vuela | Junta de Andalucía

# Dirección y Gestión de Ciberseguridad

*Curso Blended* | *Nivel Avanzado* | *40h* | *01/06 al 28/06* | *De 25 a 45 plazas*

## ¿QUÉ VAS A APRENDER?

Este curso de ciberseguridad está diseñado para proporcionar a los estudiantes una comprensión completa de los fundamentos de la ciberseguridad y su aplicación en el mundo empresarial. Los participantes aprenderán sobre la gobernanza y los frameworks de ciberseguridad, así como la gestión de riesgos, la gestión de la cadena de suministro, la gestión de la identidad y la resiliencia en el contexto de la ciberseguridad con el fin de concebirla como uno de los principales riesgos de la economía del mundo.

## Parte eLearning → 20 horas

### OBJETIVOS:

Comprender los fundamentos de la ciberseguridad, incluyendo los riesgos y amenazas que enfrentan las organizaciones en la actualidad, y cómo se puede abordar la ciberseguridad desde una perspectiva de gestión.

### CONTENIDOS:

**Módulo 1: Introducción a los fundamentos de la ciberseguridad (3 horas)**

1. Triada CIA
2. Principios de seguridad
3. Tendencias actuales
4. Seguridad en diferentes casos de uso

**Actividad** → Ejemplos reales de triada CIA.

## OBJETIVOS:

Aprender a diseñar e implementar una estrategia de gobernanza de la ciberseguridad, incluyendo la definición de políticas, normas y procedimientos para proteger los sistemas y datos de la organización.

## CONTENIDOS:

**Módulo 2: Gobernanza en la ciberseguridad (3 horas)**

1. Roles en ciberseguridad
2. Políticas de seguridad
3. Seguridad de activos
4. Formación y concienciación

**Actividad** → Elaboración de una política de seguridad

## OBJETIVOS:

Adquirir conocimientos avanzados en los frameworks de ciberseguridad, incluyendo la comprensión de los estándares internacionales y las mejores prácticas en la gestión de la seguridad de la información.

## CONTENIDOS:

**Módulo 3: Frameworks de ciberseguridad. (3 horas)**

1. Esquema Nacional de Seguridad
2. ISO 27001
3. Controles CIS
4. NIST CSF
5. Otros

**Actividad** → Ampliación de frameworks de seguridad

## OBJETIVOS:

Desarrollar habilidades avanzadas en el análisis y gestión de riesgos, incluyendo la identificación y evaluación de amenazas, la mitigación de riesgos y la implementación de controles para proteger los sistemas y datos de la organización.

## CONTENIDOS:

**Módulo 4: Análisis y gestión de riesgos (3 horas)**

1. Introducción al análisis y gestión de riesgos
2. Tipos de tratamiento de riesgos
3. Amenazas y vulnerabilidades
4. Probabilidad, impacto y riesgo
5. Contramedidas

**Actividad** → Elaboración de un caso de uso con ejemplo de tratamiento de riesgos.

## OBJETIVOS:

Aplicar técnicas avanzadas de gestión de riesgos en la cadena de suministro, diseñar y ejecutar políticas de seguridad para la selección y el monitoreo de proveedores, y desarrollar estrategias para la recuperación y continuidad del negocio frente a interrupciones en la cadena de suministro.

## CONTENIDOS:

**Módulo 5: Gestión de la cadena de suministro (2 horas)**

1. Principios de seguridad en cadena de suministro
2. Estado actual de ataques a cadena de suministro
3. Evaluación y buenas prácticas para gestionar la seguridad en los proveedores

**Actividad** → Proposición de listado de herramientas Software a usar para la gestión de la cadena de suministro

## OBJETIVOS:

Aplicar técnicas avanzadas de autenticación y autorización de usuarios, diseñar e implementar políticas de gestión de contraseñas seguras, identificar y remediar amenazas a la integridad de la identidad digital y desarrollar e implementar estrategias de gestión de identidad y acceso para proteger los sistemas y datos críticos de la organización.

