

## PRESENTACIÓN

El objetivo general del curso será que el participante reciba los conocimientos suficientes para ser capaz de preparar y dirigir el proceso de implementación del Esquema Nacional de Seguridad (ENS) en un sistema de información de un órgano de las Administraciones Públicas (AAPP) o en el de una empresa privada, con garantías suficientes para conseguir el certificado de conformidad proporcionado por una entidad de certificación acreditada.

## OBJETIVOS

El objetivo general del curso será que el participante reciba los conocimientos suficientes para ser **capaz de preparar y dirigir el proceso de implementación del Esquema Nacional de Seguridad** (ENS) en un sistema de información de un órgano de las Administraciones Públicas (AAPP) o en el de una empresa privada, con garantías suficientes para conseguir el certificado de conformidad proporcionado por una entidad de certificación acreditada.

Los objetivos específicos relacionados con aspectos organizativos, administrativos y legales son los siguientes:

- Conocer el propósito, naturaleza, estructura y contenido del ENS y el marco legal que lo sustenta.
- Conocer la normativa que regula el proceso de digitalización de las AAPP, y los sistemas y servicios con los que deberían contar dichas administraciones, con el fin de poder identificar los sistemas de información que pudieran estar sujetos al ENS.
- Conocer la estructura, naturaleza y función de los principios, requisitos y medidas de seguridad que establece el ENS.
- Poder determinar una declaración de aplicabilidad con las medidas de seguridad requeridas para un sistema de información, sustentada en el análisis de los procesos de categorización del sistema, análisis de riesgo y análisis de impacto.
- Saber desarrollar una estructura de seguridad en una organización, estableciendo los roles y responsabilidades necesarias, adaptadas a las características de dicha organización.
- Conocer el proceso de certificación y auditoría de los sistemas sujetos al EN y sea capaz de elaborar y ejecutar un plan de auditoría.
- Ser capaz de redactar la documentación necesaria establecer las directrices, configuraciones y normas internas necesarias para que el sistema de información de una organización cumpla con los preceptos del ENS.
- Conocer las particularidades y adaptaciones de cumplimiento del Esquema Nacional de Seguridad en determinadas AAPP o sistemas.
- Ser capaz de adaptar la implementación del Esquema Nacional de Seguridad para garantizar también el cumplimiento de las medidas necesarias recogidas den la Ley de Protección de Datos y del estándar ISO 27001 de gestión de la seguridad de sistemas de información.

Los objetivos específicos relacionados con aspectos operativos del sistema son los siguientes:

- Conocer las amenazas que pudieran alterar las dimensiones de seguridad de un sistema de información sujeto al ENS e identifique las medidas de protección necesarias.
- Conocer las particularidades de implementación del ENS en un entorno de Nube y sea capaz de establecer las medidas necesarias para garantizar la protección del sistema en ese entorno.
- Ser capaz analizar los factores necesarios para para la protección física de un sistema de información y sea capaz de desarrollar una norma que regule su aplicación.
- Conocer los procedimientos y mecanismos de la gestión de los servicios y pueda desarrollar la normativa asociada para regular dicho proceso de forma adecuada.
- Ser capaz de planear e implementar mecanismos de monitorización continua del sistema, y pueda contrastar la situación de protección del sistema en comparación con las métricas e indicadores adecuados.

Y los objetivos específicos relacionados con aspectos asociados a la implementación técnica de medidas de seguridad son los siguientes:

- Conocer las medidas asociadas al desarrollo e implementación técnica de una arquitectura de seguridad que implemente protección en profundidad, incluidas las medidas de control de acceso, protección de perímetro y protección de red y protección de hosts.
- Conocer las guías y recomendaciones asociadas a la implementación técnica de las configuraciones de seguridad del sistema y sea capaz de implementarlas por sí mismo, o de dar las directrices adecuadas de cómo hacerlo a un experto técnico externo.

## DIRIGIDO A

El curso va dirigido a personas con titulación de grado con conocimientos en sistemas de información, bien procedentes de titulaciones de grados de carácter técnico (ingeniería, informática, telecomunicaciones, etc.), bien por haber cursado estudios de posgrado en materia de ciberseguridad, o por haber desarrollado su actividad profesional en el ámbito de la seguridad de la información, debiendo ser capaces de poder entender los requisitos establecidos por el ENS en los aspectos administrativos, operativos y técnicos.

