

**XIII
JORNADAS
STIC
CCN-CERT**



10 AÑOS DEL ENS

**COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD**

#XIIIJORNADASCNCERT

Presentación XIII Jornadas



Miguel Ángel Amutio

Director de la División de
Planificación y Coordinación de
Ciberseguridad

Secretaría General de
Administración Digital



Pablo López

Jefe Área
Normativa y Servicios de
Ciberseguridad

Centro Criptológico Nacional

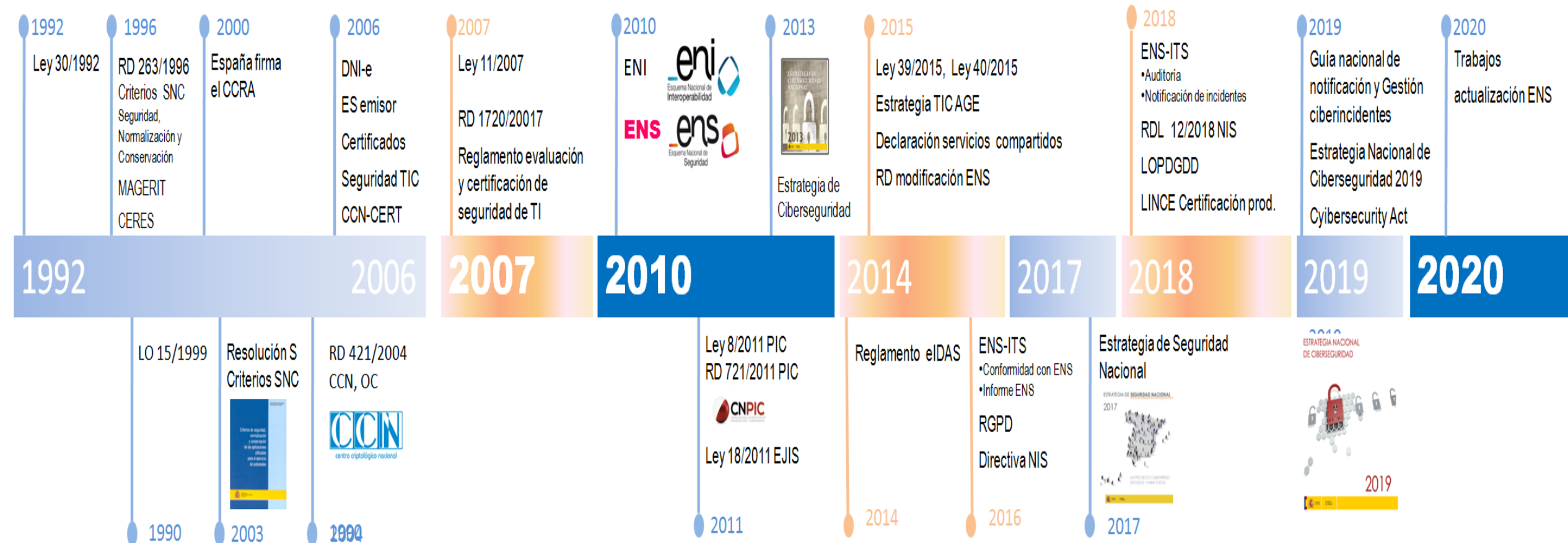
Índice

- 1. 10 años del ENS. Pasado, presente y futuro**
- 2. Actualizar el ENS**
- 3. Entorno de Validación ENS**
- 4. Conclusiones**

10 años del ens

Esquema Nacional de Seguridad

Un contexto en evolución



10 años del



Acciones de desarrollo

Actualizado en 2015

- ✓ Experiencia de aplicación
- ✓ Marco europeo (eIDAS)
- ✓ Escenario de ciberseguridad

Referente de **medidas de seguridad** para otros ámbitos /RGPD; ...)

Ámbito de aplicación



Extendido a todo el Sector Público
(leyes 39 y 40 de 2015)

4 ITS publicadas

- ✓ Informe
- ✓ Conformidad
- ✓ Auditoría
- ✓ Notificación de incidentes

Certificación de la conformidad

- ✓ Acreditación y certificación con ENAC
- ✓ Certificadores acreditados por ENAC (8)
- ✓ Entidades certificadas (públicas/privadas; >160)
- ✓ Consejo de Certificación del ENS (COCENS)



Informe INES

- ✓ 5 ediciones del informe INES
- ✓ 768 entidades en 2018, 30% que en 2017
- ✓ Actualmente, 6ª campaña



