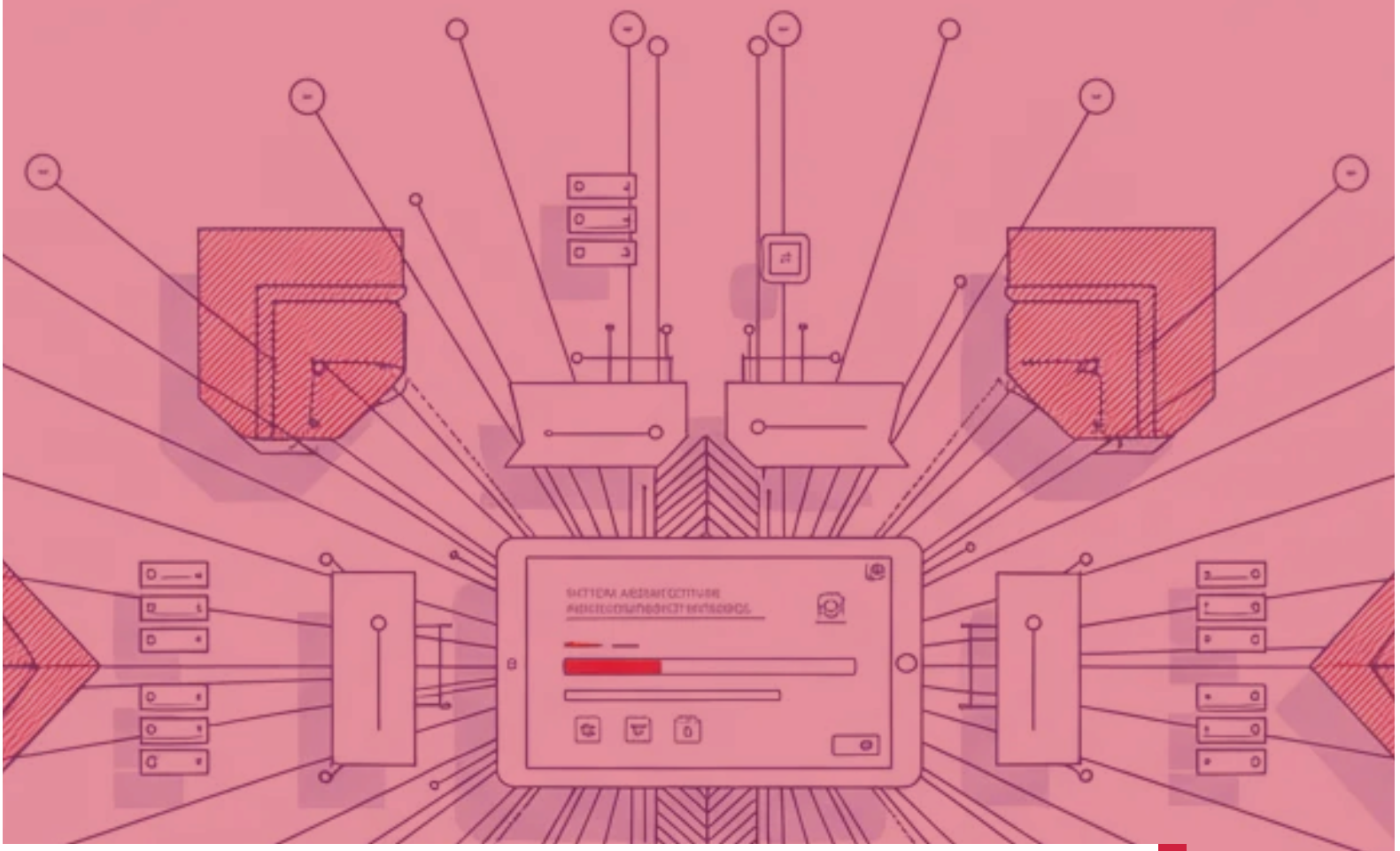


Máster online 100%

Máster en Ciberseguridad y Gestión de Riesgos en la Información + 60 Créditos ECTS

