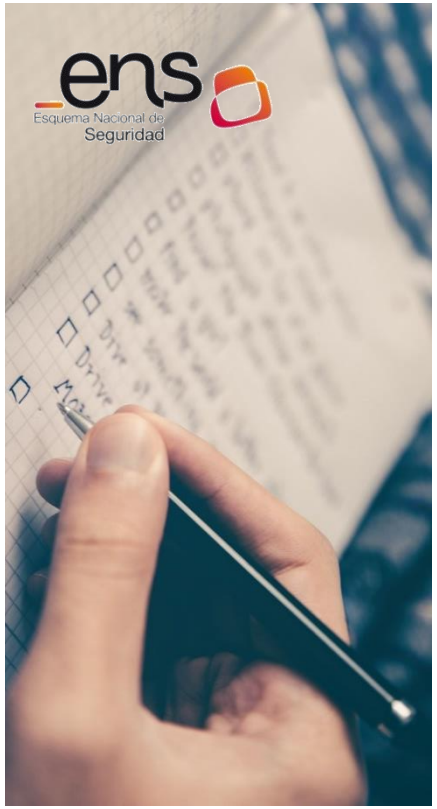
ENS y Gobernanza de la Ciberseguridad

CENTRO CRIPTOLÓGICO NACIONAL

ORGANIZAN:
málaga | Ciudad de Málaga
FEMP FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS
Plan de Formación Continua | FEMP

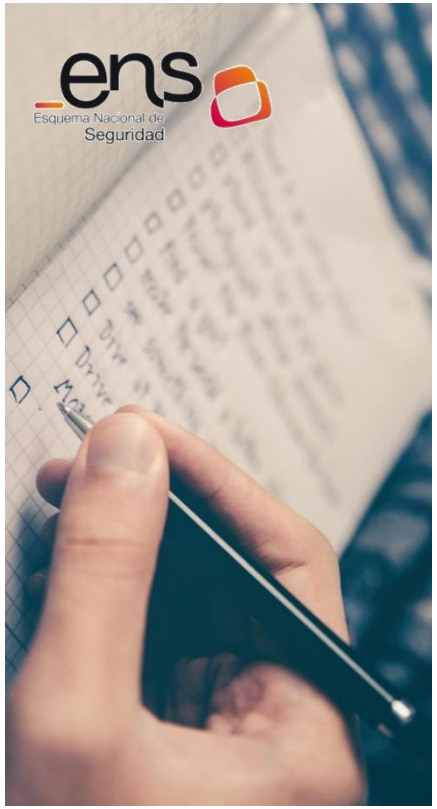
Esquema Nacional de Seguridad (ENS)



- El **Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad**, proporciona un marco normativo fundamentado en unos **principios básicos** de seguridad para los sistemas de información.
- De obligado cumplimiento para **todo el Sector Público** y para las entidades del **Sector Privado que presten servicio a las entidades del Sector Público**.
- Los sistemas se **categorizan** como **BÁSICO**, **MEDIO** o **ALTO** conforme a la evaluación de las **dimensiones** de seguridad del sistema: **Confidencialidad**, **Integridad**, **Trazabilidad**, **Autenticidad** y **Disponibilidad**.
- Existencia **Perfiles de Cumplimiento Específicos** (PCE) para cubrir **necesidades comunes** o **especiales** (PCE-RES, PCE-Sector Salud, PCE-NIS2, etc).
- Elaboración del **Informe Nacional del Estado de Seguridad (INES)** a partir de los datos recogidos en la plataforma y regulados en el ENS.

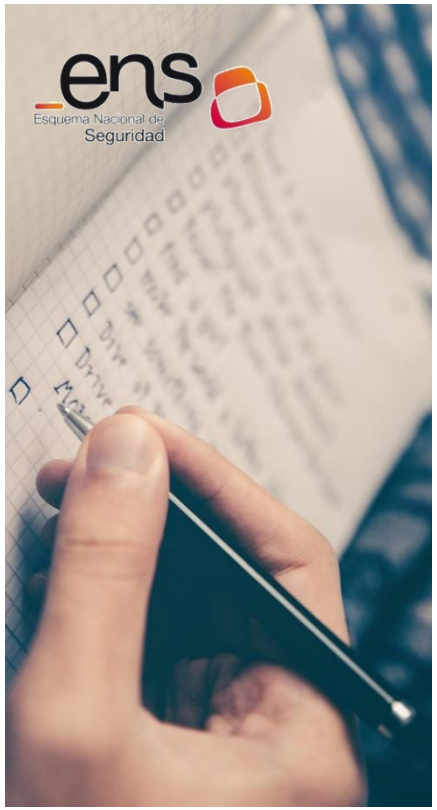
Composición ENS

¿Por qué el ENS?



