía es una agencia administrativa de las previstas en los artículos 54.2.a) y 65 de la Ley 9/2007, de 22 de octubre, de la Administración de la Junta de Andalucía, creada mediante la disposición adicional vigesimosegunda de la Ley 3/2020, de 28 de diciembre, del Presupuesto de la Comunidad Autónoma de Andalucía para el año 2021, y cuyos Estatutos se aprobaron mediante el Decreto 128/2021, de 30 de marzo.

La transformación digital y la evolución de las Tecnologías de la Información y Comunicación (TIC) han impulsado un cambio sin precedentes en la sociedad, habilitando la interconexión de personas y dispositivos a través del denominado ciberespacio, creando modelos de trabajo virtuales, y estableciendo nuevos mecanismos de tratamiento y compartición de la información.

Esta situación genera una mayor distribución de los datos, aumentando el nivel de exposición a vulnerabilidades y amenazas, cada vez más complejas, difíciles de detectar, contener y resolver.

La ciberseguridad se ha convertido, más que nunca, en un reto global que traspasa fronteras y que afecta por igual a la ciudadanía, Administraciones Públicas y empresas, tanto a nivel nacional como internacional.

La Administración de la Junta de Andalucía, consciente de la complejidad de este nuevo panorama, identifica la ciberseguridad como uno de los pilares fundamentales sobre los que construir una sociedad y una economía digital, de modo que se potencie la mejora del nivel de ciberseguridad, dotando de confianza y garantías digitales a la ciudadanía andaluza, y velando por la disponibilidad

de los operadores críticos, servicios esenciales y sectores estratégicos de la Comunidad Autónoma de Andalucía.

El Informe sobre el estado de la Ciberseguridad en la Administración de la Junta de Andalucía correspondiente al año 2022 aporta referencias y datos que justifican la necesidad de invertir en la ciberseguridad de los sistemas, en la resiliencia de los servicios, en la formación de profesionales y en el conocimiento sobre los riesgos y cómo combatirlos, que debe permear a toda la ciudadanía, al sector público y a las empresas. Se apunta también el estado de las actividades más relevantes que en el ámbito de la ciberseguridad se vienen realizando en la Administración de la Junta de Andalucía, incluyendo los datos y estadísticas más relevantes, así como la situación actualmente existente en los ámbitos europeo y nacional.

Según la Encuesta sobre Equipamiento y Uso de Tecnologías de Información y Comunicación en los Hogares (año 2022), del Instituto Nacional de Estadística (INE), el 94,5% de la población de 16 a 74 años había usado Internet en los tres meses previos a la consulta. El 87,1% de la población se conecta a Internet diariamente (86,7% en Andalucía). La evolución de hogares con acceso a Internet también es destacable: 16,3 millones de hogares (el 96,1% del total) disponen de acceso a Internet. En 2021 el porcentaje fue del 95,9%. Desde el año 2012 el comercio electrónico ha llegado casi a triplicar su uso, con el 55,3 % de las personas encuestadas en 2022 que lo han usado.

Casi ocho de cada 10 personas entrevistadas han contactado o interactuado con las administraciones o servicios públicos a través de Internet en los 12 últimos meses por motivos particulares, lo que supone un incremento de 11,0 puntos respecto a 2021. El teletrabajo tiene una incidencia media: el 14,0% de los ocupados de 16 a 74 años (3,3 millones de personas) afirma haber teletrabajado durante la semana anterior a la entrevista. La ciudadanía no es el único sector que se digitaliza: según la encuesta de uso de TIC y Comercio Electrónico (CE) en las empresas 2021-2022 (Instituto de Estadística y Cartografía de Andalucía), un 99,1% de las empresas andaluzas de más de 10 trabajadores dispone de ordenadores y el 59,7% de los empleados los usa con fines empresariales. Un 70% de las empresas dispone de página web.

Por otra parte, dado que el problema de la ciberseguridad es global, se describe previamente la evolución de las ciberamenazas, la cibercriminalidad y los ciberincidentes a nivel mundial. Ante esta situación, los gobiernos plantean actuaciones de fomento de la resiliencia y la capacidad de identificar las amenazas y proteger, detectar y responder a los ciberincidentes. A continuación, se describen las estrategias y actuaciones que se desarrollan tanto a nivel europeo y nacional.

En la Comunidad Autónoma de Andalucía, mediante Acuerdo de 18 de octubre de 2022, del Consejo de Gobierno, se aprueba la Estrategia Andaluza de Ciberseguridad 2022-2025. Esta Estrategia constituye el vínculo entre la Administración Autonómica y la ciberseguridad, estableciendo las líneas maestras que deben llevarse a cabo para dar respuesta a los retos y desafíos de la sociedad andaluza.

La Estrategia contiene los retos, objetivos y líneas de actuación en materia de ciberseguridad para los años 2022-2025, involucrando a la Administración Pública de Andalucía, la ciudadanía, el sector privado y las entidades más representativas del sector de la Ciberseguridad.

Así mismo, se hace un repaso de la situación de la Ciberseguridad en la Administración de la Junta de Andalucía, analizando:

- Estructuras y normativa a nivel global.
- Roles y procesos.

