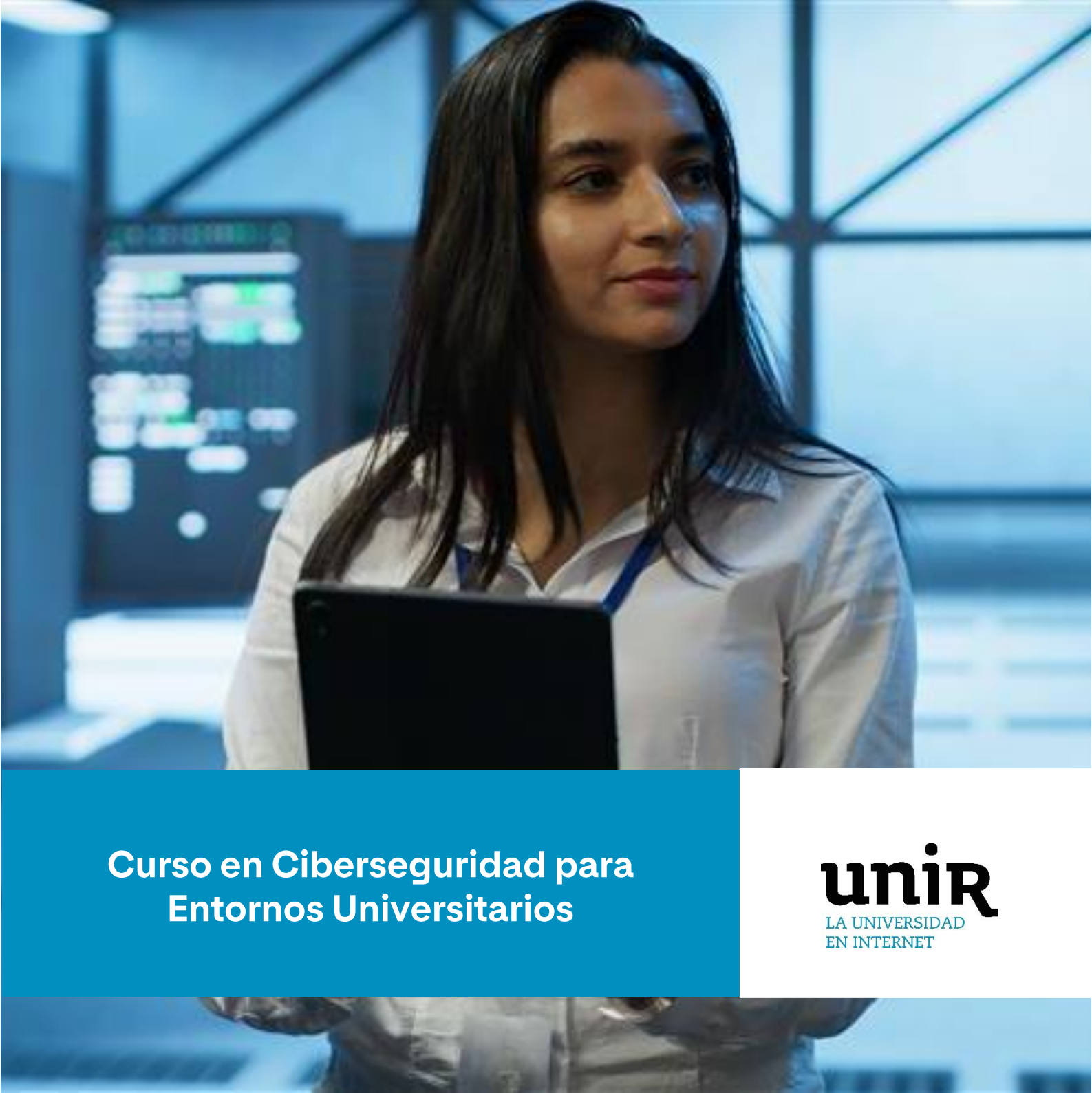

Curso en Ciberseguridad para Entornos Universitarios

unir
LA UNIVERSIDAD EN INTERNET

La Universidad en Internet

UNIR es una universidad oficial 100% online de ti- tularidad y gestión privada, que se ha consolidado como solución educativa adaptada a los nuevos tiempos y a la sociedad actual.

