UNIBE | EDUCACIÓN CONTINUA

Workshop

Ciberseguridad para todos: El arte de la autoprotección digital

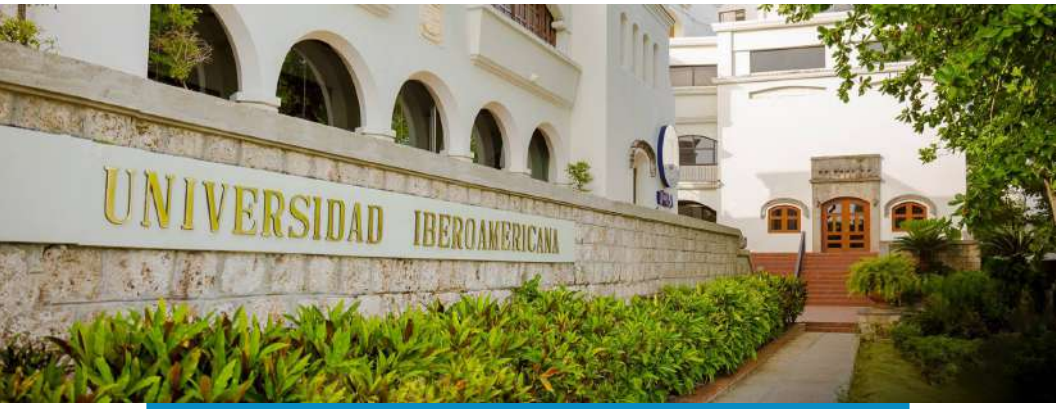
Modalidad: Presencial

Duración: 16 horas

En alianza con: INPLOG
Instituto de Capacitación Portuaria & Logística

La **Universidad Iberoamericana (UNIBE),** a través de su Departamento de Educación Continua, ofrece un amplio portafolio de programas orientados a la actualización y especialización de profesionales en diversas áreas del conocimiento. Desarrolla propuestas académicas innovadoras, alineadas con la demanda del mercado laboral nacional y global, enfocadas en el fortalecimiento de competencias para el desarrollo profesional y personal que promuevan la empleabilidad.

Ofrecemos un Aprendizaje a lo Largo de la Vida, con programas Ejecutivos y de Actualización, Salud, formación Preuniversitaria, Capacitaciones Corporativas diseñados a la medida, Microcredenciales Universitarias, Soft Skills Academy y cursos para Adultos Mayores. La integración de metodologías activas, docentes expertos y el uso de ecosistemas de aprendizaje, garantiza una experiencia formativa práctica y transformadora.



Principales Líneas Temáticas

- Gestión, Liderazgo y Transformación Organizacional
- Negocios, Marketing y Emprendimiento
- Tecnología, Operaciones y Transformación Digital
- Comunicación, Servicio y Experiencia del Cliente
- Educación, Inclusión y Desarrollo Humano
- Salud y Bienestar Integral
- Derecho y Regulación
- Sostenibilidad y Responsabilidad Social
- Arte, Cultura y Creatividad

Ejes Clave

Taller Workshop Ciberseguridad para todos: El arte de la autoprotección digital

Identidad digital

Ciberseguridad básica

Protección de datos

Prevención de amenazas

Uso seguro de IA

Respuesta a incidentes

UNIBE EDUCACIÓN CONTINUA

Descripción

El Taller Ciberseguridad para todos: El arte de la autoprotección digital está diseñado para desarrollar en los participantes las competencias necesarias para identificar, prevenir y responder ante amenazas digitales en su entorno personal y laboral. A lo largo de 16 horas de formación, y mediante un enfoque dinámico y práctico, se abordan temas clave como phishing, ingeniería social, protección de datos, identidad digital y uso seguro de la tecnología, incluyendo buenas prácticas en el uso de la inteligencia artificial. A través de ejercicios aplicados y análisis de casos, los participantes fortalecen su capacidad de tomar decisiones seguras y actuar de manera oportuna ante posibles riesgos. El taller promueve una cultura de ciberseguridad, posicionando a cada participante como parte activa de la primera línea de defensa en la protección de la información.

Objetivo

Desarrollar en los colaboradores las competencias necesarias para identificar, prevenir y responder ante amenazas de ciberseguridad, fortaleciendo su rol como primera línea de defensa, mediante la adopción de buenas prácticas en el manejo de la información, el uso seguro de la tecnología y la correcta actuación ante incidentes digitales.

Dirigido a

Personas sin conocimientos técnicos en ciberseguridad que utilizan tecnología en su día a día, incluyendo estudiantes, colaboradores de cualquier área, personal administrativo y operativo, así como profesionales que manejan información sensible. También está orientado a organizaciones interesadas en fortalecer su cultura de seguridad y reducir riesgos asociados al factor humano.

