Educación CONTINUA | UVM

DIPLOMADO

Ciberseguridad y Ciberdefensa

Aula Virtual | 8 meses

Objetivos

- Profundizar en los principales elementos de identificación, protección, detección, respuesta y recuperación ante una amenaza en términos de ciberseguridad y alinear los recursos que ofrecen las tecnologías de la información con los objetivos de negocio o institucionales.
- Dirigir desde una visión integral la gestión de los procesos asociada a la seguridad de la información en entornos empresariales y administrativos, sabiendo identificar las claves de éxito en los proyectos, y contribuyendo desde la Dirección de Seguridad de la Información en la estrategia empresarial.
- Identificar los flujos de gestión operativa a partir de la consideración, selección y puesta en marcha de procesos informatizados y de recolección de información que puede ayudar a conocer el desempeño en ciberseguridad.
- Conocer cómo optimizar los flujos de gestión operativa a partir de la consideración, selección y puesta en marcha de procesos informáticos y de recolección de información que puede ayudar a profundizar el desempeño en ciberseguridad.
- Describir como proteger los datos sensibles frente amenazas que puedan materializarse por parte de nuestros adversarios.
- Aplicar con una visión holística las tendencias en el sector de seguridad de la información, así como su empleo en los procesos de negocio y actividades comerciales.

Este curso esta dirigido a ...

- A profesionales responsable en tecnologías de seguridad de la información.

Aprenderás...

- Los participantes podrán analizar el estado del sistema de seguridad de las organizaciones para implementarlo o mejorarlo, de forma que su organización asegure la entrega de beneficios, la optimización de recursos y la optimización riesgos.
- Evaluar las capacidades y la infraestructura tecnológica para prevenir delitos cibernéticos.
- Diseñar protocolos de operación para la prevención de delitos cibernéticos.
- Definir un esquema de identificación, prevención y gestión de incidentes digitales.
- Apoyar en el fortalecimiento y esquema de identificación, prevención y gestión de incidentes digitales.
- Generar una estrategia de protección y defensa de la infraestructura crítica.
- Generar conocimiento para proteger la seguridad y privacidad digital.
- Identificar los puntos ciegos en temas de seguridad en las personas, procesos y tecnología.

- Experimentar con los participantes el valor de la seguridad.
- Identificar los riesgos y amenazas actuales dentro sus organizaciones aplicando la "defensa en profundidad".
- Emplear controles que permitan la detección de riesgos y amenazas de acuerdo con normas y estándares internacionales.
- Preparar acciones preventivas y reactivas ante riesgos y amenazas.

Requisitos para tomar el curso

- Licenciatura o ingenierías relacionadas a las Tecnologías de la Información.

Este curso incluye:

- Materiales de lectura y ejercicios complementarios.
- Ejercicios teórico prácticos enfocados a la seguridad de la información aplicable en el negocio.
- Posibilidad para solicitar una certificación de manera opcional en:
  - Fundamentos Cyber & IT Security
  - Fundamentos Seguridad de la Información basado en ISO IEC 27001
  - Fundamentos Cloud Computing
  - Ethical Hacker Certification
  - Computer Hacking Forensic Investigator.
- Diseño de un programa de ciberseguridad.
- Diploma.

MÓDULOS

01 Conociendo el ecosistema de la ciberseguridad

1. Introducción.
    - 1.1 Definiciones: ecosistema, seguridad y ciberseguridad.
    - 1.2 La idea de un ecosistema de negocios. Lectura y discusión.
    - 1.3 El enfoque clásico de personas, procesos y tecnología.
2. Conociendo el ecosistema de la ciberseguridad.
    - 2.1 Ejemplo de aplicación (Secretaría de Seguridad Pública – SMAR).
    - 2.2 Salud, viabilidad y economía de un ecosistema.
    - 2.3 Actividad: perfilando un ecosistema de la ciberseguridad.

