GESTIÓN DE SEGURIDAD Y NORMATIVAS


Amenazas para la seguridad TIC
Física
Lógica
Usuario
tic.PORTAL

ENS

- El Real Decreto 311/2022, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad(Abre en nueva ventana) sustituye al 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.

Objetivos

- Crear las condiciones necesarias de seguridad en el uso de los medio electrónicos, a través de medidas para garantizar la seguridad de los sistemas, los datos, las comunicaciones, y los servicios electrónicos, que permita el ejercicio de derechos y el cumplimiento de deberes a través de estos medios.
- Promover la gestión continuada de la seguridad.
- Promover la prevención, detección y corrección, para una mejor resiliencia en el escenario de ciberamenazas y ciberataques.

Objetivos

- Promover un tratamiento homogéneo de la seguridad que facilite la cooperación en la prestación de servicios públicos digitales cuando participan diversas entidades. Esto supone proporcionar los elementos comunes que han de guiar la actuación de las entidades del Sector Público y de sus proveedores tecnológicos en materia de seguridad de las tecnologías de la información.
- Servir de modelo de buenas prácticas, en línea con lo apuntado en las recomendaciones de la OCDE Digital Security Risk Management for Economic and Social Prosperity OECD Recommendation and Companion Document(Abre en nueva ventana) .

¿A qué empresas aplica el ENS?

- El ENS es de aplicación obligatoria para todas las empresas del sector público estatal, autonómico y local, empresas del sector privado que suministren servicios o provean de soluciones a la Administración Pública y sistemas que traten con información clasificada.