UNIR se sustenta en un modelo pedagógico único con una **eficacia avalada por los más de 43.000 egresados de 90 países** que la han elegido para realizar sus estudios.

unir
LA UNIVERSIDAD EN INTERNET

Un curso que capacita a los docentes universitarios en protección digital y seguridad de la información

Este curso está orientado a ofrecer una capacitación avanzada a profesores de Instituciones de Educación Superior de Latinoamérica para la adquisición de competencias en seguridad digital.

La ciberseguridad en el ámbito universitario es crucial debido a la cantidad de información sensible que se maneja en estas instituciones.

Objetivo

Desarrollar en el personal docente, investigador y administrativo de instituciones de educación superior las competencias necesarias para identificar, prevenir y responder a riesgos de ciberseguridad, promoviendo una cultura organizacional de protección digital que garantice la seguridad de la información, la privacidad de los datos y la integridad de los procesos académicos y administrativos en entornos tecnológicos.

Perfil de ingreso

El curso está abierto a todos aquellos docentes y trabajadores de Instituciones de Educación Superior que pretendan mejorar sus conocimientos y habilidades en el campo de la ciberseguridad.

Semana 0 (introducción al Campus) *
3 de Noviembre

Semana 1 (inicio de clases)
10 de Noviembre

Fin del curso:
25 de Enero

**** El procedimiento y las claves de acceso al curso se recibirán a lo largo de la semana 0***

unir
LA UNIVERSIDAD EN INTERNET

Curso en Ciberseguridad para Entornos Universitarios

Módulos del programa

Módulo 1: Conceptos fundamentales de ciberseguridad

1. Principios de la ciberseguridad (confidencialidad, integridad, disponibilidad, autenticidad)
2. Certificados y firma digital.
3. Gestión segura de contraseñas y uso de gestores.
4. Seguridad en capa de aplicación: antivirus y actualizaciones de ciberseguridad.
5. Configuración segura de dispositivos móviles.
6. Uso seguro de la nube.
7. Conexiones seguras: HTTPS y VPN

Módulo 2: Ecosistema de Amenazas Digitales en Educación Superior

1. Evolución de las amenazas digitales: del malware tradicional a los ataques dirigidos (APT).
2. Ciberataques recientes en universidades (casos reales y análisis).
3. Infraestructura crítica universitaria y superficies de ataque comunes.
4. Actores de amenaza: ciberdelincuencia, hacktivismo, grupos patrocinados por estados.
5. Vulnerabilidades típicas en entornos académicos y científicos.
6. Introducción a frameworks de ciberseguridad (NIST-CSF, ISO 27001).
7. Diagnóstico inicial de cultura y madurez en ciberseguridad institucional

Módulo 3: Gestión de la Identidad y Seguridad Personal Avanzada

1. Identidad digital académica y su valor estratégico.
2. Uso correcto y segmentado de cuentas institucionales, personales y públicas.
4. Autenticación multifactor (MFA), tokens físicos y biometría.
5. Ingeniería social avanzada y técnicas de spear phishing dirigidas a docentes.
6. Protección frente al robo de identidad y fraude por suplantación.
7. Uso seguro de redes WiFi públicas y empresariales. El caso de eduroam
8. Revisión de configuración segura en perfiles docentes públicos (Google Scholar, ORCID, etc.).

Módulo 4: Protección de Datos Sensibles y Cumplimiento Normativo

1. Fundamentos del RGPD / LOPDGDD para el entorno educativo.
2. Datos personales sensibles en la docencia, la investigación y la gestión académica.
3. Ciclo de vida de la información: recolección, uso, retención, destrucción.
4. Evaluación de impacto en privacidad (PIA) aplicada a herramientas educativas.
5. Herramientas y técnicas para anonimización y seudonimización de datos.
6. Riesgos asociados al uso de herramientas con IA generativa (ChatGPT, Copilot, etc.).
7. Responsabilidad del docente como custodio de datos de estudiantes y colegas.

