PROGRAMA

CIBERSEGURIDAD

SEGURIDAD 360: IDENTIFICA, PROTEGE, IMPLEMENTA

-INSCRIPCIONES ABIERTAS-

PROGRAMA ONLINE

CLASES 100% EN VIVO A TRAVÉS DE ZOOM

EELA INSTITUTE

CIBERSEGURIDAD

El crecimiento exponencial de la digitalización ha traído consigo un aumento significativo en la frecuencia, complejidad y sofisticación de los ciberataques. Desde pequeñas empresas hasta grandes corporaciones y gobiernos, ninguna organización está exenta de ser blanco de amenazas cibernéticas. La pérdida de datos, el robo de propiedad intelectual, el fraude financiero y los daños a la reputación son solo algunos de los riesgos asociados a una seguridad inadecuada.

Este programa responde a la necesidad urgente de formar profesionales capacitados que no solo comprendan la tecnología, sino que también puedan anticipar, prevenir y reaccionar eficazmente ante incidentes de seguridad. Además, en un entorno donde las regulaciones y las normativas locales exigen altos estándares de protección de datos, la formación en ciberseguridad se ha convertido en una competencia esencial y transversal para cualquier sector.

Con un enfoque práctico y actualizado, este programa no solo enseña las bases teóricas, sino que también proporciona herramientas y técnicas aplicables a situaciones reales. Así, los participantes estarán mejor preparados para proteger sus entornos digitales y contribuir activamente a la seguridad de la información en sus organizaciones.

OBJETIVO GENERAL

Capacitar a los participantes en la identificación, prevención y respuesta ante amenazas cibernéticas, utilizando herramientas y metodologías actualizadas para proteger los activos digitales y garantizar la seguridad de la información en cualquier entorno profesional.

EELA INSTITUTE

OBJETIVOS ESPECÍFICOS

1. Comprender los Fundamentos de la Ciberseguridad:

Explicar conceptos clave como confidencialidad, integridad y disponibilidad de la información.

2. Identificar Amenazas y Vulnerabilidades:

Reconocer los distintos tipos de ataques cibernéticos (phishing, malware, ransomware, etc.) y las vulnerabilidades comunes en redes, sistemas y aplicaciones.

3. Aplicar Estrategias de Protección y Mitigación:

Implementar políticas de seguridad, gestión de contraseñas, cifrado de datos y técnicas de defensa en profundidad (defense in depth).

4. Desarrollar Habilidades en Respuesta ante Incidentes:

Elaborar planes de respuesta y recuperación ante ciberataques, incluyendo análisis forense básico y procedimientos de contención.

5. Promover una Cultura de Ciberseguridad:

Fomentar prácticas seguras en el uso de tecnologías, tanto a nivel individual como organizacional, mediante campañas de concienciación y capacitación continua.

¿A QUIÉN ESTÁ DIRIGIDO?

Este programa está diseñado para un público amplio, abarcando tanto perfiles técnicos como no técnicos que deseen fortalecer sus conocimientos en ciberseguridad:

1. Profesionales de TI y Administradores de Sistemas:

Que busquen profundizar en la seguridad de redes, servidores y sistemas operativos.

2. Gerentes y Líderes de Proyectos:

Que necesiten integrar la seguridad en la gestión de proyectos tecnológicos y de negocio.

3. Emprendedores y Dueños de Negocios:

Que deseen proteger la información de sus empresas y minimizar riesgos operativos.

4. Auditores y Consultores de Seguridad:

Que requieran actualizar sus conocimientos en normativas, cumplimiento y análisis de riesgos.

5. Estudiantes y Recién Graduados en Carreras Tecnológicas:

Que deseen especializarse en ciberseguridad como una carrera en auge.

6. Personal de Recursos Humanos y Legal:

Para comprender las implicaciones legales de la protección de datos y la seguridad en el entorno laboral.

7. Cualquier Profesional Interesado en la Seguridad Digital Personal:

Que quiera proteger su identidad, dispositivos y datos personales ante las crecientes amenazas cibernéticas.