02 Ciberseguridad Operativa

1. El proceder de un hacker.
    - 1.1 ¿Qué es un hacker?
    - 1.2 Cracker.
    - 1.3 Objetivo de un hacker.
    - 1.4 Perfil de un hacker.
    - 1.5 Motivaciones.
    - 1.6 Escalas de grises.
2. Contraseñas.
    - 2.1 ¿Qué es una contraseña?
    - 2.2 Objetivo de una contraseña.
    - 2.3 ¿Cómo generar contraseñas seguras?
    - 2.4 Errores más comunes al crear una contraseña.
    - 2.5 Generadores de contraseñas.
3. Criptología.
    - 3.1 ¿Qué es la criptología?
    - 3.2 Objetivos de la criptología.
    - 3.3 Usos de la criptografía.
    - 3.4 Tipos de algoritmos.
    - 3.5 Ataques.
4. Aplicaciones criptográficas.
    - 4.1 Navegación en internet.
    - 4.2 Firma electrónica.
    - 4.3 Funciones de hash.
    - 4.4 Firma digital.
    - 4.5 HMAC.
    - 4.6 PKI.
    - 4.7 Certificado digital x.509.
    - 4.8 Autoridad de Registro (RA).
    - 4.9 Autoridad de Certificación (CA).
    - 4.10 Revocación de certificados.
    - 4.11 Distribución de certificados.
5. Control de acceso.
    - 5.1 ¿Qué es el control de acceso?
    - 5.2 Identificación.
    - 5.3 Autenticación.
    - 5.4 Autorización.
    - 5.5 Tipos de control de acceso.
    - 5.6 Amenazas.

MÓDULOS

5.7 Utilización de Passports.
5.8 Sistemas Biométricos.
5.9 Single Sign On (SSO).
5.10 Kerberos y otros protocolos SSO.
5.11 Modelos de control de acceso.
5.12 Administración de control de acceso.
5.13 Monitoreo, Auditoria y Logs.
5.14 Sistemas de Detección de Intrusos (IDS e IPS).

6. Técnicas comunes de ataques.
   6.1 Envenenamiento de la red: poisoning.
   6.2 Análisis de protocolos: sniffing.
   6.3 Impersonalización: spoofing.
   6.4 Robo de sesiones: hijacking.
   6.5 Fuerza bruta.
   6.6 Denegación de servicio.
7. Vulnerabilidades.
   7.1 Pruebas de Desbordamiento de Buffer (Overflow).
   7.2 Pruebas de Resiliencia de la Arquitectura.
   7.3 Pruebas de Denegación de Servicios (DDOS).
   7.4 Pruebas de Inyección de SQL (SQL Injection).
   7.5 Pruebas de Inyección de Sitio Cruzado (XSS).
   7.6 Pruebas de Inyección de HTML (HTML Injection).
   7.7 Pruebas de Inyección de Hoja de Estilo en Cascada (CSS Injection).
   7.8 Pruebas de Inyección de Código de Sitio con Flash (Cross site flashing).
   7.9 Pruebas de Secuestro de clic (Click jacking).
   7.10 Pruebas de Inclusión de Archivos.
   7.11 Pruebas de Validación de Canales Seguros (SSL/TLS).
   7.12 Pruebas de Información en Canales no Cifrados.
   7.13 Pruebas de Falsificación de Peticiones de Sitios Cruzados (CSRF).
   7.14 Pruebas de Búsqueda de Directorios Críticos.
   7.15 Pruebas de Debilidad en Usuari y Contraseñas.
   7.16 Pruebas de Reconocimiento Activo.
8. Vulnerabilidades en la programación.
   8.1 Programación segura.
   8.2 OWASP top 10.
9. Seguridad en las transacciones electrónicas.
   9.1 Robo de identidad.
   9.2 Seguridad personal online.
   9.3 PCI.
10. Ethical Hacking.
   10.1 Concepto de Hacking.
   10.2 Perfil de conocimientos.
   10.3 Códigos de Ética.
   10.4 Penetration Test y Ethical Hacking.
   10.5 Análisis de brecha de cumplimiento.
   10.6 Autotesteo y contratación.
   10.7 Clasificaciones.