Curso en Ciberseguridad para Entornos Universitarios

Módulos del programa

Módulo 5: Seguridad en Herramientas Colaborativas, LMS y Recursos Digitales

1. Configuración segura de Google Workspace y Microsoft 365.
2. Gestión y control de documentos compartidos.
3. Buenas prácticas en: plugins, exámenes, calificaciones.
4. Seguridad en plataformas de videoconferencia.
5. Evaluación crítica de herramientas externas y su fiabilidad
6. Protección de materiales docentes digitales frente a filtraciones o plagio.
7. Integración segura de herramientas de terceros con LMS y campus virtual.

Módulo 6: Gobernanza de la Ciberseguridad y Cultura Organizacional

1. Roles y responsabilidades en la gobernanza de la ciberseguridad universitaria.
2. Elementos clave de una política institucional de seguridad.
3. Liderazgo académico: rol del docente como agente de concienciación.
4. Diseño de campañas internas de formación y sensibilización.
5. Gestión del cambio y resistencia a las prácticas seguras.
6. Comunicación interna y externa durante incidentes.
7. Indicadores clave (KPIs) de madurez y cultura de seguridad digital.

Módulo 7: Gestión de Incidentes y Continuidad Académica

1. Tipología de incidentes más frecuentes en el entorno académico.
2. Fases del ciclo de gestión de incidentes (detección, análisis, contención, recuperación).
3. Canales y protocolos institucionales de reporte.
4. Respuesta inicial ante fuga de datos, robo de credenciales o malware.
5. Plan de continuidad docente en caso de ciberataque.
6. Ciberresiliencia y prácticas de respaldo (backups, redundancia, recuperación).
7. Simulacro guiado: incidente de ransomware en una facultad.

Módulo 8: Proyecto Aplicado – Diagnóstico y Mejora

1. Análisis de brechas de seguridad en el entorno personal o institucional.
2. Identificación de riesgos prioritarios y medidas correctivas.
3. Evaluación de cultura de seguridad en una unidad académica.
4. Elaboración de plan de acción o mejora continua.
5. Configuración segura del entorno de usuario en un equipo institucional y sus servicios.

Recursos didácticos

- Clases online en directo
- Prácticas interactivas
- Foros
- Actividades específicas
- Test de autoevaluación

Modalidad

100% online

Duración

El curso tendrá 150 horas equivalentes a 6 ECTS. Diez semanas de clases presenciales virtuales.

Evaluación del programa

La evaluación del programa será del 80% de actividad práctica y 20% asistencia a las sesiones.

CERTIFICADO

Aquellos candidatos que superen la evaluación recibirán la certificación internacional correspondiente de la Universidad Internacional de La Rioja

unir
LA UNIVERSIDAD EN INTERNET

Rectorado
Avenida de la Paz 137
26006. Logroño (La Rioja)
España
t (+34) 941 210 211
www.unir.net

Delegación Colombia
Calle 100 # 19 – 61
Edificio Centro
Empresarial
100. Oficina 801 Bogotá,
Colombia
t (+57) 1 5169659
colombia.unir.net

Delegación México
Av. Extremadura, 8
Col. Insurgentes
Mixcoac. Del. Benito
Juárez 03920,
México DF
t +52 (55) 36833800
mexico.unir.net

Delegación Ecuador
Av. De la República E7-
123 y pasaje Martín
Carrión, PB local L1,
Edificio PUCARA.
Quito
(Ecuador) t
(+593) 3931480
ecuador.unir.net

Delegación Perú
Jose Gabriel Chariarse
415, San Antonio,
Miraflores.
Lima, Perú
t (01) 496 – 8095
peru.unir.net

Delegación
Guayaquil Calle
Victor Emilio Estrada
1021 y Jiguas -
Sector Urdesa
Guayaquil (Ecuador)

unir
LA UNIVERSIDAD
EN INTERNET