THINK SMARTCITY

Ciudades que habitan el futuro



SmartCities Think Tank

Powered by


FORMACIÓN AYUNTAMIENTOS
EL CAMINO HACIA UN
MUNICIPIO
INTELIGENTE
ESTRATEGIA, FINANCIACIÓN
Y CIBERSEGURIDAD
FORMACIÓN
HÍBRIDA
ONLINE Y
PRESENCIAL
23 SEPT 2026 · 10 a 13h.
Bolbaite. Casa de la Cultura
Av. del Oeste, 8

Ciberseguridad en municipios inteligentes

Victoria Majadas, socia Smart To People

Bolbaite, 23 de septiembre de 2026

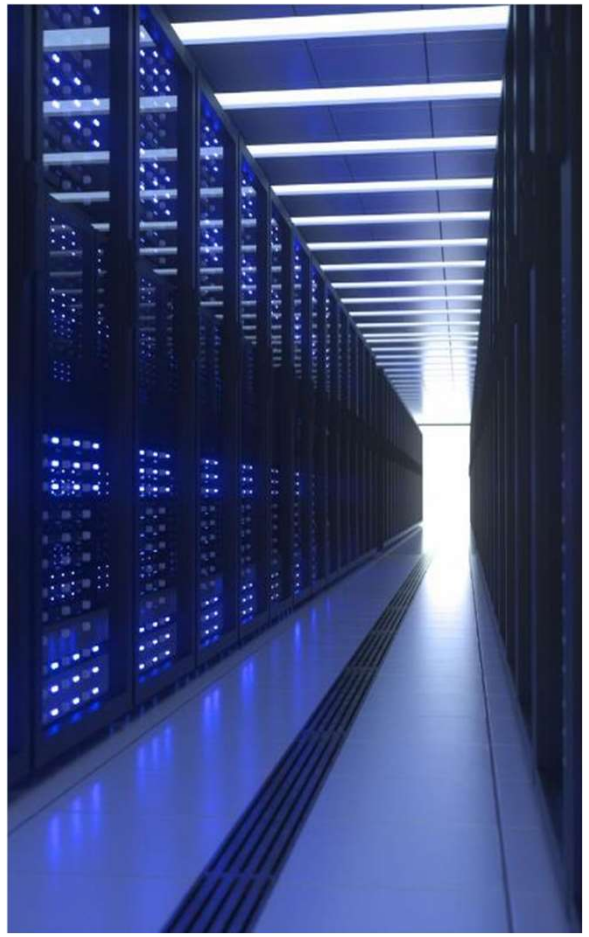
Organiza: SmartCities Think Tank | avaesen

Financiado por: GENERALITAT VALENCIANA Conselleria d'Indústria, Turisme, Innovació i Comerç

¿Qué es la ciberseguridad?

La ciberseguridad se refiere a cualquier **tecnología, medida o práctica para prevenir ciberataques** o mitigar su impacto.

La ciberseguridad tiene como objetivo **proteger** los sistemas, aplicaciones, dispositivos informáticos, datos confidenciales y activos financieros de personas y organizaciones contra virus informáticos simples y molestos, ataques sofisticados y costosos.



Organiza: SmartCities Think Tank | avaesen

Financiado por: GENERALITAT VALENCIANA Conselleria d'Indústria, Turisme, Innovació i Comerç

Tipos de ciberdelincuentes



CIBERESPIA

Roban información para vender a competidores.
Alta capacitación técnica.
Ligados a organizaciones o gobiernos.



CIBERDELINCUENTE

Cometen ciberdelito y fraude para obtener beneficios económicos.
Organizados o en solitario.
A veces ligados a movimientos ideológicos y/o políticos.



INGENIERO SOCIAL

Emplean tácticas psicológicas para engañar a las personas y obtener información confidencial, o persuadir a las personas para que realicen acciones específicas.

Organiza: SmartCities Think Tank | avaesen

Financiado por: GENERALITAT VALENCIANA Conselleria d'Indústria, Turisme, Innovació i Comerç

¿Qué quieren?