Certificación a obtener (opcional): EXIN Fundamentos Cyber & IT Security o EC-COUNCIL Ethical Hacker Certification.

MÓDULOS

03 Ciberseguridad Táctica

1. Gobernanza y administración de riesgos.
   1.1 Definición de gobernanza.
   1.2 COBIT 5. Gobernanza y gestión.
2. Gestión de riesgos: modelos generales.
   2.1 La importancia de la medición del riesgo.
   2.2 Enfoques de gestión de riesgos que crean riesgos.
   2.3 El enfoque de las normas ISO 15408 e ISO 18045.
   2.4 El ciclo clásico de gestión Planear -Hacer – Verificar – Actuar.

04 Ciberseguridad Estratégica

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

Certificación a obtener (opcional): EXIN Fundamentos de Seguridad de la Información basado en ISO IEC 27001.

MÓDULOS

05 Ciberinteligencia

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

06 Ciberseguridad en la nube, internet de las cosas

1. Seguridad en la nube.
   - 1.1 ¿Qué es la nube?
   - 1.2 Conceptos de PaaS, SaaS, IaaS.
   - 1.3 Modelo de responsabilidad compartida en la nube.
   - 1.4 Proveedores de nube y niveles de seguridad.
2. Seguridad en Internet de las cosas.
   - 2.1 ¿Qué es el internet de las cosas?
   - 2.2 Riesgos y amenazas en dispositivos de IoT.
   - 2.3 Reglas básicas de protección en IoT.
3. Seguridad en Entornos Industriales
   - 3.1 ¿Qué son los entornos industriales?
   - 3.2 Seguridad en los entornos industriales.
   - 3.3 Riesgos y Amenazas en entornos industriales.
   - 3.4 ¿Cómo protegerse en entornos industriales?
4. Advanced Persistent Security.
   - 4.1 Fases de un modelo de seguridad persistente.
   - 4.2 Modelo de protección.
   - 4.3 Modelo de Detección.
   - 4.4 Modelo de Reacción.
   - 4.5 Modelo de Implementación.
5. Análisis forense en la nube y aplicaciones móviles.
   - 5.1 ¿Qué es el análisis forense digital?
   - 5.2 Casos de uso del análisis forense.
   - 5.3 Estrategias de inspección forenses en la nube y aplicaciones móviles.
6. Microservicios.
   - 6.1. Arquitectura monolítica vs microservicios.
   - 6.2. Características de los microservicios y sus beneficios para su gestión en la nube.

Certificación a obtener (opcional): EXIN Cloud Computing Foundation.

MÓDULOS

07 Computación Forense

1. Etapas de un análisis forense.
    - 1.1 Definición de fases.
2. Adquisición de evidencias digitales.
    - 2.1 Definición de hash.
        - 2.1.1 ¿Por qué usar un valor hash?
        - 2.1.2 Función hash de archivos.
        - 2.1.3 Algoritmos válidos.
        - 2.1.4 Práctica de checksum.
    - 2.2 FTK Imager.
        - 2.2.1 Uso de FTK imager.
        - 2.2.2 Práctica de FTK imager.
3. Preservación de la integridad e identidad de las evidencias.
    - 3.1 Preservación física de la evidencia.
        - 3.1.1 Resguardo de discos duros.
        - 3.1.2 Bolsa antiestática.
        - 3.1.3 Cajas Pelican.
        - 3.1.4 Magnetismo.
    - 3.2 Bloqueadores.
        - 3.2.1 Tipos de bloqueadores.
        - 3.2.2 Ventajas de los bloqueadores.
    - 3.3 Herramientas de preservación.
4. Cadena de custodia de las evidencias.
    - 4.1 Cadena de custodia física.
    - 4.2 Metodologías de forenses informático.
    - 4.3 Estándares de forense informático.
    - 4.4 Implicaciones legales.
    - 4.5 Casos reales de violación de la cadena de custodia.
5. Análisis de las evidencias.
6. Laboratorio de análisis forense.
    - 6.1 Análisis de metadatos.
    - 6.2 Análisis de accesos al sistema operativo.
    - 6.3 Análisis de trafico de red.
    - 6.4 Análisis de navegadores.

