Esquema Nacional de Seguridad

ENS 2010 | ENS 2022
Diferencias y evolución de los principios, requisitos y medidas del ENS



Principios

Cambios realizados en los principios básicos.

ENS 2010

~~Prevención, reacción y recuperación~~

ENS 2022

Prevención, detección, respuesta y conservación

Se introduce el principio básico de Vigilancia continua.

Requisitos

Modificaciones realizadas en los requisitos mínimos.

ENS 2010

Seguridad por defecto

ENS 2022

Mínimo privilegio

***Modificación de terminología**

Medidas

Cambios realizados en las medidas de seguridad, que se recogen en el Anexo II del ENS, y que permiten el cumplimiento de los principios básicos y los requisitos mínimos.

Incorporación en el ENS 2022 de una nueva familia de medidas del Marco operacional:

Servicios en la nube

RD 2010

RD 2010

4 Marco organizativo

(1) Política de seguridad.
(1) Normativa de seguridad.
(1) Procedimiento de seguridad.
(1) Proceso de autorización.

31 Marco operacional

(5) Planificación.
(7) Control de acceso.
(11) Explotación.
(3) Servicios externos.
(3) Continuidad del servicio.
(2) Monitorización del sistema.

40 Medidas de protección

(8) Instalaciones e infraestructuras.
(5) Gestión del personal.
(4) Protección de los equipos.
(5) Protección de las comunicaciones.
(5) Protección de los soportes de información.
(2) Protección de aplicaciones informáticas.
(7) Protección de la información.
(4) Protección de los servicios.

RD 2022

NUEVO RD

4 Marco organizativo

(1) Política de seguridad.
(1) Normativa de seguridad.
(1) Procedimiento de seguridad.
(1) Proceso de autorización.

33 Marco operacional

(5) Planificación.
(6) Control de acceso.
(10) Explotación.
(4) Servicios externos.
(1) Servicio en la nube.
(4) Continuidad del servicio.
(3) Monitorización del sistema.

36 Medidas de protección

(7) Instalaciones e infraestructuras.
(4) Gestión del personal.
(4) Protección de los equipos.
(4) Protección de las comunicaciones.
(5) Protección de los soportes de información.
(2) Protección de aplicaciones informáticas.
(6) Protección de la información.
(4) Protección de los servicios.

Resumen de modificaciones a las medidas de seguridad

Aumentan considerablemente su nivel de exigencia (9)

- Identificación
- Configuración de seguridad
- Gestión de la configuración de seguridad
- Protección frente a código dañino
- Registro de actividad
- Gestión de la capacidad
- Detección de intrusión
- Sistema de métricas
- Aceptación y puesta en servicio

Aumentan ligeramente su nivel de exigencia (11)

- Requisitos de acceso
- Mantenimiento y actualizaciones de seguridad
- Gestión de cambios
- Gestión de incidentes
- Componentes certificados
- Deberes y obligaciones
- Protección de la confidencialidad
- Separación de flujos de información en la red
- Borrado y destrucción
- Copias de seguridad
- Datos de carácter personal

Nuevas medidas (6)

- Servicios en la nube
- Interconexión de sistemas
- Protección de la cadena de suministros
- Medios alternativos
- Vigilancia
- Otros dispositivos conectados a la red

Se han eliminado (9)

- Protección de los registros de actividad.
- Personal alternativo
- Medios alternativos (4)
- Cifrado
- Instalaciones alternativas
- Accesp remoto

Se han simplificado (6)

- Segregación de tareas
- Protección de los dispositivos portátiles
- Perímetro seguro
- Sellos de tiempo
- Calificación de la información
- Protección frente a denegación de servicio

Visita nuestra web
ens@ccn-cert.cni.es