Structuralia

Máster online 100%

Máster en Ciberseguridad y Gestión de Riesgos en la Información + 60 Créditos ECTS

Modalidad
Online

Idiomas
Español

Duración
1500 horas (60 ECTS)

Sin Límite
Asistente IA

¿Incluye prácticas?
NO

Instituciones Educativas

Structuralia Engineering eLearning

UNIVERSIDAD NEBRIJA

Resumen

El Máster en Ciberseguridad y Gestión de Riesgos en la Información es una especialización de alto nivel diseñada para profesionales que buscan consolidar su experiencia y desarrollar una visión estratégica en la protección de activos digitales y la resiliencia organizacional. Este programa te permite profundizar en la complejidad de las vulnerabilidades empresariales, abarcando desde el análisis de riesgos asociados a las redes sociales hasta la implementación de detección proactiva y protecciones avanzadas. Dominarás los principios y buenas prácticas para la protección integral de la información, abordando la gestión de riesgos mediante la identificación, evaluación y mitigación de amenazas sofisticadas. Explorarás el marco de normativas, regulaciones y legislación aplicable a nivel global, así como la implementación y auditoría de Sistemas de Gestión de la Seguridad de la Información (SGSI), elementos fundamentales para una gobernanza efectiva. Desarrollarás una visión estratégica para el diseño e implementación de programas de ciberseguridad robustos, preparándote para securizar entornos cloud, de Internet e industriales con soluciones de vanguardia. Esta formación te dota de las competencias para liderar iniciativas de desarrollo seguro y gestionar identidades digitales complejas, garantizando la integridad y confidencialidad de los datos críticos. El programa valida y actualiza tus conocimientos, fortaleciendo tu trayectoria

profesional en seguridad informática y gestión de riesgos, permitiéndote tomar decisiones estratégicas en un entorno digital que exige adaptación continua.

Temario

MÓDULO 1. VULNERABILIDADES EN LA EMPRESA. CIBERSEGURIDAD

1. UNIDAD DIDÁCTICA 1. VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN. ANÁLISIS DE RIESGOS ASOCIADOS A LAS REDES SOCIALES

1. Introducción
2. Estado del arte
3. Análisis
4. Actuación
5. Resumen de la unidad

2. UNIDAD DIDÁCTICA 2. DETECCIÓN, ANÁLISIS DE RIESGOS Y PROTECCIONES GENÉRICAS

1. Introducción
2. Detección
3. Análisis
4. Protecciones genéricas
5. Resumen de la unidad

3. UNIDAD DIDÁCTICA 3. PRINCIPIOS Y BUENAS PRÁCTICAS DE LA SEGURIDAD DE LA INFORMACIÓN. GESTIÓN DE RIESGOS DE SEGURIDAD. TIPOS DE AMENAZAS Y VULNERABILIDADES

1. Introducción
2. Buenas prácticas
3. Gestión de riesgos y mitigantes
4. Amenazas y vulnerabilidades
5. Resumen de la unidad

4. UNIDAD DIDÁCTICA 4. NORMATIVAS, REGULACIONES Y LEGISLACIÓN. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. Introducción
2. Definición y objetivos
3. Regulaciones
4. Sistemas de gestión de seguridad de la información
5. Resumen de la unidad

MÓDULO 2. DESARROLLO SEGURO Y GESTIÓN DE IDENTIDAD. CIBERSEGURIDAD

1. UNIDAD DIDÁCTICA 1. VULNERABILIDADES EN LA SEGURIDAD DE LA INFORMACIÓN. ANÁLISIS DE RIESGOS ASOCIADOS A LAS REDES SOCIALES