EELA INSTITUTE

ESTRUCTURA DE CONTENIDOS

Módulo 1:
Introducción a la Ciberseguridad (3 horas)

- Conceptos básicos de ciberseguridad
  - Definiciones clave: seguridad informática vs. ciberseguridad.
  - Confidencialidad, integridad y disponibilidad (Triada CIA).
- Panorama actual de amenazas
  - Amenazas internas y externas.
  - Tipos de atacantes: hackers éticos, cibercriminales, hacktivistas.
- Ética en la ciberseguridad
  - Dilemas éticos y responsabilidad profesional.

Módulo 2:
Fundamentos de Redes y Protocolos Seguros (6 horas)

- Arquitectura de redes y protocolos
  - TCP/IP, DNS, HTTP/HTTPS.
  - Conceptos de subredes y VLANs.
- Seguridad en redes
  - Firewalls, IDS/IPS, VPN.
  - Segmentación de redes y DMZ.
- Protocolos de cifrado y autenticación
  - SSL/TLS, IPsec.
  - Autenticación multifactor (MFA).

Módulo 3:
Gestión de Vulnerabilidades y Análisis de Riesgos (6 horas)

- Identificación de vulnerabilidades
  - Herramientas: Nmap, Nessus, OpenVAS.
- Evaluación y análisis de riesgos
  - Metodologías: OWASP, CVSS.
  - Priorización de amenazas.
- Planificación de remediación y mitigación
  - Gestión de parches.
  - Ciclo de vida de las vulnerabilidades.

Módulo 4:
Hacking Ético y Pruebas de Penetración (9 horas)

- Introducción al hacking ético
  - Legalidad y permisos.
- Metodologías de pruebas de penetración
  - Fases: reconocimiento, escaneo, explotación.
- Herramientas para pentesting
  - Metasploit, Burp Suite, Wireshark , entre otras.
  - Técnicas de SandBoxing.
- Análisis de resultados y elaboración de informes
  - Reportes efectivos para técnicos y ejecutivos.

Módulo 5:
Seguridad en Aplicaciones y Desarrollo Seguro (6 horas)

- Principios del desarrollo seguro
  - Secure SDLC (Ciclo de vida del desarrollo seguro).
  - Prácticas de codificación segura.
- Vulnerabilidades comunes
  - OWASP Top 10.
  - Inyección SQL, XSS, CSRF.

ESTRUCTURA DE CONTENIDOS

Módulo 6:
Seguridad en la Nube y Tecnologías Emergentes (6 horas)

- Principios de seguridad en la nube
  - Modelos SaaS, PaaS, IaaS.
  - Herramientas de seguridad en AWS, Azure, GCP.
- Amenazas y controles en la nube
  - Configuración segura y gestión de identidades.
- Tendencias en ciberseguridad
  - La Inteligencia Artificial y la Ciberseguridad, Soluciones y Herramientas
  - IoT.
  - Blockchain.
  - Criptografía PostCuántica.

Módulo 7:
Respuesta a Incidentes y Continuidad del Negocio (6 horas)

- Planes de respuesta ante incidentes (IRP)
  - Identificación, contención, erradicación, recuperación.
- Simulación de ciberataques
  - Análisis forense básico.
- Planes de continuidad y recuperación ante desastres
  - BCP, SGCN, Backup, DRaaS, DRP (Disaster Recovery Plan).

Módulo 8:
Concienciación y Cultura de Ciberseguridad (3 horas)

- Ciberseguridad para Usuarios Finales
  - Buenas prácticas en el uso del correo electrónico y redes sociales.
  - Gestión segura de contraseñas y autenticación multifactor.
- Desarrollo de una Cultura Organizacional Segura
  - Campañas de concienciación en ciberseguridad.
  - Rol del factor humano en la seguridad de la información.

