Diplomado en Blindaje Digital y Ciberseguridad

AENOR

DIRIGIDO A:

Directores(as), gerentes y profesionales de tecnologías de la información, seguridad digital, ciberseguridad y compliance que deseen fortalecer sus conocimientos y habilidades en blindaje digital y ciberseguridad. Esta formación es ideal para quienes buscan implementar sistemas de gestión de la seguridad de la información y ciberseguridad robustos y alineados con normas internacionales, protegiendo así los activos digitales y minimizando los riesgos cibernéticos en sus organizaciones.

OBJETIVOS:

- Adquirir los conocimientos y habilidades necesarios para implementar sistemas de gestión de seguridad de la información basados en la norma ISO/IEC 27001:2022, asegurando la protección integral de los activos digitales de la organización mediante un enfoque sistemático y estructurado.
- Comprender y aplicar los principios de ciberseguridad definidos en normas ISO, como la ISO/IEC 27032, para responder de manera proactiva a las amenazas y vulnerabilidades digitales, fortaleciendo la capacidad de respuesta ante incidentes y mejorando la resiliencia organizacional.
- Promover una cultura organizacional de ciberseguridad, sensibilizando a todos los niveles sobre la importancia de proteger la información y cumplir con estándares internacionales, y fomentando prácticas continuas de mejora y protección de datos.

Con esta formación contribuyes al cumplimiento de los Objetivos de Desarrollo Sostenible:

PERFIL DEL PROGRAMA:

Modalidades

Online

Presencial

Live Streaming

CONOCIMIENTOS PREVIOS:

Para aprovechar al máximo los contenidos de esta formación, es recomendable que los participantes cuenten con conocimientos básicos en gestión de tecnologías de la información, seguridad digital o experiencia en áreas de sistemas o auditoría, ya que el diplomado aborda temas avanzados de implementación de sistemas de seguridad de la información y ciberseguridad.

122h

DURACIÓN

ENTREGABLES

Porcentaje mínimo aprobatorio 80%

- **Diploma AENOR** de aprobación o asistencia (según acreditación de la formación) con reconocimiento internacional
- **Constancia AENOR** por módulo
- **Certificado AENOR** sobre el/los módulos de auditorías aplicables

INCLUYE:

Normas propias del curso en formato digital.

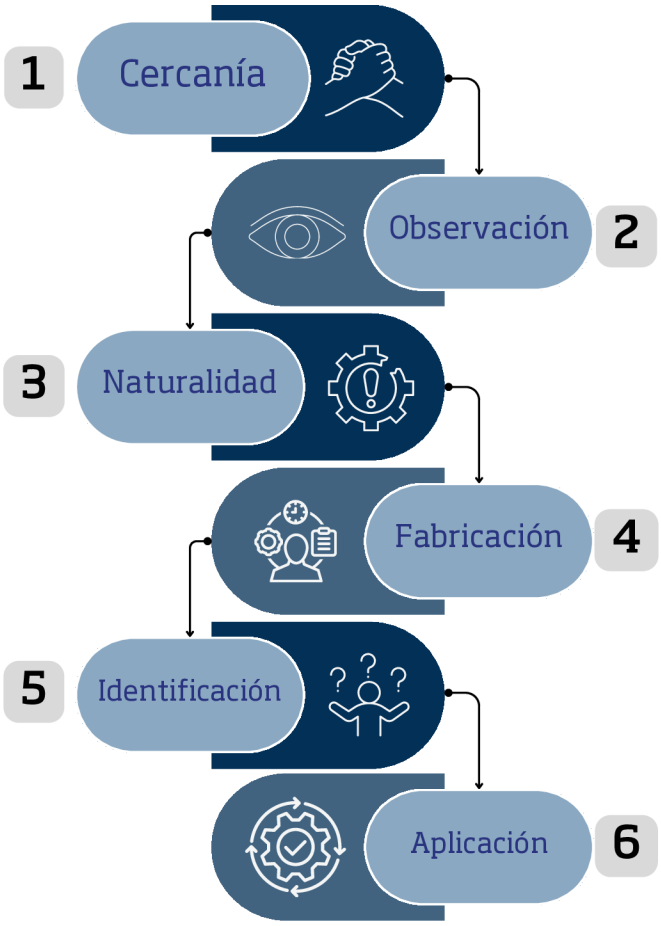
Material en formato digital

AENOR

NUESTRA PROPUESTA DE VALOR

- Nuestros instructores e instructoras utilizan la metodología de enseñanza exclusiva: **CONFIA**, diseñada por **Campus AENOR** específicamente para el sector empresarial.
- En un entorno laboral **dinámico y exigente**, esta metodología ofrece un marco **adaptable y práctico** que fomenta la autodirección y aprovecha la experiencia previa de los participantes, asegurando que el conocimiento adquirido sea relevante y aplicable en su **entorno laboral inmediato.**

METODOLOGÍA CONFIA



Ofrecemos **dos tipos de formación** adaptadas a tus necesidades:

