CETYS UNIVERSIDAD | Educación Continua

CAMPUS MEXICALI

Diplomado en Ciberseguridad

MODALIDAD HÍBRIDA

www.cetys.mx/educon

CAMPUS MEXICALI

Diplomado en Ciberseguridad

Objetivo

Curso de ciberseguridad de nivel intermedio a avanzado, cubriendo temas de seguridad informática, seguridad operacional y seguridad de la información, reforzando los aspectos teóricos pertinentes y su aplicación práctica en un entorno organizacional.

Dirigido a

Orientado al profesional de tecnologías de la información, seguridad industrial, encargado de área que resguarde o procese información sensible y egresados de programas STEM.

Contenido

Módulo I. Introducción a la ciberseguridad

1.1. La naturaleza insegura de la tecnología
1.2. Enfoque de sistemas
1.3. Arquitectura de computadoras
1.4. Seguridad en redes de cómputo
1.5. Seguridad de la información
1.6. Ciberseguridad personal y familiar
1.7. Ciberseguridad organizacional
1.8. Seguridad en los Sistemas de Control Industrial (ICS)
1.9. Taller: Seguridad de los sistemas operativos
1.10. Taller: Análisis de tráfico con Wireshark

Módulo II. Vulnerabilidades y mecanismos de ataque

2.1. Hackers y otros actores
2.2. Vulnerabilidades en hardware y software
2.3. El entorno físico
2.4. Cadenas de suministro
2.5. Gestión de vulnerabilidades
2.6. Introducción al ciber riesgo humano
2.7. Explotación
2.8. Malware
2.9. Advanced Persistent Threats (APT)
2.10. Caso de estudio: Log4j
2.11. Taller: Escaneo de vulnerabilidades
2.12. Taller: Pentest de una aplicación web con OWASP ZAP
2.13. Caso de estudio o taller: Simulación de Ransomware

Módulo III. Gestión de riesgos y respuesta a incidentes

3.1. Valoración del impacto de los riesgos de ciberseguridad
3.2. Afectación en la seguridad de la información
3.3. Integrando mecanismos (controles) de mitigación de riesgos
3.4. El plan de respuesta a incidentes
3.5. Investigación post evento (forensics)
3.6. Taller: Elaboración de un atlas de riesgos cibernéticos para su organización

Módulo IV. Ciber riesgo humano

4.1. Protección de la información
4.2. Cuidado de las credenciales de acceso
4.3. Navegación
4.4. Correo
4.5. Acceso vía redes públicas
4.6. Ingeniería social
4.7. Consideraciones sobre el uso de móviles
4.8. BYOD
4.9. Dispositivos móviles
4.10. Hablando con los empleados sobre ciberseguridad
4.11. Caso de estudio: MGM Resorts
4.12. Taller: Instalar herramientas de detección de URLs malignos en browsers
4.13. Taller: Herramienta de campañas phishing

Módulo V. Normatividad y marcos de referencia

5.1. