

DIPLOMADO EN INFORMÁTICA FORENSE Y CIBERSEGURIDAD

AULA VIRTUAL
(96 horas)

Objetivo:

- Desarrollarás competencias para investigar incidentes digitales, preservar evidencias informáticas y aplicar estrategias de ciberseguridad para prevenir, detectar y responder ante delitos cibernéticos.

Dirigido a:

- Profesionales de tecnologías de la información, seguridad de la información, derecho digital, auditoría, fuerzas del orden y consultores que buscan fortalecer sus capacidades en investigación digital y gestión de ciberincidentes.

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 65 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:

Detectar y analizar incidentes de seguridad informática.



Preservar y presentar evidencias digitales en investigaciones tecnológicas.



Implementar medidas de protección para la infraestructura digital.



Coordinar investigaciones de ciberincidentes con enfoque técnico y legal.



MÓDULOS

01 Fundamentos Estratégicos de la Investigación Digital y Responsabilidad Ejecutiva

1. Panorama del Riesgo Digital en México
 - a. Tendencias de ciberdelito en México
 - b. Impacto financiero y reputacional en empresas
 - c. Casos reales en el sector corporativo mexicano
 - d. Responsabilidad del mando medio en incidentes digitales
2. Evidencia Digital con Valor Legal
 - a. Qué constituye evidencia digital válida
 - b. Integridad, autenticidad y trazabilidad
 - c. Evidencia volátil y no volátil
 - d. Errores comunes que invalidan procesos
3. Cadena de Custodia en Entornos Corporativos
 - a. Procedimientos formales en México
 - b. Documentación y registro adecuado
 - c. Coordinación con áreas jurídicas
 - d. Responsabilidad administrativa
4. Caso Ejecutivo Introductorio
 - a. Simulación de incidente interno
 - b. Evaluación de riesgos
 - c. Decisiones inmediatas del ejecutivo
 - d. Lecciones estratégicas

02 Supervisión Ejecutiva de la Adquisición de Evidencia Digital

1. Métodos de Adquisición
 - a. Adquisición lógica y física
 - b. Clonado y preservación certificada
 - c. Validación hash
 - d. Aseguramiento en entorno empresarial
2. Herramientas y Control Ejecutivo
 - a. Plataformas forenses más utilizadas
 - b. Herramientas open source relevantes
 - c. Limitaciones técnicas y legales
 - d. Criterios para evaluar proveedores tecnológicos
3. Evidencia en Dispositivos Móviles y Nube
 - a. Mensajería corporativa y WhatsApp
 - b. Evidencia en servicios cloud
 - c. Riesgos de jurisdicción internacional
- b. Gestión de terceros tecnológicos
4. Checklist Ejecutivo de Supervisión
 - a. Validación de procedimientos técnicos
 - b. Indicadores de alerta
 - c. Control documental
 - d. Elaboración de reporte preliminar para dirección

03 Investigación Digital Aplicada a Fraude Corporativo

1. Reconstrucción de Eventos Digitales
 - a. Interpretación de logs
 - b. Línea de tiempo digital
 - c. Metadatos relevantes
 - d. Identificación de patrones anómalos
2. Fraude Electrónico y Suplantación
 - a. Phishing corporativo
 - b. Suplantación de identidad empresarial
 - c. Análisis de correos electrónicos
 - d. Prevención interna
3. Análisis de Redes en Entornos Empresariales
 - a. Interpretación ejecutiva de tráfico sospechoso
 - b. Detección de intrusiones internas
 - c. Riesgos en redes corporativas
 - d. Indicadores de compromiso
4. Comunicación de Hallazgos
 - a. Traducción técnica a lenguaje ejecutivo
 - b. Presentación ante comité directivo
 - c. Determinación de responsabilidades
 - d. Recomendaciones estratégicas

04 Gestión Estratégica de Ciberincidentes y Continuidad del Negocio

1. Amenazas Relevantes en México
 - a. Ransomware corporativo
 - b. Fraude digital organizado
 - c. Ingeniería social avanzada
 - d. Ataques a cadenas de suministro
2. Respuesta Ejecutiva a Incidentes
 - a. Activación de protocolo interno
 - b. Contención inmediata
 - c. Coordinación con jurídico y TI
 - d. Comunicación interna y externa
3. Impacto y Continuidad Operativa
 - Evaluación financiera del incidente
 - Gestión reputacional
 - Plan de recuperación
 - Relación con aseguradoras
4. Simulación de Comité de Crisis
 - a. Análisis de incidente en tiempo real
 - b. Decisiones bajo presión
 - c. Elaboración de reporte ejecutivo
 - d. Evaluación estratégica

05 Marco Legal Mexicano y Responsabilidad Corporativa

1. Delitos Informáticos en México
 - a. Código Penal Federal
 - b. Fraude y acceso ilícito
 - c. Responsabilidad de administradores
 - d. Consecuencias penales y civiles
2. Protección de Datos y Autoridad Reguladora en México
 - a. Ley Federal de Protección de Datos Personales
 - b. Obligaciones corporativas
 - c. Multas y sanciones
 - d. Auditorías y cumplimiento
3. Evidencia Digital en Juicio
 - Valor probatorio
 - Dictamen pericial
4. Gobierno Corporativo Digital
 - a. Políticas internas de ciberseguridad
 - b. Gestión de riesgos tecnológicos
 - c. Ética profesional
 - d. Buenas prácticas internacionales
5. Comparecencia en tribunal
 - a. Estrategia probatoria

06 Taller Ejecutivo Integrador: Gestión Integral de Incidente Digital

1. Presentación del Caso Corporativo
 - a. Incidente complejo empresarial
 - b. Evidencias iniciales
 - c. Identificación de riesgos
 - d. Asignación de roles ejecutivos
2. Investigación y Evaluación
 - a. Validación técnica
 - b. Reconstrucción de hechos
 - c. Determinación de impacto
 - d. Evaluación de responsabilidades
3. Elaboración de Informe Ejecutivo
 - a. Estructura del dictamen
 - b. Integración de anexos probatorios
 - c. Conclusiones estratégicas
 - d. Recomendaciones preventivas
4. Simulación de Comité Directivo
 - a. Presentación del caso
 - b. Interrogatorio cruzado
 - c. Toma de decisiones estratégicas
 - d. Retroalimentación final

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 10 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