- Crear las **CONDICIONES NECESARIAS DE CONFIANZA** en el uso de los medios electrónicos, a través de **medidas** para garantizar la **seguridad,** que permita a los ciudadanos y a las AA.PP., **el ejercicio de derechos y el cumplimiento de deberes** a través de estos medios.
- Promover la **GESTIÓN CONTINUADA DE LA SEGURIDAD**, al margen de impulsos puntuales, o de su ausencia.
- Contemplar los aspectos de **PREVENCIÓN**, **DETECCIÓN** y **RESPUESTA**.
- Promover un **TRATAMIENTO HOMOGÉNEO** de la seguridad que facilite la cooperación cuando participan diversas entidades, mediante **lenguaje y elementos comunes**, para facilitar la implementación de medidas, la interacción entre AA.PP. y la comunicación de requisitos de seguridad a la industria.
- Proporcionar **liderazgo** en materia de **BUENAS PRÁCTICAS**.

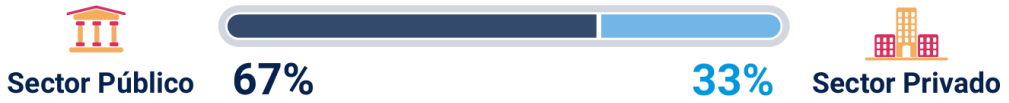
¿Por qué el ENS?



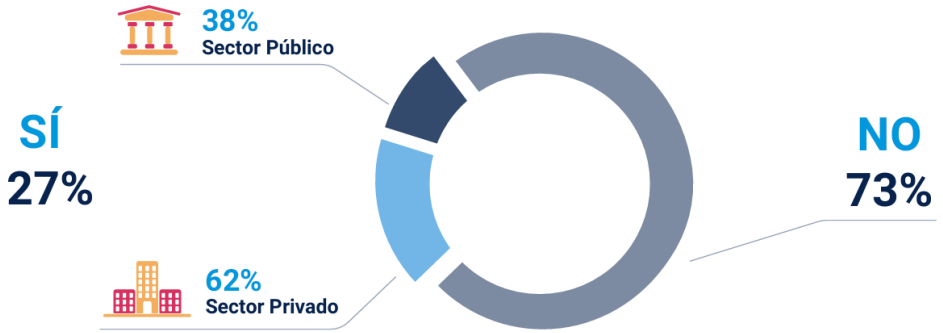
74%
ENCUESTADOS

CONSIDERA QUE EL ENS HA MEJORADO LA CIBERSEGURIDAD DE SU ORGANIZACIÓN.

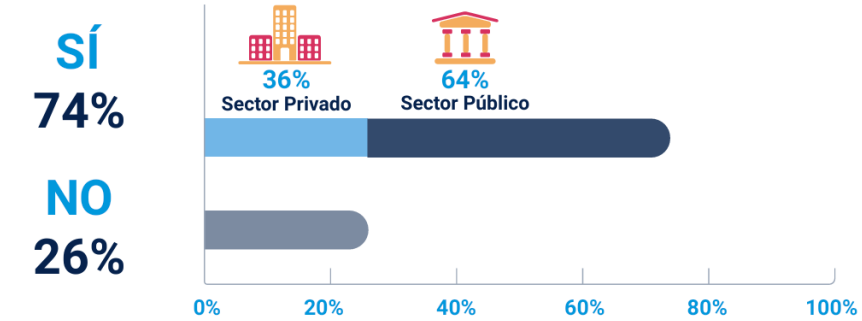
1.633
PARTICIPANTES



¿DISPONÍA SU ORGANIZACIÓN DE ALGUNA CERTIFICACIÓN PREVIA AL ENS?



¿HA MEJORADO EL ENS LA CIBERSEGURIDAD DE SU ORGANIZACIÓN?



