DMC | Google Partner

> Especialización en

CYBERSECURITY SPECIALIST

56 horas académicas

100% Online **en vivo**

Certificación:

- **Por DMC:** Por haber aprobado la Especialización en **Cybersecurity Specialist**
- **Por CertiProf:** Ethical Hacking Professional Certification - CEHPC

Presentación

El trabajo con datos es indispensable en toda industria y áreas laborales, por lo que ha cobrado gran relevancia su acopio y almacenamiento para su posterior explotación. Consecuentemente, también lo ha hecho su seguridad tanto a aplicada a las redes que los transportan como a los dispositivos y medios que los almacenan.

La **Especialización en Cybersecurity Specialist** te capacitará en la aplicación de técnicas, herramientas y buenas prácticas orientadas a la detección de vulnerabilidades de seguridad en redes de datos, entornos cloud y dispositivos IoT.

Sobre esta Especialización

14	56	08
sesiones	horas académicas	talleres prácticos

¿Cómo impulsamos tu carrera?

- Sesiones 80% **enfocadas en la práctica.**
- Enfoque en **Casos Aplicados a Negocio,** enfrentando los retos del mercado.
- Énfasis en **habilidades técnicas.**
- **Mentoría especializada** con docentes expertos.
- Acompañamiento **constante.**

Objetivos de la Especialización

OBJETIVO GENERAL:

• Detecta vulnerabilidades de seguridad en redes de datos, entornos cloud y dispositivos IoT a través de la aplicación de diversas técnicas, herramientas y buenas prácticas provenientes del Ethical Hacking y marcos normativos.

OBJETIVOS ESPECÍFICOS:

• Detecta vulnerabilidades de ciberseguridad en redes inalámbricas empleando como herramienta la distribución Kali Linux y técnicas como WPA Wordlist, Web Craking y Fake Authentication.

• Detecta vulnerabilidades de ciberseguridad en entornos cloud tanto para la infraestructura como para los datos y sus medios de almacenamiento.

• Detecta vulnerabilidades de ciberseguridad en hardware y software orientado al control de procesos industriales y a sus redes de datos (redes OT).

Requisitos

• Contar con por lo menos un año de experiencia laboral en áreas de sistemas, informática, desarrollo de software, o seguridad de datos específicamente.
• Contar con una laptop o computadora de escritorio con disponibilidad de micrófono y cámara web.
• Tener instalado los softwares y herramientas señalados en la sección Contenidos.

Dirigido a

• Analistas de seguridad de datos Jr.
Profesionales que desempeñan esta labor y busquen:
- Especializarse en herramientas y técnicas de vanguardia en la seguridad de datos.

• Analista de sistemas e informática
Profesionales que desempeñan esta labor y busca:
- Especializarse e incursionar en el cambio de la seguridad de datos y la ciberseguridad.
- Cambiar de área laboral, hacia aquellas relacionadas a seguridad de la información y continuidad de negocio.

Malla Curricular

I. Ethical Hacking Foundation

1. Fundamentos de Linux y Shell

• Distribuciones Linux para escritorio y servidores.
• Proceso de instalación de una distribución de escritorio en máquina virtual (Descriptivo).
• **Taller:** Gestión de directorios y ficheros mediante línea de comandos.
• **Taller:** Gestión de usuarios y permisos mediante línea de comandos.
• **Taller:** Diseño, ejecución y automatización de scripts.

2. Fundamentos de Kali Linux

• Definición, importancia y funcionalidad en ciberseguridad.
• Revisión de requisitos para la configuración de Kali Linux.
• Instalación de Kali Linux en una máquina virtual (Descriptivo).

3. Fundamentos de Ethical Hacking

• Introducción al Ethical Hacking, su ejecución y mejores prácticas.
• Estructura de un proyecto de Hacking Ético.
• Fundamentos de la Cadena de Ataque.

4. Ethical Hacking: Técnicas de reconocimiento

• Principales técnicas de reconocimiento y footprinting.
• Principales técnicas de escaneo y enumeración.
• **Taller:** Ataques de reconocimiento.

