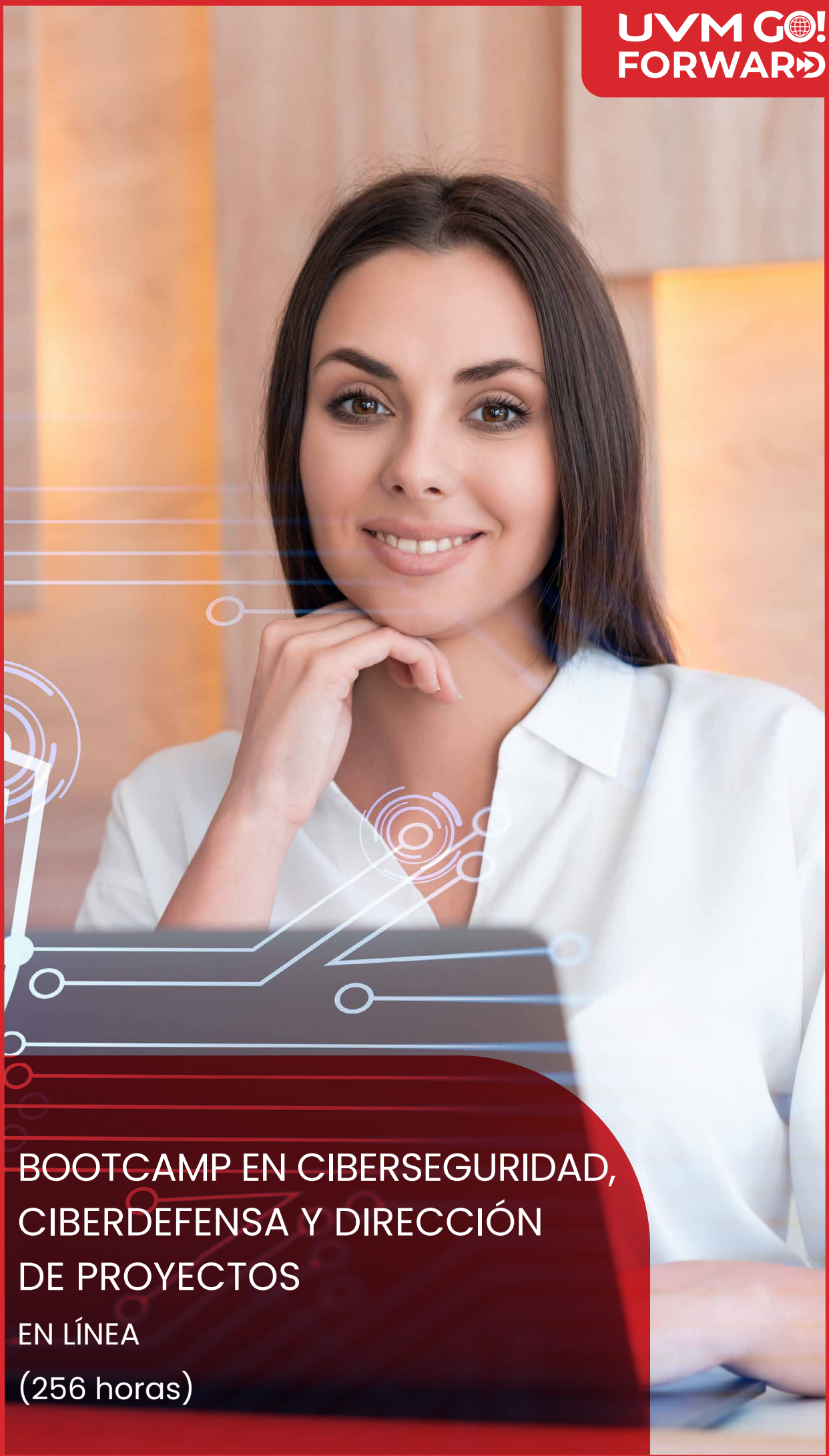
UVM GO! FORWARD



BOOTCAMP EN CIBERSEGURIDAD, CIBERDEFENSA Y DIRECCIÓN DE PROYECTOS

EN LÍNEA

(256 horas)

Objetivo:

— Formar profesionales capaces de diagnosticar vulnerabilidades, responder a ciberataques y liderar proyectos tecnológicos con base en estándares internacionales de ciberseguridad y PMI.

Dirigido a:

— Técnicos y líderes de IT, ingenieros, desarrolladores y gestores de proyectos con al menos 6 meses de experiencia en sectores como tecnología, finanzas y telecomunicaciones.