ORGANIZAN:

málaga | Ciudad de Málaga

FEMP
FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

Plan de Formación Continua FEMP

Conformidad con el ENS

Sector Público

Sector Privado

Adecuación al ENS

Entidades de Certificación

Órganos de Auditoría Técnica

Entidades de Certificación

Auditoría de Conformidad con ENS

Certificado

Amenazas Entidades Locales

Mecanismos adecuados de acceso a los sistemas y a la información

Inventario de activos

Proteger la navegación

Proteger el correo electrónico

VPN y 2FA

MicroClaudia + A-V de nueva generación

Bastionado y mantenimiento (parcheado)

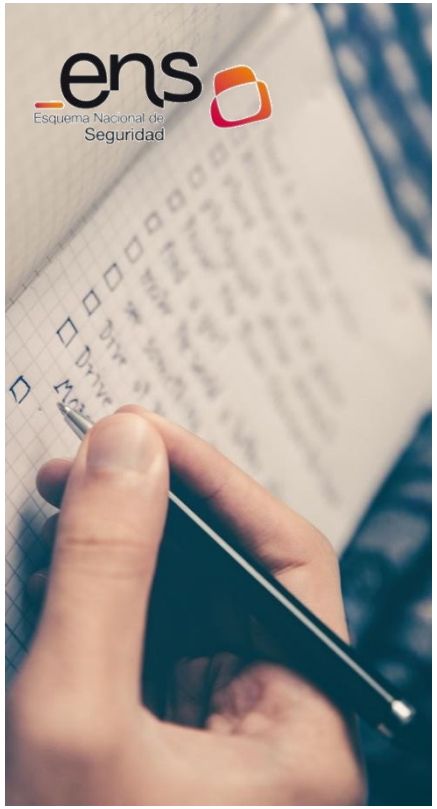
Aislamiento

Concienciación en ciberseguridad

Aislar equipos, recuperación (copias de seguridad) investigación(logs)

Cifrado y control del dato

Perfil de Cumplimiento Específico (PCE)



- Permiten alcanzar una **adaptación** al **ENS** más **eficiente**, racionalizando los recursos requeridos sin menoscabo de la protección perseguida y exigible.
- Definen una **postura de seguridad, en base a los riesgos** a los que están expuestos determinados colectivos de entidades o determinados ámbitos tecnológicos.
- El **Centro Criptológico Nacional**, en el ejercicio de sus competencias, **validará y publicará** los correspondientes **Perfiles de Cumplimiento** que se determinen para garantizar la seguridad de los sistemas de tecnologías de la información en las entidades del Sector Público.

	Declaración de Aplicabilidad Inicial			Perfil de Cumplimiento		
	Medida de seguridad	Aplica	Nivel de exigencia	Medida de seguridad	Aplica	Nivel de exigencia
→	[op.ext.2]	Aplica	Alto	[op.ext.2]	Aplica	Medio
→	[op.cont.1]	Aplica	Alto	[op.cont.1]	No Aplica	No aplica
→	[mp.if.4]	Aplica	Bajo	[mp.if.4]	Aplica	Alto
→	[mp.if.7]	No Aplica	No Aplica	[mp.if.7]	Aplica	Alto
→	[mp.if.9]	Aplica	Alto	[mp.if.9]	Aplica	Compensada
	[mp.exp.1]	Aplica	Alto	[mp.exp.1]	Aplica	Alto

CCN VALIDADO

Aplicabilidad ENS en Entidades Locales: PCE-RES y PCE-EELL

PCE-RES

Guía de Seguridad de las TIC CCN-STIC 890A

Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad (Entidades Locales)

< 5000 habitantes

Guía de Seguridad de las TIC CCN-STIC 883

Anexo I. Plan de Adecuación al ENS Ayuntamientos <20.000 habitantes

5000 < habitantes < 20000

Guía de Seguridad de las TIC CCN-STIC 883

Anexo II. Plan de Adecuación al ENS 20.000>Ayuntamientos <75.000 (habitantes)

20000 < habitantes < 75000

Guía de Seguridad de las TIC CCN-STIC 883

Anexo III. Plan de Adecuación al ENS Diputaciones, Cabildos, Consejos Insulares y órganos competentes equivalentes