Certificación a obtener (opcional): EC-COUNCIL - Computer Hacking Forensic Investigator.

MÓDULOS

08 Ciberdefensa

1. Ciberpatrullaje.
    1.1 Inspección de medidas de seguridad en el entorno.
    1.2 Que activos debo de proteger.
    1.3 Activos vulnerables dentro de la organización.
2. Estrategias de ciberdefensas.
    2.1 Modelos protección de la seguridad.
    2.2 ¿Cómo protegerme?
    2.3 Modelos de ciberdefensas.
3. Ciberdefensa personal.
    3.1 Esquemas de protección de seguridad informática personal.
    3.2 Contramedidas de protección.
    3.3 Software y herramientas de protección.
4. Ciberdefensa organizacional.
    4.1 ¿Cómo proteger mi organización?
    4.2 Modelos de protección en capas.
    4.3 Medidas para proteger los activos organizacionales.

09 Proyecto: Diseño de un Programa de Ciberseguridad

1. Diseño del Programa.
    1.1 Estrategias para diseñar un Programa de Ciberseguridad
    1.2 Aspectos a tener en cuenta en el diseño.
2. Modelado de amenazas.
    2.1 Estrategias para la detección de amenazas.
    2.2 Estrategia para modelar las amenazas.
3. Respuesta a incidentes.
    3.1 Categorización y priorización de incidentes.
    3.2 Estrategias de respuesta ante incidentes.
4. Reacción inmediata.
    4.1 Estrategias para la detección de ataques.
    4.2 Diseño.
5. Funciones y responsabilidades del CISO.
    5.1 Funciones del Director de Seguridad de la Información dentro de la organización.
    5.2 Responsabilidad del Director de Seguridad de la Información dentro de la organización.
    5.3 Funciones y responsabilidades del CISO dentro de un Plan de Ciberseguridad.
6. Casos de negocio.
    6.1 Análisis de casos de negocio en ciberseguridad.
    6.2 Detección de casos de negocios y aplicabilidad en ciberseguridad.

PROFESORES

Raymundo Adrián Sánchez Becerril

ESTUDIOS REALIZADOS

- Licenciatura en Tecnologías de la Información, en Universidad La Salle.

EXPERIENCIA LABORAL

- Su experiencia profesional se basa en actividades como Hacking Ético y Pentesting, Análisis Forense Digital, Planificación de la Continuidad del Negocio, Planificación y Recuperación de Desastres, Administración y Seguridad Informática en Sistemas GNU/Linux, UNIX y Windows, Seguridad en Redes y Telecomunicaciones y Programación ANSI "C", UNIX, GNU/Linux, Shell, Python y GOLang.
- Se ha desarrollado como docente especializado en Seguridad de la Información y Áreas Relacionadas Creación y Coordinación Académica de los Talleres de Seguridad Informática.

CERTIFICACIONES

- CCNA CISCO, CCNA SECURITY CISCO, CCNP CISCO, Relaciones Públicas, Redes Sociales y Manejo de Situaciones de Crisis (War-Room), e-Commerce, Sistema de InteligenciaComercial, ACE v7, C|EH - Certified Ethical Hacker v11, C|EH Master - Certified Ethical Hacker Master, Analysis of crimes and criminal behavior.

