

¿QUÉ ES EL ESQUEMA NACIONAL DE SEGURIDAD?



Normativa pionera y referente en la Unión Europea en materia de ciberseguridad que tiene por objeto **establecer la política de seguridad del sector público** y de los proveedores que le dan servicio. Su objetivo es asegurar el acceso, la confidencialidad, la integridad, la trazabilidad, la autenticidad, la disponibilidad y la conservación de los datos, la información y los servicios utilizados por medios electrónicos por parte de la Administración.

En su elaboración y desarrollo han tenido un papel fundamental, tanto el **CCN** como la **Secretaría General de Administración Digital**.



ACTUALIZACIONES NORMATIVAS

Desde su primer desarrollo en **2010**, el Esquema Nacional de Seguridad ha estado en constante evolución:

2010

REAL DECRETO 3/2010

De 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica.

2015

REAL DECRETO 951/2015

De 23 de octubre, de modificación del RD 3/2010, de 8 de enero, por el que se regula el ENS en el ámbito de la Administración Electrónica.

2022

REAL DECRETO 311/2022

De 3 de mayo, por el que se regula el Esquema Nacional de Seguridad.

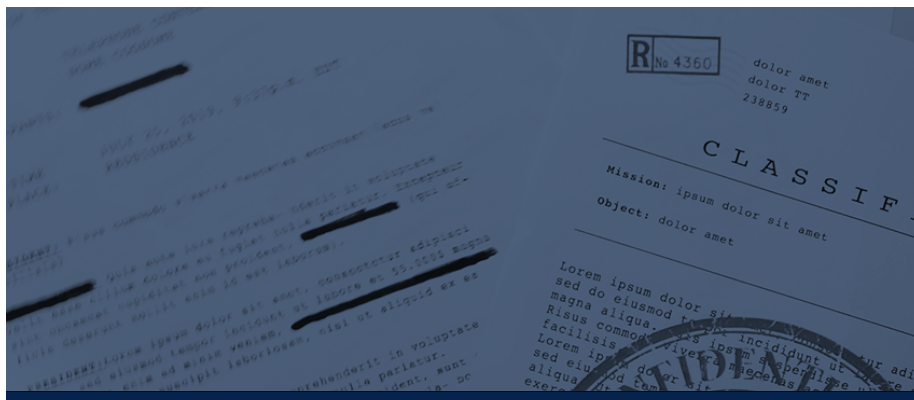
ÁMBITO DE APLICACIÓN



ENTIDADES DEL
SECTOR PÚBLICO



ENTIDADES DEL SECTOR
PRIVADO QUE PRESTAN
SERVICIOS AL SECTOR
PÚBLICO



SISTEMAS QUE TRATAN
INFORMACIÓN
CLASIFICADA

EL PAPEL DEL CCN EN EL ENS

El CCN proporciona la metodología y las herramientas necesarias para que las entidades del ámbito de aplicación del ENS realicen un análisis de riesgos para identificar las dificultades, brechas de seguridad, riesgos y amenazas potenciales a las que se enfrentan las entidades, organismos u organizaciones. Además de ello, el CCN valida y publica los **Perfiles de Cumplimiento Específico (PCE)**, ayudando con los mismos a las entidades a adaptarse de manera más eficiente al ENS y garantizando que las **medidas de seguridad** implementadas sean adecuadas y proporcionales al contexto de la amenaza, nivel de madurez, riesgo residual asumible y recursos disponibles.

73 MEDIDAS DE SEGURIDAD

4

MARCO ORGANIZATIVO

Relacionadas con la organización global de la seguridad.

33

MARCO OPERACIONAL

Dirigidas a proteger la operación del sistema como conjunto integral de componentes para un fin.

36

DE PROTECCIÓN

Centradas en activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad.

PROMOCIÓN DE SU DESARROLLO
Y APLICACIÓN



FORMACIÓN

+2.900

HORAS DE
FORMACIÓN

32.955

MATRICULACIONES

25 CURSOS Y JORNADAS DE CAPACITACIÓN



FORMACIÓN, CAPACITACIÓN Y
TALENTO EN CIBERSEGURIDAD

1. Esquema Nacional de Seguridad.
2. Análisis y Gestión de Riesgos de los Sistemas de Información.

3. Aproximación práctica al Esquema Nacional de Seguridad.
4. Auditorías en el ENS.
5. µCeENS.

DESARROLLO DE SOLUCIONES



INFORME NACIONAL DEL
ESTADO DE SEGURIDAD

Solución desarrollada por el CCN para la **gobernanza de la ciberseguridad**, que permite evaluar regularmente el estado de la seguridad de los sistemas TIC de las entidades, organismos y organizaciones, además de **facilitar la adecuación e implantación del Esquema Nacional de Seguridad (ENS)**.

Las **guías CCN-STIC**, elaboradas y difundidas por el CCN, ayudan a los responsables de los sistemas TIC a **implantar de forma rápida y efectiva las medidas de seguridad del ENS** que les resultan de aplicación.