PCE-RES	PCE-EELL < 20000	PCE-EELL 20000 < x < 75000 Diputaciones
35	48	64

ENS Cat. BÁSICA	ENS Cat. MEDIA
56	68

Aplicabilidad de controles conforme a los Perfiles de Cumplimiento Específicos de EELL		PCE-RES <5.000 hab.	PCE-EELL - CCN-STIC-883 < 20.000 hab.	PCE-EELL - CCN-STIC-883 >20.000 hab. Diputaciones
Control	Medidas Anexo II	Aplicación	Aplicación	Aplicación
[org]	Marco organizativo	BAJO	MEDIO	MEDIO
[op]	Marco operacional	BAJO	MEDIO	MEDIO
[mp]	Medidas de protección	n/a o BAJO	MEDIO	MEDIO
[op.acc.7]	Acceso remoto	MEDIO	MEDIO	MEDIO
[op.exp.5]	Gestión de cambios	n/a	n/a	MEDIO
[op.exp.7]	Gestión de incidentes	MEDIO	MEDIO	MEDIO
[mp.com.2]	Protección de la confidencialidad	MEDIO	MEDIO	MEDIO
[mp.com.4]	Segregación de redes	n/a	ALTO	ALTO

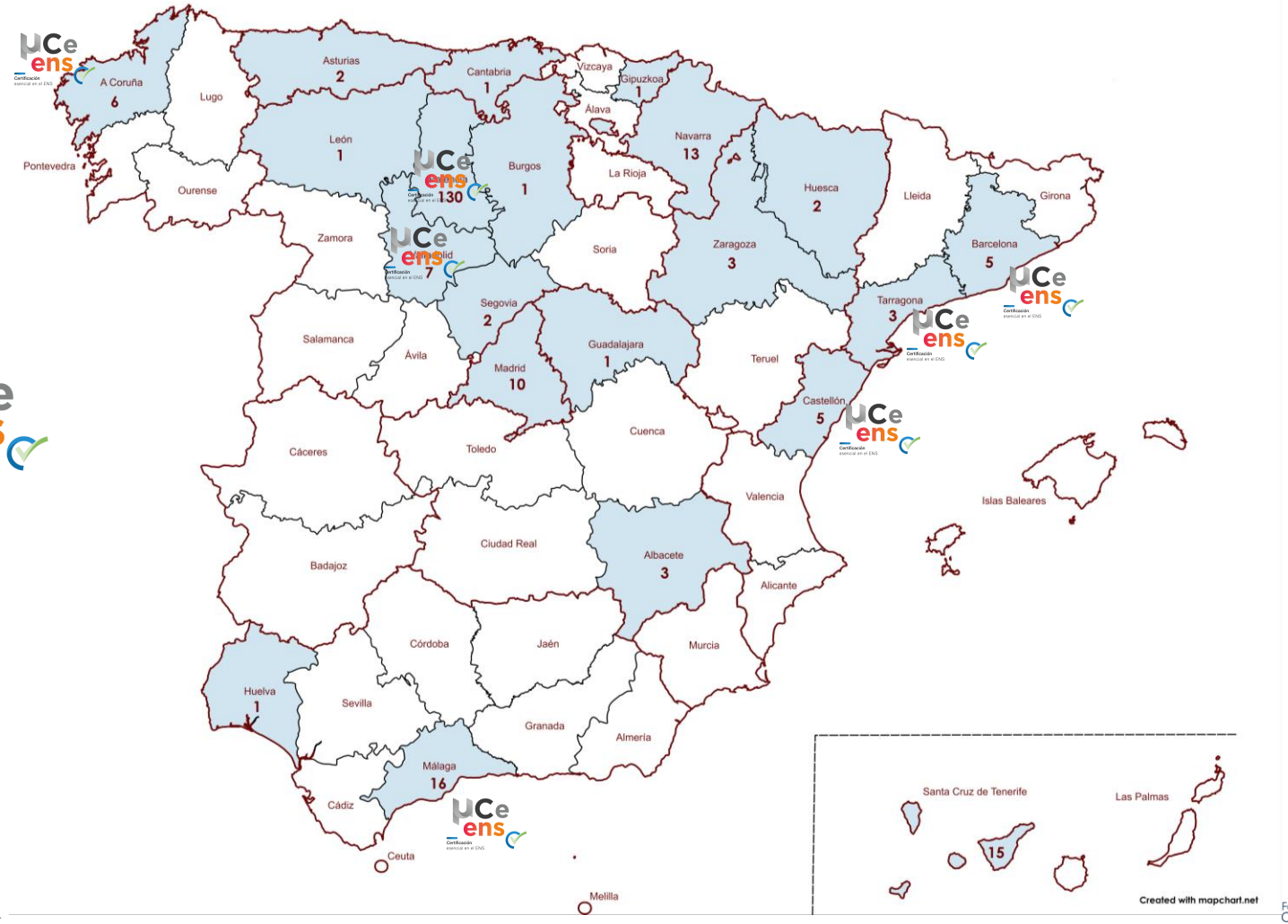
Entidades Locales Certificadas en el ENS