Carlos Anuar Canales Gómez

ESTUDIOS REALIZADOS

- Ingeniería en Comunicaciones y Electrónica, con especialidad en Comunicaciones, en Instituto Politécnico Nacional.

EXPERIENCIA LABORAL

- Cuenta con más de 11 años de experiencia en el sector privado como consultor independiente y encargado del Área de Ciberseguridad, realizando actividades como: establecimiento del NIST como los cimientos de ciberseguridad, recomendar un modelo de desarrollo seguro con base en OWASP, diseño e implementación de servicios especializados como: análisis de vulnerabilidades, pruebas de penetración, análisis forense, desarrollo seguro, respuesta a incidentes y consultoría en ciberseguridad.

CERTIFICACIONES

- Certified Ethical Hacking V10), CTIA Certified Threat Intelligence Analyst y, -ECIH v2 Certified Incident Handler.

Juan Francisco Padilla Suaste

ESTUDIOS REALIZADOS

- Lic. en Informática en Universidad de Negocios ISEC.

EXPERIENCIA LABORAL

- Más de 16 años en el sector público como Analista de ciberseguridad, Chief Technical Officer, Forensics Examiner & Ethical Hacker, Administrador de Servidor, Programador Informático, Soporte Técnico y Programación.

CERTIFICACIONES

- Certified Ethical Hacker (Practical), Computer Hacking Forensic Investigator, CIW Web Security Specialist, CIW Web Security Professional. Además, ha obtenido varios reconocimientos, algunos de estos son: Unix Badge / License number: PTLU1550 y White Badge / License number: PTLW1294.

Juan Gálvez Hernández

ESTUDIOS REALIZADOS

- Licenciado en Administración Industrial, en Instituto Politécnico Nacional.

EXPERIENCIA LABORAL

- Más de 15 años en el sector privado realizando actividades relacionadas con la Seguridad de la Información/Ciberseguridad, Continuidad de Negocio, Riesgos, Seguridad Física y Políticas y Procedimientos, Control Interno del Marco de Control Interno de Tecnologías de Información conforme a COBIT. También ha realizado actividades como Análisis de los Quebrantos Operacionales, Jurídicos y Tecnológicos para determinar causas que los originaron y sugerir controles para evitar la reincidencia de los eventos de riesgo. Ha sido Instructor CISA / CISM e ISO 27001 Fundamentos y Auditor Líder y Profesor Diplomado Ciberseguridad UVM.

CERTIFICACIONES

- Certified Information SystemAuditor (CISA), Fundamentos de ITIL V2, V3, V4, COBIT 4.1, Instructor ISO 27001 y, Auditor Líder ISO 27001.

PROFESORES

Hans Von Herrera Ortega

ESTUDIOS REALIZADOS

- Licenciado en Ingeniería en Computación, en Universidad del Valle de México UVM.

EXPERIENCIA LABORAL

- Cuenta con experiencia en el sector público y privado como consultor e instructor de Ciberseguridad en Ethical Hacking e Informática Forense. Se ha encargado del mantenimiento de los Sistemas Informáticos del 9-1-1 Nacional. Se ha desempeñado como administrador de contrato de licitaciones y procesos administrativos del Área de Informática y, como encargado de la continuidad y disponibilidad de los servicios informáticos.

- Es creador de contenidos e instructor de los talleres del Ciclo de Vida de Desarrollo Seguro en la Secretaría de Relaciones Exteriores y ha impartido un taller de repaso para el examen EGEL de Desarrollo de Software en UVM Campus San Ángel.

CERTIFICACIONES

- Certified Ethical Hacker, Computer Hacking Forensic Investigator y OSSTM.

Lázaro Santiago Cruz

ESTUDIOS REALIZADOS

- Licenciatura en Ingeniería en Computación, en la UNAM.