## CONTENIDOS:

**Módulo 6: Gestión de la identidad (3 horas)**

1. Control de acceso
2. Tipos de autenticación
3. Mecanismos de autorización
4. Ciclo de vida

**Actividad** → Caso de uso para implantar IAM

## OBJETIVOS:

Diseñar e implementar un plan de continuidad del negocio para minimizar el impacto de incidentes de ciberseguridad, analizar y evaluar la efectividad de los controles de seguridad existentes y desarrollar estrategias de recuperación y respuesta a incidentes de ciberseguridad, incluyendo la capacidad de identificar y mitigar amenazas persistentes avanzadas y mantener la disponibilidad de los sistemas y datos críticos de la organización en situaciones de crisis.

## CONTENIDOS:

**Módulo 7: Resiliencia (3 horas)**

1. Continuidad del Negocio y Recuperación ante desastres
2. Gestión de incidentes
3. Registros y monitorización

**Actividad** → Listado de escenarios para la recuperación ante desastres

# Sesiones online en directo → 20 horas

## OBJETIVOS:

El principal objetivo de estas sesiones es que apliquen la parte elearning mediante ejercicios prácticos. Por ello, se usará la metodología flipped clasroom.

## CONTENIDOS:

**Sesión 1 Gestión de activos → 4 horas.**
(Relacionado con módulo 2).

- **Temática a tratar**: Implantación y uso de una herramienta de gestión de activos para automatizar partes del ciclo de vida de la gestión de activos.

**Sesión 2 Aplicación de un framework de ciberseguridad→ 4 horas.**
(Relacionado con módulo 3).

- **Temática a tratar:** Aplicación de un framework de ciberseguridad para un caso de uso a tratar

**Sesión 3 Análisis y gestión de riesgos→ 4 horas.**
(Relacionado con módulo 4)

- **Temática a tratar:** Ejercicio práctico de análisis y gestión de riesgos a través de una herramienta que automatiza partes del proceso.

**Sesión 4 Modelado de amenazas → 4 horas.**
(Relacionado con módulo 4)

- **Temática a tratar:** Elaboración de modelado de amenazas a través de metodología STRIDE usando una herramienta que usa diagramas para ello.

**Sesión 5 Ejercicios de recuperación ante desastres→ 4 horas.**
(Relacionado con módulo 7).

- **Temática a tratar:** Planteamiento de distintos escenarios con toma de decisiones en recuperación ante desastres.

Para la impartición de esta AAFF se realizará mediante la modalidad flipped classroom más online en directo de la siguiente forma:

- El **contenido interactivo** estará **disponible** en la **plataforma** online, de manera que será de **libre consulta** para el alumnado y este deberá haberse organizado de manera autónoma bajo las recomendaciones que se le marquen para haber consultado la lección o módulo correspondiente.
    - Con ello lo que se busca es un mayor protagonismo en el proceso de E-A y que el alumnado se involucre más en el mismo, mejorando su trabajo individual.
- Posteriormente, en la **sesión online**, se tratará el caso de uso de lo que ya el estudiante ha visto y leído, por lo que su participación y motivación será mucho más activa.
    - El objetivo de esto es fomentar un aprendizaje más profundo y significativo de manera que son ellos los que buscan construir sus conocimientos, a la par que esto permitirá mejorar el trabajo colectivo mediante los proyectos que compartan

### Valor añadido → Permite atender a la diversidad del aula

Los alumnos visionan los contenidos tantas veces como quieran y tienen a las tutorías del profesor para resolver sus dudas de manera individualizada.

## ¿A QUIÉN ESTÁ DIRIGIDO?

- Profesionales del sector TIC en Andalucía.
- Perfiles TIC de empresas de Andalucía.

## REQUISITOS DE ACCESO:

Podrá participar cualquier trabajador de empresas del sector TIC andaluz, o que tenga perfil TIC y que trabaje en una empresa andaluza de cualquier otro sector.

Estricto orden de llegada hasta completar plazas.

## CONOCIMIENTOS MÍNIMOS REQUERIDOS:

- Acceso a Internet
- Conocer algún lenguaje de programación.
- Conocimientos de ciberseguridad a nivel básico/medio.