PCE-RES - CCN-STIC-890 A

178 sistemas certificados

PCE-EELL- CCN-STIC-883

50 sistemas certificados



Metodología µCeENS

µCeENS: Es el **proceso completo** para obtener la **certificación de Conformidad** en el ENS para **Categoría BÁSICA**, conforme a los **Requisitos Esenciales de Seguridad** definidos en el **Perfil de Cumplimiento Específico de Requisitos Esenciales** PCE-RES

µCe ens
Certificación esencial en el ENS

ORGANIZAN:

málaga | Ciudad de Málaga

FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

Plan de Formación Continua FEMP

µCeENS: Automatización en Gobernanza

Si se da de alta un Sistema con µCeENS :

1. Rellenar Cuestionario ENS.
2. Aparecen completados tanto el Plan de Adecuación como la Implantación.
   - Se cargará automáticamente el Plan de Adecuación con los Servicios y el perfil de cumplimiento de Requisitos Esenciales de seguridad
   - Documentación de seguridad rellena (a falta de revisión de datos) y medidas implementadas.
3. Solicitar Certificación de Conformidad.
4. El CCN revisará y validará el proceso, para expedir el correspondiente Certificado de Conformidad para categoría BÁSICA, en base al Perfil de Cumplimiento Específico para Requisitos Esenciales de seguridad.

µCeENS: Automatización en Gobernanza – Plan de Adecuación

Metodología µCeENS

- Requisitos Esenciales de Seguridad descritos en el Perfil de Cumplimiento Específico **PCE-RES**
- Se realiza una **Auditoría por una Entidad de Certificación** (conforme con ITS e IC-01-19):
  - El equipo auditor requiere y obtiene las evidencias pertinentes y verifica los criterios de auditoría (no equiparable a una Autoevaluación).
  - Interviene el Centro Criptológico Nacional como Entidad de Certificación.
  - Revisión documental y toma de evidencias.
  - Automatización de procesos en Gobernanza con INES y AMPARO
  - Sujeta a una inspección o visita.
- Dedicarle **un apartado específico en el Portal del ENS**.

µCe ens Certificación esencial en el ENS

Directiva NIS2

- Proporciona **MEDIDAS LEGALES** para impulsar el nivel general de **CIBERSEGURIDAD** en la UE y la resiliencia de las **infraestructuras críticas** y de los servicios digitales en Europa.
- El Centro Criptológico Nacional (CCN) ha publicado la guía **CCN-STIC 892** que corresponde al "*Perfil de Cumplimiento Especifico para organizaciones en el ámbito de aplicación de la Directiva NIS2 (**PCE-NIS2**)*".
- Amplia alcance en cuanto a sectores de aplicación, pero **no** contemplan grandes cambios respecto al ENS.
- Se señala que los Estados miembros podrán disponer que la presente Directiva se aplique a las **entidades de la Administración pública a nivel local**.
  - ENS sigue aplicando a EELL pequeñas.
  - EELL de gran población serían entidades esenciales.
  - EELL mayores de 20000 habitantes, sin ser de gran población, se considerarían importantes.

Directiva NIS2

¿QUÉ ENTIDADES DEL SECTOR PÚBLICO DEBEN CUMPLIR CON LA NIS2?

Entidades a las que les aplica el ens

Administración General del Estado (AGE)

Organismos dependientes o vinculados a la Administración General del Estado*

*Aplicación pendiente de trasposición al ordenamiento jurídico español

Administración autonómica

Administración local*

*Aplicación pendiente de trasposición al ordenamiento jurídico español

Entidades del sector público que presten servicio a Administración General del Estado | Administración Autonómica | Administración local en:

Sectores alta criticidad | Entidades esenciales:

- **Energía** — Electricidad, calefacción y crudo, gas, hidrógeno
- **Transporte** — Aéreo, ferrocarril, marítimo, carretera
- **Banca**
- **Espacio**
- **Sanitario** — Asistencia, laboratorios
- **Agua Potable**
- **Agua Residuales**
- **Gestión de servicios TIC**
- **Infraestructura digital** — Servicios DNS, registros nombres de dominio, cloud, centro de datos, redes de contenidos, comunicaciones electrónicas
- **AAPP central y autonómica** — Exclusión del poder judicial, parlamento y banco central
- **Infraestructuras de los mercados financiaros**