1. Introducción
2. Estado del arte
3. Análisis
4. Actuación
5. Resumen de la Unidad Didáctica

2. UNIDAD DIDÁCTICA 2. DETECCIÓN, ANÁLISIS DE RIESGOS Y PROTECCIONES GENÉRICAS

1. Introducción
2. Detección
3. Análisis
4. Protecciones genéricas
5. Resumen de la Unidad Didáctica

3. UNIDAD DIDÁCTICA 3. PRINCIPIOS Y BUENAS PRÁCTICAS DE LA SEGURIDAD DE LA INFORMACIÓN. GESTIÓN DE RIESGOS DE SEGURIDAD. TIPOS DE AMENAZAS Y VULNERABILIDADES

1. Introducción
2. Buenas prácticas
3. Gestión de riesgos y mitigantes
4. Amenazas y vulnerabilidades
5. Resumen de la Unidad Didáctica

4. UNIDAD DIDÁCTICA 4. NORMATIVAS, REGULACIONES Y LEGISLACIÓN. SISTEMAS DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

1. Introducción
2. Definición y objetivos
3. Regulaciones
4. Sistemas de gestión de seguridad de la información
5. Resumen de la Unidad Didáctica

MÓDULO 3. IDENTIDAD DIGITAL, REPUTACIÓN. FAKE NEWS, SOCINT Y DOCXING. CIBERSEGURIDAD

1. UNIDAD DIDÁCTICA 1. TIPOLOGÍA DE REDES SOCIALES

1. Introducción
2. Tipos de Redes Sociales
3. Conceptos en Redes Sociales
4. Seguridad en Redes Sociales
5. Resumen de la Unidad
6. Referencias

2. UNIDAD DIDÁCTICA 2. AMENAZAS Y MITIGANTES EN REDES SOCIALES

1. Introducción
2. Amenazas en Redes Sociales
3. Mitigantes
4. Herramientas de Seguridad
5. Resumen de la Unidad

3. UNIDAD DIDÁCTICA 3. DOXXING Y SOCINT

1. Introducción
2. Técnicas de Doxxing
3. Técnicas Socmint

4. Herramientas
5. Resumen de la Unidad
6. Referencias

4. UNIDAD DIDÁCTICA 4. INTOXICACIÓN DE LA INFORMACIÓN. FAKE NEWS. TÉCNICAS Y ANÁLISIS

1. Introducción
2. Intoxicación de la Información
3. Análisis de la Información
4. Técnicas de Detección de Fake News
5. Resumen de la Unidad
6. Referencias Bibliográficas

MÓDULO 4. MALWARE Y CÓDIGOS MALICIOSOS. CIBERSEGURIDAD

1. UNIDAD DIDÁCTICA 1. CONCEPTOS BÁSICOS DE ATAQUES

1. Introducción
2. Definición y Tipos de Malware
3. Análisis Estático y Dinámico
4. Terminología
5. Resumen de la Unidad
6. Referencias