EXPERIENCIA LABORAL

- Cuenta con las de 11 años realizando actividades como, Análisis del Tráfico en la Red Interna para capturar usuarios y contraseñas, Administración de Infraestructura y Herramientas de seguridad y Administración de Red Interna.
- Ha participado en eventos como: Ponente, 4ta semana nacional de ciberseguridad y Miembro del Comité Organizador de la 7ma, 8va y 9na Semana de la Seguridad.

CERTIFICACIONES

- OSSTMM OPSA ISECOM, Mile2 CPTE, EXIN Ethical Hacking, 70- 346 Managing Office 365 Identities and Requirements, 70-347 Enabling Office 365 Services, MCSA Office 365 2015, Security Appliance(ESA), Web Security Appliance(WSA), Web Security(CWS), IMSVA – Trend Micro y, PaloAlto ACE 2014.

Rubén Cabanzo Becerril

ESTUDIOS REALIZADOS

- Bachelor's Degree in Information Technology, in ISEC University.
- Postgraduate Specialist in Networking, in UNITEC.

EXPERIENCIA LABORAL

- Responsible of the assessments about Information Security: Identity and Access Management, Information Protection, Privacy, Security Incident Management, Physical Security, Asset Management, Security Engineering and Architecture, Security Governance, Security Operations.

CERTIFICACIONES

- ITIL-F v2 (ITIL Foundations) /// ISEB, CSwT (Certified in Software Testing) /// ISEB, CSSGB (Certified Six Sigma: Green Belt) /// ING Mexico y BS-7799 LA (Information Security Management Systems Lead Auditor ISO 27001) /// BSI.

Beneficios de estudiar un diplomado

Temas actualizados y de vanguardia

Con gran capacidad de actualización y reinvención al ser de una duración más corta que otros posgrados, un diplomado te ofrece una capacitación enfocada en temas relevantes y de alta demanda para el mercado laboral.

Capitaliza lo aprendido

El alto enfoque práctico y estratégico de un Diplomado hace que cada módulo sea aplicable desde el primer día 1 en tus actividades profesionales y desarrollo personal.

Mejora tus oportunidades laborales

Enriquece tu CV especializándote y posiciónate como el mejor candidato.

Networking

No solo compartirás salón de clases con buenos compañeros, también con excelentes profesionistas con los que podrás compartir puntos de vista, tips e incluso oportunidades de negocio.

Profesores con más 15 años en experiencia profesional

Toma clases de la mano de expertos en su disciplina con amplia experiencia compartiendo su conocimiento y trabajando en las mejores empresas nacionales e internacionales.

Duración

La duración promedio de un Diplomado o Certificación es de 4 a 6 meses, así podrás aplicar lo aprendido muy rápidamente y seguir creciendo profesionalmente.

Diploma

Todos nuestros Diplomados y Certificaciones tienen validez curricular.

Más beneficios >

Beneficios de la modalidad aula virtual

- Sesiones en tiempos real:

  Todas las clases son en vivo, así podrás tener una interacción con los profesores y alumnos más dinámica y enriquecedora.

- Sesiones grabadas y en tiempo real

  Estudia a tu ritmo, puedes consultar todas las sesiones en el horario que más te convenga.

- Contenido siempre disponible:

  Podrás consultar y / o descargar el material desde plataforma en cualquier momento del día.
  Además, nuestra plataforma es multidispositivo, podrás estudiar en cualquier computadora de escritorio, laptop, tableta o Smartphone.

- Soporte técnico:

  El equipo de soporte técnico estará tu disposición en todo momento para ayudarte a resolver cualquier situación.

- Asesoría y acompañamiento:

  Cuentas con un tutor a través de la plataforma en enlaces en vivo, chat o Whatsapp a distancia en tiempo real, para resolver tus dudas y dar retroalimentación.

- Diploma Virtual:

  Al finalizar tu diplomado te entregaremos un documento digital con validez y valor curricular.

Educación CONTINUA | UVM

uvm.mx