- Gobierno a nivel de cada organismo, gestión del riesgo y cumplimiento.
- Protección, detección y respuesta.
- Formación y Concienciación.
- Colaboración con otras administraciones y entidades y difusión.
- Actuaciones en materia de ciberseguridad orientadas a empresas y ciudadanía.

Como elemento destacado de la Estrategia se crea el Centro de Ciberseguridad de Andalucía, que se pondrá en marcha próximamente.

Por otra parte, las actuaciones para el fomento de la ciberseguridad en las empresas andaluzas y para la preparación de la ciudadanía ante los riesgos digitales se han canalizado en 2022 a través de las iniciativas Andalucía Vuela y Andalucía Conectada.

Por último, AndalucíaCERT como centro experto para la prevención, detección y respuesta a incidentes y amenazas de seguridad en el ámbito de la Administración de la Junta de Andalucía, ha realizado en el año 2022 los siguientes servicios:

- Detección y respuesta a incidentes de seguridad: habiendo gestionado 7.479 incidentes de seguridad.
- Alerta temprana de ciberamenazas: se han cursado 29 avisos y alertas de campañas activas y amenazas inminentes a través de la lista de distribución de AndalucíaCERT.
- Informes divulgativos de ciberseguridad: se han publicado 2 informes divulgativos en materia de ciberseguridad.
- Análisis de vulnerabilidades: se han efectuado 17 análisis de vulnerabilidades.
- Difusión de IOC: se han publicado 75 listas negras.
- Informes post-mortem: se ha realizado 10 informes de post-mortem de revisión de incidentes de seguridad.
- Análisis forense: se han efectuado 2 análisis forense de incidentes especialmente graves.
- Respuesta in-situ: se ha efectuado 0 asistencia de respuesta in-situ en incidentes especialmente graves.

Por todo lo expuesto, se considera oportuno que el Informe sobre el estado de la Ciberseguridad en la Administración de la Junta de Andalucía correspondiente al año 2022 sea conocido en el seno del Consejo de Gobierno.

En su virtud, de conformidad con el artículo 27.22 de la Ley 6/2006, de 24 de octubre, del Gobierno de la Comunidad Autónoma de Andalucía, a propuesta del Consejero de la Presidencia, Interior, Diálogo Social y Simplificación Administrativa, y previa deliberación del Consejo de Gobierno, en su reunión del día 1 de marzo de 2023,

ACUERDO

Tomar conocimiento del Informe sobre el estado de la Ciberseguridad en la Administración de la Junta de Andalucía correspondiente al año 2022.

Sevilla, 1 de marzo de 2023

Juan Manuel Moreno Bonilla
PRESIDENTE DE LA JUNTA DE ANDALUCÍA

Antonio Sanz Cabello

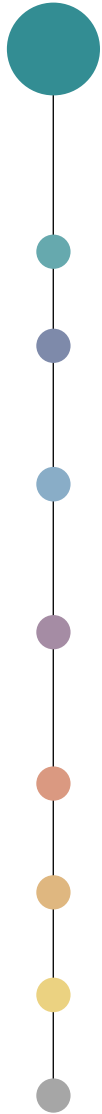
CONSEJERO DE LA PRESIDENCIA, INTERIOR, DIÁLOGO SOCIAL
Y SIMPLIFICACIÓN ADMINISTRATIVA



Estado de la ciberseguridad en la Administración Andaluza en 2022

Agencia Digital de Andalucía

Febrero 2023



Índice

Tabla de contenidos

Introducción – P3

Estrategia Andaluza de
Ciberseguridad 2022-2025 – P5

Estructura de gobierno de
la ciberseguridad – P6

Gobierno, gestión del
riesgo y cumplimiento – P7

Protección, detección y respuesta
– P8

Formación y concienciación - P11

Colaboración y difusión - P12

Actuaciones hacia empresas
y ciudadanía - P13



Introducción y contexto

La transformación digital y la evolución de las TIC han habilitado una **mayor interconexión de personas y dispositivos a través del ciberespacio**, con nuevos modelos de trabajo virtuales, y nuevos mecanismos de tratamiento y compartición de la información.

Esto genera mayor distribución de los datos, aumentando el nivel de **exposición a vulnerabilidades y amenazas cada vez más complejas**, difíciles de detectar, contener y resolver.

La ciberseguridad se ha convertido, más que nunca, en un reto global que traspasa fronteras y que afecta por igual a la **ciudadanía, Administraciones Públicas y empresas**, tanto a nivel nacional como internacional.

Ante esta situación, la **respuesta de los gobiernos** ha sido llevar a cabo múltiples actuaciones para fomentar la resiliencia y fortalecer la capacidad de protección, detección de amenazas y gestión de los ciberincidentes.

La **Junta de Andalucía** dispone de una vasta infraestructura para gestionar la información de la ciudadanía a la que presta servicios:



85 organismos



Miles de sedes



900 aplicaciones



Cientos de miles de equipos

La gran cantidad de información tratada y los servicios públicos que se prestan deben ser protegidos ante un **escenario de riesgos de ciberseguridad que cambia continuamente**.

