

DIPLOMADO EN CIBERSEGURIDAD
Y CIBERDEFENSA
AULA VIRTUAL
(9 meses)

DIPLOMADO EJECUTIVO

¡Transforma tu perfil profesional y destaca en el mercado laboral!

- Obtén tres insignias digitales que validan tus habilidades.
- Credenciales verificables con tecnología blockchain, que fortalecen tu perfil profesional.
- Accede a +20 programas en diversas áreas de estudio, diseñados para responder a las demandas actuales de los empleadores



Reconocimiento Diplomado Ejecutivo

Obtén un Constancia digital UVM del programa con tecnología blockchain y código de verificación



Reconocimiento Curso IA

Adquiere nuevos conocimientos y desarrolla tus habilidades para el uso práctico y estratégico de las herramientas de IA en tu entorno profesional.



Constancia DC-3 por STPS

Documento avalado por la Secretaría de Trabajo y Previsión Social (STPS) que acredita las habilidades y competencias adquiridas.

Objetivo:

- Desarrollar habilidades analíticas, críticas y creativas para la protección y defensa de sistemas y redes en un entorno interconectado y digitalizado.

Dirigido a:

- Profesionales de Tecnologías de la Información (TI), profesionales de seguridad informática, responsables de seguridad de la información, consultores y auditores de seguridad, emprendedores y empresarios.

Reconocimiento:

- Al finalizar tu programa recibirás:
 - **Diploma Digital** con **validez curricular** y **tecnología Blockchain** con código QR y de verificación.

¿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:

Analizar el estado actual de la Seguridad de la Información de las organizaciones.



Definir un esquema de identificación, prevención y gestión de incidentes digitales.



Emplear controles que permitan la detección de riesgos y amenazas de acuerdo con normas y estándares internacionales.



Generar una estrategia de protección y defensa de la infraestructura crítica.



MÓDULOS

01 El Ecosistema de la Ciberseguridad

1. Introducción
 - a. Definiciones: ecosistema, seguridad y ciberseguridad
 - b. La idea de un ecosistema de negocios: Lectura y discusión
 - c. El enfoque clásico de personas, procesos y tecnología
2. Conociendo el Ecosistema de la Ciberseguridad
 - a. Ejemplo de aplicación (Secretaría de Seguridad Pública – SMAR)
 - b. Salud, viabilidad y economía de un ecosistema
 - c. Actividad: perfilando un ecosistema de la ciberseguridad