5. Ethical Hacking: Técnicas de escalalamiento y explotación

• Principales técnicas de escalamiento y privilegios.
• Principales técnicas de explotación

6. Ethical Hacking: Técnicas Post Explotación y Escalamiento

• Principales técnicas de post-evaluaciónes y escalada de privilegios.
• Amenazas a la seguridad de la información y evaluación de vulnerabilidades.
• **Taller:** Detección de actividades anómalas.

II. Cloud CiberSec (AWS)

7. Introducción a entornos Cloud

• Arquitecturas de nube y tipos de servicios.
• Modelos de costos y buenas prácticas.
• Proceso de creación de una cuenta en AWS (Descriptivo).

8. Cloud Infrastructure CyberSec

• Identificación de vulnerabilidades orientadas a la infraestructura y estrategias sugeridas de seguridad.
• Identificación de vulnerabilidades orientadas a la red y estrategias sugeridas de seguridad.
• Gestión de accesos y permisos.
• Estrategias de seguridad.
• Gestión de riesgos y seguridad.
• **Taller:** Diseño de una estrategia integral de seguridad On-Cloud (recuperación de desastres).

9. Cloud Data CyberSec

• **Taller:** Identificación de vulnerabilidades y estrategias sugeridas de seguridad para el dato en la nube.

III. Industrial & IoT CyberSec

10. Fundamentos de Operational Technology Networks (Redes OT)

• Tecnología operativa (OT). Introducción y conceptos generales.
• Control de Supervisión y Adquisición de Datos (SCADA).
• Sistemas de control industrial (ICS).
• Brecha y convergencia de TI/OT.
• Controles de ciberseguridad para OT.

11. Riesgos en redes OT

• Identificación de vulnerabilidades y evaluación de gaps.
• Identificación y evaluación de controles.
• Análisis de impacto al negocio en activos críticos.
• **Taller:** Evaluación de riesgos OT.

12. Privacidad IoT

• Principios de privacidad por diseño.
• Privacidad en dispositivos IoT.

Nuestra Propuesta de Capacitación

Las metodologías que aplicamos

Desarrollo de competencias clave en el mundo de los datos

Analiza · Innova · Transforma

Aprendizaje Secuencial

- Descubre conocimiento de vanguardia
- Explora con la guía del experto
- Aplica lo aprendido

Aprendizaje basado en práctica (Learning by Doing)

- Resuelve retos
- Aprende en base a proyectos
- Analiza casos

Docentes Expertos

Aprende con los líderes de las mejores empresas de Latam.

Jhon Jona

Network Specialist

UNIVERSIDAD esan

Ernesto Landa

Information Security Officer

tgp TRANSFORMANDO CON ENERGÍA

Miguel García

Especialista en TI

E2E

*En caso de contingencias podría cambiar alguno de los docentes por otro profesional de similar perfil.

DMC | Google Partner

¿Qué certificado obtendrás?

• Certificado por aprobación de la Especialización Cibersecurity Specialist, por un total de 56 horas académicas.

¿Qué certificado obtendrás?

Al completar la Especialización, también contarás con la oportunidad de rendir el **Ethical Hacking Professional Certification (CEHPC) emitido por Certiprof, por solo 50 dólares (opcional).**

El costo real del examen Certiprof es de 150 dólares

El alumno tendrá hasta 02 oportunidades de aprobar el examen por el pago realizado.

** Para acceder al beneficio, el alumno debe aprobar satisfactoriamente la especialización.*
** El alumno tiene libre disposición para decidir si aplica o no a la certificación de CertiProf. En caso de aplicar, deberá pagar el derecho de examen y aprobarlo para obtener el certificado.*
** La certificación no es automática.*

¿Por qué elegirnos?

- Somos los primeros en Perú en apostar por el desarrollo de profesionales y empresars en data & analytoics con más de 15 años de experiencia.
- Las empresas worldclass de Latam confían en nosotros para acompañarlas en su transformación hacia el enfoque data driven.
- Nuestros docentes son destacados expertos en data & analytics que lideran equipos de alto rendimiento en las empresas más grandes de Latam.
- Nuestra metodología “Aprende haciendo” ha logrado que nuestra comunidad de +25K profesionales en todo Latam mejoren su situación laboral.
- Tenemos el portafolio más completo con +150 capacitaciones sincrónicas y asincrónicas que se ajustan a diferentes perfiles y niveles de conocimiento.

DMC | Google Partner

www.dmc.pe