1. **La formación abierta** es ideal para quienes buscan interactuar con profesionales de diversas industrias y fomentar el **intercambio de ideas y experiencias valiosas.**

2. Por otro lado, **la formación In Company** es perfecta para aquellos que desean una formación personalizada que aborde **temas y desafíos específicos** de su empresa u organización, alineándose con **sus objetivos y cultura organizacional.**

AENOR

CONTENIDO

- **MÓDULO 1. Introducción (2 h)**

  - Presentación del curso
  - Objetivo
  - Importancia
  - Alcance
  - Criterios de evaluación y dinámica grupal
  - Material de los participantes
  - Resolución de dudas

- **MÓDULO 2. Interpretación ISO 27001:2022 y Gestión de Riesgos en Seguridad de la Información ISO 27005:2018 (20 h)**

  - Introducción al Sistema de Gestión de Seguridad de la Información (SGSI)
  - Conceptos clave y beneficios de implementar un SGSI
  - Antecedentes de la norma ISO/IEC 27001
  - Evolución histórica y relación con otras normas ISO de seguridad de la información
  - Requisitos y directrices del SGSI
  - Objetivo y campo de aplicación
  - Referencias normativas
  - Términos y definiciones relevantes
  - Análisis detallado de los requisitos de ISO/IEC 27001:2022
  - Contexto de la organización
  - Liderazgo
  - Planificación
  - Apoyo
  - Operación
  - Evaluación del desempeño
  - Mejora continua
  - Introducción a la gestión de riesgos en seguridad de la información

CONTENIDO

- Importancia del análisis y gestión de riesgos en un SGSI
- Normas aplicables al proceso de gestión de riesgos
- UNE 71504, ISO/IEC 27005 e ISO/IEC 31000
- Análisis de riesgos
- Procesos de identificación y valoración de riesgos
- Valoración de impactos, amenazas y riesgos (uso de matriz)
- Gestión de riesgos
- Procesos de selección de controles (criterios y objetivos)
- Evaluación del riesgo residual
- Desarrollo de un proyecto de análisis y gestión de riesgos
- Diseño de un proyecto de gestión de riesgos aplicable a casos reales
- Aplicación del análisis y gestión de riesgos a un caso práctico desarrollado a lo largo del módulo
- Certificación del sistema de gestión de la seguridad de la información
- Requisitos y pasos clave para obtener la certificación conforme a ISO/IEC 27001

- **MÓDULO 3. Implementación de un SGSI Basado en ISO/IEC 27001:2022 (20 h)**

  - Estructura del SGSI: aplicación práctica de ISO/IEC 27001.
  - Enfoque detallado en la implementación de controles técnicos y operativos.
  - Ejercicio práctico: Creación de políticas, procedimientos y planes de acción.
  - Ejercicio práctico: Plan de una auditoría interna

- **MÓDULO 4. Auditorías Internas de Sistemas de Gestión de la Información según ISO/IEC 19011 (16 h)**

  - Razones y objetivos para realizar auditorías internas de un SGSI
  - Normas aplicables: ISO/IEC 27001, ISO/IEC 27002 e ISO 19011
  - Procesos y fases de auditoría

CONTENIDO

- Planificación
- Desarrollo
- Elaboración de informes
- Ejercicio práctico: Simulación de una auditoría interna

- **MÓDULO 5. Gestión de Ciberseguridad según ISO/IEC 27032 (20 h)**

  - Principios de ciberseguridad según ISO/IEC 27032
  - Identificación y evaluación de ciberamenazas
  - Respuesta a incidentes: detección, contención, erradicación y recuperación
  - Gestión de ciberseguridad en la cadena de suministro ISO/IEC 27036
  - Ejercicio práctico: Diseño de un plan de respuesta ante amenazas digitales

- **MÓDULO 6. Seguridad en la Nube y Privacidad de Datos ISO/IEC 27017, 27018 y 27701 (20h)**

  - Principios de seguridad y controles específicos para la nube ISO/IEC 27017
  - Protección de datos personales en servicios cloud ISO/IEC 27018
  - Gestión de privacidad y cumplimiento normativo ISO/IEC 27701
  - Evaluación de riesgos y controles en un entorno cloud

- **MÓDULO 7. ·Resiliencia Organizacional y Continuidad del Negocio ISO/IEC 22301 (6 h)**

  - Introducción a la resiliencia organizacional y continuidad del negocio
  - Diseño de planes de recuperación tras ciberincidentes
  - Simulación de un plan de continuidad del negocio

CONTENIDO

- **MÓDULO 8. Cultura Organizacional y Métricas en Seguridad de la Información ISO/IEC 27004 (12 h)**
    - Definición y medición de indicadores clave de desempeño (KPIs)
    - Estrategias para sensibilización y cultura organizacional de ciberseguridad
    - Ejercicio práctico: Diseño de un programa de sensibilización para empleados
- **MÓDULO 9. Presentación de proyectos y clausura (6 h)**
    - Presentación de proyectos
    - Clausura
    - Sesión de networking en modalidad presencial o virtual según la disponibilidad de los y las participantes