



Instituto Nacional de Tecnologías de la Comunicación (INTECO)

**Centro de referencia en
ciberseguridad**

INTECO



SECRETARÍA DE ESTADO
DE TELECOMUNICACIONES
Y PARA LA SOCIEDAD DE
LA INFORMACIÓN



Instituto Nacional
de Tecnologías
de la Comunicación



Entidad de referencia

Confianza digital

Ciberseguridad



Actividad

Servicios

Investigación

Coordinación



inteco
(cert)

Contexto: retos actuales de seguridad

Una cita:

«Cuanta más gente dependa de Internet, más gente dependerá de que la red sea segura. Una red segura protege nuestros derechos y libertades y nuestra capacidad de ejercer actividades económicas. Ha llegado el momento de coordinar nuestra acción: el coste de la inacción es mucho más elevado que el de la acción.»

[Neelie Kroes. Vicepresidenta de la Comisión Europea como comisaria de Agenda Digital]



- Escenario cambiante: nuevos jugadores (hacktivismo, ciberguerra, ciberespionaje...) y mayor dependencia de la tecnología
- Los gobiernos, las naciones y sus IICC son nuevos objetivos de los ciberataques
- Impacto:
 - El cibercrimen tiene un impacto de más de **300.000 millones de euros** en la economía mundial.
 - **1,5 millones** de víctimas al **día**
 - Algunas empresas sufren hasta **400** ataques **diarios**.

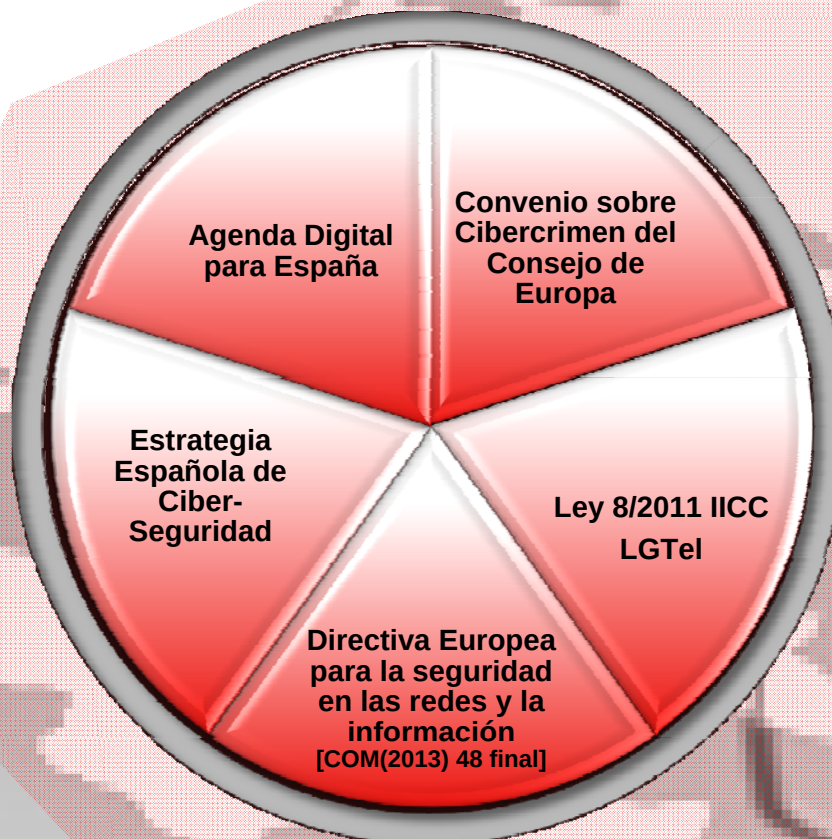
Las sociedades necesitan ciberseguridad

Ciberseguridad: compromiso global



Principales estrategias de ciberseguridad

Ciberseguridad: compromiso nacional



Estrategia en España

El papel de INTECO



=

Centro de referencia en **ciberseguridad**



Anterior

Nuevo

Agenda Digital para España

(Aprobada Consejo de Ministros 15/02/2013)

Objetivo:

Reflejar la estrategia del Gobierno en el ámbito digital y de las telecomunicaciones con el objetivo de trasladar los beneficios de las nuevas tecnologías a los ciudadanos, las empresas y la administración. Además, marca la hoja de ruta para el cumplimiento de los objetivos de la Agenda Digital para Europa en 2015 y en 2020.

(6 Objetivos)

Objetivo 4. Reforzar la confianza en el ámbito digital

4.2. Reforzar las capacidades para la confianza digital



=

Centro de referencia en
Confianza digital y ciberseguridad

- Extender la participación a todos los ámbitos de la confianza.
- Situar a INTECO como entidad de referencia en ciberseguridad (sectores estratégicos, empresas y ciudadanía)
- Establecer las capacidades necesarias para estudiar riesgos emergentes y poder anticipar necesidades y adoptar medidas preventivas.



Estrategia española: EECS

Estrategia Española de Ciberseguridad (en desarrollo)



Objetivo: Lograr que España haga un uso seguro de las redes y sistemas de información, fortaleciendo las capacidades de prevención, detección y respuesta a los ciberataques.

- Reforzar la capacidad de prevención, detección y respuesta ante ciberamenazas.
- Impulsar la seguridad y resiliencia de las redes y sistemas de información (IICC, sectores estratégicos).

- Otras líneas:
 - Sensibilización.
 - Formación de profesionales.
 - Desarrollo del sector de la seguridad.
 - Organización y coordinación nacional e internacional.

