

TEC

PROGRAMA DE
CAPACITACIÓN
EN COMPUTACIÓN



CURSO DE

CIBERSEGURIDAD

**APOYADA CON HERRAMIENTAS DE
INTELIGENCIA ARTIFICIAL - NIVEL I**

100% VIRTUAL

MATRÍCULA ABIERTA

PROTEGÉ LA INFORMACIÓN CON TECNOLOGÍA INTELIGENTE



CIBERSEGURIDAD APOYADA CON HERRAMIENTAS DE IA – NIVEL I

Con este curso podés desarrollar conocimientos fundamentales en ciberseguridad y comprender cómo la Inteligencia Artificial está transformando la detección, el análisis y la respuesta ante amenazas digitales. Durante el programa aprenderás sobre protección de la información, redes seguras, malware, gestión de registros, respuesta a incidentes y fundamentos de Machine Learning aplicados al ámbito de la seguridad informática.

Este curso es ideal para personas interesadas en iniciar su formación en ciberseguridad, fortalecer sus conocimientos tecnológicos y conocer herramientas actuales para identificar riesgos y proteger sistemas e información

AL INSCRIBIRTE OBTENÉS



¡Matrícula GRATIS!



Plataforma virtual de alta calidad y recursos descargables



Certificado oficial del TEC al completar el curso



Profesores con la calidad TEC

INVERSIÓN REGULAR

€475.000 + 2% IVA

Podés elegir el método de pago que más te convenga de una forma totalmente segura.

MODALIDAD

100% Virtual Sincrónico

Todas las clases son en línea y se imparten en tiempo real con horario fijo. Tenés que conectarte en los días y horas programados, interactuás en vivo con el profesor y tus compañeros como si fuera una clase presencial, pero por internet.



pcc@itcr.ac.cr



8660 1701 | 8890 4555 | 8583 4209

¿QUÉ ES CIBERSEGURIDAD APOYADA CON HERRAMIENTAS DE IA – NIVEL I?

Ciberseguridad apoyada con herramientas de IA – Nivel I es un curso introductorio diseñado para construir las bases operativas de la seguridad informática y relacionarlas con los principales conceptos de Inteligencia Artificial.

El curso aborda los pilares tradicionales de la ciberseguridad, como la confidencialidad, la integridad y la disponibilidad de la

información, y explica cómo la automatización, el aprendizaje automático y las herramientas inteligentes pueden apoyar la identificación de amenazas.

Además, las personas participantes conocerán conceptos fundamentales sobre redes seguras, malware, auditoría de sistemas, gestión de registros, operaciones de seguridad, Machine Learning y uso responsable de la IA.

OBJETIVO GENERAL

Desarrollar conocimientos fundamentales de ciberseguridad e Inteligencia Artificial mediante actividades teóricas y prácticas que permitan identificar amenazas, analizar eventos de seguridad y aplicar controles básicos para proteger sistemas, redes e información.

A QUIÉN VA DIRIGIDO

Está dirigido a profesionales de Tecnologías de Información, estudiantes de informática, sistemas, redes o áreas relacionadas, analistas junior de seguridad, personas encargadas de la gestión de riesgos, profesionales interesados en fortalecer la seguridad de sus organizaciones y personas entusiastas que desean iniciar su formación en ciberseguridad e IA.

No se requiere experiencia avanzada en ciberseguridad.

OBJETIVOS ESPECÍFICOS

- **Comprender los principios esenciales de la ciberseguridad y la protección de la información.**
 - Identificar amenazas digitales, tipos de malware y técnicas de ingeniería social.
- **Reconocer el funcionamiento básico de redes, protocolos y controles de seguridad.**
 - Analizar registros y eventos para detectar posibles incidentes.
- **Conocer el funcionamiento general de un Centro de Operaciones de Seguridad.**
- **Comprender los principios elementales de Machine Learning aplicados a la ciberseguridad.**
 - **Aplicar criterios de uso seguro, ético y responsable de herramientas de IA.**





¡FORTALECÉ TUS CONOCIMIENTOS Y PROTEGÉ EL ENTORNO DIGITAL!