Para ello se necesita compromiso, una estructura dedicada, recursos y especialización, a fin de disponer de las **capacidades óptimas** para afrontar los desafíos futuros.

La UE desarrolló en 2020 la **Estrategia Europea de Ciberseguridad** para la década digital, que busca:

- Aumentar la seguridad de los servicios esenciales y dispositivos conectados.
- Reforzar capacidades colectivas para responder a ciberataques principales.
- Cooperar con socios a nivel mundial para garantizar la estabilidad en un ciberespacio global, abierto, estable y seguro, basado en Estado de Derecho.



Introducción y contexto

Diferentes **estrategias e instituciones españolas** buscan resguardar la ciberseguridad:

- Estrategia Nacional de Ciberseguridad (2019), para garantizar el uso seguro del ciberespacio.
- Foro Nacional de Ciberseguridad (2020), que fomenta la colaboración público-privada en torno a la cultura de ciberseguridad, la industria I+D+i, la formación y el talento.
- Estrategia de Seguridad Nacional (2021), que establece la defensa del ciberespacio como una prioridad de organizaciones y CCAA.



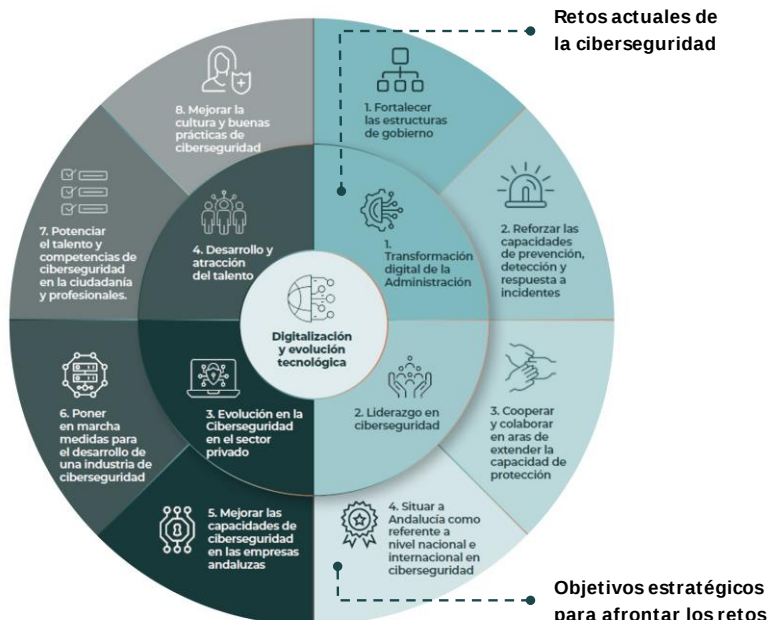
“Los **ciberataques y la ciberdelincuencia** están aumentando en toda Europa y cada vez son más sofisticados. Esta tendencia seguirá agravándose en el futuro, ya que se espera que **22.300 millones de dispositivos** en todo el mundo estén conectados a la internet de las cosas de aquí a 2024”



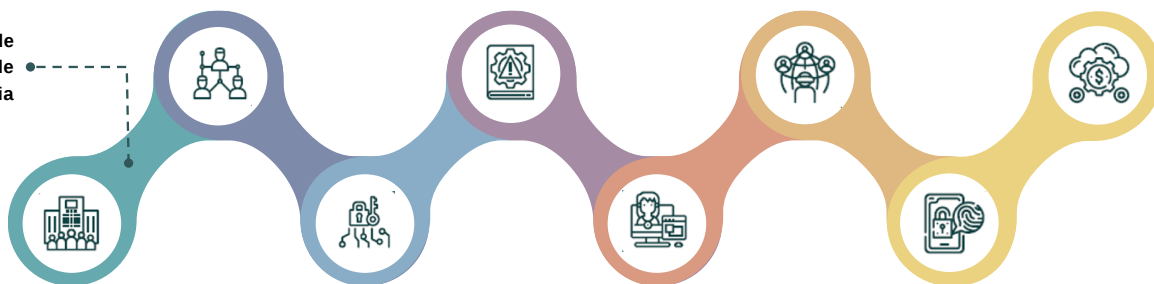
Estrategia Andaluza de Ciberseguridad 2022-2025

Contiene los **retos, objetivos y líneas de actuación** en materia de ciberseguridad para los próximos 3 años, involucrando a la Administración Pública de Andalucía, la ciudadanía, el sector privado y las entidades más representativas del sector.

La Administración Autonómica debe afrontar cuatro grandes retos, derivados de la **digitalización y evolución tecnológica de la sociedad**, a los que se dará respuesta a través de un escenario objetivo que permita a Andalucía convertirse en un **territorio de referencia en materia de ciberseguridad**.