Módulo 9:
Protección de Datos y Cumplimiento Legal (9 horas)

- Introducción a la Protección de Datos
  - Datos personales y datos sensibles. Ciclo de vida de los datos: recopilación, almacenamiento y eliminación.
- Regulaciones y Normativas
  - GDPR, CCPA, y leyes locales de protección de datos.
  - Derechos de los usuarios y obligaciones de las organizaciones.
  - Multas y consecuencias del incumplimiento.
- Políticas de Privacidad y Seguridad de la Información
  - Elaboración de políticas de protección de datos.
  - Evaluación de impacto de privacidad (PIA).
  - Protocolos para la gestión de incidentes de datos.

Módulo 10:
Ciberseguridad con Inteligencia Artificial (6 horas)

CLAUSTRO ACADÉMICO

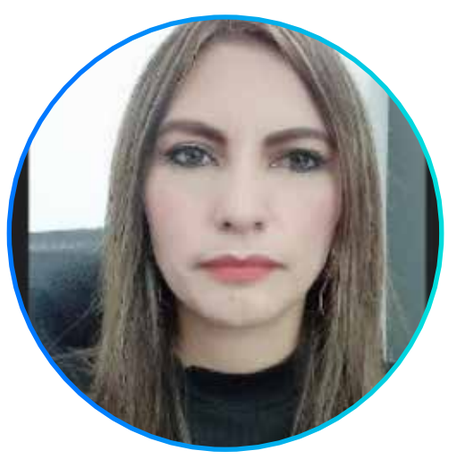
LUIS ALBERTO PAZMIÑO

- Banco Pichincha: Gerente Ciberdefensa
- Universidad de Las Américas (EC) - Docente Maestría en Gestión de la Seguridad de la Información.
- Universidad Tecnológica Equinoccial (EC) - Docente Maestría en Gestión de la Seguridad de la Información.
- Pontificia Universidad Católica del Ecuador - Docente de la Maestría en Ciberseguridad.
- Cisco Systems - Instructor.
- Escuela Superior Politécnica de Chimborazo - Docente de la Maestría en Seguridad Telemática.
- Asesor de Seguridad Nacional.
- Corporacion Nacional de Telecomunicaciones - Analista de Seguridad de la Información.

JAIME VINUEZA

- Director de Gestión Estratégica - CELEC.
- Docente de Posgrados y Director de Tesis en: UDLA, UDLH EELA, Tecnológico de Monterrey, UISEK, ESPE, CEC-EPN.
- Consultor Experto BI, BA, DWH, BigData, AE, SOA, BPM, PMP Industrias de: Retail, Seguros, Banca y Servicios Financieros, Salud, Wholesale, Petróleos & Energía, Utilities, Educación, Empresa Pública, Consumo Masivo, Manufactura & Producción.
- Ex - CEO en Empresas Multinacionales de Retail y Servicios Financieros (EC, CR).
- Ex – Business Intelligence Regional Manager Empresa de Retail Multinacional. (CO, EC, PR, CL, BO, MX, PA).
- Ex – Gerente Regional de Servicios y Proyectos Empresa Consultora Multinacional (CO, EC, CL).

MARY CARMEN VARGAS



- Cuenta con más de 20 años de trayectoria profesional en áreas clave como Tecnología de la Información, Seguridad de la Información, Control Interno y Gestión de Riesgos, con especialización en Gerencia de Proyectos, Ciberseguridad IT /OT y Seguridad Informática.
- Ha liderado equipos y proyectos enfocados en fortalecer la ciberseguridad en instituciones tanto privadas como públicas.
- Actualmente es Coordinadora del Centro de Ciberseguridad Industrial en Ecuador y miembro activo del equipo de ciberseguridad de la CIER (Comisión de Integración Energética Regional), y CiberWarmi Ecuador.
- Fue parte del equipo multidisciplinario que desarrolló la Estrategia Nacional de Ciberseguridad del Ecuador y actualmente apoya al Ministerio de Energía y Minas.
- Premiada en 2 ocasiones como CISO a nivel nacional por IT Ahora.

