HENRY

CURSO UPSKILLING

CIBERSEGURIDAD

SOBRE EL CURSO

Este contenido está dirigido a personas interesadas a dar un salto al mundo de Ciberseguridad y que se encuentran en búsqueda de desarrollar habilidades básicas de análisis de redes, amenazas y vulnerabilidades, como así también capacidades en torno a seguridad informática.

CARACTERÍSTICAS

✅ **Duración y dedicación semanal:** 10 semanas - 80 horas.

✅ **Dedicación aproximada:** 8 horas semanales.

✅ **Temáticas principales:** El curso ofrece un programa que tiene por objetivo sentar sólidas bases de conocimiento sobre Fundamentos de Ciberseguridad. El estudiante contará con un primer acercamiento a este mundo, en el que aprenderá los conceptos básicos y lo pertinente en torno al término de seguridad informática. Luego, avanzará hacia un módulo dedicado a redes en el que se espera que el estudiante aprenda a manejar y diseñar redes con fundamentos de seguridad. Por último, se brindará un módulo específico de análisis de amenazas y vulnerabilidades para que el estudiante pueda desarrollar las skills necesarias para identificarlas y generar los planes de acción para mitigar sus riesgos.

✅ **Stack Tech:** LastPass, Dashlane,, Nmap, Nessus, Wireshark, Qualys, OpenVAS, CIS Benchmarks, OWASP.

✅ **Público objetivo:** El público objetivo de este curso son personas con uno o más años de experiencia laboral en roles de tecnología o personas con conocimientos básicos en IT que deseen incursionar en el mundo de Ciberseguridad.

✅ **Requisitos:** Se recomienda contar con experiencia laboral de uno o más años en roles de tecnología, producto, negocio, soporte, administrativos, o afines. O bien, contar con un entendimiento básico de conceptos técnicos y/o de IT como sistemas operativos, redes, entre otros.

✅ **Requisitos técnicos:** Computadora 8 GB de memoria RAM y 20 GB de espacio de almacenamiento y, al menos, un procesador i5 5ta generación.

✅ **Outcome:** Al concluir este curso, los participantes habrán consolidado una base sólida de conocimientos en Ciberseguridad. Se destacan los siguientes logros anticipados:

- **Competencias básicas en Fundamentos de Ciberseguridad:** Desarrollo de habilidades prácticas como el uso de la línea de comando y la gestión de usuarios y permisos. Comprensión de los principales métodos de protección y los principios esenciales de redes y sistemas operativos.
- **Manejo responsable de redes y diseño de redes:** Capacidad de analizar una red, identificar amenazas y diseñar una red. Habilidades y criterios de clasificación de la información, protección de datos, riesgos y amenazas.
- **Dominio de habilidades para el análisis profesional de amenazas y vulnerabilidades:** Capacidad para recopilar, analizar y categorizar información sobre sistemas, políticas de seguridad y vulnerabilidades. Desarrollo de habilidades para comprender y presentar los resultados de los análisis y los planes de acción de forma clara y concisa, para priorizar y mitigar los riesgos de manera efectiva.

DINÁMICA DE CURSADA

✅ **Prework:** El Upskilling cuenta con una lección asíncrona de **Prework** que tendrá por objetivo nivelar a los estudiantes, para que puedan iniciar el Upskilling con todo el contexto y conocimiento necesario, independientemente del background que tengan. En este prework se abordarán conceptos básicos de seguridad informática tales como CIA (Confidencialidad, Integridad y Disponibilidad), Amenazas y vulnerabilidades comunes, Controles de seguridad, Ataques a la red y Vulnerabilidades de software. Es opcional, sin embargo, te recomendamos realizarlo.

✅ **Lecciones asincrónicas:** Dos lecciones asincrónicas por semana para consumir en los tiempos deseados, que incluye tanto teoría como práctica.

✅ **Proyecto Integrador:** Se realizan tres proyectos integradores a lo largo del curso. El primero aborda el módulo de Fundamentos a la Ciberseguridad, el segundo todo lo relativo a Redes y el tercero trabaja sobre Análisis de Amenazas y Vulnerabilidades.

✅ **Espacios en vivo:** Cada semana tendrá dos espacios en vivo de 90’ destinado a repasar lo más importante del contenido asincrónico y enfocar en la práctica junto a instructores especializados.

TABLA CON CONTENIDOS

El curso puede adaptarse a la cantidad de módulos/lecciones necesarias dado su carácter modular.

MÓDULOS	TEMAS
Prework (Opcional / Recomendado)	→ Introducción a la Ciberseguridad
1. Fundamentos de Ciberseguridad	→ Seguridad de Sistemas I: Endurecimiento de sistemas operativos → Seguridad de Sistemas II: Control de acceso y gestión de cuentas → Seguridad de Sistemas III: Protección contra malware y software no deseado → Criptografía y Seguridad de la

	Información → Seguridad del código fuente → Implementación de prácticas de seguridad en el desarrollo de software.
2. Redes	→ Arquitecturas de redes → Fundamentos de Redes y Ciberseguridad → Análisis de Redes → Detección de Intrusiones → Implementación de Redes & Casos prácticos → VPN y Protección → Firewall de Aplicaciones → Panorama del mercado laboral en Ciberseguridad
3. Análisis de amenazas y vulnerabilidades	→ Análisis de Vulnerabilidades: Pruebas de seguridad de aplicaciones → Análisis de Vulnerabilidades II: Identificación de vulnerabilidades y medidas de mitigación → Inteligencia de Amenazas I → Inteligencia de Amenazas II: Tendencias y medidas de defensa → Análisis Forense Digital → Análisis Forense Digital II: Causa y recuperación → Plan de Respuesta a Incidentes → Creación del Plan de Respuesta a Incidentes → Profesional en Ciberseguridad e Informática