Líneas de actuación de la estrategia



Evolución y mejora de las **estructuras organizativas** en materia de ciberseguridad dando cobertura a la visión interna y externa de la Administración de la Junta de Andalucía

Definición e implantación de un plan de desarrollo y mejora continua de las capacidades de **prevención, detección y respuesta** a incidentes de AndalucíaCERT

Fortalecimiento y desarrollo de marcos de **cooperación y colaboración** en diferentes ámbitos, tanto a nivel autonómico, nacional e internacional

Creación y desarrollo de un plan de promoción de Andalucía, posicionándola como **territorio de referencia** en materia de ciberseguridad

Estructura de gobierno de la ciberseguridad

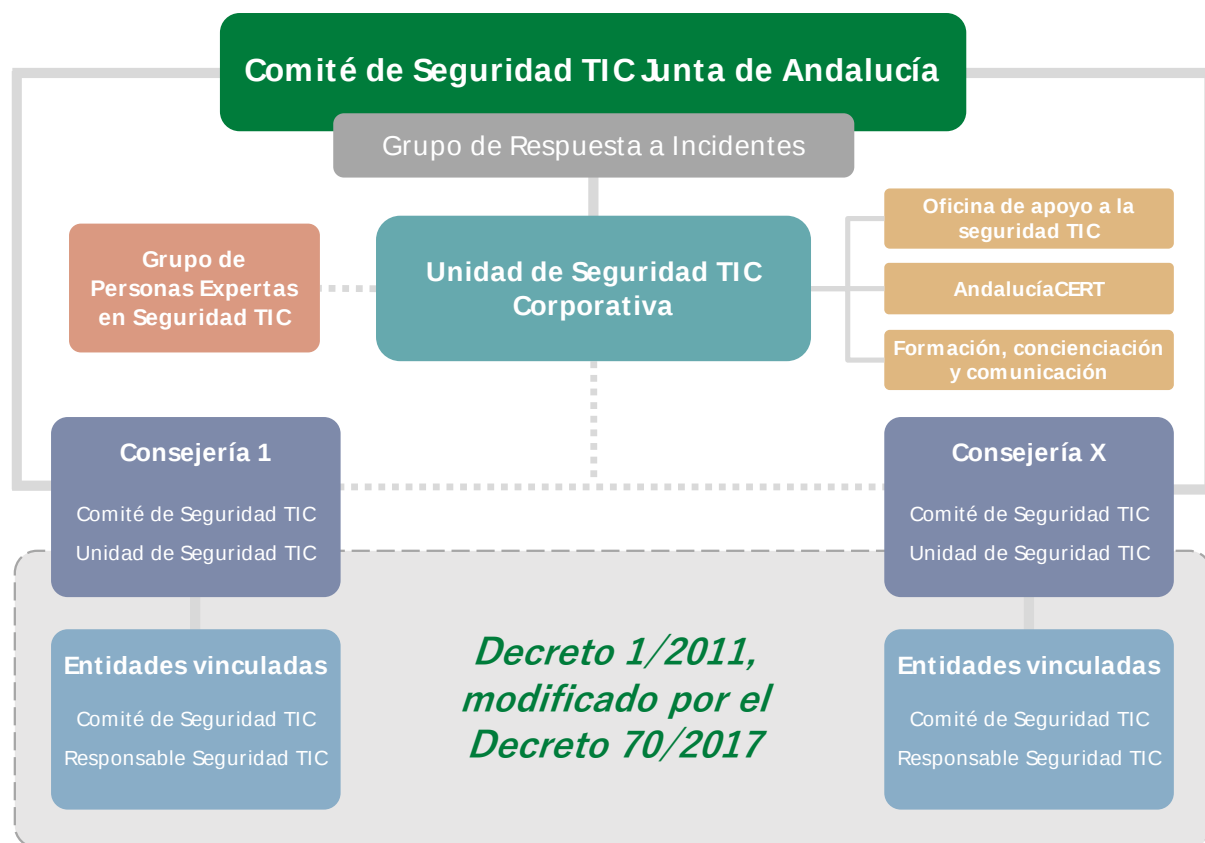


Agencia Digital de Andalucía

La Administración de la Junta de Andalucía cuenta con una estructura organizativa que le permite atender a todos los aspectos de la ciberseguridad, dando **cumplimiento normativo** a los requerimientos y extendiendo la aplicación de **buenas prácticas**.

Está en curso la elaboración de una **nueva norma organizativa** que actualizará la organización, simplificará y facilitará el cumplimiento, incrementará el nivel de exigencia para **alcanzar una mayor madurez**, y permitirá integrar requisitos de otras normativas: protección de datos, servicios esenciales, infraestructuras críticas, etc.

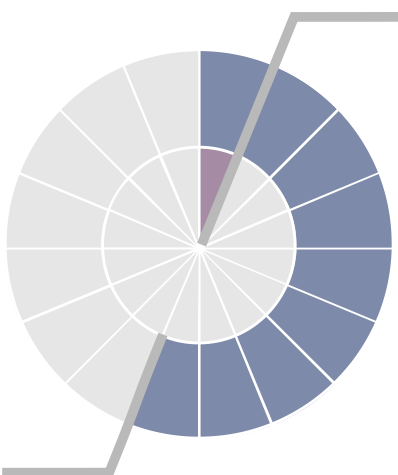
La futura Política de Ciberseguridad de la Administración de la Junta de Andalucía reflejará el papel de la **Agencia Digital de Andalucía (ADA)** como entidad de coordinación y ejecución de políticas de ciberseguridad.