2. UNIDAD DIDÁCTICA 2. TIPOS DE MALWARE I

1. Introducción
2. Virus y Gusanos
3. Troyanos
4. Spyware y Phising
5. Resumen de la Unidad
6. Referencias

3. UNIDAD DIDÁCTICA 3. TIPOS DE MALWARE II

1. Introducción
2. Rootkits
3. Ransomware
4. Otros Tipos
5. Resumen de la Unidad
6. Referencias

4. UNIDAD DIDÁCTICA 4. VULNERABILIDADES, EXPLOITS Y PAYLOADS

1. Introducción
2. Arquitectura de Metasploit
3. Exploits
4. Payloads
5. Resumen de la Unidad
6. Referencias

MÓDULO 5. CRIPTOGRAFÍA PARA EMPRESAS. CIBERSEGURIDAD

1. UNIDAD DIDÁCTICA 1. CONCEPTOS BÁSICOS DE ATAQUES

1. Introducción
2. Tipos y definiciones
3. Análisis estático
4. Análisis dinámico
5. Resumen de la Unidad Didáctica

2. UNIDAD DIDÁCTICA 2. TIPOS DE MALWARE (I)

1. Introducción
2. Virus y gusanos
3. Troyanos
4. Spyware, Phising
5. Resumen de la Unidad Didáctica

3. UNIDAD DIDÁCTICA 3. TIPOS DE MALWARE (II)

1. Introducción
2. Rootkits
3. Ransomware
4. Otros tipos
5. Resumen de la Unidad Didáctica

4. UNIDAD DIDÁCTICA 4. VULNERABILIDADES, EXPLOITS Y PAYLOADS

1. Introducción
2. Vulnerabilidades
3. Exploits
4. Payloads
5. Resumen de la Unidad Didáctica

MÓDULO 6. SEGURIDAD EN REDES CORPORATIVAS INTRODUCCIÓN. CIBERSEGURIDAD

1. UNIDAD DIDÁCTICA 1. SEGURIDAD EN REDES LOCALES

1. Introducción
2. Protocolos En Redes Locales
3. Análisis En Redes Locales
4. Identificación De Amenzas Y Vulnerabilidades
5. Resumen De La Unidad
6. Bibliografía

2. UNIDAD DIDÁCTICA 2. COMUNICACIÓN Y REDES LOCALES DISTRIBUIDAS. EXTRANET

1. Introducción
2. Accesos Externos A Redes Locales. Vpn
3. Comunicaciones Entre Redes Locales
4. Vulnerabilidades En Extranets
5. Como Ver Que Pasa En Nuestra Red
6. Referencias

3. UNIDAD DIDÁCTICA 3. SEGURIDAD EN ARQUITECTURAS BASADAS EN LINUX

1. Introducción
2. Definiciones De Políticas De Accesos
3. Accesos A Servidores Locales. Acl
4. Firewalls, Proxies Y Otros Mecanismos
5. Arquitecturas Basadas En Linux
6. Referencias

4. UNIDAD DIDÁCTICA 4. SEGURIDAD EN ARQUITECTURAS BASADAS EN CLOUD

1. Introducción A La Seguridad En Arquitecturas Cloud
2. Arquitecturas Típicas
3. Opciones, Proveedores Y Objetivos
4. Gestión De Acceso E Identidades
5. Políticas De Seguridad De La Red
6. Referencias

MÓDULO 7. SEGURIDAD WEB. CIBERSEGURIDAD

1. UNIDAD DIDÁCTICA 1. ¿CÓMO FUNCIONA LA WEB?

1. ¿Cómo funciona la web?
2. Protocolos Http Y Https
3. Dominios Y Dns
4. Servidores
5. Puertos Y Otros Protocolos
6. Referencias

2. UNIDAD DIDÁCTICA 2. SEGURIDAD WEB

1. Tipos De Amenazas Web
2. Objetivos
3. Objetivos (II)
4. Objetivos (III)
5. Objetivos (IV)
6. Referencias

3. UNIDAD DIDÁCTICA 3. TÉCNICAS DE ATAQUE A SITIOS WEB

1. Introduccion
2. Cross Site Scripting Xss
3. Sql Injection
4. Pérdida De Autenticación
5. Otras Vulnerabilidades
6. Referencias

4. UNIDAD DIDÁCTICA 4. ACCIONES PARA MEJORAR LA SEGURIDAD WEB

1. Servidor Seguro
2. Servidores Web. Securización De Apache (I)
3. Securización De Apache (II)
4. Nginx
5. Otras Medidas

6. Referencias

MÓDULO 8. SEGURIDAD OSINT, INVESTIGACIÓN EN FUENTES ABIERTAS.CIBERSEGURIDAD

1. UNIDAD DIDÁCTICA 1. ¿CÓMO FUNCIONA LA WEB?

1. ¿Cómo funciona la web?
2. Protocolos HTTP y HTTPS
3. Dominios y DNS
4. Servidores
5. Puertos y otros protocolos