CCN-CERT

- ✓ 56 guías CCN- STIC de la serie 800.
- ✓ 14 soluciones de ciberseguridad

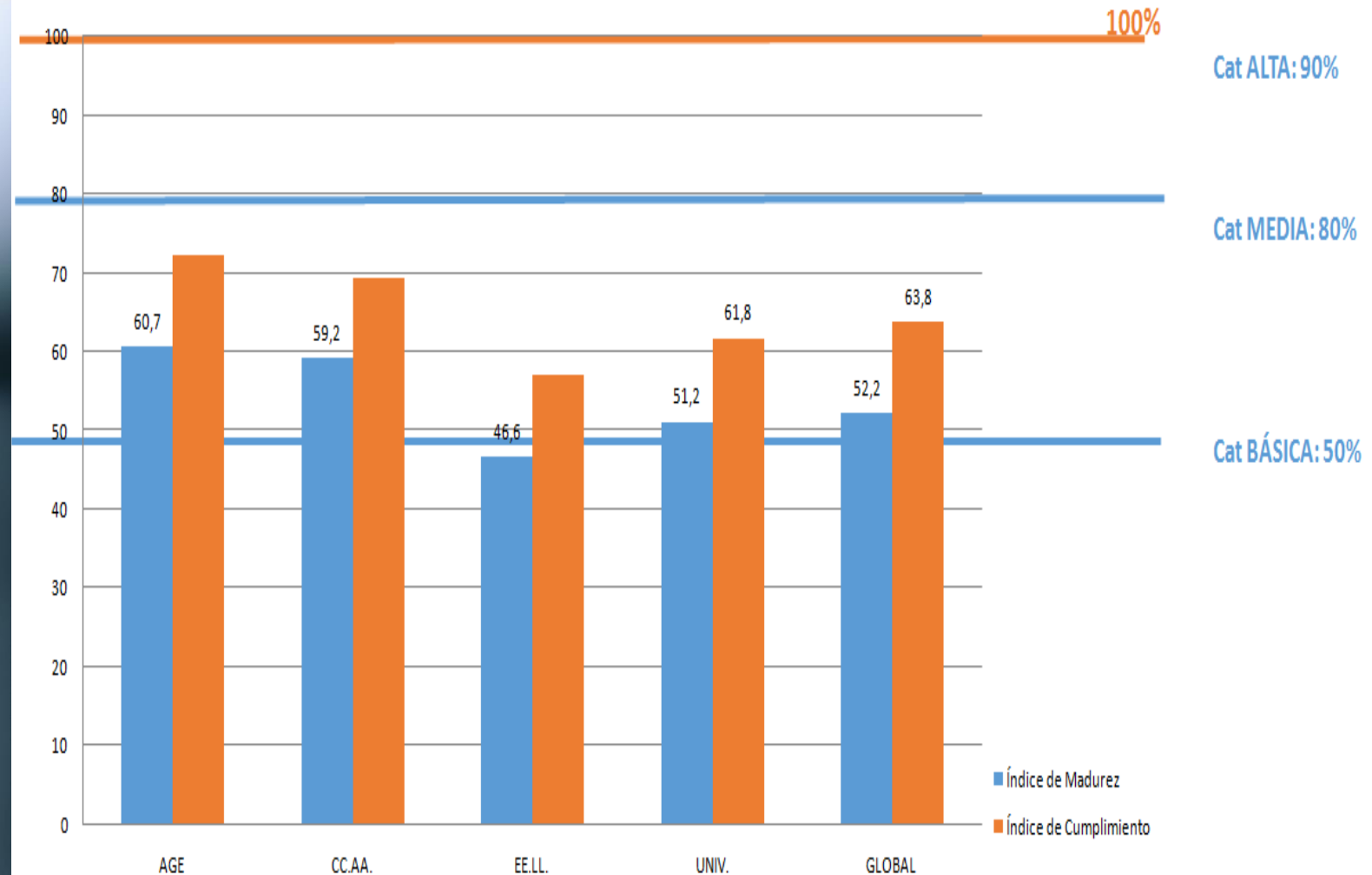


10 años del **ens**
Esquema Nacional de Seguridad

Resultados globales Informes INES 2018



Photo by [Kobu Agency](#) on [Unsplash](#)



Estrategia Nacional de Ciberseguridad

Contribuir al uso seguro y fiable del ciberespacio



OBJETIVOS DE LA ESTRATEGIA

OBJETIVO GENERAL

En línea con la Estrategia de Seguridad Nacional, España garantizará el uso seguro y fiable del ciberespacio, protegiendo los derechos y las libertades de los ciudadanos y promoviendo el progreso socio económico.



Objetivo

01

Seguridad y resiliencia de las redes y los sistemas de información y comunicaciones del sector público y de los servicios esenciales.



Objetivo

02

Uso seguro y fiable del ciberespacio frente a un uso ilícito o malicioso.



Objetivo

03

Protección del ecosistema empresarial y social de los ciudadanos.



Objetivo

04

Cultura y compromiso con la ciberseguridad y protección de las capacidades humanas y tecnológicas.



Objetivo

05

Seguridad del ciberespacio en el ámbito internacional.



Estrategia Nacional de Ciberseguridad

Contribuir al uso seguro y fiable del ciberespacio



LÍNEA DE ACCIÓN 2

Garantizar la seguridad y resiliencia de los activos estratégicos para España.

Esta línea de acción responde al Objetivo I de la Estrategia.