Gobierno, gestión del riesgo y cumplimiento

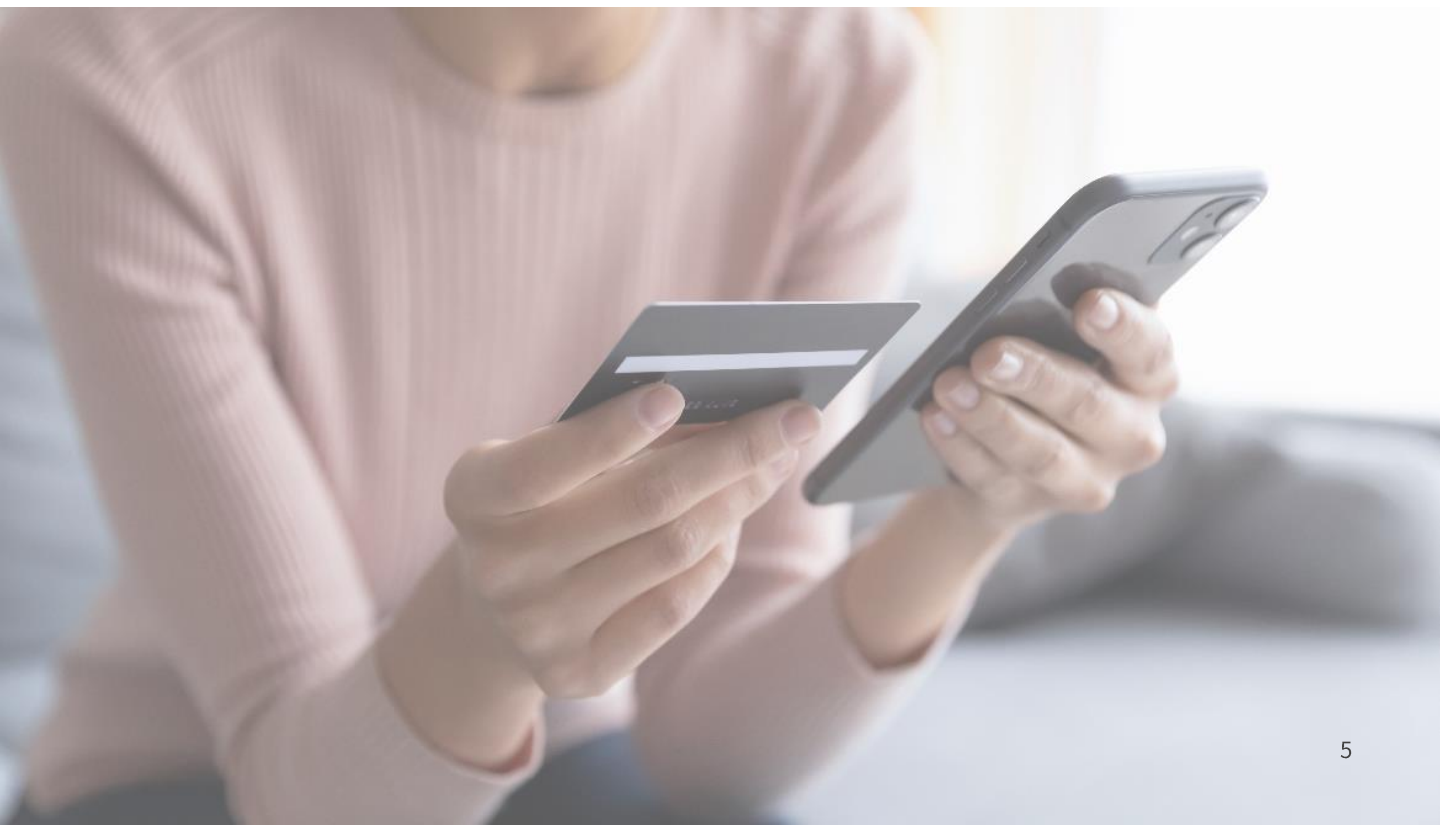
La Junta de Andalucía es la Comunidad Autónoma con **mayor número de certificaciones de conformidad con el ENS** de sistemas de información categoría media y alta, con **30 certificaciones obtenidas**. En el Centro Criptológico Nacional (CCN-CERT), el Sector Público Andalúz registra:

24 certificaciones ENS de un total de 46 en la sección de **Comunidades Autónomas**



6 certificaciones ENS de un total de 55 en la sección **Sector Público Institucional**

La **Oficina de Apoyo a la Seguridad TIC** es el proyecto horizontal de la Junta de Andalucía dedicado a coordinar las actuaciones en ciberseguridad, proporcionando un contexto normativo para su ejecución, realizando seguimiento de las mismas, y apoyando la adecuación de los sistemas de información al **Esquema Nacional de Seguridad (ENS)**.