Reconocimiento:

— Al finalizar tu programa recibirás:

- **Diploma Digital** con **validez curricular** y **tecnología Blockchain** con código QR y de verificación.
- Dos certificados internacionales digitales **Blockchain de Embiz Foundation**: Certificado Digital Internacional de Ciberseguridad y Ciberdefensa y Certificado Digital Internacional de Dirección de Proyectos.
- Dos certificados **Ibaktor DC3 de competencias laborales**: Certificado Ibaktor DC-3 de Competencias Laborales de Ciberseguridad y Ciberdefensa y Certificado Ibaktor DC-3 de Competencias Laborales de Dirección de Proyectos

UVM GO! FORWARD

¿Por qué UVM?

Tenemos **más de 60 años** de **experiencia académica**, más de **150 programas educativos** y más de **180 programas de excelencia** a nivel nacional.

Adquieres **conocimientos** y **habilidades esenciales** que puedes **aplicar de inmediato** en tu **actividad profesional**.

Los **profesores** que imparten las **Certificaciones y Diplomados** son **expertos reconocidos** en **sus campos**.

Tienes **flexibilidad educativa** que te permite **estudiar a tu ritmo**, a **cualquier hora** y en **cualquier lugar**.

Los **Diplomados y Certificaciones UVM** enriquecen tu **CV** y te posicionan como **el mejor candidato**.

Al estudiar el programa podrás:

Diagnosticar vulnerabilidades, prevenir y responder a ciberataques, liderar proyectos tecnológicos, obtener certificaciones internacionales y aplicar herramientas en tu entorno laboral.

UVM GO! FORWARD

BLOQUES DE APRENDIZAJE

Fundamentos de la ciberdefensa y ciberseguridad y de dirección de proyectos

Comprender principios clave de ciberseguridad, gestión de riesgos, continuidad del negocio y protección de sistemas, así como fundamentos PMI y estructura del examen PMP.

Configuración y operaciones de sistemas

Configurar y fortalecer Linux y Windows, automatizar tareas con Bash y PowerShell, gestionar y centralizar *logs*, optimizar servicios y administrar Active Directory para mejorar la seguridad operativa.

Redes, seguridad en comunicaciones y *cloud*

Diseñar y operar redes seguras, implementar segmentación, proteger comunicaciones y datos, aplicar cifrado, asegurar entornos *cloud* y virtualizados, y gestionar identidades y accesos.

Respuesta a incidentes, forense y monitoreo

Planificar y ejecutar respuesta a incidentes, detectar y mitigar amenazas, realizar análisis forense digital, recuperar datos y configurar SIEM para monitoreo y correlación de eventos en tiempo real.

Hacking ético, pruebas de penetración y vulnerabilidades

Aplicar metodologías OWASP y PTES para pruebas de penetración, identificar y explotar vulnerabilidades, ejecutar post-explotación y generar reportes técnicos con planes de remediación.

BLOQUES DE APRENDIZAJE

Desarrollar ejercicios Red/Blue Team, realizar OSINT, simular ataques en entornos controlados, diseñar campañas de concienciación y analizar ingeniería social y amenazas persistentes avanzadas.

Ejercicios prácticos de adversario y concienciación

Planeación, ejecución, monitoreo, control y cierre: Aplicar buenas prácticas PMI para planificar, ejecutar, monitorear y cerrar proyectos, gestionando alcance, costos, riesgos, recursos y asegurando valor para el negocio.

Dirección de proyectos

Utilizar *design thinking* para innovar, liderar con enfoque ágil, aplicar *management* 3.0 y *lean change management* para gestionar el cambio organizacional.

Dirección de proyectos: innovación, *design thinking, management* 3.0 y *change management*

Preparar certificaciones PMI-ACP y SCRUM, aplicar marcos ágiles, gestionar proyectos con ciclos iterativos e incrementales y promover cultura ágil a nivel organizacional.