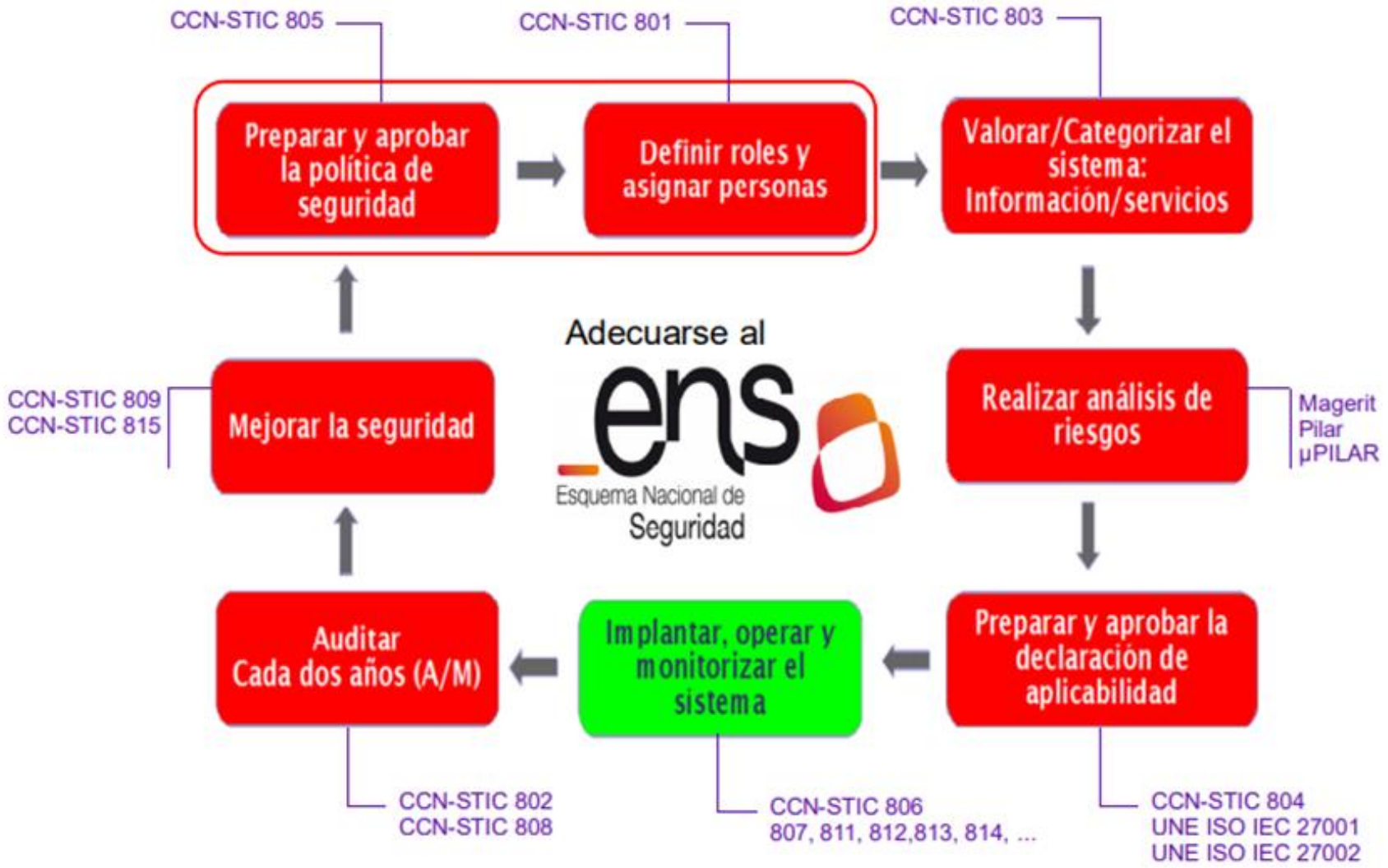
ENS 2010

- **Principios básicos:** prevención, reacción y recuperación.
- No existía el principio básico de **Vigilancia continua**.
- Menor visibilidad al **componente certificado** de hardware y software.
- **Requisitos**: seguridad por defecto.
- No existía el servicio en la nube en las medidas del marco operacional.
- **4** marcos organizativos.
- **31** marcos operacionales.
- **40** medidas de protección.
- **Refuerzos** en los mecanismos de autenticación.

ENS 2022

- **Principios básicos:** prevención, detección, respuesta y conservación.
- Se introduce el principio básico de **Vigilancia continua** (auditoría obligatoria anualmente).
- Máxima importancia **componente certificado** de hardware y software.
- **Requisitos**: mínimo privilegio (modificación de terminología).
- Nueva familia de medidas del marco operacional: **servicio en la nube.**
- **4** marcos organizativos (se mantiene el número).
- **33** marcos operacionales (aumentan 2 marcos).
- **36** medidas de protección (se reducen 4 marcos).
- Mayores **refuerzos** en los mecanismos de autenticación.

Elementos del Esquema Nacional de Seguridad



75 MEDIDAS DE SEGURIDAD RECOGIDAS EN EL ENS

MARCO ORGANIZATIVO

El marco organizativo está constituido por un conjunto de medidas relacionadas con la organización global de la seguridad

- POLÍTICA DE SEGURIDAD
- NORMATIVA DE SEGURIDAD
- PROCEDIMIENTOS DE SEGURIDAD
- PROCESO DE AUTORIZACIÓN

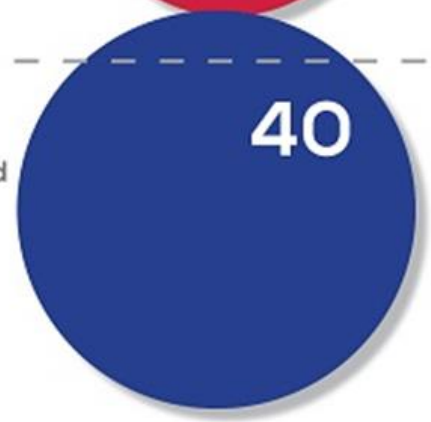
MARCO OPERACIONAL

El marco operacional está constituido por las medidas a tomar para proteger la operación del sistema como conjunto integral de componentes para un fin

- PLANIFICACIÓN
- CONTROL DE ACCESO
- EXPLOTACIÓN
- SERVICIOS EXTERNOS
- CONTINUIDAD DEL SERVICIO
- MONITORIZACIÓN DEL SISTEMA

MEDIDAS DE PROTECCIÓN

Las medidas de protección, se centrarán en activos concretos, según su naturaleza, con el nivel requerido en cada dimensión de seguridad



- INSTALACIONES E INFRAESTRUCTURAS
- GESTIÓN DEL PERSONAL
- PROTECCIÓN DE LOS EQUIPOS
- PROTECCIÓN DE LAS COMUNICACIONES
- PROTECCIÓN SOPORTES DE INFORMACIÓN
- PROTECCIÓN APLICACIONES INFORMÁTICAS
- PROTECCIÓN DE LA INFORMACIÓN
- PROTECCIÓN DE LOS SERVICIOS