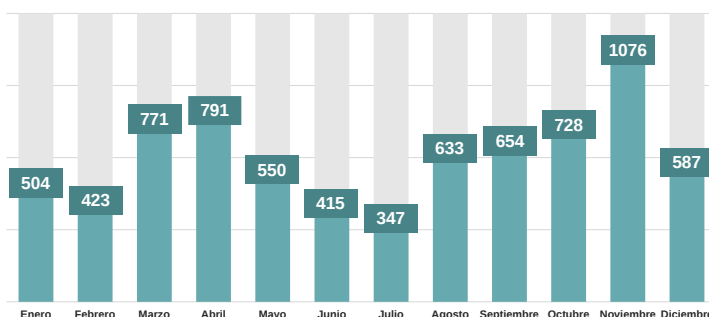


Protección, detección y respuesta

En 2022, AndalucíaCERT:

- Gestionó **7.479 incidentes de seguridad**, un 5% más que el año anterior
- Cursó **29 avisos y alertas** sobre campañas activas y amenazas inminentes
- Publicó **2 informes** en materia de ciberseguridad
- Llevó a cabo **17 análisis de vulnerabilidades**
- Realizó **10 informes post-mortem** de revisión de incidentes de seguridad
- Efectuó **2 análisis forenses** de incidentes especialmente graves

Desde 2010, **AndalucíaCERT** es el centro de operaciones de seguridad y el equipo de respuesta a ciberincidentes (SOC/CSIRT) autonómico. Su finalidad es **prevenir, detectar y responder eficazmente a los incidentes de seguridad**, limitando daños y garantizando la continuidad de los servicios. El Grupo Atendido por AndalucíaCERT lo conforman **121 entidades adscritas** al servicio.



Principales hitos

Grupo atendido

- Ampliación del Grupo Atendido en 2 entidades
- Certificación ENS categoría MEDIA en sistemas que dan soporte a las acciones centralizadas para la prevención, detección y respuesta a incidentes en el ámbito de la Junta de Andalucía

Procesos internos

- Introducción de mejoras en el diseño de los procesos internos del Centro

Red de colaboración

- Fomento a la colaboración con equipos de respuesta a incidentes públicos y privados de ámbito nacional
- Participación en ENISA CyberEurope 2022, dedicado al Sector Salud, en coordinación con el SAS.
- Adhesión a la Red Nacional de Centros de Operaciones de Seguridad (SOC)
- Participación en las reuniones del foro CSIRT.es
- Participación como público en las XVI Jornadas STIC del CCN-CERT

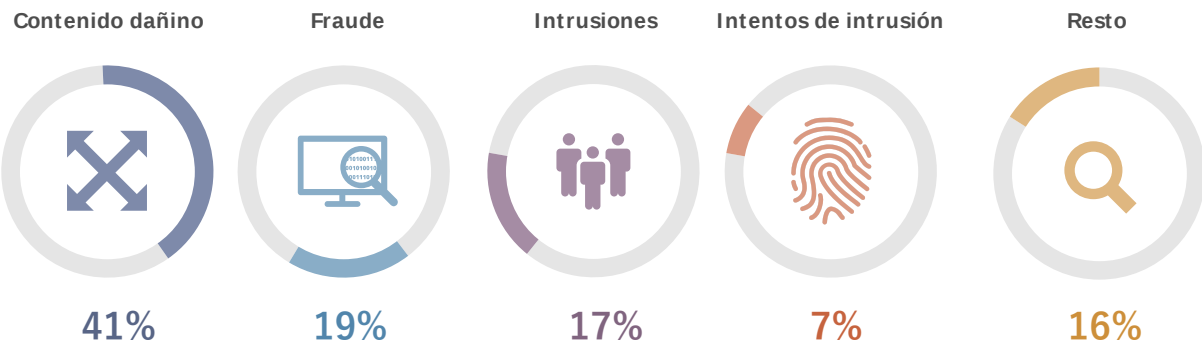
Capacidades de detección

- Mejora de capacidades de detección de incidentes mediante incorporación de fuentes de inteligencia de ciberamenazas y detección de amenazas avanzadas persistentes
- Monitorización del tráfico de la red troncal de la Red Corporativa de la Junta de Andalucía
- Monitorización de determinados organismos
- Adaptación a nuevas fuentes de inteligencia de sistema REYES v4 del CCN-CERT
- Mejora continua de capacidades de detección, desarrollo de nuevos casos de uso

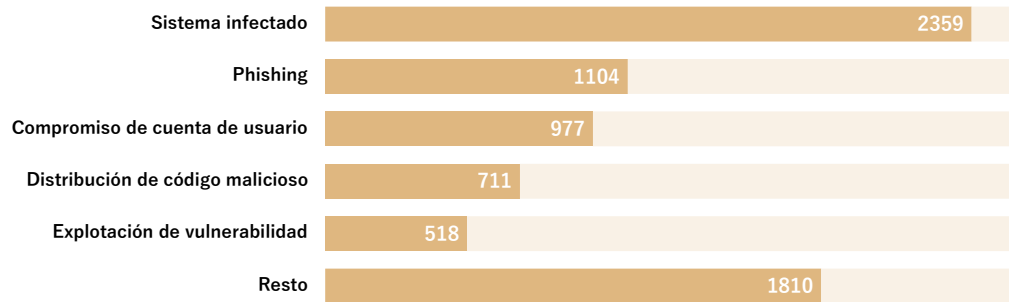
AndalucíaCERT
CENTRO DE SEGURIDAD TIC

Protección, detección y respuesta

Incidentes de seguridad gestionados según clase y tipo



Aunque son menores en número, los incidentes que han causado una mayor preocupación han sido las amenazas de **compromiso de la información** (1%). Concretamente, han consistido en campañas de propagación de ransomware (secuestro de información).