02 Ciberseguridad Operativa

1. El proceder de un hacker
 - a. ¿Qué es un hacker?
 - b. Cracker
 - c. Objetivo de un hacker
 - d. Perfil de un hacker
 - e. Motivaciones
 - f. 6 Escalas de Grises
2. Contraseñas
 - a. ¿Qué es una contraseña?
 - b. Objetivo de una contraseña
 - c. Como generar contraseñas seguras
 - d. Errores más comunes al crear una contraseña
 - e. Generadores de contraseñas
3. Criptología
 - a. ¿Qué es la criptología?
 - b. Objetivos de la criptología
 - c. Usos de la criptografía
 - d. Tipos de algoritmos
 - e. Ataques
4. Aplicaciones criptográficas
 - a. Navegación en internet
 - b. Firma electrónica
 - c. Funciones de Hash
 - d. Firma digital
 - e. HMAC
 - f. PKI
 - g. Certificado digital x.509
 - h. Autoridad de Registro (RA)
 - i. Autoridad de Certificación (CA)
 - j. Revocación de certificados
 - k. Distribución de certificados
5. Control de acceso
 - a. ¿Qué es el control de acceso?
 - b. Identificación
 - c. Autenticación
 - d. Autorización
 - e. Tipos de control de acceso
 - f. Amenazas
 - g. Utilización de Passports
 - h. Sistemas Biométricos
 - i. Single Sign On (SSO)
 - j. Kerberos y otros protocolos SSO
 - k. Modelos de control de acceso
 - l. Administración de control de acceso
 - m. Monitoreo, Auditoria y Logs
 - n. Sistemas de Detección de Intrusos (IDS e IPS)
6. Técnicas generales de ataques
 - a. Envenenamiento de la red: Poisoning
 - b. Análisis de protocolos: Sniffing
 - c. Impersonalización:
 - d. Robo de sesiones: Hijacking Spoofing
 - e. Fuerza bruta
 - f. Denegación de servicio
7. Vulnerabilidades
5.
 - a. Pruebas de Desbordamiento de Buffer (Overflow)
 - b. Pruebas de Resiliencia de la Arquitectura
 - c. Pruebas de Denegación de Servicios (DDOS)
 - d. Pruebas de Inyección de SQL (SQL Injection)
 - e. Pruebas de Inyección de Sitio Cruzado (XSS)
 - f. Pruebas de Inyección de HTML (HTML Injection)
 - g. Pruebas de Inyección de Hoja de Estilo en Cascada (CSS Injection)
 - h. Pruebas de Inyección de Código de Sitio con Flash (Cross site flashing)
 - i. Pruebas de Secuestro de clic (Click jacking)
 - j. Pruebas de Inclusión de Archivos
 - k. Pruebas de Validación de Canales Seguros (SSL/TLS)
 - l. Pruebas de Información en Canales no Cifrados
 - m. Pruebas de Falsificación de Peticiones de Sitios Cruzados (CSRF)
 - n. Pruebas de Búsqueda de Directorios Críticos
 - ñ. Pruebas de Debilidad en Usuario y Contraseñas
 - o. Pruebas de Reconocimiento Activo
8. Vulnerabilidades en la programación
 - a. Programación segura
 - b. OWASP top 10
9. Seguridad en las transacciones electrónicas
 - a. Robo de identidad
 - b. Seguridad personal online
 - c. 3 PCI
10. Ethical Hacking
 - a. Concepto de Hacking
 - b. Perfil de conocimientos
 - c. Códigos de ética
 - d. Penetration Test y Ethical Hacking
 - f. Análisis de brecha de cumplimiento
 - g. Autotesteo y contratación
 - h. Clasificaciones

03 Ciberseguridad Táctica

1. Gobernanza y Administración de Riesgos
 - a. Definición de gobernanza
2. b. COBIT 5. Gobernanza y gestión
Gestión de riesgos: modelos generales
 - a. La importancia de la medición del riesgo
 - b. Enfoques de gestión de riesgos que crean riesgos
 - c. El enfoque de las normas ISO 15408 e ISO 18045
 - d. El ciclo clásico de gestión: Planear, Hacer, Verificar, Actuar

04 Ciberseguridad Estratégica

1. Entorno Global y Marco Normativo de la Ciberseguridad
 - a. El valor de los estándares y buenas prácticas
 - b. Las normas ISO 27000
 - c. Revisión de las normas ISF, NIST, COBIT 5 y PCI-DSS
 - d. La necesidad de las políticas de ciberseguridad
2. Gobierno de Seguridad de la Información
 - a. Gobierno de Seguridad de la Información y Administración de la Seguridad
 - b. Principios de Gobierno de Seguridad y resultados deseables
 - c. Componentes, enfoque y evaluación del Gobierno de la Seguridad
 - d. Mejores prácticas en Gobierno de Seguridad