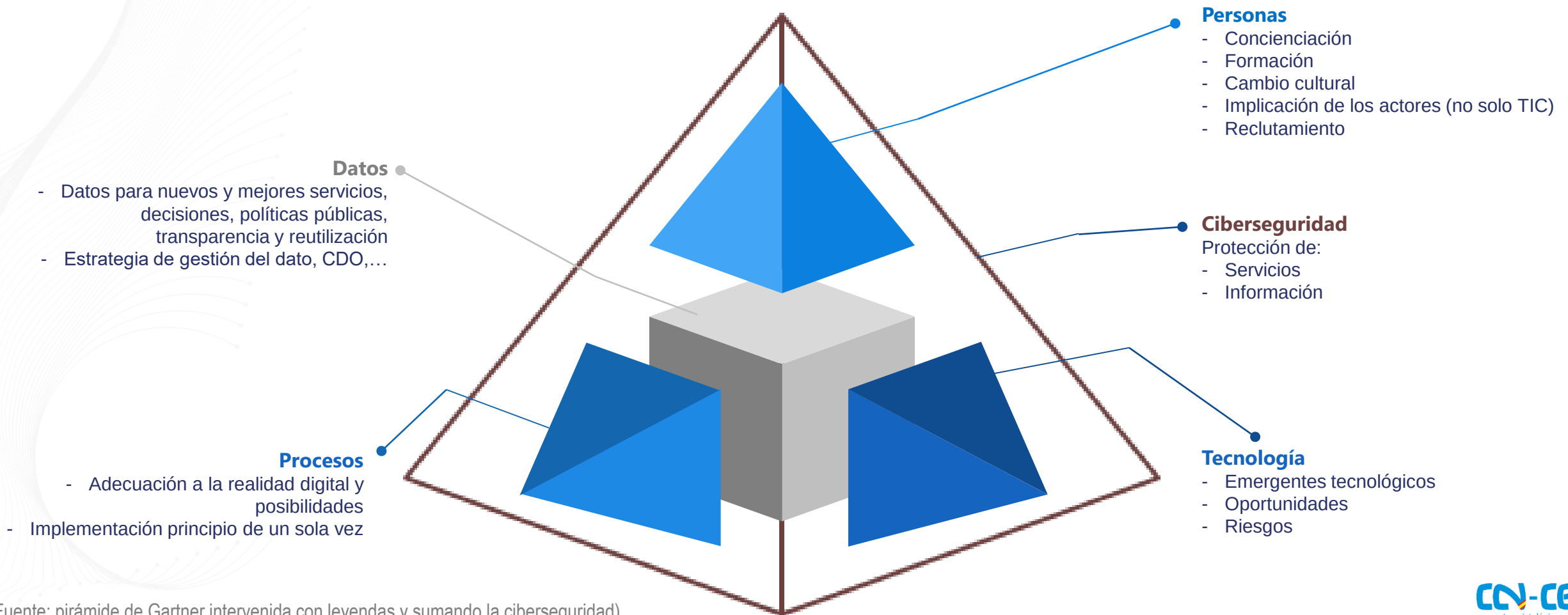
MEDIDAS

1. Ampliar y fortalecer las capacidades de prevención, detección, respuesta, recuperación y resiliencia a los ciberataques dirigidos al sector público, a los servicios esenciales y a empresas de interés estratégico.
2. Potenciar el desarrollo de la normativa sobre protección de infraestructuras críticas, reforzando la seguridad de las redes y sistemas de información que las soportan.
3. Asegurar la plena implantación del Esquema Nacional de Seguridad, del Sistema de Protección de las Infraestructuras Críticas, y el cumplimiento y armonización de la normativa sobre protección de infraestructuras críticas y servicios esenciales, con un enfoque prioritario basado en el riesgo.
4. Potenciar, en el marco de sus competencias, la progresiva implicación y creación de infraestructuras de ciberseguridad en las Comunidades Autónomas, las Ciudades Autónomas, las Entidades Locales y en sus organismos vinculados o dependientes que cooperarán y se coordinarán con las estructuras nacionales en pro de la mejora de la ciberseguridad nacional.
5. Desarrollar el Centro de Operaciones de Ciberseguridad de la Administración General del Estado que mejore las capacidades de prevención, detección y respuesta, e impulsar el desarrollo de centros de operaciones de ciberseguridad en el ámbito autonómico y local.
6. Reforzar la implantación de infraestructuras y servicios de telecomunicaciones y sistemas de información horizontales comunes, y compartidos por las Administraciones Públicas, potenciando su uso y sus capacidades de seguridad y resiliencia, asegurando a la par, la coordinación con los primeros en aquellos casos que no se utilicen las infraestructuras y servicios comunes.

-Siguen hasta la medida [12] -

Transformación digital

Personas, procesos, tecnología, datos y ciberseguridad





Transformación digital y evolución de la ciberseguridad



Photo by [Annie Spratt](#) on [Unsplash](#)



Alinear y mejorar el ENS

Para facilitar la seguridad en la Administración Digital.



Flexibilizar

Para facilitar la aplicación del ENS a necesidades específicas.