Los incidentes de código dañino fueron, en su mayor parte, intentos de distribución o detección de malware (software malicioso) en la red o en equipos finales.

La práctica totalidad de los incidentes de fraude consistieron en la distribución de correos de phishing (suplantación de identidad).

Un elevado porcentaje de los incidentes de intrusión consistieron en cuentas de usuario comprometidas.

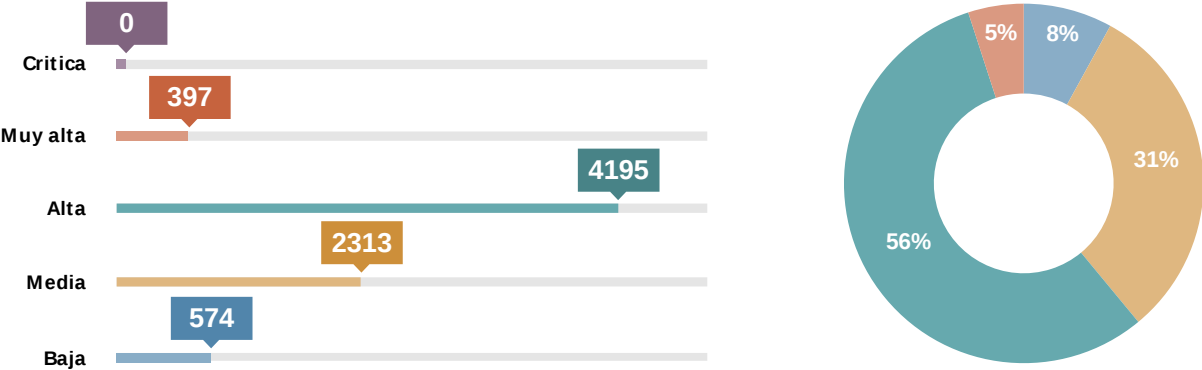
Los intentos de intrusión se relacionan con intentos de explotación de vulnerabilidades.

Protección, detección y respuesta

Incidentes de seguridad según nivel de peligrosidad

El 87% de los incidentes de seguridad tratados tuvieron un nivel de peligrosidad media o alta.

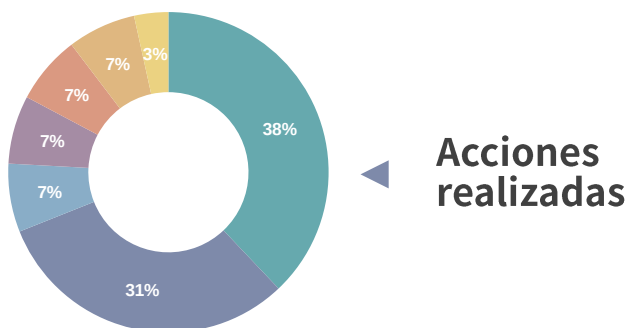
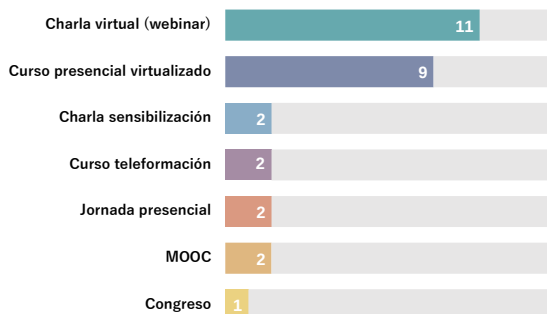
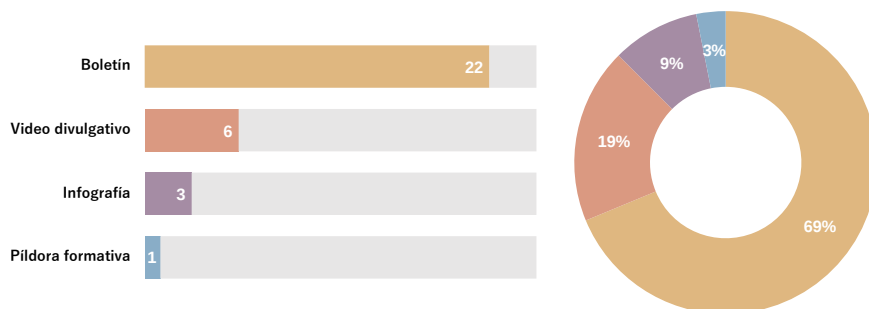
Solo el 5% de los incidentes, aproximadamente 33 al mes, entrañaron un riesgo muy alto y requirieron un tratamiento excepcionalmente rápido y ágil