05 Ciberinteligencia

1. Fundamentos
2. Inteligencia de Fuentes Abiertas
3. Metadatos
4. Deep Web

06 Ciberseguridad en Entornos Cloud, Internet de las Cosas y entornos

1. Seguridad en Entornos Cloud
 - a. ¿Qué son los Entornos Cloud?
 - b. Conceptos de PaaS, SaaS, IaaS
 - c. Modelo de responsabilidad compartida en la nube
 - d. Proveedores de Nube y niveles de seguridad
2. Seguridad en Internet de las Cosas
 - a. ¿Qué es el Internet de las Cosas?
 - b. Riesgos y amenazas en dispositivos de IoT
 - c. Reglas básicas de protección en IoT
3. Seguridad en Entornos Industriales
 - a. Que son los Entornos Industriales
 - b. Seguridad en los Entornos Industriales
 - c. Riesgos y Amenazas en Entornos Industriales
 - d. Como protegerse en Entornos Industriales
4. Advanced Persistent Security
 - a. Fases de un modelo de seguridad persistente
 - b. Modelo de Protección
 - c. Modelo de Detección
 - d. Modelo de Reacción
 - e. Modelo de Implementación
5. Análisis Forense en Cloud y Aplicaciones Móviles
 - a. Que es el análisis forense digital
 - b. Casos de uso del análisis forense
 - c. Estrategias de inspección forenses en Cloud y Aplicaciones Móviles
6. Microservicios
 - a. Arquitectura monolítica vs. microservicios
 - b. Características de los microservicios y sus beneficios para su gestión en la nube

07 Computación Forense

1. Etapas de un análisis forense
 - a. Definición de fases
2. Adquisición de evidencias digitales
 - a. Definición de HASH
 - i. ¿Por qué usar un valor hash?
 - ii. Función hash de archivos
 - iii. Algoritmos validos
 - iv. Practica de checksum
 - b. FTK Imager
 - i. Uso de FTK imager
 - ii. Practica de FTK imager
3. Preservación de la integridad e identidad de las evidencias
 - a. Preservación física de la evidencia
 - i. Resguardo de discos duros
 - ii. Bolsa anti estática
 - iii. Cajas Pelican
 - iv. Magnetismo
 - b. Bloqueadores
 - i. Tipos de bloqueadores
 - ii. Ventajas de los bloqueadores
 - iii. Herramientas de preservación
4. Cadena de custodia de las evidencias
 - a. Cadena de custodia física
 - b. Metodologías de forenses informático
 - c. Estándares de forense informático
 - d. Implicaciones legales
 - e. Casos reales de violación de la cadena de custodia
 - f. Análisis de las evidencias
5. Laboratorio de análisis forense
 - a. Análisis de metadatos
 - b. Análisis de accesos al sistema operativo
 - c. Análisis de trafico de red
 - d. Análisis de navegadores

08 Ciberdefensa

1. Ciberpatrullaje
 - a. Inspección de medidas de seguridad en el entorno
 - b. Que activos debo de proteger
 - c. Activos vulnerables dentro de la organización
2. Estrategias de Ciberdefensas
 - a. Modelos protección de la seguridad
 - b. Como protegerme
 - c. Modelos de ciberdefensas
3. Ciberdefensa Personal
 - a. Esquemas de protección de seguridad informática personal
 - b. Contramedidas para protegerme
 - c. Software y herramientas para protegerme
4. Ciberdefensa Organizacional
 - a. Como proteger mi organización
 - b. Modelos de protección en capas
 - c. Medidas para proteger los activos organizacionales

09 Proyecto: Diseño de un Programa de Ciberseguridad

1. Diseño del Programa.
 - a. Estrategias para diseñar un programa de ciberseguridad.
 - b. Aspectos a tener en cuenta en el diseño
2. Modelización de Amenazas
 - a. Estrategias para la detección de amenazas
 - b. Estrategia para modelar las amenazas
3. Respuesta a Incidentes.
 - a. Categorización y priorización de incidentes
 - b. Estrategias de respuesta ante incidentes
4. Reacción inmediata en Ciberseguridad
 - a. Estrategias para la detección de ataques
 - b. Diseño
5. Funciones y responsabilidades del CISO
 - a. Funciones del director de seguridad de la información dentro de la organización
 - b. Responsabilidad del Director de Seguridad de la información dentro de la organización
 - c. Funciones y responsabilidades del CI

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.

Asesoría y acompañamiento. Cuentas con un facilitador por módulo para guiarte durante tu curso.

Aplica lo que aprendas de forma inmediata.

Nota: Si no asistes a las sesiones en vivo con el profesor en las fechas y horarios establecidos, tendrás 30 días naturales para ver completa la grabación de la clase en Teams® y realizar la actividad asignada para que acredites el módulo.

SÉ PARTE DE LA UVM



@uvmmx



uvm



@uvmmx



uvm.mx