JOMCAL XII Jornadas de Modernización y Calidad en la Administración Local

Ciberseguridad, situación y retos

Miguel A. Amutio Gómez

Director de Planificación y Coordinación de Ciberseguridad
Secretaría General de Administración Digital
Ministerio para la Transformación Digital y de la Función Pública

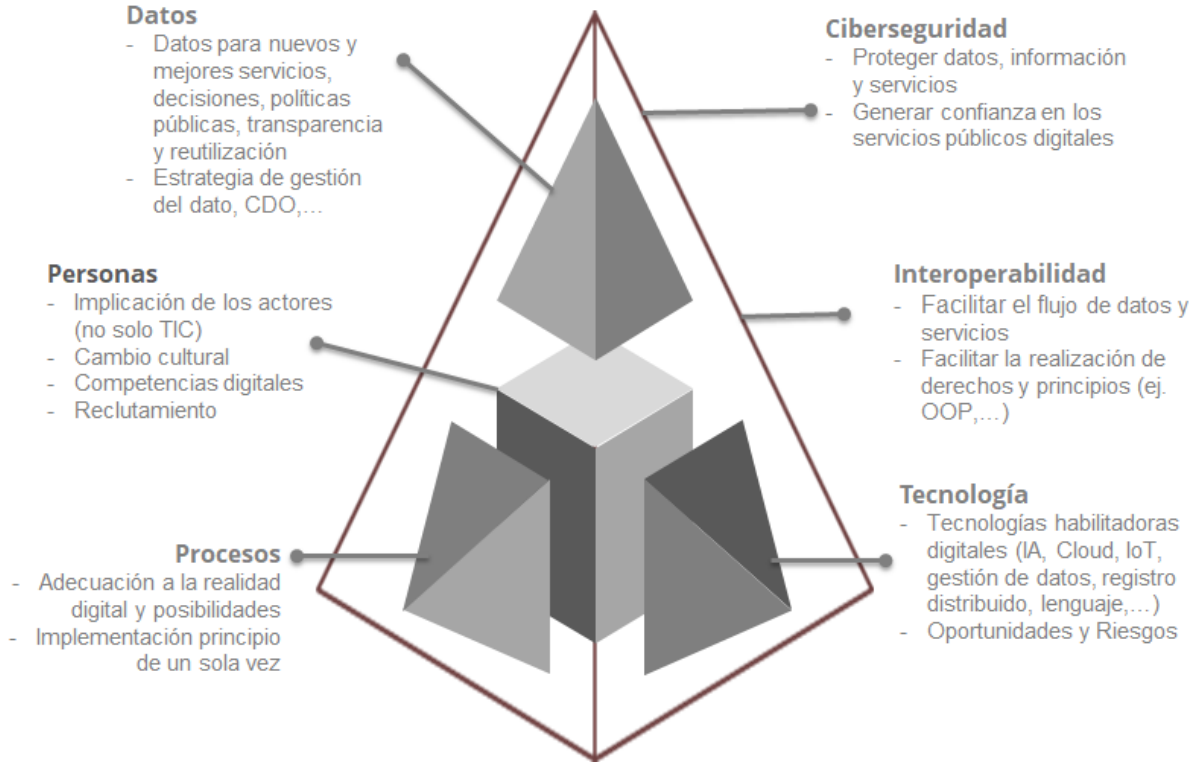
ORGANIZAN:

málaga | Ciudad de Málaga

FEMP FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

Plan de Formación Continua | FEMP

Transformación digital cibersegura



Mayor dependencia de la tecnología:
- ✓complejidad
- ✓interdependencia
- ✓ mayor superficie de exposición.

Los **ciberincidentes crecen** en frecuencia, alcance, sofisticación y severidad del impacto.

Provocan **daño y socavan la confianza** en el uso de las tecnologías.

La transformación digital ha de ir acompañada de **robustez en ciberseguridad.**

+ Contexto de derechos fundamentales y valores democráticos de nuestra sociedad

Fuente gráfico: Miguel A. Amutio. parte de la pirámide de Gartner intervenida para reubicar a las personas en el centro, añadiéndose las leyendas y el contexto de derechos y valores compartidos, con apoyo de edición del equipo de CCN-CERT.