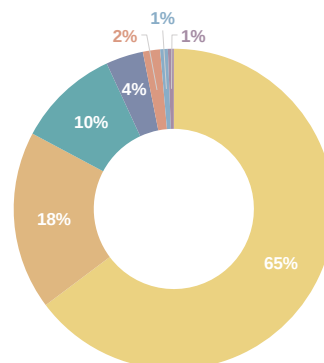
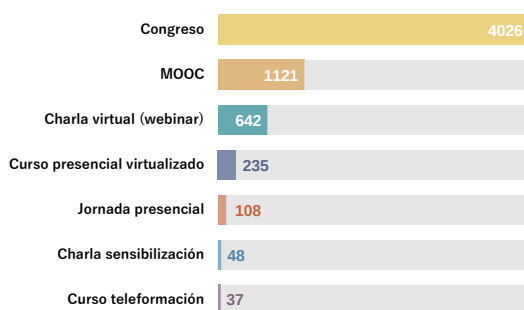
Formación y concienciación

La formación y la concienciación en el ámbito de la ciberseguridad buscan que los empleados públicos sepan proteger la información que manejan y los servicios que prestan mediante **buenas prácticas de seguridad digital** en el puesto de trabajo, a fin de ser capaces de detectar y responder en primera instancia a las ciberamenazas. La Oficina de Formación y Concienciación es la responsable del diseño y ejecución del **Plan Anual de Formación y Concienciación** en Ciberseguridad.

Materiales producidos



Participantes por tipo de acción



Colaboración y difusión

Centro Criptológico Nacional

En el marco del **protocolo general de actuación en materia de ciberseguridad** firmado en 2019 entre el Centro Criptológico Nacional (CCN-CERT) del Centro Nacional de Inteligencia (CNI) y la Administración de la Junta de Andalucía, en julio de 2022 tuvo lugar la **reunión anual de la Comisión de Seguimiento**.



Administraciones Locales

Se han mantenido reuniones con las Diputaciones Provinciales y con el CCN-CERT para avanzar el diseño de un **modelo federado de ciberseguridad** que permita optimizar esfuerzos, aprovechar las herramientas comunes y compartidas que proporciona el CCN-CERT y **compartir ciberinteligencia e información sobre incidentes** de manera fluida y rápida.

El modelo de adscripción voluntaria en base a convenios de colaboración se enmarcará en el ámbito de la **Red Nacional de Centros de Operaciones de Seguridad (SOC)**, centros especializados en la prevención, detección y respuesta a ciberincidentes.

Congreso de Ciberseguridad

En marzo de 2022 se celebró en Málaga el I Congreso de Ciberseguridad de Andalucía, un espacio de encuentro para tratar los **retos y desafíos en materia de ciberseguridad** dirigido a Administración Pública, empresas del sector y ciudadanía.



1583

Asistentes presenciales



2443

Asistentes vía streaming



30

Empresas patrocinadoras

Actuaciones hacia empresas y ciudadanía

Las actuaciones para el **fomento de la ciberseguridad** en las empresas andaluzas y para la preparación de la ciudadanía ante los riesgos digitales se canalizaron a través de las iniciativas **Andalucía Vuela** y **Andalucía Conectada**.



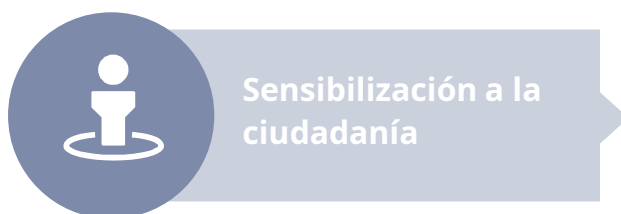
2 ediciones del curso para una certificación que acredita el conocimiento técnico en la gestión de la seguridad de la información en organizaciones

13 acciones de formación hacia empresas y ciudadanía, entre las que destacan:



- Los ciberdelitos: cómo protegernos en Internet
- Tus datos en Internet: información y consentimiento
- Protege y mejora la seguridad de tu red WiFi
- Conoce tus derechos en Internet: los derechos digitales
- Controla tu huella digital y ejerce tu derecho al olvido
- ¿Están seguros tus datos? Ciberseguridad para la vida diaria
- Pasos a seguir para comprar por Internet con total seguridad
- Cómo realizar pagos seguros por Internet

Lanzamiento de **4 guías y acciones** en diferentes épocas del año:



- Día de Internet: acción “Internet para las personas mayores y el envejecimiento saludable”
- Mes Europeo de Ciberseguridad: guía “Navega hacia un Internet seguro”
- Black Friday, Cyber Monday y compras navideñas: decálogo “10 claves para comprar por Internet con éxito y seguridad”
- Navidades: guía “Cómo acertar con regalos tecnológicos para menores”



Junta de Andalucía