Coordinación de iniciativas público-privadas de ciberseguridad



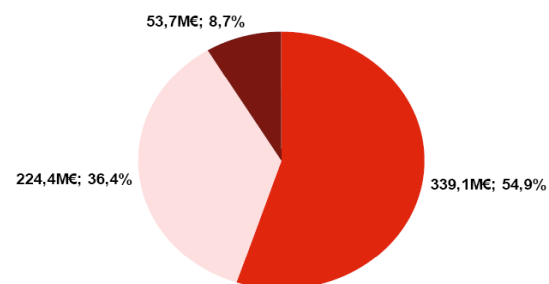
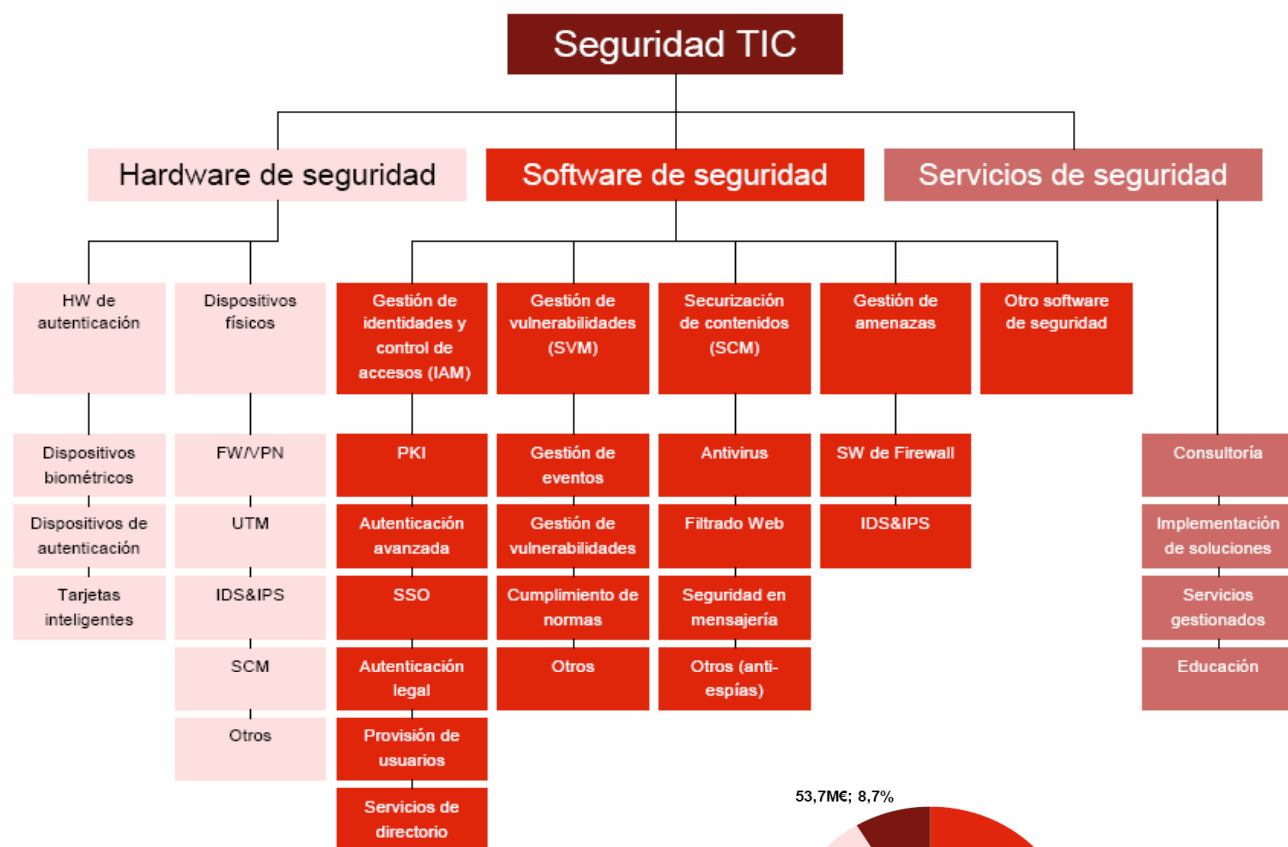
Capacidades reactivas y preventivas frente a incidentes



Estrategia española: Convenio SES-SETSI



Cooperación público-privada



■ Servicios de seguridad

■ Software de seguridad

■ Hardware de seguridad



•PRIMER EJE: Especialización en ámbitos TIC de Liderazgo Tecnológico

- SEGURIDAD DE LA INFORMACIÓN
- INNOVACIÓN EN LAS TIC



•SEGUNDO EJE: Sinergias con el entorno empresarial

- Sectores estratégicos territoriales como los siguientes:
 - SECTORES ESTRATÉGICOS DE LA INDUSTRIA
 - INFRAESTRUCTURAS CRÍTICAS

•TERCER EJE: Círculo Virtuoso de la Innovación

- EMPRESAS INNOVADORAS + CENTROS TECNOLÓGICOS+ UNIVERSIDADES



•CUARTO EJE: Alineación con políticas públicas



- Planes estatales
- Eje peninsular
- Programas Europeos

AEI Seguridad

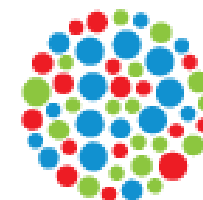


aeiseguridad

Agrupación Empresarial Innovadora
para la seguridad de las redes
y los sistemas de información



Cooperación Portugal-España



aicep Portugal Global





Gracias
por su atención