NUESTRA INFORMACIÓN

ROBAR



Secretos industriales, Propiedad intelectual, Datos de clientes. Información de mercado o negocio. Nuestras cuentas bancarias.

SECUESTRAR



Cifrar y pedir un rescate a cambio de la clave de descifrado.

FILTRAR



Generar pérdida de imagen y de reputación.
Generar problemas legales y económicos.

Organiza: SmartCities Think Tank | avaesen

Financiado por: GENERALITAT VALENCIANA Conselleria d'Indústria, Turisme, Innovació i Comerç

incibe_
INSTITUTO NACIONAL DE CIBERSEGURIDAD

BALANCE DE CIBERSEGURIDAD 2025

26% más que en 2024

122.223 incidentes de ciberseguridad

Cualquier problema digital que ponga en riesgo los datos o la seguridad de los dispositivos, como, por ejemplo, un virus informático.

237.028 sistemas vulnerables

Un sistema vulnerable es como una casa con una cerradura rota. Es más fácil para los intrusos entrar y causar problemas.

401 operadores esenciales e importantes*

Empresas o servicios que son muy importantes para el funcionamiento diario de la sociedad. Incluye sectores, como la energía, el agua o las comunicaciones.

- **34%** Banca
- **14%** Transporte
- **8%** Energía
- **7%** Infraestructura de los mercados financieros
- **6%** Aseguradoras y fondos de pensiones

*Entidades alineadas con la terminología de la directiva NIS2

355 entidades adscritas a los servicios de INCIBE (un 8% más que en 2024)

25% de las cuales ya forman parte del **Portal de Servicios a Entidades Privadas** (PSE).

PSE PORTAL DE SERVICIOS ENTIDADES PRIVADAS incibe-cert_

INCIDENTES **MÁS FRECUENTES**

25.133 incidentes son ***phishing****

*Suplantación a empresas o personas de confianza que se ponen en contacto con las posibles víctimas, a través de correos electrónicos falsos, intentando engañarles para proporcionar información personal o bancaria.

45.445

4 de cada 10 incidentes son **fraude *online***

19% más que en 2024

4.600 **dominios.es** fraudulentos **cerrados** en colaboración con red.es

principalmente **tiendas fraudulentas**

55.411 incidentes relacionados con ***malware***

(**+45%** del total de incidentes) como los virus informáticos

392 incidentes son ***ransomware*** (secuestros digitales) donde los ciberdelincuentes bloquean el acceso a los archivos o sistemas, pidiendo dinero para devolvérselos a las víctimas

85% de los sistemas **infectados** por *malware* y controlados por un ciberdelincuente (***botnet***) están relacionados con **dispositivos inteligentes (IoT)**, como televisores, decodificadores, reproductores multimedia, etc.

3.849 **robos de información***

*Acceso o sustracción no autorizada de datos digitales y/o confidenciales

Todos estamos expuestos

Existen dos tipos de organizaciones: las que han sido **hackeadas** y las que **aún no saben** que fueron hackeadas

John Chambers
Chief Executive Officer of Cisco



España, uno de los países más ciberatacados



CincoDías

EMPRESAS Y FINANZAS · MERCADOS · ECONOMÍA · COTIZACIONES · FONDOS Y PLANES · ÚLTIMAS NOTICIAS · OPINIÓN | EL PAÍS — SUSCRÍBETE · INICIAR SESIÓN

Smartlife

EN COLABORACIÓN CON adslzone

SMARTPHONES · TABLETS · SMART TV · GADGETS · LIFESTYLE · MOTOR · PYMES

CRÓNICA DE BOLSA El Ibex cotiza en tablas con el petróleo de nuevo al alza

LIFESTYLE >

España, entre los tres países con más ciberamenazas detectadas del mundo

Somos uno de los principales objetivos de los ciberdelincuentes

España vuelve a estar en el punto de mira de los ciberdelincuentes. O esto es lo que se desprende del último informe de ESET, donde en su Threat Report H1 2026 han dejado claro que nuestro país se sitúa como el tercer territorio del mundo con más ciberamenazas detectadas durante el primer semestre del año, solo por detrás de Japón y Polonia.