Actualizar

Para facilitar una mejor respuesta a las necesidades de ciberseguridad: reducir vulnerabilidades y promover la defensa activa

Actualizar el

Esquema Nacional de Seguridad

Aspectos a considerar



Photo by [Alex Perez](#) on [Unsplash](#)



Alinear y mejorar el ENS

Para facilitar la seguridad en la Administración Digital.



Actualizar referencias: Leyes 39 y 40/2015, RGPD, LO 3/2018...



Alinear con el contexto estratégico: ENCS 2019.



Mejorar el texto: clarificar, precisar, eliminar aspectos no necesarios o excesivos, homogeneizar, simplificar, o actualizar referencias.

Actualizar el

Esquema Nacional de Seguridad

Aspectos a considerar



Photo by [Claudio Schwarz](#) | [@purzlbaum](#) on [Unsplash](#)



Flexibilizar

Para facilitar la aplicación del ENS a necesidades específicas.



Introducir los **perfiles de cumplimiento** específicos, validados y adaptados a aquellas soluciones, tecnologías y entidades con necesidades especiales



Ejemplos: EE.LL., servicios en la nube



Opciones:

- Añadir o eliminar medidas
- Incluir medidas compensatorias
- Incrementar o decrementar el nivel de ciertas medidas



Redefinir ciertas medidas para mejor adaptación a los sistemas y equilibrio de seguridad y operatividad.

Actualizar el

Esquema Nacional de Seguridad

Aspectos a considerar



Photo by [You X Ventures](#) on [Unsplash](#)



Actualizar

Para facilitar una mejor respuesta a las necesidades y necesidades de ciberseguridad: reducir vulnerabilidades y promover la defensa activa.



Fuentes: experiencia, caudal de preguntas, input por canales formales e informales, informes INES, auditorías.



Revisión: principios básicos, requisitos mínimos, medidas de seguridad.