METODOLOGÍA

El curso se desarrolla mediante un enfoque teórico-práctico.

Cada bloque temático incluye una introducción conceptual y un desafío técnico de ejecución que permite aplicar los conocimientos adquiridos en situaciones relacionadas con la seguridad informática. Durante el curso se realizarán ejercicios guiados sobre análisis de amenazas, revisión de permisos, inspección de tráfico de red, gestión de registros, clasificación de incidentes y uso introductorio de herramientas de Inteligencia Artificial.

Las prácticas se realizarán en entornos controlados y con fines exclusivamente educativos, priorizando el uso responsable, ético y seguro de las herramientas tecnológicas. La participación, el compromiso y la puntualidad serán fundamentales para aprovechar adecuadamente las actividades prácticas del curso.

DURACIÓN

30 horas

Distribuidas en 10 sesiones de 3 horas,
una sesión por semana.

REQUISITOS

- Conocimientos generales de computación.
- Manejo básico de sistemas operativos.
- Conocimientos básicos de redes.
- Poseer una computadora con acceso estable a internet.
- Contar con permisos para instalar herramientas, cuando sea necesario.
- No se requieren conocimientos previos avanzados de IA.
- No se requiere experiencia profesional previa en ciberseguridad.

EVALUACIÓN

Este curso es de aprobación **(calificación igual o superior a 70)**, por lo que se realizará una evaluación en la última sesión.

Para la calificación se tomará en cuenta el trabajo en clase, las prácticas y la participación.

CONTENIDO

No dejés pasar esta
oportunidad de estudiar en el TEC

1. Introducción a la ciberseguridad y la tríada CIA

- Glosario esencial de seguridad, los pilares de confidencialidad, integridad y disponibilidad (tríada CIA), y políticas de control de acceso.
- **Desafío técnico de ejecución**

2. Panorama global de amenazas y malware

- Taxonomía del software malicioso (virus, troyanos, ransomware, phishing) y el ciclo de vida de una infección en sistemas corporativos.
- **Desafío técnico de ejecución**

3. Fundamentos de redes seguras y protocolos de comunicación

- El modelo OSI, funcionamiento de protocolos críticos (TCP/IP, DNS, HTTP/S) y el rol de los firewalls en la segmentación de tráfico.
- **Desafío técnico de ejecución**

4. Gestión de registros y auditoría de sistemas

- Importancia de la telemetría, estructura de los registros del sistema (logs) en entornos Windows/Linux y centralización de eventos.
- **Desafío técnico de ejecución**

5. Metodologías de ataque y fases del hacking ético

Estudio de las etapas de una intrusión (reconocimiento, escaneo, ganancia de acceso, mantenimiento de acceso) desde la perspectiva defensiva.

Desafío técnico de ejecución



¿Lista/o para fortalecer tus conocimientos en ciberseguridad? ¡Inscríbete ya!

6. Introducción a las operaciones de seguridad y el SOC

- Ciclo de vida de la respuesta a incidentes, roles dentro de un centro de operaciones de seguridad (SOC) y el uso de plataformas SIEM para la gestión de alertas.
- **Desafío técnico de ejecución**

8. Principios elementales de Machine Learning para TI

- Qué es el machine learning, tipos de aprendizaje (supervisado y no supervisado) y su aplicación para clasificar eventos limpios de actividades maliciosas.
- **Desafío técnico de ejecución**

7. Evolución de la ciberseguridad hacia la Inteligencia Artificial

- Limitaciones de la ciberseguridad basada en firmas estáticas frente a ataques dirigidos y el surgimiento de la IA como solución predictiva.
- **Desafío técnico de ejecución**

9. Preparación de datos de seguridad para IA

- Traducción de infraestructura técnica a datos algorítmicos. métodos para limpiar y transformar logs textuales en matrices numéricas aptas para modelos predictivos.
- **Desafío técnico de ejecución**

10. Gobernanza, ética y marcos de control de IA

Políticas de uso seguro de la IA generativa en las organizaciones, riesgos de fuga de información y conceptos del marco de gestión de riesgos NIST AI RMF.

Desafío técnico de ejecución



TEC | Tecnológico
de Costa Rica