NIS / NIS2

- La Directiva NIS2, Directiva (UE) 2022/2555 (correspondiente con las siglas de Network and Information Security), establece un marco de seguridad de la información para garantizar la protección de los sistemas y las redes de información en la Unión Europea, con el fin de prevenir ataques y garantizar la continuidad de los servicios.
- La Directiva establece obligaciones de ciberseguridad para los Estados miembros, medidas para la gestión de riesgos de ciberseguridad y obligaciones de notificación para las entidades en su ámbito de aplicación, obligaciones relativas al intercambio de información sobre ciberseguridad, así como obligaciones de supervisión y ejecución para los Estados miembros

Novedades

- Sanciones más severas para aquellos que incumplen sus obligaciones, incluyendo multas significativas y sanciones administrativas. Las amonestaciones, instrucciones y multas podrían ser de hasta dos millones de euros e incluso llegar a suponer el 2% de los ingresos anuales de la organización.
- Responsabilidad de los directivos de las empresas. Se establece la obligación de que los órganos de dirección aprueben y supervisen la puesta en práctica de medidas técnicas, operativas y de organización, pero también para prevenir y minimizar el impacto de los incidentes en caso de producirse.
- Nuevos requisitos de seguridad. Se añaden nuevas obligaciones como pudieran ser el uso de cifrado de extremo a extremo o la asistencia a formaciones a los miembros de dirección de las entidades esenciales, así como formaciones similares a sus empleados de forma periódica. Se impone la privacidad por defecto y desde diseño, la gestión de crisis, la certificación de sus servicios, productos y/o sistemas bajo esquemas europeos de certificación de la ciberseguridad, o el tratamiento y divulgación de vulnerabilidades.
- Refuerzo de la seguridad de las cadenas de suministro, así como las relaciones con los proveedores. Para ello, en caso de tratarse de operadores críticos, se permite a las empresas exigir a sus proveedores el cumplimiento de la normativa.
- Informe de incidentes obligatorio: Al igual que dicta el RGPD, la Directiva NIS2 requiere a los operadores de servicios esenciales y a los proveedores de servicios digitales que informen sobre ciertos tipos de incidentes graves a las autoridades relevantes en un plazo de 72 horas. Asimismo, se recoge la obligación de notificar a sus CSIRT de referencia sin demora indebida, incidentes de seguridad que tengan un impacto significativo.
- Integración plena con normativa sectorial, como puede ser la Directiva para la Resiliencia Operativa Digital para el sector financiero (DORA) y la Directiva de Resiliencia de Entidades Críticas (CER).

¿A qué empresas aplica la Directiva NIS2?

- La Directiva NIS-2 será de obligado cumplimiento para empresas de más de 250 empleados y con un volumen de facturación anual de 50 millones de euros en adelante. Al mismo tiempo, también estarán obligados a su cumplimiento los operadores que presten servicios esenciales y los proveedores de servicios digitales que operan en la Unión Europea. Estos servicios incluyen, entre otros, servicios energéticos, transporte, salud, banca y finanzas, y servicios de telecomunicaciones.

REGLAMENTO DE RESILIENCIA OPERATIVA DIGITAL (DORA)

- Esta normativa tiene por objetivo garantizar que el sector financiero en Europa sea capaz de responder de forma sólida en caso de una disrupción operativa severa, creando un marco normativo sobre la resiliencia operativa digital por el que todas las entidades deben asegurarse de poder afrontar, responder y recuperarse de todo tipo de perturbaciones y amenazas relacionadas con las TIC.

- DORA comenzará a aplicar a partir de **enero de 2025**.
-

- **Perímetro y Gobernanza TIC**. DORA establece requisitos uniformes relativos a la seguridad de las redes y los sistemas de información de las entidades financieras, así como de terceros de importancia crítica que les prestan servicios relacionados con las TIC, como las plataformas en la nube o los servicios de análisis de datos. Por otro lado, establece las responsabilidades del Órgano de Dirección e identifica la figura de un encargado de monitorizar los acuerdos con proveedores terceros de servicios de TIC.
- **Riesgos TIC.** Las entidades financieras deberán:
  - Identificar y clasificar, según criticidad, funciones y activos soporte TIC, así como sus interdependencias con terceros.
  - Identificar de forma continua las fuentes de riesgo.
  - Evaluar de manera anual los riesgos específicos en todos los sistemas TIC legacy.
  - Llevar a cabo un Business Impact Analysis (BIA) de las exposiciones a interrupciones severas del negocio en términos de continuidad para evaluar su impacto potencial.

