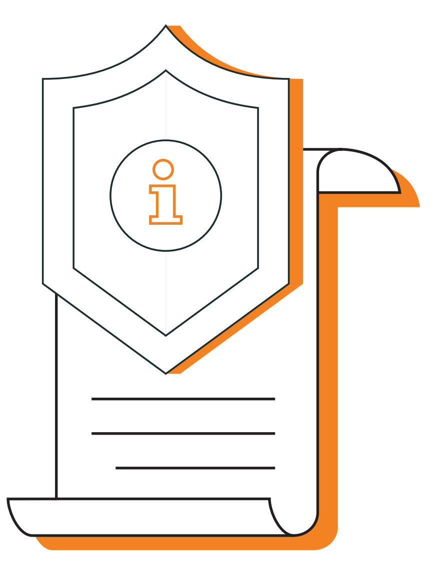
Esquema Nacional de Seguridad

ENS 2022
Principios básicos, requisitos mínimos y medidas de seguridad



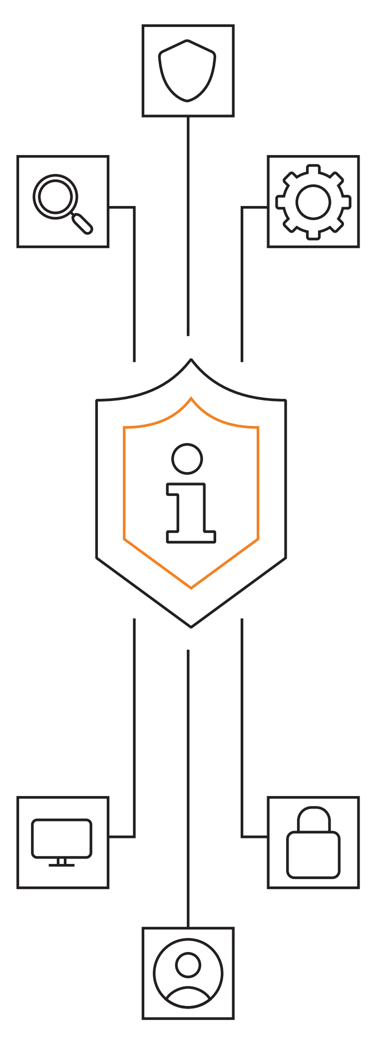
Principios

Los **principios básicos** a tener en cuenta para garantizar que una organización puede cumplir sus objetivos, desarrollar sus funciones y ejercer sus competencias utilizando sistemas de información:

1. **La seguridad como un proceso integral.**
2. **Gestión de la seguridad basada en los riesgos.**
3. **Prevención, detección, respuesta y conservación.**
4. **Existencia de líneas de defensa.**
5. **Vigilancia continua.**
6. **Reevaluación periódica.**
7. **Diferenciación de responsabilidades.**

Requisitos mínimos

Los **requisitos mínimos** para permitir una protección adecuada de la información y los servicios son:



1. **Organización e implantación del proceso de seguridad.**
2. **Análisis y gestión de los riesgos.**
3. **Gestión de personal.**
4. **Profesionalidad.**
5. **Autorización y control de los accesos.**
6. **Protección de las instalaciones.**
7. **Adquisición de productos de seguridad y contratación de servicios de seguridad.**
8. **Mínimo privilegio.**
9. **Integridad y actualización del sistema.**
10. **Protección de la información almacenada y en tránsito.**
11. **Prevención ante otros sistemas de información interconectados.**
12. **Registro de la actividad y detección de código dañino.**
13. **Incidentes de seguridad.**
14. **Continuidad de la actividad.**
15. **Mejora continua del proceso de seguridad.**

Medidas de seguridad

Para lograr el cumplimiento de los principios básicos y requisitos mínimos establecidos, se aplican las **medidas de seguridad** que recogen en el Anexo II del ENS y que se dividen en tres grupos:

Marco organizativo

Constituido por el conjunto de medidas relacionadas con la organización global de la seguridad.

[org]

- **Política de seguridad**
- **Normativa de seguridad**
- **Procedimientos de seguridad**
- **Proceso de autorización**

Marco operacional

Formado por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin.

[op]

1 Planificación
- Análisis de riesgos.
- Arquitectura de Seguridad.
- Adquisición de nuevos componentes.
- Dimensionamiento/gestión de la capacidad.
- Componentes certificados.

2 Control de acceso
- Identificación.
- Requisitos de acceso.
- Segregación de funciones y tareas.
- Proceso de gestión de derechos de acceso.
- Mecanismo de autenticación (usuarios externos).
- Mecanismo de autenticación (usuarios de la organización).

3 Explotación
- Inventario de activos.
- Configuración de seguridad.
- Gestión de la configuración de seguridad.
- Mantenimiento y actualizaciones de seguridad.
- Gestión de cambios.
- Protección frente a código dañino.
- Gestión de incidentes.
- Registro de la actividad.
- Registro de la gestión de incidentes.
- Protección de claves
- criptográficas.

4 Recursos externos
- Contratación y acuerdos de nivel de servicio.
- Gestión diaria.
- Protección de la cadena de suministro.
- Interconexión de sistemas.

5 Servicios en la nube
- Protección de servicios en la nube.

6 Continuidad del servicio.
- Análisis de impacto.
- Plan de continuidad.
- Pruebas periódicas.
- Medios alternativos.

7 Monitorización del sistema.
- Detección de intrusión.
- Sistema de métricas.
- Vigilancia.

Medidas de protección

Se centran en proteger activos concretos, según su naturaleza y la calidad exigida por el nivel de seguridad de las dimensiones afectadas.

[mp]

1 Protección de las instalaciones e infraestructuras
- Áreas separadas y con control de acceso.
- Identificación de las personas.
- Acondicionamiento de los locales.
- Energía eléctrica.
- Protección frente a incendios.
- Protección frente a inundaciones.
- Registro de entrada y salida de equipamiento.

2 Gestión del personal
- Caracterización del puesto de trabajo.
- Deberes y obligaciones.
- Concienciación.
- Formación.

3 Protección de los equipos
- Puesto de trabajo despejado.
- Bloqueo de puesto de trabajo.
- Protección de dispositivos portátiles.
- Otros dispositivos conectados a la red.

4 Protección de las comunicaciones.
- Perímetro seguro.
- Protección de la confidencialidad.
- Protección de la integridad y de la autenticidad.
- Separación de flujos de información en la red.

5 Protección de los soportes de información
- Marcado de soportes.
- Criptografía.
- Custodia.
- Transporte.
- Borrado y destrucción.

6 Protección de las aplicaciones informáticas
- Desarrollo de aplicaciones.
- Aceptación y puesta en servicio.

7 Protección de la información
- Datos personales.
- Calificación de la información.
- Firma electrónica.
- Sellos de tiempo.
- Limpieza de documentos.
- Copias de seguridad.

8 Protección de los servicios
- Protección del correo electrónico.
- Protección de servicios y aplicaciones web.
- Protección de la navegación web.
- Protección frente a denegación de servicio.

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