2. UNIDAD DIDÁCTICA 2. SEGURIDAD WEB

1. Tipos de amenazas web
2. Objetivos (I)
3. Objetivos (II)
4. Objetivos (III)
5. Objetivos (IV)

3. UNIDAD DIDÁCTICA 3. TÉCNICAS DE ATAQUE A SITIOS WEB

1. Introducción
2. Cross-site scripting (XSS)
3. SQL injection
4. Pérdida de autenticación
5. Otras vulnerabilidades

4. UNIDAD DIDÁCTICA 4. ACCIONES PARA MEJORAR LA SEGURIDAD WEB

1. Servidor seguro
2. Securización de apache (I)
3. Securización de apache (II)
4. INGINX
5. Otras medidas

MÓDULO 9. SEGURIDAD INTERNET DE LAS COSAS. CIBERSEGURIDAD

1. UNIDAD DIDÁCTICA 1. ¿QUÉ ES IOT?

1. Introducción al internet de las cosas (IoT)
2. Historia de IoT
3. DAFO de IoT
4. Áreas y sectores
5. Seguridad y privacidad de IoT

2. UNIDAD DIDÁCTICA 2. RETOS DE IOT

1. Introducción a la arquitectura de IoT
2. Modelos de capas
3. Arquitectruas específicas
4. Openfog
5. Desarrollo IoT

3. UNIDAD DIDÁCTICA 3. SEGURIDAD IOT EN PROVEEDORES CLOUD

1. IoT y Big data
2. Aplicaciones IoT
3. Analítica
4. Aplicaciones de la analítica IoT
5. Agregación e integración de datos

4. UNIDAD DIDÁCTICA 4. FRAMEWORKS EN SEGURIDAD IOT

1. Sensores
2. Protocolos de comunicación de sensores, controladores e interfaces
3. Protocolos de comunicación
4. Ataques y medidas preventivas
5. Herramientas y casos prácticos

MÓDULO 10. TFM. MÁSTER EN CIBERSEGURIDAD Y GESTIÓN DE RIESGOS EN LA INFORMACIÓN

Titulación

Titulación Universitaria en Máster de Formación Permanente en Ciberseguridad y Gestión de Riesgos en la Información expedida por la Universidad Antonio de Nebrija con 60 Créditos Universitarios ECTS. Enseñanzas no conducentes a la obtención de una titulación de carácter oficial

Objetivos

- • Liderarás la implementación de programas de defensa digital integrales, adaptados a las necesidades estratégicas de cualquier organización. • Diseñarás arquitecturas de protección robustas para entornos cloud, de Internet e industriales, mitigando vulnerabilidades avanzadas. • Gestionarás eficazmente los riesgos de la información, aplicando metodologías de análisis y evaluación para proteger activos críticos. • Integrarás los Sistemas de Gestión de la Seguridad de la Información (SGSI) con las normativas y regulaciones internacionales, asegurando el cumplimiento legal. • Evaluarás el impacto de las amenazas y vulnerabilidades emergentes, desarrollando estrategias proactivas de detección y respuesta. • Tomarás decisiones estratégicas en la protección de datos y sistemas, basándote en un profundo conocimiento de las buenas prácticas y principios de protección digital. • Implementarás soluciones de desarrollo seguro y gestión de identidad, fortaleciendo la postura de protección desde la fase de diseño. • Dirigirás equipos multidisciplinares en la respuesta a incidentes de seguridad digital, minimizando el daño y garantizando la continuidad operativa.

¿Para qué te prepara?

Este programa te dota de las competencias necesarias para liderar la estrategia de defensa digital en cualquier organización. Adquirirás la capacidad de diseñar e implementar programas de seguridad informática robustos, abarcando desde la identificación proactiva de vulnerabilidades hasta la gestión integral de riesgos. Desarrollarás habilidades para establecer políticas y estrategias efectivas que reduzcan la exposición a amenazas y salvaguarden la información crítica. El Máster en Ciberseguridad y Gestión de Riesgos en la Información te especializa en la evaluación del impacto de las amenazas, permitiéndote asegurar la conformidad y la resiliencia de los sistemas. Estarás preparado para tomar decisiones informadas sobre normativas, regulaciones y legislación aplicable, transformando la forma en que tu organización aborda la seguridad de la información y fortaleciendo su postura ante los desafíos actuales.