Un dato que confirma una tendencia muy preocupante: **España se ha consolidado como uno de los grandes objetivos de la actividad cibercriminal a nivel global.**

ESET advierte: España es uno de los principales objetivos de los ciberdelincuentes

El informe, elaborado a partir de la telemetría de ESET y del trabajo de sus investigadores entre diciembre de 2025 y mayo de 2026, señala que **España concentró el 7,43% de todas las detecciones registradas por la compañía.** Japón lidera la clasificación con un 10,15%, seguido de Polonia con un 7,77%. Por detrás quedan países como Estados Unidos o China.

Además, este informe advierte de que las amenazas tradicionales no están desapareciendo, sino evolucionando. De esta manera, **el ransomware, los infostealers y los troyanos bancarios siguen teniendo mucho peso**, pero ahora cuentan con herramientas más complejas y campañas mejor diseñadas.

Top 3 mundial

Ciberseguridad en municipios inteligentes

Tres líneas de trabajo:

LÍNEA 01

Concienciación

Capacitación continua para empleados públicos y divulgación digital segura para la ciudadanía.

LÍNEA 02

Seguridad Técnica

Protección de red, firewalls y cumplimiento estricto del Esquema Nacional de Seguridad (ENS).

LÍNEA 03

Ciberseguro

Póliza especializada para mitigar el impacto económico y respaldar la gestión de crisis.

Ciberseguridad en municipios inteligentes

Apoyo en el CSIRT-CV:

https://csirtcv.gva.es/csirt-cv/



Ciberseguridad en municipios inteligentes

Consejos en ciberseguridad:

1. Mantén actualizados tus dispositivos y apps.



Las actualizaciones, a menudo, corrigen vulnerabilidades de seguridad que podrían ser aprovechadas por los ciberdelincuentes.

2. No olvides el antivirus.



Mantén siempre tu antivirus actualizado y en ejecución.

3. Presta atención a los "Archivos descargables" y/o a los "Adjuntos sospechosos".



Evita descargar archivos adjuntos desconocidos que recibas por correo electrónico, ya que podrían infectar tus dispositivos.

4. Evita utilizar Redes Wi-Fi públicas.



Este tipo de redes suelen carecer de medidas de seguridad. En caso de necesidad, te recomendamos utilizar una conexión VPN (*Virtual Private Network*, o red privada virtual).

Ciberseguridad en municipios inteligentes

Consejos en ciberseguridad:

5. Navega por páginas HTTPS.



Prioriza los sitios web que utilicen conexiones seguras (HTTPS). Verifica que la página web tiene el certificado válido, buscando el candado en la barra de tu navegador.

6. No hagas clic en enlaces sospechosos o desconocidos.



Si recibes correos electrónicos o SMS con archivos o enlaces a direcciones, no los abras si no puedes asegurar que no son maliciosos.

7. Cierra sesión en tus cuentas después de utilizarlas.



Garantiza que nadie pueda tener acceso a tu información, aunque tenga acceso a tu dispositivo.

8. Utiliza contraseñas seguras.



Crea contraseñas fuertes y únicas para cada cuenta. Considera el uso de gestores de contraseñas para una mayor seguridad.

Organiza: SmartCities Think Tank | avaesen

Financiado por: GENERALITAT VALENCIANA Conselleria d'Indústria, Turisme, Innovació i Comerç

T H I N K S M A R T C I T Y

Energía que habita el futuro

CIBERSEGURIDAD EN MUNICIPIOS INTELIGENTES

Bolbaite, 23 de septiembre de 2026

Victoria Majadas Morales

SMART TO PEOPLE

Tel. 627499852

Mail: vmajadas@smarttopeople.es



Organiza: SmartCities Think Tank | avaesen

Financiado por: GENERALITAT VALENCIANA Conselleria d'Indústria, Turisme, Innovació i Comerç