## EQUIPO DOCENTE

### Ismael Morales Alonso

Ingeniero Técnico en Informática de Sistemas, Ingeniero en Informática y Máster de Investigación en Ingeniería de Sistemas y de la Computación por la Universidad de Cádiz. Auditor Jefe y Especialista Implantador de ISO 27001 por AENOR, CISSP por ISC2, CSX por ISACA y SCCISP por IoTSI Institute. CISO en Swapcard. Ha trabajado para numerosos proyectos de ciberseguridad para el sector público y privado, centrándose en los últimos años a la ciberseguridad en el entorno de las Smart Cities.

https://www.linkedin.com/in/ismaelmoralesalonso/

### Enrique Villa Crespo

Ingeniero de Telecomunicaciones por la Universidad de Sevilla. Profesor del Máster de Ciberseguridad de la Universidad de Sevilla. SCCISP por IoTSI Institute y Cisco CCNP/CCDP. CEO de IRIS Sentinel y CTO de Wellness Techgroup. Ha trabajado en el ciclo de vida completo del negocio de desarrollo e implantación de productos de IoT para Smart Cities, y en proyectos de Ciberseguridad IT/OT/IoT nacionales e internacionales en el sector público y privado.

https://www.linkedin.com/in/enrique-villa-crespo-65643713/

## CALENDARIO:

- **Fecha inicio del curso:**
  01/06/2023
- **Fecha impartición sesiones online en directo:**
- 15, 19, 20 21 y 22 de junio en horario de 16:30 a 20:30
- **Fecha fin del curso:**
  28/06/2023

## EVALUACIÓN:

**Obligatorio para obtener el certificado:**

- **[20%] La asistencia a las clases** o su visionado posterior. Estos vídeos se subirán a la plataforma y se establecerán los mecanismos para verificar que el alumnado que no asistió sí que visualizó el vídeo de manera asíncrona.
  - El mínimo de vídeos o asistencia a las clases para la titulación es de 4.
- **[30%] Visualización de contenido formativo.** Por medio de la lectura del SCORM.
  - Deberán ver al menos el 75% del contenido o lo que equivale a 6 módulos.
- **[30%] Realización de pruebas de conocimientos.** Que se colgarán mediante una batería de preguntas en la plataforma con orden aleatorio.
  - Deberán sacar un mínimo de un 5 al menos en 6 de los 7 módulos.

**No es obligatorio pero sí muy recomendable:**

- **[20%] Actividades.** Serán de carácter no evaluable pero servirá de preparación para las sesiones online en directo y además se ofrecerá retroalimentación.

## CERTIFICADO

Una vez superadas todas las evaluaciones de los módulos del curso y habiendo asistido al número mínimo de clases exigido, podrás obtener la certificación.

El certificado se emitirá digitalmente en formato pdf incluyendo la siguiente información:

- Datos del alumno.
- Datos del curso: título, fecha de impartición, duración, contenidos impartidos.
- Sello y firma digitalizada de la empresa impartidora del curso. El certificado no lleva firma digital ni sello/firma de la Junta de Andalucía

Ten en cuenta que estos cursos no tienen validez académica ni acreditación de créditos universitarios.

**Es obligatoria la entrega de la Declaración Responsable firmada electrónicamente para la obtención del certificado del curso.**

## OTRAS CUESTIONES DE INTERÉS SEGÚN LA TIPOLOGÍA DE AAFF:

Una posible orientación al tiempo dedicado al estudio, lectura y visualización del contenido sería la siguiente:

- Tiempo de consulta de contenidos y vídeos: 15 horas.
- Tiempo de realización de actividades: 1,5 horas.
- Tiempo de realización de exámenes: 2 horas.
- Tiempo de consulta en foros e interacción con los compañeros: 1,5 horas.
- Asistencia a las sesiones online en directo: 20 horas.

De todas formas y al tratarse de un curso abierto y parcialmente en línea, cada alumno podrá seguir su propio ritmo de aprendizaje siempre y cuando cumpla con los criterios mínimos de evaluación para la obtención del certificado de formación.