¿A quién va dirigido?

Este programa está dirigido a profesionales del sector de la seguridad informática y de los sistemas que ya ejercen en el ámbito de la protección de datos y la gestión de la seguridad de la información. Si buscas validar y actualizar tus conocimientos para fortalecer tu trayectoria profesional con una especialización de alto nivel, este máster te ofrece las herramientas para ello. Es ideal para quienes desean profundizar en la detección de vulnerabilidades, el análisis de riesgos avanzados y la respuesta a incidentes, consolidando su experiencia técnica y estratégica. También está pensado para perfiles orientados a la dirección estratégica de la seguridad digital, con un marcado interés en la implementación de sistemas de gestión de la seguridad y el cumplimiento normativo a escala global.

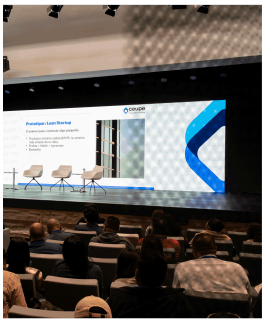
Carácter Oficial

La presente formación no está incluida dentro del ámbito de la formación oficial reglada (Educación Infantil, Educación Primaria, Educación Secundaria, Formación Profesional Oficial FP, Bachillerato, Grado Universitario, Master Oficial Universitario y Doctorado). Se trata por tanto de una formación complementaria y/o de especialización, dirigida a la adquisición de determinadas competencias, habilidades o aptitudes de índole profesional, pudiendo ser baremable como mérito en bolsas de trabajo y/o concursos oposición, siempre dentro del apartado de Formación Complementaria y/o Formación Continua siendo siempre imprescindible la revisión de los requisitos específicos de baremación de las bolsa de trabajo público en concreto a la que deseemos presentarnos.

Salidas Profesionales

- La especialización en la protección de sistemas y la gestión de riesgos te posicionará estratégicamente en el mercado, permitiéndote asumir roles de alta responsabilidad y liderazgo. Podrás desempeñarte como Consultor en Seguridad Digital, aportando soluciones avanzadas en la defensa de infraestructuras críticas y la evaluación de riesgos empresariales. Destacarás como Auditor de Seguridad de la Información, evaluando la robustez de los sistemas y garantizando el cumplimiento normativo de los SGSI. Contribuirás como Ingeniero de Seguridad de Sistemas, integrando la seguridad desde las fases iniciales del desarrollo y la arquitectura tecnológica. Esta formación impulsa tu progresión hacia la dirección técnica y estratégica en el ámbito de la seguridad digital, incluyendo funciones como Analista Forense o Hacker Ético, fortaleciendo la postura de seguridad de cualquier organización.







Vive Madrid

Vive la Semana Internacional

Como complemento adicional a tu formación, podrás formar parte de la SIM: Semana Internacional en Madrid. Un encuentro único que reúne a estudiantes de todo el mundo. Durante siete días podrás vivir una experiencia académica y cultural en el corazón de Europa, culminando con el acto de graduación en Madrid.

- Conferencias y talleres con expertos internacionales
- Visitas a empresas y organismos de referencia
- Networking con alumnos de diferentes países
- Actividades culturales y descubrimiento de Madrid
- Acto de graduación

Structuralia

Structuralia es una institución educativa líder en formación online de posgrado y alta especialización, enfocada en los ámbitos de la ingeniería, la arquitectura, la construcción, la energía, la tecnología y la transformación digital.