Para obtener el título de Experto se requerirá:

- Titulación Universitaria o
- Ciclos formativos de grado superior con experiencia superior a 3 años en el sector (Para el reconocimiento de la experiencia profesional se solicitará se entregue CV, vida laboral y se realizará una entrevista)

## PROGRAMA

### **Módulo 1 Estructura, contenido y requisitos del ENS**

1.1. Aspectos generales

1 Naturaleza, finalidad, alcance, estructura y medidas de seguridad en el ENS

2	Guías STIC e Instrucciones Técnicas asociadas
3	Proceso de implementación / adecuación
4	Cargos y responsabilidades en el ENS
5	Implementación medidas de seguridad organizativas y operativas
6	Implementación medidas de protección
7	Políticas, normas y procedimientos
1.2	Análisis de riesgos y categorización
1	Análisis de riesgos: metodología Magerit y Pilar
2	Metodología Margferit y Pilar-1
3	Metodología Margerit y Pilar-2
1.3.	Los sistemas de información de las AAPP
1	Legislación de los sistemas de información de las AAPP
2	Portales y servicios digitales de las AAPP
3	Declaración de aplicabilidad y perfiles de cumplimiento específicos
	<b>Examen módulo 1/1 (1.1, 1.2, 1.3, 1.4)</b>
1.4	Formación, seguridad física y seguridad de las personas
1	Seguridad física y control de acceso físico
2	Seguridad de personas.
3	Formación y concienciación
1.5	Gestión de servicios
1	Marco de referencia en la gestión de servicios. ITIL
2	Gestión de inventario, adquisiciones y cambios
3	Gestión de cambios y configuración
1.6	Ciberamenazas y mecanismos de protección
1	Conceptos generales sobre malware y protección anti-malware en el ENS
2	Configuración segura DNS y protección contra Denegación de Servicio
3	Configuración segura de servicios Web y correo electrónico

### **Examen módulo 1/2 (1.5, 1.6, 1.7)**

1.7 Monitorización de sistemas, métricas y gestión de incidentes

1 Concepto general de gestión de incidentes

2 Concepto de monitorización de sistemas de información (log,s, SIEM, IDS)

3 Herramientas de seguridad

4 Análisis forense y cadena de custodia

5 Generalidades sobre metodologías de configuración segura

6 Registro de actividad de usuarios

7 Métricas en el ENS

8 Herramientas de monitorización, gestión de incidentes y métricas en el ENS

1.8 Continuidad, respaldo y resiliencia

1 Plan de continuidad y análisis de impacto

2 Sistemas de respaldo y recuperación. Gestión y destrucción de dispositivos de almacenamiento.

1.9 Control de acceso, autenticación y criptografía

1 Generalidades sobre criptografía y pseudonimización

2 Generalidades sobre autenticación, accesos remotos y VPN

3 Criptografía, autenticación y firma digital en el ENS

### **Examen módulo 1/3 (1.8, 1.9, 1.10)**

1.10 Implementación técnica.

1 Conceptos generales de redes: routers, switches, cortafuegos

2 Securización de firewalls, routers, switches, cortafuegos en el ENS

3 Interconexión de sistemas en el ENS

4 Securización de redes Wi-fi y Bluetooth

5 Seguridad de dispositivos móviles

6 Conceptos generales sobre arquitectura de sistemas Windows (AD, Kerberos, etc.)

7 Seguridad de servidores Windows miembro y controlador de dominio

8 Seguridad de cliente Windows 10 aislado y en dominio

9	Seguridad de otros servidores Windows: impresoras, servidor ficheros
10	Empleo de herramienta auditoría Windows CLARA
11	Conceptos generales arquitectura sistemas Linux
12	Seguridad en un sistema servidor Linux
13	Generalidades sobre la nube
14	Perfil de cumplimiento sistemas en la nube privados
15	Sistemas MS Azure. Teoría.
16	Configuración de seguridad Azure. Aplicación.
17	Perfil de cumplimiento SAAS: Office 365.
18	Conceptos básicos de virtualización y contenedores
19	Seguridad de la virtualización en el ENS