93 DOCUMENTOS (SERIE 800 DE LAS GUÍAS CCN-STIC Y ABSTRACTS)

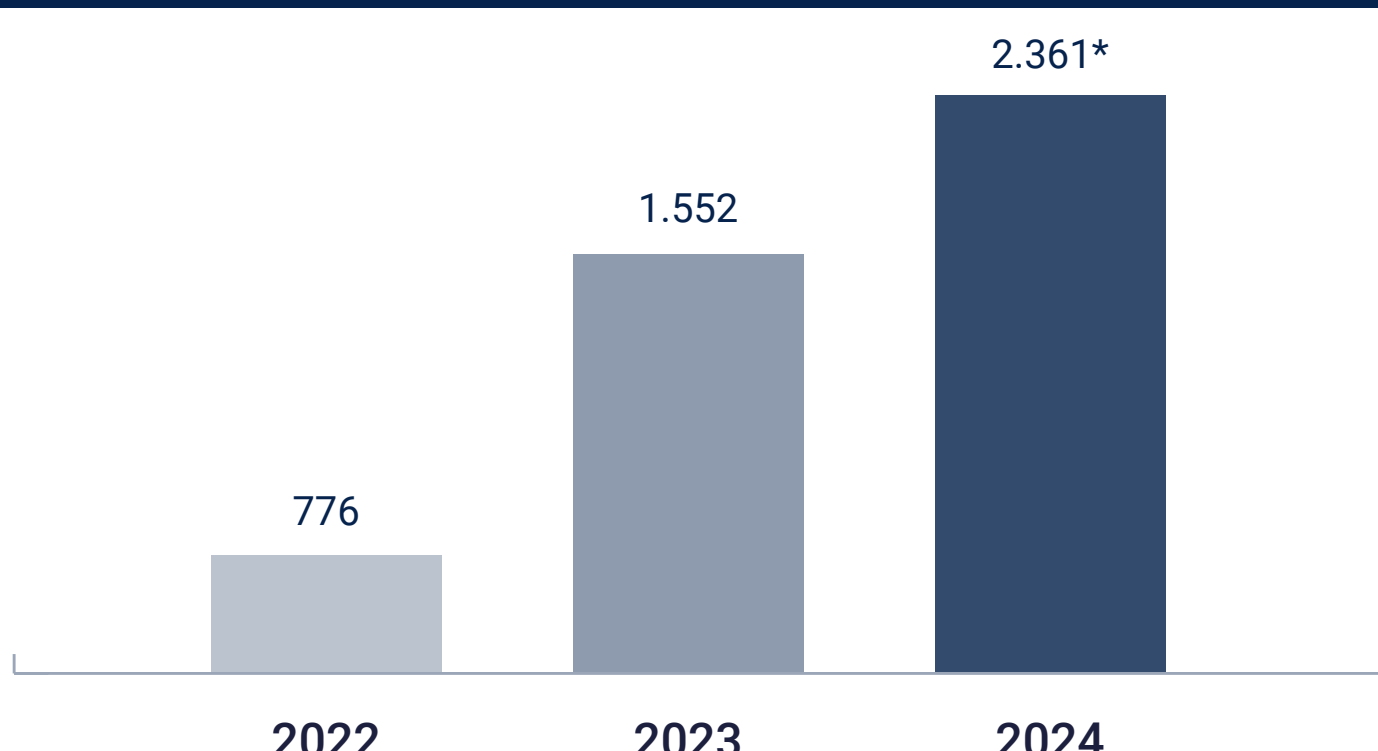
CERTIFICACIÓN DE CONFORMIDAD CON EL ENS



1.585*

CERTIFICADOS

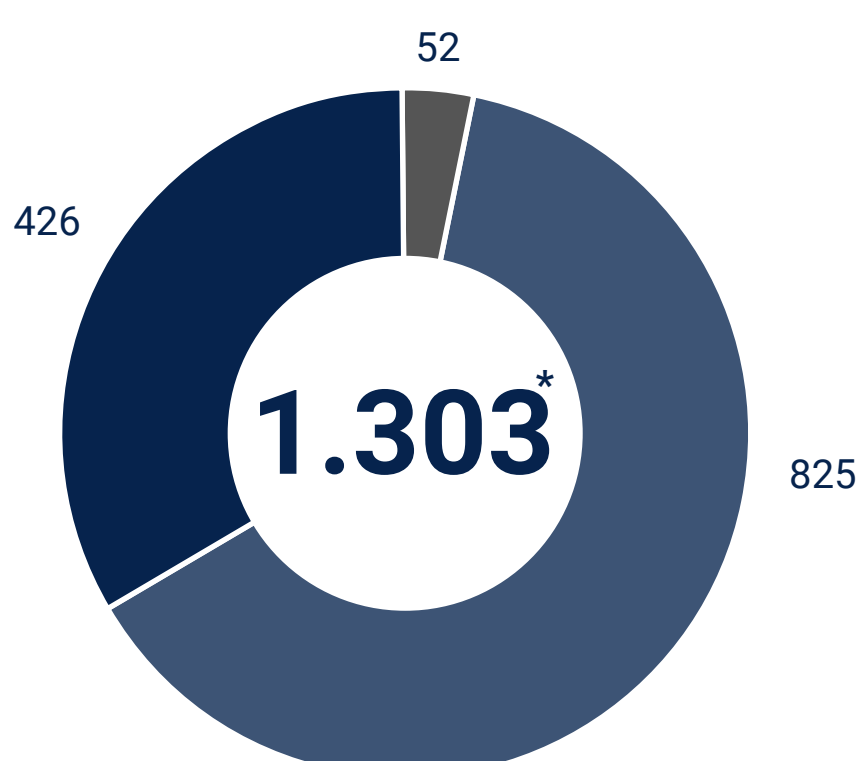
EVOLUCIÓN DE LOS CERTIFICADOS



*20 de septiembre de 2024.

SISTEMAS CERTIFICADOS

Entidades privadas y públicas cuyos sistemas de información han sido certificados en el ENS.



Alta

Media

Básica

PERFIL DE CUMPLIMIENTO ESPECÍFICO

Entidades públicas cuyos sistemas de información han sido certificados conforme al Perfil de Cumplimiento Específico de Requisitos Esenciales de Seguridad, validado por el CCN.



Requisitos esenciales

*20 de septiembre de 2024.