UNIBE EDUCACIÓN CONTINUA

Microcredencial

Ciberseguridad para Profesionales

Incluye Insignia Digital

Modalidad: Autogestionado

Duración: 40 horas

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

Ciberseguridad para Profesionales

Gestión de riesgos digitales

Fundamentos de ciberseguridad

Control de accesos y credenciales

Protección de dispositivos y datos

Detección de amenazas y fraudes

Gestión y respuesta a incidentes

UNIBE EDUCACIÓN CONTINUA

Descripción

Este curso está diseñado para fortalecer la protección de la información personal y organizacional mediante un enfoque práctico y basado en riesgo. A lo largo del programa, se traducen principios clave de ciberseguridad en decisiones concretas para prevenir amenazas, gestionar accesos y responder de manera efectiva ante incidentes. Se trabajan escenarios reales de oficina y trabajo remoto, incluyendo correos sospechosos, enlaces fraudulentos, uso de contraseñas seguras, autenticación multifactor, protección de dispositivos y buenas prácticas en el manejo de datos sensibles. Asimismo, se desarrolla el criterio para identificar fraudes digitales y actuar con seguridad en entornos digitales. Como resultado, se adquieren habilidades aplicables desde el primer día para tomar decisiones informadas y seguras, manteniendo la productividad en el entorno laboral.

Objetivo

Desarrollar en los participantes las competencias fundamentales para proteger la información personal y organizacional mediante la aplicación de buenas prácticas de ciberseguridad, la gestión de riesgos digitales y la respuesta efectiva ante incidentes, favoreciendo una toma de decisiones segura en entornos laborales y digitales.

Dirigido a

Profesionales de cualquier área que utilicen herramientas digitales en su entorno laboral y deseen fortalecer sus prácticas de seguridad de la información. También está orientado a colaboradores de empresas, emprendedores y equipos administrativos o técnicos que manejan datos sensibles, trabajan de forma remota o utilizan plataformas en la nube, y requieren desarrollar criterios básicos para prevenir riesgos y actuar adecuadamente ante incidentes de ciberseguridad.

Beneficios

Al finalizar este programa el egresado estará capacitado para:

- **Proteger** la información personal y organizacional mediante buenas prácticas de ciberseguridad.
- **Identificar** riesgos digitales
- **Prevenir** amenazas comunes en entornos laborales.
- **Gestionar** accesos de forma segura, aplicando contraseñas robustas y autenticación multifactor.
- **Reconocer** intentos de fraude, phishing e ingeniería social.
- **Aplicar** medidas básicas de protección en dispositivos y herramientas digitales.
- **Responder** de manera efectiva ante incidentes de ciberseguridad sin afectar la productividad.

Contenido

Módulo I:
Introducción a la Ilustración Digital

- Qué es la ciberseguridad en mi contexto profesional (y qué estoy protegiendo)
- Panorama de amenazas actuales: cómo ocurren y qué señales dejan
- Principios CIA y enfoque basado en riesgo para priorizar acciones

Módulo II:
Herramientas Digitales Esenciales

- Higiene digital: hábitos diarios que reducen exposición sin frenar productividad
- Gestión efectiva de parches: cómo priorizo, calendario y verifico actualizaciones
- Errores comunes en higiene y parcheo: casos típicos y preguntas críticas

Módulo III:
Principios del Diseño Gráfico en Ilustración

- Endurecimiento (hardening) esencial en PC y móvil: base mínima profesional
- Antimalware/EDR básico y controles del sistema: qué activo y cómo lo compruebo
- Casos reales de compromiso de endpoint: aprendizaje y pensamiento crítico

Módulo IV:
Técnicas de Dibujo Digital

- Riesgos reales de Wi-Fi (público y corporativo) y qué asumo cuando me conecto
- Estándar de conexión segura para teletrabajo: configuraciones recomendadas
- VPN: cuándo aporta valor, limitaciones y errores comunes

Módulo V:
Teoría del Color en la Ilustración Digital

- Contraseñas y frases de paso: diseño robusto y mantenimiento seguro
- Gestores de contraseñas: cómo elegir, configurar y usarlos en mi flujo diario
- MFA en la práctica: qué tipo uso y en qué cuentas es obligatorio

Módulo VI:
Creación y Desarrollo de Personajes

- Mínimo privilegio: cómo reduzco el “radio de explosión” de un incidente
- Clasificación y manejo seguro de información: de la etiqueta al control
- Estrategias de empresas: permisos bien diseñados y fallas comunes (análisis crítico)

Módulo VII:

Capas y Efectos Avanzados

- Cómo se ejecuta un phishing moderno y qué debo detectar en segundos
- Manejo seguro de enlaces y adjuntos: mi procedimiento paso a paso
- Casos de éxito y fallas: qué hacen bien los equipos que reducen el phishing

Módulo VIII:

Ilustraciones Vectoriales y Rasterizadas

- Riesgos del navegador: sitios falsos, descargas y extensiones peligrosas
- HTTPS, permisos y privacidad operativa: qué configurar y por qué
- Buenas prácticas en descargas y verificación: pensamiento crítico aplicado

Módulo IX:

Exportación y Publicación de Ilustraciones

- Ingeniería social: cómo piensan los atacantes y qué sesgos explotan
- Ciberestafas típicas (B2B y personales): guiones, canales y señales de alerta
- Ciberestafas típicas (B2B y personales): guiones, canales y señales de alerta

Módulo IX:

Tendencias Actuales y Conclusiones

- Colaboración en la nube (SaaS): permisos, enlaces y MFA como controles mínimos
- Copias de seguridad y recuperación: resiliencia ante ransomware y errores humanos
- Incidentes: ciclo de vida, evidencia y escalamiento para no técnicos

Requisitos de aprobación:

- Completar el 100 % de las asignaciones del programa académico.
- Obtener una calificación promedio mínima de 70 puntos en las actividades y evaluaciones.

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