- **Reporte de incidentes TIC**. Las entidades financieras deberán:
  - Definir, establecer y aplicar un proceso de gestión de incidentes relacionados con las TIC para detectar, gestionar y notificar los incidentes relacionados con estas.
  - Clasificar los incidentes relacionados con las TIC y determinar su impacto en función de los criterios establecidos (e.g. el número y/o la importancia de los clientes o las contrapartes financieras afectadas), así como clasificar las ciberamenazas en función de la importancia de los servicios en riesgo.
  - Presentar una notificación inicial e informes sobre incidentes relevantes relacionados con las TIC a la autoridad competente pertinente. El feedback recibido debe evaluarse y proporcionará orientaciones a la entidad financiera, en particular para discutir las soluciones a nivel de la entidad o las formas de minimizar el impacto adverso en todos los sectores.

Normativas mas frecuentemente utilizadas para la gestión de la seguridad

- Norma internacional ISO/IEC 27002
- **ISO 31000** y la **ISO 27001**
- **ISO 33010** (gestión de riesgos de viajeros),
- **ISO 23234** (criterios y recomendaciones de seguridad para planificar la seguridad de edificios)
- **ISO 22341** (CPTED, Diseño del Entorno para la Prevención del Crimen)

Normativa ISO 27002

- Norma internacional ISO/IEC 27002,

- Se centra en las buenas prácticas para gestión de la seguridad de la información.

- Es fundamental para la consolidación de un Sistema de Gestión de Seguridad de la Información (SGSI), garantizando la continuidad y el mantenimiento de los procesos de seguridad, alineados a los objetivos estratégicos de la organización.

ISO 31000

- La **ISO 31000** es una norma internacional que ofrece las directrices y principios para gestionar el riesgo de las organizaciones.
- Esta norma fue publicada en 2018 por la Organización Internacional de Normalización (ISO) en colaboración con IEC, y tiene por objetivo que organizaciones de todos los tipos y tamaños puedan gestionar los **riesgos** en la empresa de forma efectiva, por lo que recomienda que las organizaciones desarrollen, implanten y mejoren continuamente un marco de trabajo cuyo objetivo es integrar el proceso de gestión de **riesgos** en cada una de sus actividades.

Norma ISO 27001,

- cuyo estándar promueve la implementación de un **Sistema de Gestión de Seguridad de la Información**. Esta norma sigue siendo el estándar favorito de las empresas para su gestión interna y para la evolución de sus servicios y productos.
- También incluye un dominio relativo a la seguridad física y del entorno, focalizado en prevenir el acceso físico no autorizado a la información y a las instalaciones de procesamiento de información de las empresas.

Objetivo 1:
Áreas seguras

- Evitar accesos físicos no autorizados, daños e interferencias contra las instalaciones de procesamiento de información y la información de la organización
- **11.1.1 Perímetro de seguridad física**
- **11.1.2 Controles de acceso físico**
- **11.1.3 Seguridad de oficinas, despachos e instalaciones**
- **11.1.4 Protección contra amenazas externas y del ambiente**
- **11.1.5 El trabajo en las áreas seguras**
- **11.1.6 Áreas de entrega y de carga**

Objetivo2:
Equipamiento

- Prevenir pérdidas, daños, hurtos o comprometer los activos así como la interrupción de las actividades de la organización.
- **11.2.1 Ubicación y protección del equipamiento**
- **11.2.2 Elementos de soporte**
- **11.2.3 Seguridad en el cableado**
- **11.2.4 Mantenimiento del equipamiento**
- **11.2.5 Retiro de bienes**
- **11.2.6 Seguridad del equipamiento y de los activos fuera de las instalaciones**
- **11.2.7 Seguridad en la reutilización o eliminación de equipos**
- **11.2.8 Equipamiento desatendido por el usuario**
- **11.2.9 Política de escritorio y pantalla limpios**

Metodología ITIL : Librería de infraestructuras de las tecnologías de la información

- Es un marco diseñado para estandarizar la selección, planificación, entrega y mantenimiento de los servicios de TI dentro de una empresa.