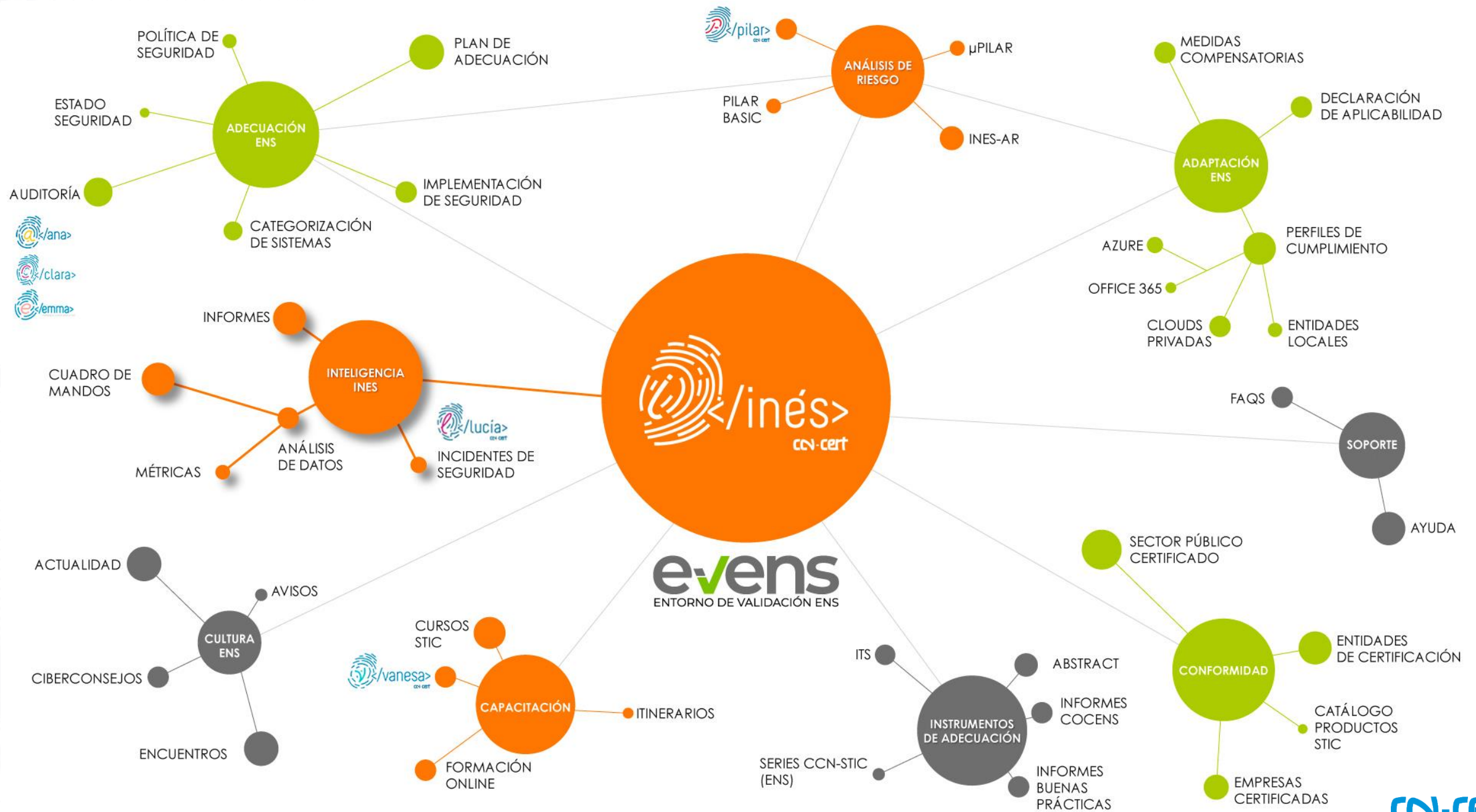


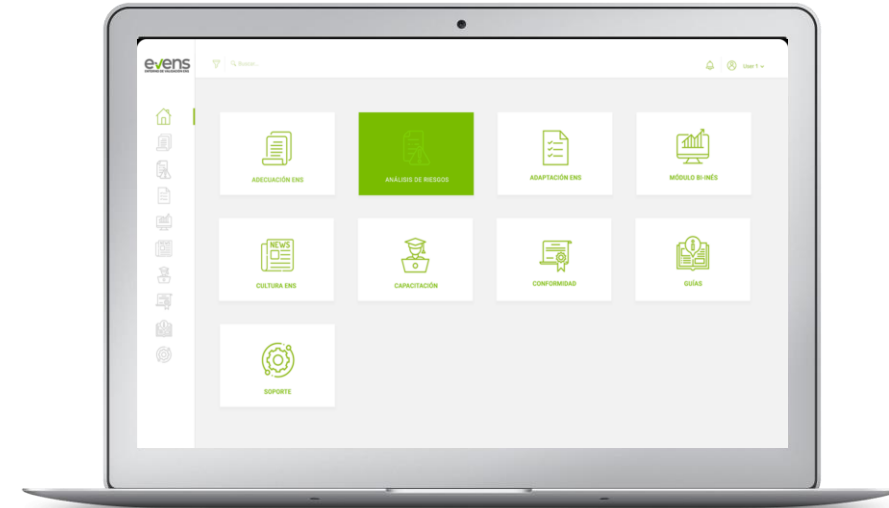
A considerar:

- Codificar las precisiones de las medidas de seguridad
- El concepto de “refuerzo” para fortalecer la seguridad de los sistemas y facilitar su implementación y auditoría
- Nuevas medidas: protección de datos, servicios en la nube, monitorización, protección de equipos
- Modificación en ciertas medidas: monitorización, comunicaciones, explotación
- También eliminación de algunas medidas.