Dirección de proyectos: innovación, *agile management* y SCRUM

BLOQUES DE APRENDIZAJE

Fundamentos de la ciberdefensa y ciberseguridad y de dirección de proyectos

1. Conceptos básicos
    a. Definición de ciberseguridad
    b. Principios de la ciberseguridad
2. Gobernanza, riesgo y cumplimiento
    a. Gobernanza de la ciberseguridad
    b. Análisis y mitigación del riesgo
    c. Cumplimiento normativo
3. Planificación de la continuidad del negocio
    a. *Business Continuity Planning* (BCP)
    b. *Disaster Recovery* (DR)
4. Infraestructura y seguridad en sistemas operativos
    a. Configuración segura
    b. Tareas y automatización
    c. Monitorización y *logging*
5. Desafíos actuales y tendencias en ciberseguridad
    a. Amenazas emergentes
    b. Soluciones y tendencias
6. Fundamentos de dirección de proyectos: Marco conceptual y el grupo de procesos de inicio
    a. El examen de certificación PMP (nueva estructura del examen por dominios: personas, procesos y ambiente de negocios)
    b. Propósito de la gestión de proyectos
    c. Principios de la gestión de proyectos y su alineación con la estrategia organizacional
    d. Los dominios de desempeño de la gestión de proyectos
    e. Entorno en el que operan los proyectos
    f. Rol de administrador del proyecto
    g. Definiciones: proyecto, *stakeholders*, programa, director de proyecto
    h. Características del director de proyectos
    i. Sistemas organizacionales en los que operan los proyectos
    j. Ciclo de administración de proyectos (cascada, ágil, híbrido)
    k. Grupo de procesos de inicio

Configuración y *Hardening* de Sitemas Operativos

1. Configuración de Linux
    a. Introducción a HTML
    b. Configuración de Windows
    c. *Hardening* de sistemas
2. Automatización y tareas programadas
    a. Tar, Cron, Cronjobs
    b. Automatización en Windows
3. *Logging* y monitorización
    a. Gestión de registros en Linux
    b. Gestión de registros en Windows
    c. Centralización de *logs*
4. *Scripting* y automatización avanzada
    a. *Bash Scripting*
    b. *PowerShell* en Windows
5. Administración de directorio activo y autenticación
    a. Introducción al *Active Directory*
    b. Kerberos

Redes, seguridad en comunicaciones y *cloud*

1. Arquitectura y diseño de redes
    a. Fundamentos de redes
    b. Diseño de red seguro
2. Operaciones de red y seguridad
    a. Operación de redes y monitoreo
    b. *Port scanning* y reconocimiento
    c. Defensa y mitigación
3. Análisis de tráfico y herramientas
    a. Introducción a *Wireshark*
    b. Detección de anomalías
4. Comunicación segura y protección de datos
    a. *E-mail security*
    b. *Wireless security*
    c. *Cryptography* y *Encryption*
5. Seguridad en cloud y virtualización
    a. Fundamentos del *cloud computing*
    b. Configuración y *hardening* en la nube
    c. Virtualización y contenedores

Respuesta a incidentes, forense y monitoreo

1. Conceptos básicos de respuesta a incidentes
    a. Introducción a la respuesta a incidentes
    b. Equipos de respuesta a incidentes (CERT/CSIRT)
2. Preparación y detección de incidentes
    a. Planificación de respuesta a incidentes
    b. Detección de incidentes
3. Gestión y mitigación de incidentes
    a. Análisis y valoración
    b. Contención y erradicación
4. Forense digital y análisis post-incidente
    a. Introducción a la forense digital
    b. Extracción y análisis de evidencia
    c. *Data recovery*
5. Monitoreo proactivo y herramientas
    a. Introducción a *splunk*
    b. Otras soluciones de monitoreo y *logging*
    c. Integración y correlación de eventos

Hacking ético, pruebas de penetración y vulnerabilidades

1. Introducción al *hacking* ético y pruebas de penetración
    a. Conceptos básicos
    b. Metodologías de prueba
2. Reconocimiento y escaneo
    a. Técnicas de reconocimiento
    b. Escaneo y enumeración
3. Explotación y post-explotación
    a. Vulnerabilidades *web* y explotación
    b. *Frameworks* de explotación
    c. *Pivoting* y movimiento lateral
4. Herramientas avanzadas y técnicas
    a. Burp Suite
    b. Otras Herramientas
5. Reporte y remediación
    a. Generación de informes
    b. Estrategias de remediación

Ejercicios prácticos de adversario y concienciación

1. Red team vs Blue team
    a. Dinámica de equipos y objetivos
    b. Herramientas y metodologías
2. Programas de concienciación
    a. Importancia de la educación en ciberseguridad
    b. Diseño de campañas
3. Simulación de ataques
    a. Escenarios de ataques
    b. Entornos controlados
4. Psicología en ciberseguridad
    a. Comportamiento humano y seguridad
    b. Cultura de seguridad
5. Técnicas OSINT (*Open Source Intelligence*)
    a. Herramientas y plataformas
    b. Aplicaciones y limitaciones
6. Ciberespionaje
    a. Tácticas y herramientas
    b. Defensas y contramedidas
7. Estudio de APTs (Amenazas Persistentes Avanzadas)
    a. Características y metodologías
    b. Caso práctico