En el punto de mira de los ciberataques

Administración Pública, el sector más atacado (~19%), seguido de personas objetivo (~11%), salud (~8%), infraestructura digital (~7%) y manufactura, finanzas y transporte. Fuente: ENISA Threat Landscape 2023

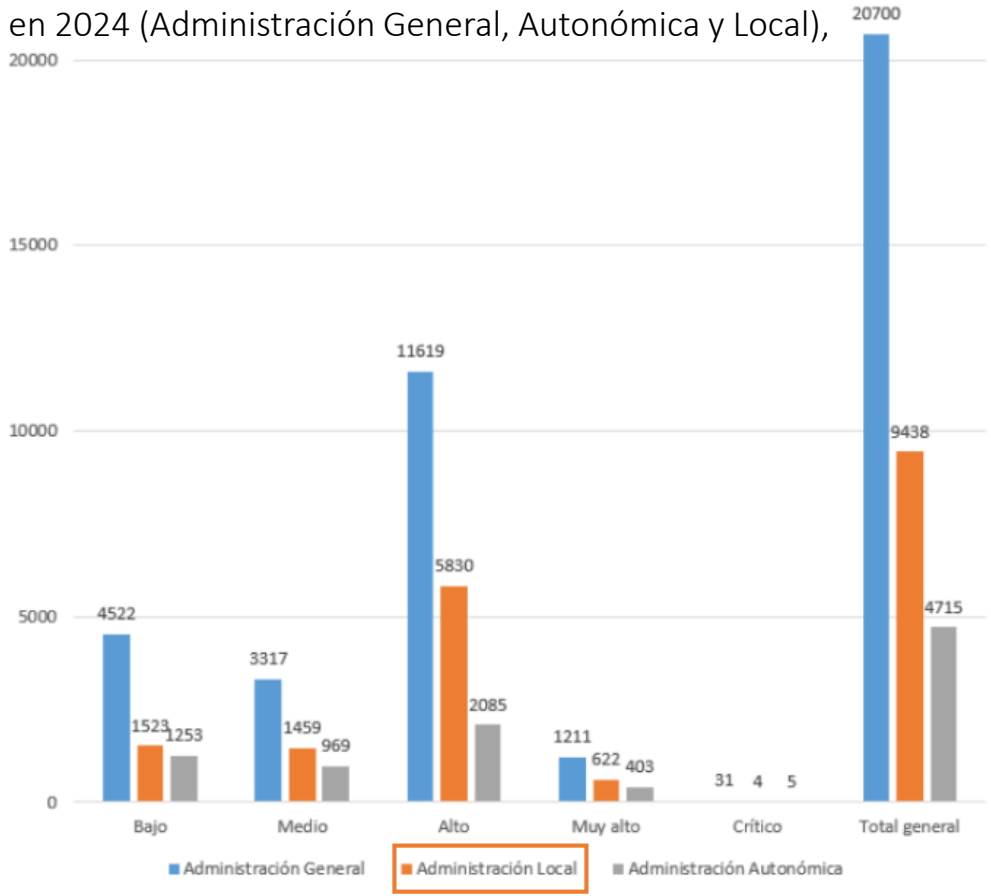
Orientados a la información
- Robo o sustracción de datos (con o sin revelación)
- Destrucción (incluyendo el cifrado irrecuperable de datos y documentos)
- Alteración, manipulación (incluyendo el fraude por inserción de documentos falsos)

Orientados a los servicios
- Quiebra en la disponibilidad de los servicios y en el acceso a la información

Combinados, a la información y a los servicios

Impacto
- Ejercicio de derechos y libertades; cumplimiento de deberes
- Normal desenvolvimiento de la sociedad, instituciones, empresas y ciudadanía
- Esfuerzo de recuperación ante incidentes (coste)
- Esfuerzo de comunicación y Daño reputacional

Peligrosidad de los incidentes gestionados por el CCN-CERT en 2024 (Administración General, Autonómica y Local),



Panorama de amenazas y medidas

1. Ransomware
2. Malware
3. Amenazas de ingeniería social
4. Amenazas a los datos
5. Amenazas contra la disponibilidad de los servicios
6. Amenazas contra la disponibilidad de internet
7. Manipulación de la información e interferencia
8. Ataques contra la cadena de suministro

Fuente: ENISA Threat Landscape 2023

Intensificación de las ciberamenazas y ciberincidentes

Avance de las tecnologías

- ✓ Mayor demanda de **gobernanza**, coordinación, cooperación
- ✓ Desarrollo de **capacidades conjuntas** y de interconexión
- ✓ Requisitos evolutivos y crecientes: **adaptación permanente**

Para hacer frente a estas amenazas :