Fundada en 2001 con un fuerte ADN industrial, fruto de la colaboración entre grandes empresas del sector y la Universitat Politècnica de Catalunya (UPC), desde hace más de 25 años acompañamos a profesionales técnicos en su desarrollo académico y profesional mediante una formación práctica, flexible y alineada con la realidad del mercado laboral.

uestra propuesta formativa conecta conocimiento técnico avanzado, empleabilidad real y proyección internacional, actuando como apoyo clave en la evolución profesional de quienes buscan especializarse, crecer profesionalmente y generar impacto en su sector, con un firme compromiso con la democratización del acceso a la excelencia técnica.

+350.000

Estudiantes han pasado por nuestras aulas virtuales

+20 años

Experiencia en el sector de la formación

5 estrellas

Ranking QS en educación online

EDUCA EDTECH Group

Educa Edtech GROUP

Al matricularte en un curso o máster, obtendrás una suscripción gratuita a MyLXP mientras dure tu formación. Tendrás acceso a más de 400 cursos clave (soft skills, idiomas, competencias digitales, etc.) y otras sorpresas. Regístrate y comprueba cómo MyLXP mejora tu aprendizaje.

Metodología EDUCA LXP

La experiencia integral de educación online a medida

EDUCA LXP es más que una metodología, es una experiencia educativa completamente personalizada gracias a todas las posibilidades que ofrece la inteligencia artificial. Ahora el contenido se adapta a ti, tus necesidades y preferencias, mientras te ofrece acceso a contenidos actualizados y prácticos que realmente marcan la diferencia en el mercado laboral.

Flexibilidad

Aprendizaje 100% online y adaptado a tu horario: estudia desde cualquier dispositivo donde, cuando y como quieras.

Personalización

Contenidos e itinerarios formativos adaptados a tus necesidades, gracias a la IA.

Innovación

Desarrollos tecnológicos en permanente evolución impulsados por la AI mediante Learning Experience Platform.

Inteligencia artificial

Descubre PHIA, tu asistente de aprendizaje que te ayudará en cada paso.

Acompañamiento docente

Empatía humana y orientación académica por parte de un equipo docente especializado.

Experiencia Educativa

Enfoque didáctico orientado al trabajo por competencias, que favorece un aprendizaje práctico y significativo.

MY LXP

Al matricularte en un curso o máster, obtendrás una suscripción gratuita a MyLXP mientras dure tu formación

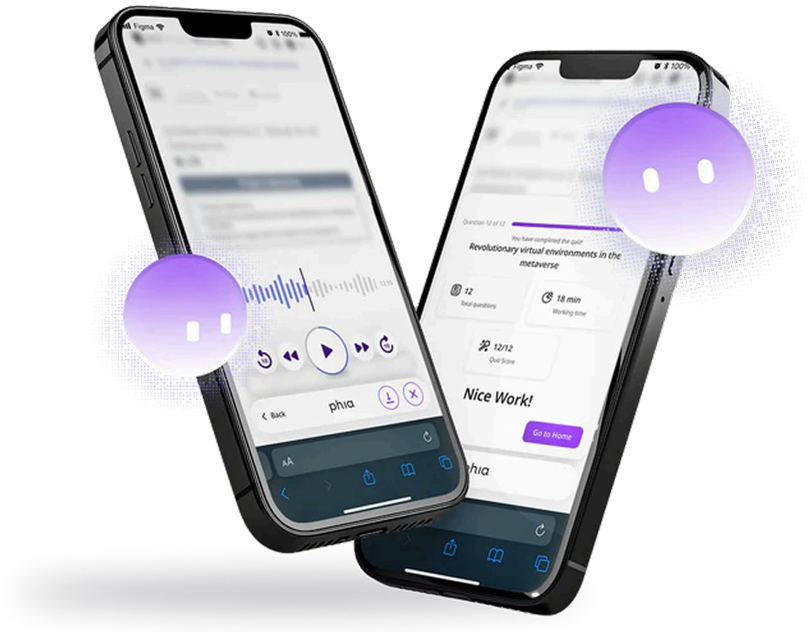
Tendrás acceso a más de 400 cursos clave (soft skills, idiomas, competencias digitales, etc.) y otras sorpresas. Regístrate y comprueba cómo MyLXP mejora tu aprendizaje.