Dirección de proyectos: planeación, ejecución, monitoreo, control y cierre

1. Grupo de procesos de planeación (creando un equipo de alto desempeño)
   a. Construir un equipo
   b. Definir reglas básicas del equipo
   c. Negociar acuerdos de proyectos
   d. Capacitar y formar a los miembros del equipo e interesados
   e. Involucrar y apoyar a los equipos virtuales
   f. Construir un entendimiento compartido sobre un proyecto
   g. Los cómos del proyecto
   h. Los qué del proyecto
2. Grupo de procesos de ejecución (iniciar y hacer el trabajo)
   a. Gestionar
   b. Ejecutar el proyecto para generar valor al negocio
   c. Administrar las comunicaciones
   d. Involucrar a los interesados
   e. Crear artefactos del proyecto
   f. Administrar los cambios del proyecto
   g. Gestionar los cambios del proyecto
   h. Garantizar la transferencia de conocimientos para la continuidad del proyecto
   i. Procesos involucrados
3. Grupo de procesos de monitoreo y control (mantener al equipo en buen camino)
   a. Liderar un equipo
   b. Apoyar el desempeño del equipo
   c. Abordar y eliminar impedimentos, obstáculos y bloqueadores
   d. Manejar conflictos
   e. Colaborar con los interesados
   f. Asesorar a los interesados relevantes
   g. Aplicar la inteligencia emocional para promover el desempeño del equipo
   h. Procesos involucrados
4. Grupo de procesos de cierre (tener en cuenta al negocio)
   a. Administrar los requisitos de cumplimiento
   b. Evaluar y entregar los beneficios y el valor del proyecto
   c. Evaluar y abordar los cambios internos y externos del entorno empresarial
   d. Apoyar el cambio organizacional
   e. Procesos involucrados
   f. Mapa de integración de los 49 procesos

MODULO MHS: Dirección de proyectos: Innovación, *design thinking*, *management* 3.0, *change management*

1. Innovación & *design thinking*
    a. Creatividad e innovación
    b. Introducción al *design thinking*
    c. Proceso del *design thinking*

2. Liderazgo, *management* 3.0 y *change management*
    a. El factor liderazgo
    b. Los roles en métodos ágiles
    c. Las prácticas esenciales de métodos ágiles
    d. *Management* 3.0 y *lean change management*

MODULO MIC: Dirección de proyectos: Innovación, *agile management* y SCRUM

1. PMI® *Agile Certified Practicioner*
    a. Introducción a los modelos ágiles de gestión del proyecto
    b. Selección del ciclo de vida
    c. Creación de entornos ágiles
    d. Entregas bajo un entorno ágil
    e. Consideraciones organizacionales para la agilidad del proyecto
2. SCRUM
    a. Introducción a los métodos ágiles de desarrollo
    b. Marco de referencia SCRUM a detalle
    c. SCRUM en práctica
3. Implementación de la administración de proyectos ágil en la organización
    a. Entender la administración de proyectos organizacional
    b. Los pilares de la administración de proyectos organizacional
    c. Pasos para implementar la administración de proyectos organizacional
    d. Personalización de procesos para establecer el modelo ágil o híbrido para la gestión de proyectos
    e. Revisión de proyectos de los participantes
    f. Presentación de proyectos de los participantes
    g. Cierre y premiación a mejores proyectos

UVM GO! FORWARD

Beneficios de la modalidad

Clases en vivo, actividades interactivas y casos prácticos. Puedes interactuar con profesores y otros alumnos para tener una experiencia más enriquecedora.

Networking. Tienes la oportunidad de construir una red de contactos profesionales con otras personas que tienen intereses similares o se desempeñan en el mismo ámbito.

Estudia a tu ritmo. Consulta todas las sesiones grabadas en el horario que más te convenga.

Soporte técnico. Cuentas con atención técnica en todo momento para ayudarte a solucionar cualquier problema que se presente.

Asesoría y acompañamiento. Tienes un tutor que te brindará apoyo a través de enlaces en vivo, chat o WhatsApp para resolver cualquier duda.

UVM GO! FORWARD

SÉ PARTE DE LA UVM

@uvmmx uvm @uvmmx uvm.mx