La importancia de Medir la Seguridad



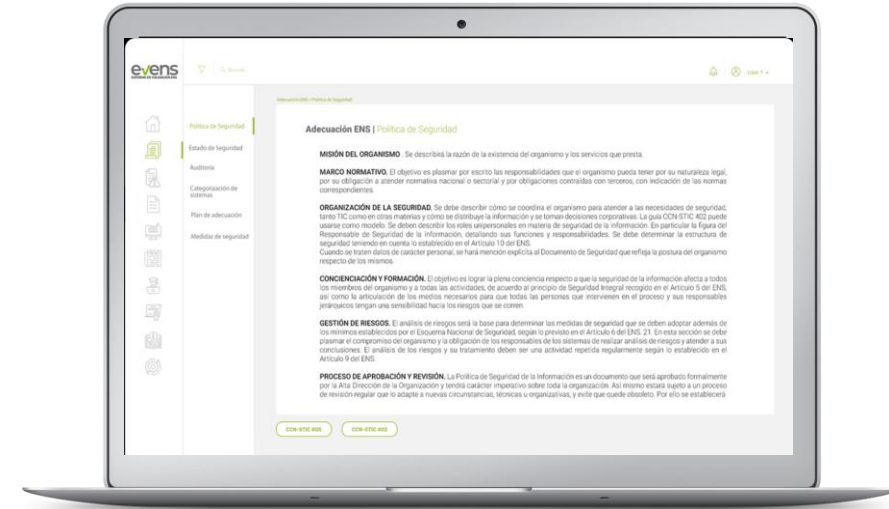




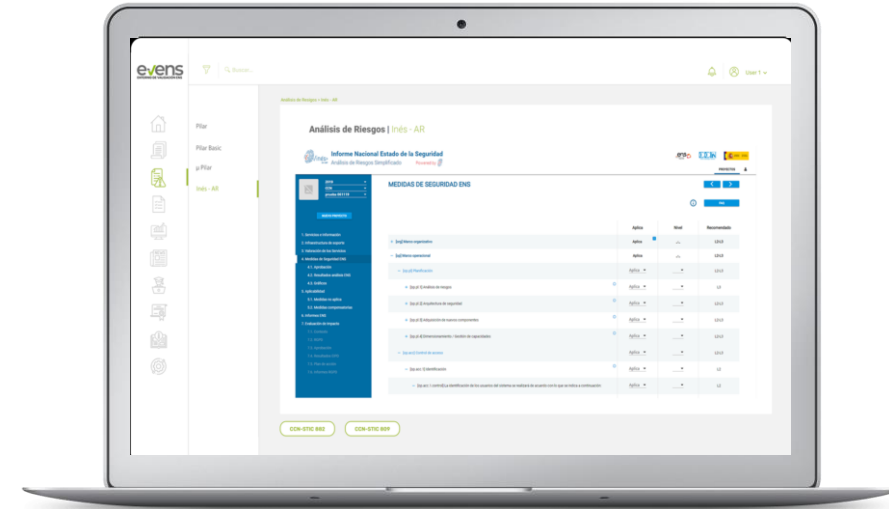
- **El CCN-CERT cada vez ofrece más servicios** que buscan facilitar la implementación de seguridad para, en última instancia, conseguir el cumplimiento con ENS.
- Entorno que **engloba todo lo referente al ENS** para facilitar el acceso a la información y la correcta implantación y validación de normativa.
- **Características principales:**
 - Simplicidad y potencia.
 - Facilidad de navegación y búsqueda.
 - Colaboración.
 - Reutilización de recursos.
 - Indicadores de situación.
 - Estrategia y ayuda en la toma de decisiones.



- La solución INES facilita la **recogida y consolidación de información** para el Informe del Estado de la Seguridad.
- A partir de 2020, **campaña abierta todo el año para cargar/actualizar datos** por parte de las entidades, solo se cierra para consolidar la base de datos en febrero de cada año.
- Las **EE.LL. y las universidades** son las entidades que necesitan realizar un mayor esfuerzo para conseguir la adecuación con el ENS.
- Las **auditorías de adecuación** empiezan a formar parte del calendario de ciberseguridad de las entidades.



- La adecuación al Esquema Nacional de Seguridad requiere:
 - Política de seguridad** incluyendo la definición de roles y la asignación de responsabilidades.
 - Categorizar** los sistemas.
 - Realizar el **análisis de riesgos**.
 - Preparar y aprobar la **Declaración de Aplicabilidad**.
 - Elaborar un **plan de adecuación** para la mejora de la seguridad.
 - Implantar, operar y monitorizar las **medidas de seguridad**.
 - Auditar la seguridad**.
 - Informar sobre el **estado de la seguridad**.



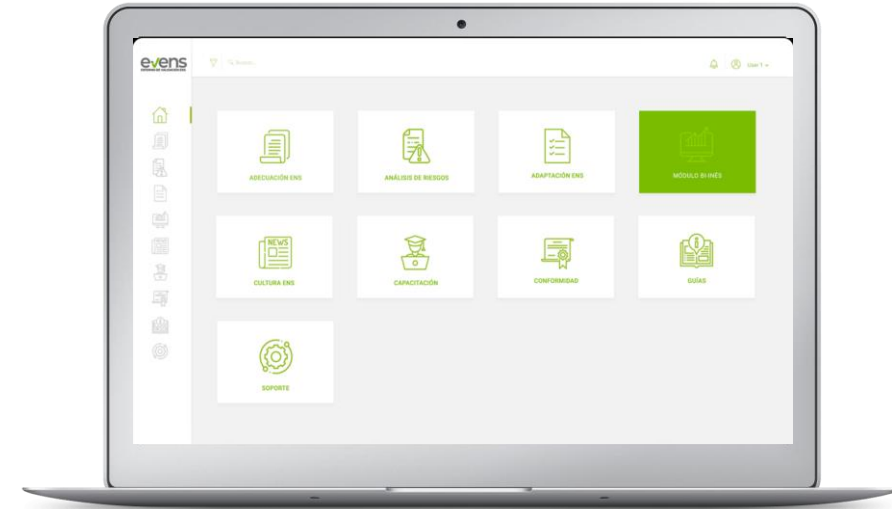
- Módulo de AR (**Análisis de Riesgos Simplificado**)
- Permite realizar análisis de riesgos simplificados con objeto de **facilitar la actualización de los mismos** a lo largo del tiempo.
- Entre sus capacidades destacan:
 - **Declaración de aplicabilidad.**
 - **Evaluación de impacto.**