Conoce a PHIA, tu asistente de aprendizaje personalizado

Utiliza todas las posibilidades de la inteligencia artificial para sacarle el máximo partido a tu formación

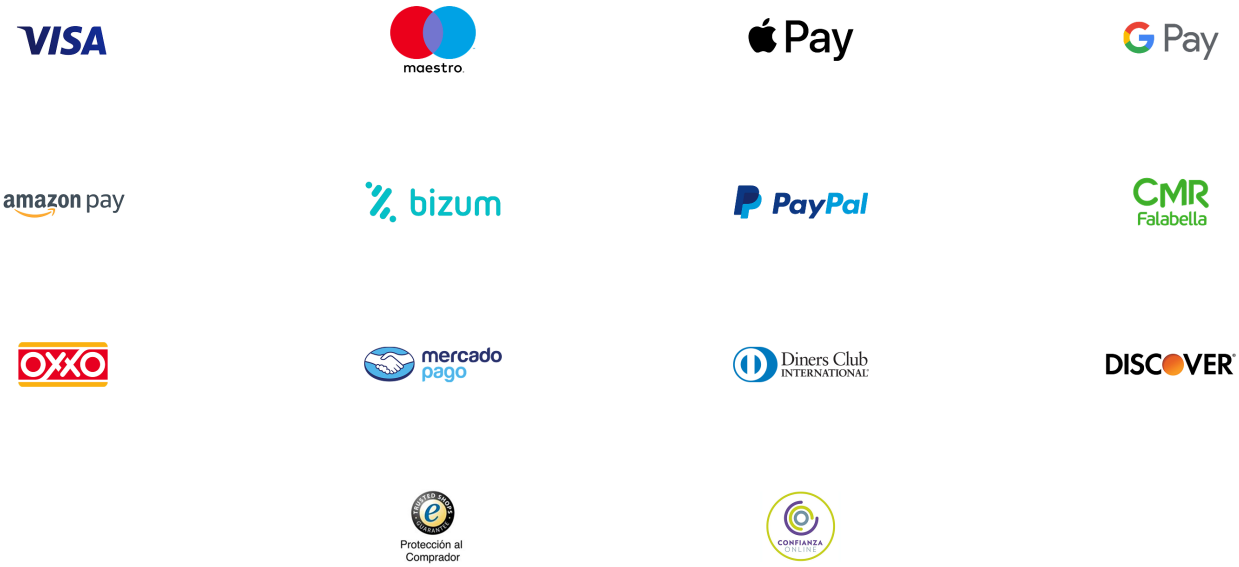
EDUCA EDTECH Group lidera la revolución digital en la educación, impulsando el aprendizaje continuo y la transformación tecnológica. El grupo está formado por reconocidas instituciones de formación y tiene como misión democratizar el acceso a la educación, fomentar la transferencia de conocimiento, el desarrollo tecnológico y la investigación.

Con la experiencia acumulada a lo largo de más de 20 años, hemos perfeccionado nuestra plataforma de aprendizaje EDUCA LXP (Learning Experience Platform), la base de nuestra metodología educativa, que brinda a los estudiantes una formación online práctica y significativa.



Descubre todas las facilidades de pago

Nos adaptamos a todos los métodos de pago internacionales.



Financiación y becas

Financia tu curso o máster y disfruta de las becas disponibles. Contacta con nuestro equipo experto para saber cuál se adapta más a tu perfil.

25%
Beca Alumni

15%
Beca recomienda

20%
Beca Diversidad Funcional

20%
Beca desempleo

15%
Beca GRUPO

20%
Beca para Profesionales, Sanitarios, colegiados/as

15%
Beca emprende

20%
Beca Familia numerosa