JOHANNA LEÓN

- Líder en Ciberseguridad y Diversidad Tecnológica con más de 10 años de experiencia en el sector tecnológico.
- Ha liderado y desarrollado proyectos que abordan los desafíos actuales de ciberseguridad.
  Su enfoque profesional está orientado a crear estrategias innovadoras de protección y mitigación de riesgos digitales.
- Ha colaborando con organizaciones para construir entornos cibernéticos más seguros y apoyando iniciativas que reduzcan la brecha de género en tecnología y fortalecer el talento local enEcuador.
- Cuenta con formación en Ingeniería de Sistemas, una Maestría en Ciberseguridad y especialización en Protección de Datos Personales.
- Presidenta del Grupo Cyber Warmi a nivel nacional.

WILSON FERNANDO FREIRE

- Diseño/Instalación/Configuración/Troubleshooting de Soluciones de Networking.
- Especialización en Tecnologías Cisco para Comunicaciones Unificadas y Data Center.
- Líder de proyectos de consultoría e implantación de soluciones de Networking.
- Puntonet S.A. - Jefe de Cloud y Data Center.
- Megasupply - Ing. Post Venta.
- Cuenta con estudios en Ingeniería en Electrónica y Telecomunicaciones, Maestría en Gerencia de Sistemas y Tecnologías de la Información, Diplomado en Desarrollo Estrategico y Habilidades Directivas, Master en Gestión de Proyectos.

DOBLE CERTIFICACIÓN

EELA INSTITUTE

José López

Ha completado satisfactoriamente el Programa

CIBERSEGURIDAD

Habiendo cumplido con todas las exigencias académicas, técnicas y administrativas requeridas para otorgar el presente certificado.

Inicio: 11 de julio 2022
Finalización: 16 de agosto 2023
Duración: 90 horas
Aval: Universidad Hemisferios

MIAMI, FLORIDA, AUGUST 16TH, 2023

RENZO X. AGUIRRE IDROVO
Director General
EELA Education

CERTIFICADO DE FINALIZACIÓN

UNIVERSIDAD HEMISFERIOS

LA UNIVERSIDAD HEMISFERIOS A TRAVÉS DE SU ESCUELA
DE EDUCACIÓN ONLINE Y EDUCACIÓN CONTINUA
CONFIERE EL PRESENTE CERTIFICADO
A

JOSÉ LÓPEZ

POR HABER APROBADO TODOS LOS REQUISITOS ACADÉMICOS DE LA CERTIFICACIÓN

" PROGRAMA CIBERSEGURIDAD"

DADO EN LA CIUDAD DE QUITO
DEL 11 DE JULIO DE 2022 AL 16 DE AGOSTO DE 2023,
CON UNA DURACIÓN DE 90 HORAS ACADÉMICAS.

José Luis Acosta Haro, MBA.
Decano de Escuela Online y Educación Continua
Universidad Hemisferios

Diego Jaramillo Arango, Phd.
Rector
Universidad Hemisferios

EN Educación Continua

DOBLE CERTIFICACIÓN:

EELA | UNIVERSIDAD HEMISFERIOS

CERTIFICADO POR:

+ 60 Horas en vivo

30 Horas trabajo autónomo

Preparación gratuita para la Certificación Cybersecurity Awareness

Horario Lunes a Miércoles
19h00 a 22h00

VALOR DEL PROGRAMA

APROVECHA AHORA: $397

Formas de Pago

Tarjeta de crédito: (hasta 3 meses sin intereses) $427

Transferencia Bancaria: $397

Ex alumnos EELA, Universidad Hemisferios: 20% de descuento

Nota: Para iniciar el programa debe cancelarse el 100% del valor total para ingresar a las clases online y a la plataforma Moodle

*EELA se reserva el derecho de no iniciar el Programa en caso de no reunir el mínimo de participantes, reestructurar el orden de los módulos, modificar el contenido, fechas o instructor con el fin de asegurar la calidad del mismo.

DUCACIÓN no es lo mismo **SIN** E ELA

EDÚCATE CON NOSOTROS

“La **decisión** más importante es **empezar.**”

POSTULA AHORA

www.eelaedu.com

COMUNÍCATE CON NOSOTROS:

+593 98 349 0192
m.jaramillo@amdbglobal.com - info@eelaedu.com

EELA INSTITUTE