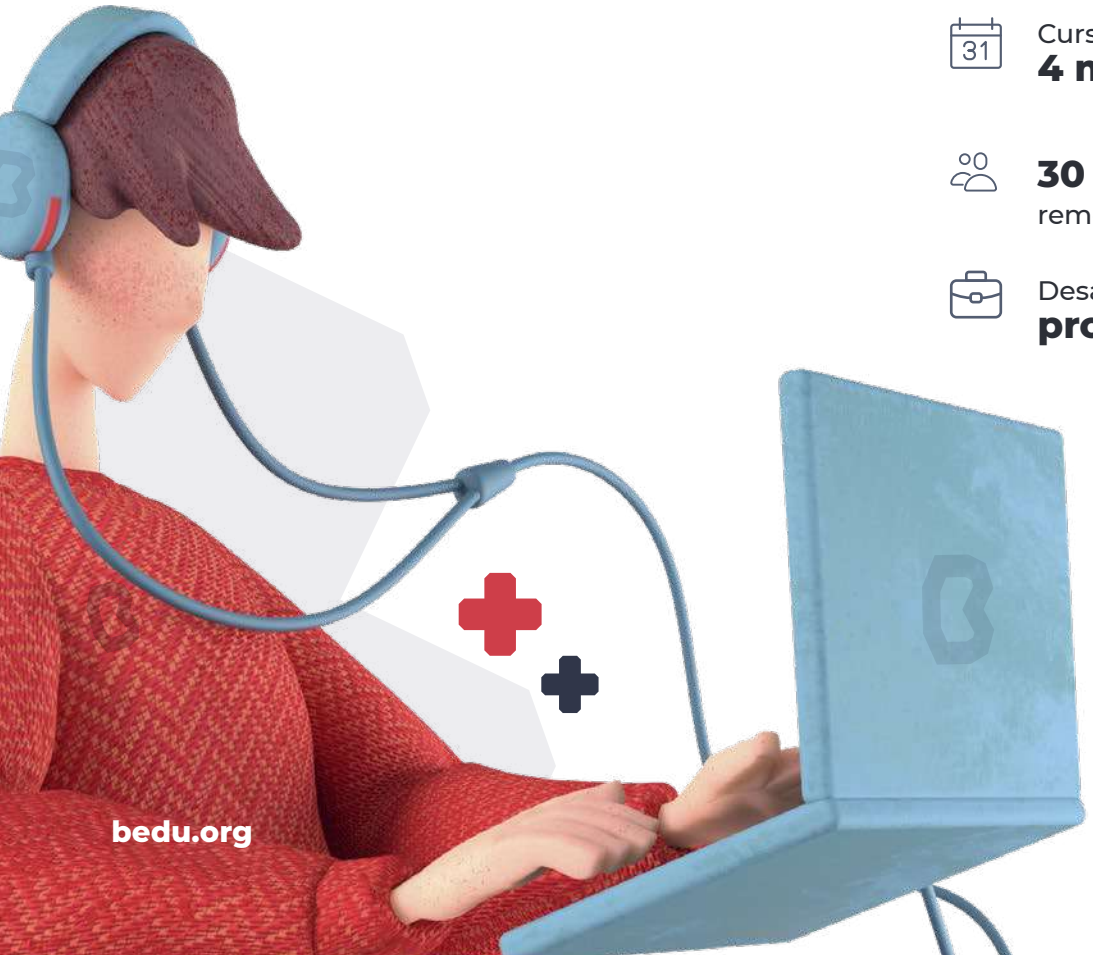
BEDU / Santander

Disruptive Skills: Ciberseguridad

El objetivo del programa es aplicar los conceptos fundamentales de ciberseguridad, identificar las herramientas para mantener y mejorar la seguridad de la información tanto personal como organizacional, identificar las principales amenazas de seguridad, gestionar recursos, aplicación de políticas de seguridad para mejorar la protección de proyectos y activos. Evaluar las brechas de seguridad en sistemas y redes, como también seguridad en la Nube.



Curso de
4 meses

30 sesiones
remotas en vivo

Desarrollo de
proyectos propios

Temario

Aprende los fundamentos de ciberseguridad, así como las herramientas necesarias para mantener la seguridad de información, evaluar sistemas, redes y la Nube.

Conocimientos / Habilidades recomendadas

- Acercamiento básico a la terminal o sistema operativo GNU/Linux
- Conocimiento para la instalación de programas y ejecutarlos
- Manejo de navegador Web

Requerimientos técnicos

- Computadora con al menos 16gb en memoria RAM
- Procesador 4 o más núcleos
- Windows 10 (Uso de Maquinas Virtuales Linux), MacOS (MacOS for Pentester) o GNU/Linux (Kali Linux)

Temario

Módulo I | User Security Awareness

Nivel uno

Objetivo del módulo. El participante conocerá los conceptos, herramientas y mejores prácticas para mantener y mejorar la seguridad de la información, tanto personal como de la organización, a través de los usuarios sin importar si estos se encuentran centralizados, distribuidos o en un esquema híbrido.

Temario

1. Confidencialidad, integridad y disponibilidad de la información
2. Riesgo y vulnerabilidad comunes para usuarios y organizaciones (ejemplos apegados a sistema de gestión de la seguridad de la información)
3. Cuentas, credenciales e identidad
4. Protección de hardware, software y archivos
5. Comunicación, canales y dispositivos seguros en el trabajo
6. Ingeniería social y phishing
7. Ciberataques más comunes: DoS, Malware, Ransomware y Virus
8. Búsqueda segura y privacidad en la web

Temario

Módulo II | Cyber Security Introduction
Nivel dos

Objetivo del módulo. El participante conocerá las bases fundamentales de ciberseguridad para tener una aplicación inmediata en su ámbito laboral, con independencia de la industria en la que se ejecute.

Temario

1. Fundamentos de ciberseguridad
2. Ciberamenazas
3. Normativas generales
4. Estrategias para el cumplimiento de las normativas
5. Metodologías: ciberseguridad
6. Perfiles de trabajadores de ciberseguridad / Ramas ciberseguridad
7. Ciberseguridad aplicada
8. Introducción a la seguridad en la Nube

Módulo III | Cyber Security Ops
Nivel tres

Objetivo del módulo. El participante evaluará las brechas de seguridad de los sistemas informáticos de la empresa, para solventarlas y tomar decisiones adecuadas para la mitigación de riesgos y responder a diferentes escenarios de ataque.

Temario

1. Introducción al Hacking Ético: Kali Linux (Metasploit, Hashcat, etc.)
2. Mejores prácticas en arquitectura de red y Linux
3. Administración y monitoreo de redes (Wireshark)
4. Metodologías para realizar pruebas de penetración:
   PTES (Penetration Testing Execution Standard) NIST 800-115
5. Reconocimiento pasivo y activo
6. Recolección de Información y escaneo del objetivo
7. Análisis de vulnerabilidades y riesgos, explotación de vulnerabilidades y reporte de hallazgos
8. Procesos y metodologías para manejo de incidentes y recuperación

¡Prepárate para retar tu potencial!

/BeduOrg

@Bedu_Org

@Bedu_org

Bedu

bedu.org