- ✓ Aplicación del ENS (Sector Público, proveedores, cadena de suministro)
- ✓ Despliegue de capacidades de ciberseguridad (AGE, CCAA, EELL)
- ✓ Atención a medidas con impacto práctico: doble factor de antenticacion, EDR, Anti-ransomware, parches de seguridad, vigilancia continua

ens Esquema Nacional de Seguridad

ccns Centro de Operaciones de Ciberseguridad

Red Nacional de SOC

Foco en ejecución del Plan de Recuperación, Transformación y Resiliencia, PRTR

Un esfuerzo colectivo sostenido en el tiempo

- ✓ El largo camino…
- ✓ Esfuerzo colectivo, multidisciplinar y continuado en el tiempo

1992 - 2006

Ley 30/1992 PAC
RD 263/1996
Ley 59/2003 Firma electrónica

2007 - 2014

Ley 11/2007
RD 1671/2009
RD 3/2010 ENS
RD 4/2010 ENI
Normas Técnicas de Interoperabilidad
Reglamento 910/2014 eIDAS
Estrategia de Ciberseguridad Nacional 2013

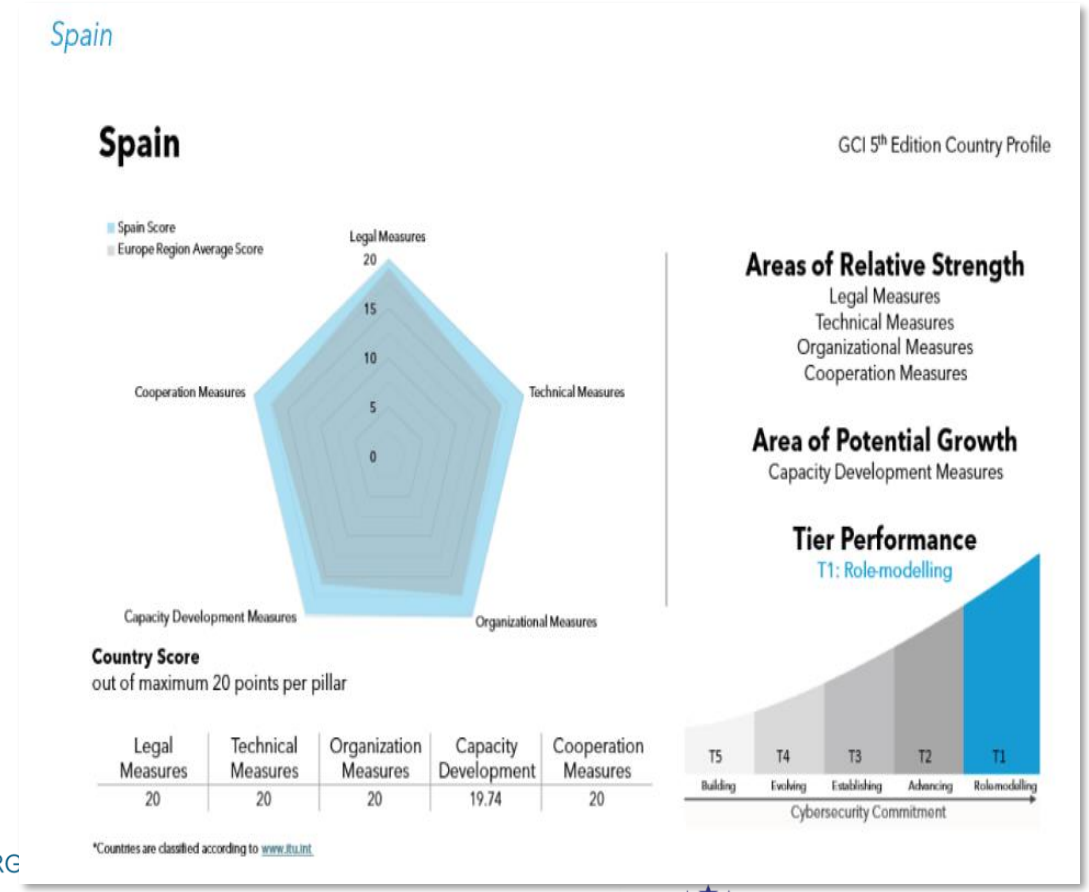
2015 - 2019

Ley 39/2015
Ley 40/2015
Declaración de Servicios Compartidos
RGPD
LO 3/2018 LOPDGDD
Actualización del ENS (RD 951/2015)
Instrucciones Técnicas de Seguridad
Directiva NIS
RDL 12/2018 Transposición NIS
Reglamento Single Digital Gateway
Estrategia Nacional de Ciberseguridad 2019

2020 - 2025

PRTR
España Digital 2025
Plan de Digitalización AAPP
Carta de Derechos Digitales
Declaración Europea sobre los Derechos
RD 203/2021
RD 43/2021 (Desarrollo RDL 12/2018)
RD 311/2022 ENS
EU Digital Strategy
EU Cybersecurity Package
Directiva 2022/2555 **NIS2**
Reglamento 2022/2554 DORA
Directiva 2022/2557 CER
Reglamento Europa interoperable
Reglamento eIDAS2
Reglamento de Inteligencia artificial
Reglamento ciberseguridad instituciones EU
Esquema Europeo de Ciberseguridad - EUCC

Índice Global de Ciberseguridad 2024



Global Cybersecurity Index 2024, ITU - Publicado el 12.09.2024

España en el nivel 1 (T1).