Beneficios

Al finalizar este programa el egresado estará capacitado para:

- **Identificar** riesgos y amenazas de ciberseguridad en su entorno laboral y personal.
- **Prevenir** ataques comunes como phishing, ingeniería social y suplantación de identidad.
- **Aplicar** buenas prácticas en el manejo seguro de la información y los datos sensibles.
- **Gestionar** de forma segura contraseñas, accesos y uso de redes digitales.
- **Utilizar** la inteligencia artificial de manera responsable, evitando riesgos de fuga de información.
- **Actuar** de forma oportuna ante incidentes digitales, siguiendo protocolos adecuados.

Contenido

Módulo I:

Conceptos Básicos de Ciberseguridad: El Escudo Humano y el Arte del Engaño

- Definición e importancia.
- Nuestro Rol en la Seguridad
- El Factor Humano
- Phishing y Spear Phishing
- Regla de Oro contra el Phishing
- Ingeniería Social
- Deepfake y suplantación con IA
- Videos Falsos (CEO Fraud)
- Llamadas con Voz Clonada
- Casos Reales
- Actividades: Práctica

Módulo II:

Identidad Digital y Conectividad Segura

- Buenas Prácticas de Contraseñas
- Autenticación de Doble Factor (2FA)
- Riesgos del Wi-Fi Público
- Fundamentos de Navegación Segura
- ¿Qué ganamos con la Ciberseguridad?
- Actividades: Práctica

Módulo III:

Protección y Clasificación de los Datos

- La Importancia de los Datos
- Clasificación de la Información
- Etiquetas de Información:
  a. Pública
  b. Interna
  c. Confidencial
- Confidencial Externo
- Caso de Estudio: Mislabeling
- DLP (Data Loss Prevention)
- Riesgos de usar IA con información corporativa
  a. Privacidad en la Nube
  b. Fuga de Información
  c. Shadow AI
- Actividades: Práctica

Módulo IV:

Respuesta, Buenas Prácticas y Evaluación

- Cómo usar IA de forma segura (De riesgo a aliado)

- **Qué SÍ hacer:**
  a. Pedir resúmenes de textos que no contengan datos sensibles.
  b. Generar ideas generales o estructuras para presentaciones.
  c. Anonimizar datos antes de pegarlos (cambiar nombres reales por "Persona A").

- **Qué NO hacer:**
  a. Subir archivos de nómina o datos personales de RRHH.
  b. Subir contratos, acuerdos de confidencialidad o estrategias de precios.
  c. Subir credenciales, tokens o código fuente interno.

- Respuesta ante Incidentes
- Detección y Reporte Inmediato
- Resumen de Supervivencia
- Reglas de Oro Finales
- Evaluación y Cierre
- Actividades: Práctica

Nelson José Mieses Hernández

Facilitador

Especialista en ciberseguridad y arquitectura de infraestructura tecnológica, con amplia experiencia en el diseño e implementación de entornos seguros en organizaciones públicas y privadas. Es Ingeniero en Sistemas, con maestría en Ciberseguridad y formación en Inteligencia Artificial, integrando tecnologías emergentes a la protección de la información.

Se desempeña como docente en áreas de ciberseguridad y redes, y cuenta con trayectoria en operaciones de seguridad (SOC), análisis de vulnerabilidades y cumplimiento de normativas, especialmente en los sectores financiero y público. Es fundador de ITgenics y colaborador honorífico de la Policía Cibernética (DICAT) y el DICRIM, destacándose por su enfoque estratégico, liderazgo técnico y compromiso con la seguridad digital.

Nicaury Sánchez

Facilitadora

Especialista en ciberseguridad e infraestructura tecnológica, con experiencia en la gestión de entornos críticos y la protección de la información en sectores de alta exigencia como el financiero y gubernamental. Es Ingeniera en Sistemas y se encuentra en formación en Ingeniería en Ciberseguridad, con especialización en Transformación Digital con IA y automatización.

Fundadora de Blue Primer, lidera proyectos de consultoría en ciberseguridad y adopción de tecnologías emergentes. Ha dirigido áreas de TI y ciberseguridad, enfocándose en la definición de estrategias, gestión de riesgos, monitoreo de infraestructuras y respuesta ante incidentes. Se destaca por su enfoque en gobierno, riesgo y cumplimiento (GRC), seguridad de redes, continuidad operativa e integración de inteligencia artificial en la protección organizacional.

UNIBE | EDUCACIÓN CONTINUA

¡Adquiere las *herramientas clave* para destacar en esta apasionante industria!

Para más información
Contáctanos

809-689-4111
Exts.: 2203 y 2407

e.continua@unibe.edu.do

ASISTENTE VIRTUAL
Aurora

809-255-4111

aurora@unibe.edu.do

aurora.unibe.edu.do

educacioncontinua.unibe.edu.do

¡Escanea y comienza hoy!