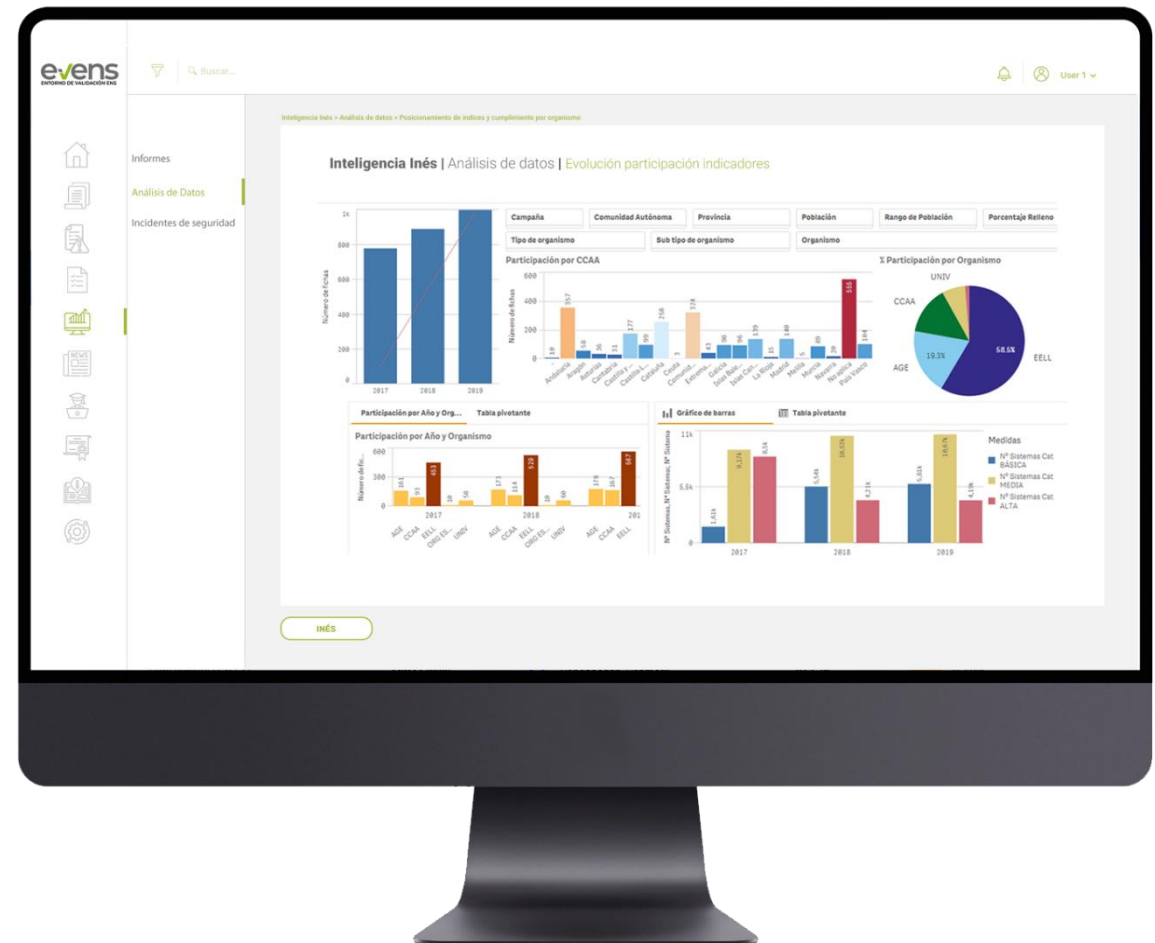
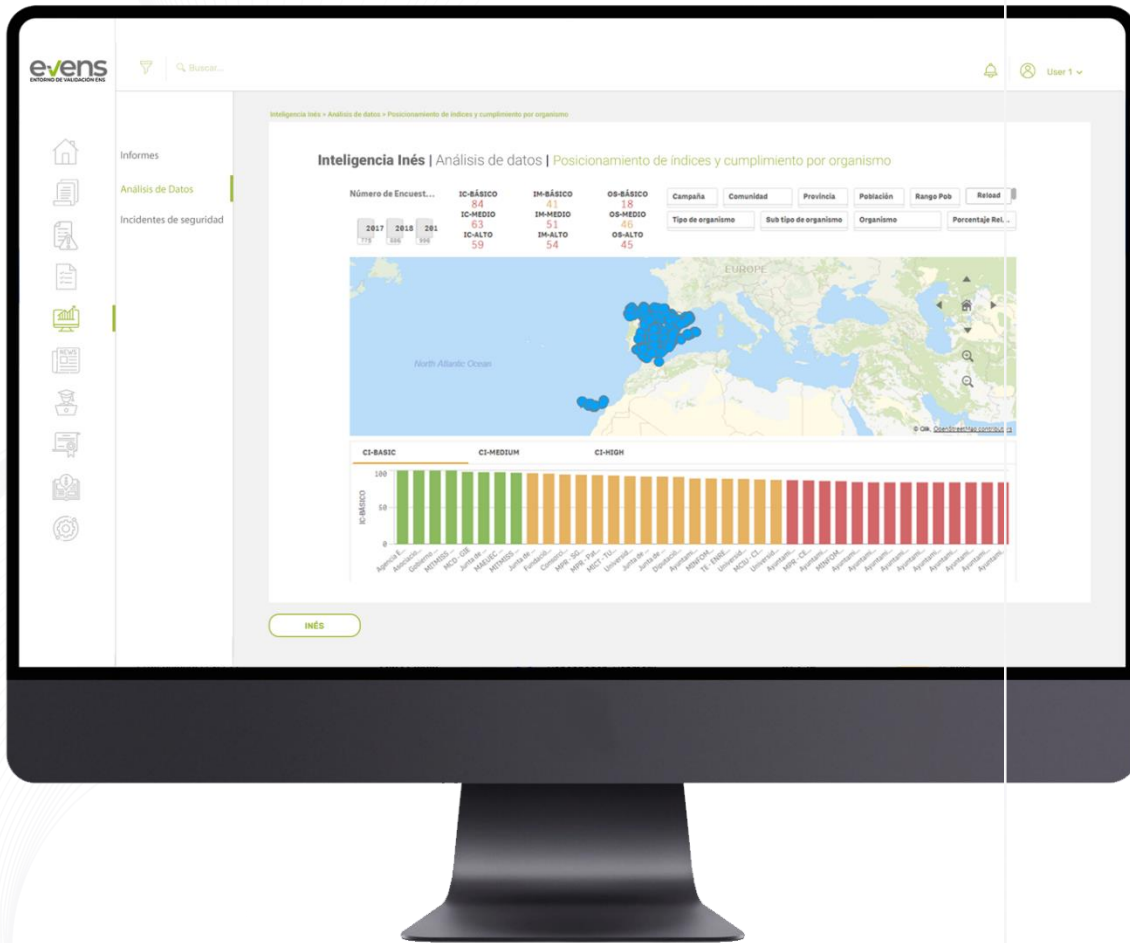
Estudio Simplificado de Riesgos