Puntúa prácticamente al máximo en los 5 **pilares** medidos por Índice.

Se posiciona **por encima de la media de la UE**.

Esquema Nacional de Seguridad

Base legal

- ✓Real Decreto 3/2010
- ✓Actualizado en 2015
- ✓**Real Decreto 311/2022**
- ✓Anclado en leyes 40/2015 y 39/2015
- ✓ + Instrucciones Técnicas de Seguridad

Ámbito de aplicación

- ✓Sector Público
- ✓Información clasificada
- ✓Proveedores

Referente

- ✓ Ley Orgánica 3/2018
- ✓ RD-l 12/2018 Real Decreto 43/2021

4 ITS publicadas

- ✓ Informe estado de la seguridad
- ✓ Conformidad con el ENS
- ✓ Auditoría
- ✓ Notificación de incidentes

Conformidad

- ✓Acreditación con ENAC
- ✓ Certificadores acreditados por ENAC
- ✓ Entidades certificadas (públicas/privadas)
- ✓ Consejo de Certificación del ENS (CoCENS)

Perfiles de Cumplimiento

- ✓ > 12 Perfiles:
  - Entidades Locales
  - Entornos Cloud
  - Organismos pagadores…

Soporte

- ✓ >100 **guías** CCN-STIC Serie 800
- ✓ 23 **Soluciones de** ciberseguridad

Monitorización - Informe INES

- ✓ 9 ediciones del informe INES

Esfuerzo colectivo, multidisciplinar, sostenido en el tiempo + liderazgo conjunto de:

ENS: Respuesta a necesidades específicas

Foto de Claudio Schwarz en Unsplash

Perfiles de Cumplimiento Específicos: conjunto de medidas de seguridad que, resultando del análisis de riesgos, resulten idóneas…

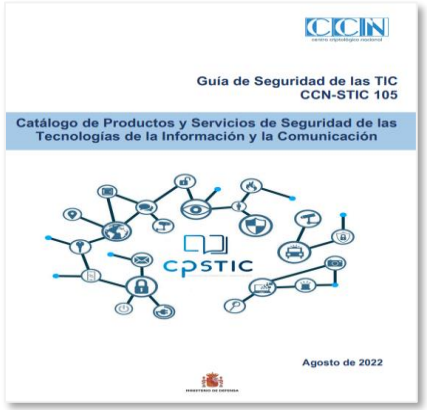
Persiguen introducir la capacidad de **ajustar los requisitos del ENS a necesidades específicas de determinados**

- Colectivos: **Entidades Locales,** Universidades, Organismos Pagadores,…
- Ámbitos tecnológicos: servicios en la nube,

Ej.:

- ✓ CCN-STIC 883A Perfil de Cumplimiento Específico Ayuntamientos pequeños (< 5.000 habitantes)
- ✓ CCN-STIC 883B Perfil Cumplimiento Específico Ayuntamientos de menos de 20.000 habitantes
- ✓ CCN-STIC 883C Perfil de Cumplimiento Específico Ayuntamientos de entre 20.000 y 75.000 habitantes
- ✓ CCN-STIC 883D Perfil de Cumplimento Específico Diputaciones
- ✓ CCN-STIC-891 PCE para Salud Prestación sanitaria a pacientes
- ✓ CCN-STIC-892 PCE para organizaciones en el ámbito de aplicación de la Directiva NIS2
- ✓ CCN- SITC-893 PCE – Requisitos intermedios de seguridad
- ✓ …

ENS: Productos y servicios de seguridad



ENS, art. 19: Uso de productos certificados conforme al principio de proporcionalidad.

ENS, [op.pl.5]: Se utilizará el Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC).

CPSTIC, productos de referencia cuyas medidas de seguridad han sido verificadas y certificadas:

- Aprobados (para manejo de información clasificada);
- Cualificados (para ámbito ENS).