#### **Examen módulo 1/4 (1.11)**

### **Módulo 2 Auditoría y certificación en el ENS**

2.1. La auditoría-1

2.1 La auditoría del ENS

2.2. La certificación del ENS, certificación de productos y personas

#### **Examen módulo 2**

### **Módulo 3 ENS y gestión empresarial**

3.1. La Seguridad Nacional. Derecho de la ciberseguridad

3.2 ENS - ISO 27001

3.3 ENS - RGPD

3.4 Protección de instalaciones críticas. Legislación

3.5 Protección de instalaciones críticas. Sistemas de información

#### **Examen módulo 3**

## **METODOLOGÍA**

Las sesiones síncronas se realizarán los lunes, miércoles y viernes de 16:00 a 19:00.

Las clases presenciales (tele-formación) se impartirán en sesiones de tres horas con dos tipos de contenidos:

1. Sesiones expositivas. El profesor o profesora expondrá los contenidos de una forma clara, amena y estructurada, de forma que el estudiante sea capaz de asimilarlos, entenderlos y aplicarlos.
2. Sesiones demostrativas. El profesor o profesora llevará a cabo la implementación de una configuración técnica o la redacción de un documento, paso a paso, para que el estudiante pueda conocer en detalle el proceso, entenderlo, y ser capaz de hacerlo por sí mismo cuando sea necesario.

La duración total de las sesiones presenciales será de 175 horas

Además de las clases presenciales, la superación del curso y la obtención del diploma y del certificado de experto en ENS requiere del estudiante la resolución de un caso práctico que confirme que ha asimilado los conocimientos recibidos y es capaz de desarrollar por sí mismo el conjunto de documentación necesaria para la correcta implementación del Esquema Nacional de Seguridad. El participante recibirá una documentación preparatoria asociada a un escenario representativo. Sobre dicho escenario, el participante deberá ser capaz de redactar adecuadamente, al menos, los documentos siguientes:

- La política de seguridad de la organización, incluida la estructura de seguridad.
- Los procedimientos y normas de seguridad asociados a las medidas de seguridad aplicables.
- El proceso del análisis de riesgos y su resultado.
- El proceso de categorización del sistema y su resultado.
- El análisis de impacto y los resultados en cuanto a disponibilidad.
- La declaración de aplicabilidad.
- El plan de adecuación de la organización.
- El plan de auditoría del sistema.

Se estima que la resolución del caso práctico planteado requerirá una carga lectiva de 80 horas aproximadamente.

El caso práctico será evaluado por los docentes. Para poder obtener el certificado final del curso será necesario obtener una puntuación de 8/10.

Además, la obtención del Curso de Experto en el Esquema Nacional de Seguridad requiere la superación de seis exámenes a lo largo del curso y un examen final.

El formato de los exámenes será el de preguntas con respuesta múltiple. El mecanismo de remisión del examen, su compleción y remisión en tiempo se ajustará a las características del sistema de tele-formación empleado durante el curso.

## COORDINACIÓN

El curso está dirigido y coordinado por:

**José Salvador.**

Coronel ejército de Tierra en Reserva. CISA, Cybersecurity Auditor, más de 20 años de experiencia en Sistemas de información.

**Jesús Lizarraga**

Profesor de Mondragon Unibertsitatea y coordinador del área de Telemática y Ciberseguridad de la Facultad de Ingeniería.

El equipo docente está integrado por profesionales con amplia experiencia tanto en la implantación del ENS como en la realización de auditorías de su cumplimiento.

## **ORGANIZACIÓN**

Este curso está organizado en colaboración con IVAC Instituto de Certificación

## **TITULACIÓN QUE SE OBTIENE**

Título de Experto Universitario en el Esquema Nacional de Seguridad por Mondragon Unibertsitatea.

Los que no cumplan las condiciones para obtener el título de experto universitario, recibirán diploma acreditativo de la realización del curso experto

---

<https://www.mondragon.edu/cursos/es/curso/None>