Esquema Nacional de Seguridad

Novedades del ENS 2022



Incorporación de la figura del perfil de cumplimiento

Objetivo

Capacidad de adaptación.

Alcanzar una adaptación al ENS más eficaz y eficiente, racionalizando recursos requeridos sin menoscabo de la protección perseguida y exigible.

Aplicación

Conjunto de medidas de seguridad, comprendidas o no el en Anexo II del ENS que, como consecuencia del preceptivo análisis de riesgos, resulten de aplicación a una entidad o sector de actividad concreta y para una determinada categoría de seguridad.

Se persigue introducir la capacidad de ajustar los requisitos del ENS a necesidades específicas:

A determinados colectivos de entidades: Entidades Locales, Universidades, Organismos Pagadores…

O a determinados ámbitos tecnológicos: servicios en nube…

Dando respuesta a las nuevas demandas provenientes de unas organizaciones más maduras y unos ciudadanos más exigentes con sus derechos, para una aplicación más eficaz y eficiente del ENS, sin menoscabo de la ciberseguridad.

Metodología

En un perfil de cumplimiento específico, respecto de una declaración de aplicabilidad inicial para una categoría determinada se puede:

- Suprimir medidas o incluir la aplicabilidad de otras.
- Aumentar o disminuir la exigencia del nivel de implantación de alguna medida.
- Proponer medidas compensatorias o complementarias de vigilancia.

Establecimiento de protocolo de actuación ante ciberincidentes

Objetivo

Articular la respuesta a incidentes de seguridad de la información.

Establecer las condiciones de notificación de incidentes al CCN-CERT, coordinador nacional e internacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática.

Aplicación

El Centro Criptológico Nacional articula la respuesta a los incidentes de seguridad.

Establece la obligación de notificar al CCN-CERT los incidentes de seguridad:

Las **entidades del sector** público notificarán al CCN aquellos incidentes que tengan un impacto significativo en la seguridad de los sistemas de información concernidos.

INCIBE-CERT pondrá inmediatamente en conocimiento del CCN-CERT los incidentes que afecten a las organizaciones del sector privado que presten servicios a las entidades públicas.

Asigna al **CCN** las siguientes funciones:

Determinar técnicamente el riesgo de reconexión de un sistema, tras un incidente de seguridad.

Indicar los procedimientos a seguir y las salvaguardas a implementar para reducir el impacto del incidente.

Articular la respuesta a incidentes de seguridad de la información.

Establecer las condiciones de notificación de incidentes al CCN-CERT, coordinador nacional e internacional de la respuesta técnica de los equipos de respuesta a incidentes de seguridad informática.

Nuevo sistema de codificación de los requisitos de las medidas de seguridad

Objetivo

Facilitar de manera proporcionada la seguridad de los sistemas de información, su implantación y su auditoría.

Aplicación

Se han codificado los requisitos de medidas y se han organizado de la siguiente forma:

- Requisitos base.
- Posibles refuerzos de seguridad (R), alineados con el nivel de seguridad perseguido, que se suman (+) a los requisitos base de la medida, pero que no siempre son incrementales entre sí; de forma que, en ciertos casos, se puede elegir entre aplicar un refuerzo u otro.