Los instrumentos de contratación centralizada se refieren al ENS

ej. SISTEMA DINÁMICO DE ADQUISICIÓN DE SUMINISTRO DE SOFTWARE DE SISTEMA, DESARROLLO Y APLICACIÓN (SDA 25/2022)

Las especificaciones para las adquisiciones incluyen:

- Requisitos de Seguridad
- Cómo demostrar el cumplimiento de los requisitos de seguridad mediante referencias a:
  - Conformidad con el Esquema Nacional de Seguridad (ENS)
  - Catálogo de Productos y Servicios de Seguridad de las Tecnologías de la Información y Comunicación (CPSTIC) o equivalente
  - Referencia a esquemas de certificación europeos (EUCC, EUCS).

ENS: Demostrar la conformidad

Los sujetos responsables de los sistemas de información darán publicidad a las declaraciones y certificaciones de conformidad con el ENS.

Entidades del Sector Público, **prestadores de servicios o proveedores de soluciones:** mismos procedimientos y documentos.

Certificación de Conformidad

de aplicación **obligatoria** a sistemas de información de categoría **Media o Alta** y **voluntaria** en categoría **Básica**.
Auditoría para la certificación.

Declaración de Conformidad

de aplicación a sistemas de información de categoría **Básica**.
Autoevaluación para la declaración.

Entidades de certificación:

Acreditación por ENAC Entidad Nacional de Acreditación **conforme a** UNE-EN ISO/IEC 17065:2012, para certificación de sistemas del ámbito de aplicación del **ENS**.

Distintivos

Directiva NIS2: Obligaciones para entidades

AA.PP. en el ámbito de aplicación de NIS2**:** entidades de AGE, CCAA; **a determinar EELL**.

Obligaciones principales para las entidades en su ámbito**:**

Gobernanza
Responsabilidad de órganos de gestión

Notificación de incidentes con impacto significativo

Utilización de esquemas europeos de certificación de la ciberseguridad

Intercambio voluntario de información

Medidas para la gestión de riesgos de ciberseguridad

- **Políticas de seguridad**
- **Gestión de incidentes (prevención, detección y respuesta)**
- **Continuidad de las actividades**
- **Seguridad de la cadena de suministro**
- **Seguridad en adquisición, desarrollo y mantenimiento** de redes y sistemas. Cadena de suministro
- Políticas y procedimientos para **evaluar la eficacia de las medidas**.
- **Prácticas básicas de ciberhigiene y formación** en ciberseguridad.
- Políticas y procedimientos relativos a **criptografía y de cifrado**
- **Seguridad de recursos humanos**, …
- Vulnerabilidades específicas de proveedor y prestador servicios.

Directiva NIS2: ENS facilitador para Sector Público y proveedores

ens Esquema Nacional de Seguridad

Posiciona a España en condición favorable para implementar NIS2 de forma ágil, eficaz y eficiente.

- ✓ **Compatible** con NIS2.
- ✓ **Satisface las medidas para la gestión de riesgos** de ciberseguridad previstos en el artículo 21 de NIS2.
- ✓ **Flexibilidad** para su aplicación gracias a los **Perfiles de Cumplimiento Específicos – PCE NIS2**
- ✓ **Conformidad con ENS** en colaboración con ENAC.
- ✓ **+ Capacidades de ciberseguridad** que facilitan la notificación y el intercambio de información de ciberamenazas y ciberincidentes

Qué retos tenemos por delante

1. Un **marco legal** crecientemente exigente.
2. Más **capacidades de ciberseguridad** adaptadas a las tendencias de ciberamenazas y ciberataques.
3. **Gobernanza** de la ciberseguridad: **responsable de la seguridad** adecuadamente ubicado en la estructura y con recursos humanos cualificados y dotación presupuestaria.
4. **Medir la ciberseguridad**: ¿funciona?, ¿mejoramos?, ¿cumplimos?
5. **Impacto de la Inteligencia Artificial**: uso dual.
6. …

Qué esperamos por vuestra parte


Foto de Annie Spratt en Unsplash

1. Que seáis **partícipes y agentes activos de la ciberseguridad**, para contribuir a la defensa frente a las ciberamenazas y los ciberataques.
2. Si trabajáis para el Sector Público (directa o indirectamente), **vuestra colaboración para la aplicación del ENS** y la gobernanza de la ciberseguridad.
3. Vuestra **colaboración en la implantación de las capacidades de ciberseguridad**.

Muchas gracias

Miguel A. Amutio Gómez

Director de Planificación y Coordinación de Ciberseguridad
Secretaría General de Administración Digital
Ministerio para la Transformación Digital y de la Función Pública