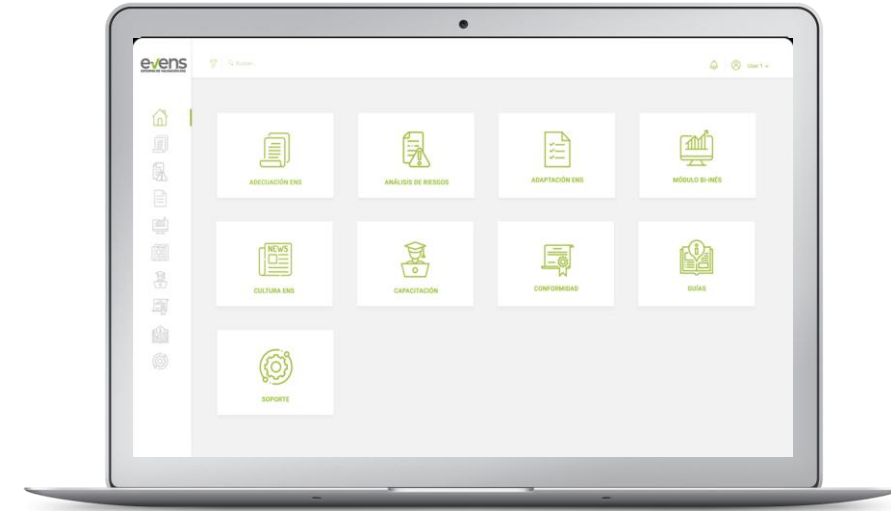
- **Facilitar el cumplimiento del ENS** y que los servicios se presten de acuerdo a **unos niveles mínimos de confianza**.
- La inclusión del **Análisis de Riesgos** en el **proceso de determinación de la Declaración de Aplicabilidad** resulta en perfil de cumplimiento.
- Un perfil de cumplimiento implica:
 - Un **conjunto de medidas de seguridad**.
 - La **implementación concreta y detallada** de cada medida de seguridad.
 - **Aceptación del riesgo residual** obtenido tras la implementación de las medidas de seguridad.



- Módulo de INES, que aúna estrategias y herramientas para **transformar la información en conocimiento**.
- Objetivo de **mejorar el proceso de toma de decisiones** del organismo.
- Informes, resúmenes, cuadros de mando, gráficos y mapas con **información analítica** detallada sobre estado de cumplimiento del ENS.
- Análisis de información desde la **siguientes perspectivas**:
 - Cumplimiento, madurez y organización de la seguridad.
 - Evolución de participación e índices.
 - Análisis referente a cuestiones e indicadores.



Inteligencia y Explotación de los Datos



- Se dotará a la administración pública de una potente solución que **ayude simplificar** todos los aspectos referentes al ENS, incluida la toma de decisiones.
- Los organismos sabrá su **estado de cumplimiento y madurez** en cada momento.
- El objetivo principal es **facilitar la integración** de todo lo referente al ENS.

Conclusiones



[CL/01]

Necesaria **implicación de todos los elementos técnicos, humanos, materiales, organizativos:** personas, procesos, tecnología, datos y ciberseguridad



[CL/02]

El ENS, aplicable a todo el Sector Público, proporciona un **planteamiento común** para la protección de la información y los servicios. **Referente para otros ámbitos**



[CL/03]

Seguir trabajando:

- Todos, para lograr la plena implantación del ENS
- Actualizar el ENS para mejor respuesta a tendencias y necesidades de ciberseguridad. Proceso que llevará tiempo y dará cabida a la participación (como en ocasiones anteriores).



COMUNIDAD Y CONFIANZA,
BASES DE NUESTRA CIBERSEGURIDAD

#XIIIJORNADASCNCERT

OC.CCN.CNI.ES

WWW.CCN.CNI.ES

WWW.CCN-CERT.CNI.ES

**XIII
JORNADAS
STIC
CCN-CERT**

ccn-cert
centro criptológico nacional