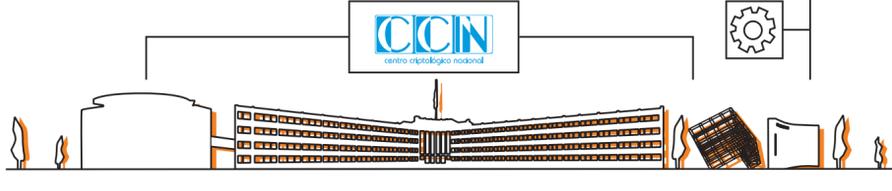


# El papel del CCN en el nuevo ENS

El Real Decreto 311/2022, del nuevo ENS, asigna al Centro Criptológico Nacional las siguientes funciones.



## Respuesta incidentes

CCN-CERT, coordinador a nivel público estatal de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática.



### Protocolo de respuesta ante un incidente

#### 1. Notificación

¿Qué incidentes se deben notificar al CCN-CERT?



##### Incidentes

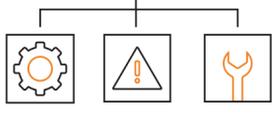
Incidentes que tengan un impacto significativo en la seguridad de los sistemas de información del sector público.

##### Organismo responsable de notificar al CCN-CERT



Organismo afectado.

Incidentes del sector privado que presten servicios a las entidades públicas.



#### 2. Soporte y coordinación

El CCN-CERT ofrece soporte y coordina el tratamiento de vulnerabilidades y la resolución de incidentes de seguridad.

#### 3. Respuesta técnica

El CCN-CERT determina técnicamente el riesgo de reconexión de un sistema, tras un incidente de seguridad.

El CCN-CERT indica los procedimientos a seguir y las salvaguardas a implementar para reducir el impacto y evitar que se den las circunstancias que lo propiciaron.

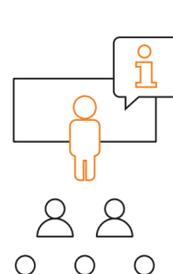


## Formación, concienciación y sensibilización

El nuevo ENS encomienda al CCN y al Instituto Nacional de Administración Pública el desarrollo de programas de sensibilización, concienciación y formación, dirigidos al personal de las entidades del sector público.

### Objetivo

- Asegurar un adecuado despliegue de la información y las capacidades jurídicas, organizativas y técnicas relacionadas con la ciberseguridad de los sistemas de información públicos.
- Mejorar las capacidades para la prevención, detección y gestión de incidentes.
- Garantizar el conocimiento permanente del ENS.



## Divulgación de buenas prácticas y avisos de ciberseguridad

### Desarrollo de Guías CCN-STIC

#### Objetivo

- Ofrecer normas, instrucciones, guías y recomendaciones para aplicar el ENS.
- Garantizar la seguridad de los sistemas de información del ámbito de aplicación del presente real decreto.



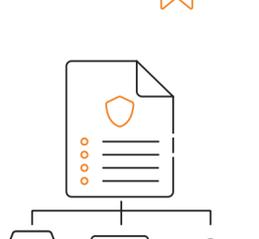
Ofrecer información sobre vulnerabilidades, alertas y avisos de nuevas amenazas a los sistemas de información.

## Perfil de cumplimiento específico y acreditación de entidades de implementación de configuraciones seguras

El CCN, en el ejercicio de sus competencias, validará y publicará los correspondientes perfiles de cumplimiento específicos que se definan y los esquemas de acreditación y validación, de acuerdo con las instrucciones técnicas de seguridad y guías de seguridad.



**Perfil de cumplimiento específico**  
Conjunto de medidas de seguridad que, tras el preceptivo análisis de riesgos, resulten idóneas para una categoría de seguridad concreta.



**Esquemas de certificación y acreditación**  
Las correspondientes ITS o, en su caso, las guías de seguridad, precisarán las condiciones a las que deberán sujetarse las implementaciones en modo local de productos, sistemas o servicios originariamente prestados en la nube o en forma remota, así como las condiciones específicas para su evaluación y auditoría.