Otros sectores críticos | Entidades importantes:

- **Químico**
- **Proveedores de servicios digitales**
- **Servicios postales y de mensajería**
- **Investigación**
- **Gestión de Residuos**
- **Alimentación**
- **Fabricación** — Productos sanitarios/informáticos/ eléctrico/maquinaria/transporte

Otros sectores no incluidos en los apartados anteriores*

*Aplicación pendiente de trasposición al ordenamiento jurídico español

ORGANIZAN:

málaga | Ciudad de Málaga

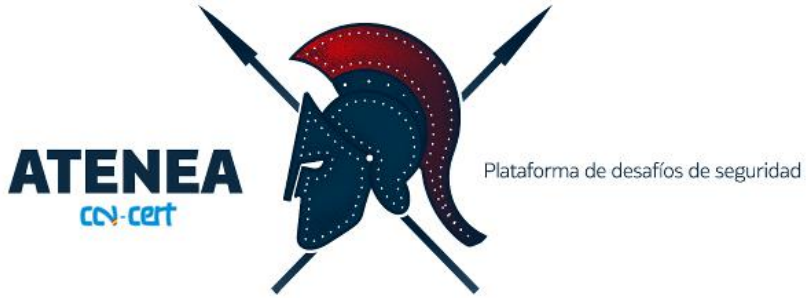
FEMP FEDERACION ESPAÑOLA DE MUNICIPIOS Y PROVINCIAS

Plan de Formación Continua FEMP

Plataforma de formación

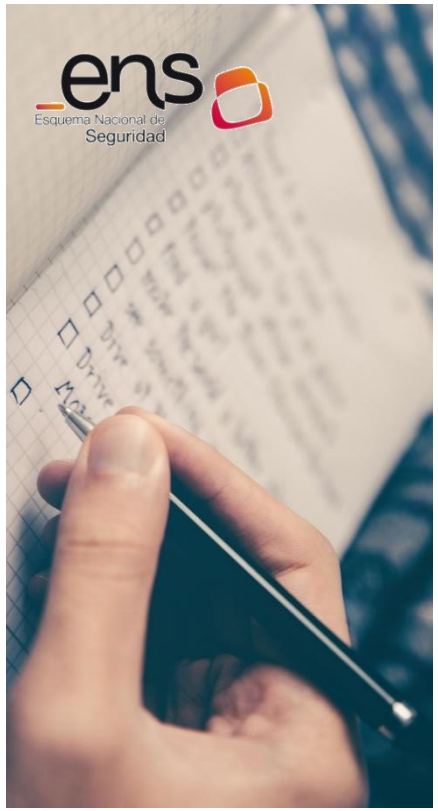
ángeles
Formación, capacitación y talento en ciberseguridad

- En **ÁNGELES** se encuentran disponibles **cursos online** para mejorar tu nivel de conocimiento en ciberseguridad.
  - Cursos generales
  - Cursos familiarización en ciberseguridad
  - Cursos capacitación ENS
  - Cursos especialización
  - Cursos ad-hoc
- Al mismo tiempo, los usuarios pueden visualizar **webinars** sobre ciberseguridad.



- En **ATENEA** podrás demostrar tu conocimiento y destreza ante diferentes **desafíos** de seguridad.
- Encontrarás retos de distinta dificultad y temáticas:
  - Criptografía y Esteganografía
  - Forense
  - Análisis de tráfico
  - Reversing
  - Hacking web
  - OSINT
  - Análisis de memoria
  - Básico: ransomware, red, telefonía móvil, correo electrónico, web

Conclusiones



- Los **Perfiles de Cumplimiento Específicos** y las **herramientas** desarrolladas por el **CCN** están facilitando la adecuación al **ENS** a las **Entidades Locales**.
- El **PCE-RES** ha **triplicado** en los 2 últimos años el número de **EELL** certificadas en el **ENS**.
- Los organismos certificados en **ENS** se encuentran más maduros para una futura certificación de la Directiva **NIS2**.

¡MUCHAS GRACIAS!

www.ccn.cni.es

www.ccn-cert.cni.es

oc.ccn.cni.es

ens.ccn.cni.es