- El objetivo es mejorar la eficiencia y lograr una prestación de servicios predecible

Marco de procesos de ITIL

- ITIL abarca un marco de cinco publicaciones principales, que se revisan y actualizan periódicamente a medida que cambian las tecnologías.
- Cada libro recopila las mejores prácticas para cada fase importante del ciclo de vida de la gestión de servicios de TI (ITSM).

Marco de procesos de ITIL

- Los libros y sus conceptos básicos son:
- **Estrategia de servicio:** describe las metas comerciales y los requisitos del cliente y cómo alinear los objetivos de ambas entidades.
- **Diseño de servicios:** describe las prácticas para la producción de políticas, arquitecturas y documentación de TI.
- **Transición del servicio:** asesora sobre la gestión de cambios y las prácticas de lanzamiento; guía a los administradores a través de interrupciones y cambios ambientales.
- **Operación del servicio:** ofrece formas de administrar los servicios de TI de forma diaria, mensual y anual.
- **Mejora continua del servicio:** cubre cómo introducir mejoras y actualizaciones de políticas dentro del marco del proceso ITIL.
- La adopción y el mantenimiento de ITIL requieren expertos capacitados y certificados para guiar a una empresa y su personal de TI. Empresas como Microsoft, IBM y Hewlett Packard Enterprise (HPE) utilizan ITIL como base para sus propias directrices operativas internas.

Certificaciones

- Los administradores completan la capacitación y certificación de ITIL con una combinación de capacitación en el aula y un examen de certificación escrito. Hay cinco certificaciones principales:
- **Base (*Foundation*):** esta certificación de nivel de entrada cubre conceptos, elementos y terminología clave utilizados para el ciclo de vida del servicio ITIL y contribuciones a los servicios de gestión.
- **Practicante (*Practitioner*):** este nivel ayuda a los profesionales a adaptar ITIL a sus organizaciones para que respalde los objetivos comerciales. Los administradores pueden tomar el curso en cualquier momento después de una certificación Base; este módulo también cubre la gestión del cambio organizacional, la comunicación y las métricas, que no están disponibles en todas las certificaciones.
- **Intermedio (*Intermediate*):** cada módulo de esta certificación abarca diferentes componentes de ITSM, pero requiere un conocimiento más detallado que los exámenes de nivel básico. La pista se divide en módulos de capacidad de servicio y ciclo de vida del servicio.
- **Experto (*Expert*):** en esta etapa, los administradores están interesados en demostrar el esquema ITIL completo. Los expertos en ITIL obtienen un conjunto de habilidades completas relacionadas con las mejores prácticas de ITIL. Los administradores deben completar 17 créditos de módulos anteriores, el módulo *Gestión a Través del Ciclo de Vida* y un examen para obtener una certificación de experto.
- **Máster:** en el nivel de maestría, los administradores deben explicar cómo eligieron sus áreas de estudio, principios y métodos, así como las técnicas que utilizaron dentro de su organización para lograr los resultados comerciales deseados. Para lograr el estatus de Maestro no hay examen de certificación; los administradores completan una serie de tareas escritas y entrevistas orales.

Beneficios e inconvenientes

- ITIL no se trata solo de habilidades de TI sencillas y de memoria. La certificación también analiza cómo los administradores pueden aplicar sus conocimientos dentro del alcance más amplio de su organización y alinearse con las prácticas comerciales. Esto significa que los administradores ahora tienen mejores prácticas más coherentes al abordar todas las facetas de la gestión de TI. Con esto en mente, hay seis beneficios principales identificables de ITIL:
- Mejor alineación de objetivos entre los departamentos de TI y la empresa
- Mejores plazos de servicio y satisfacción del cliente
- Reducción de los costos operativos debido a una mejor utilización de los recursos
- Mayor visibilidad de los costos y activos de TI
- Gestión y respuesta simplificadas a las interrupciones del servicio
- Entorno de servicio más flexible que puede adaptarse fácilmente al cambio.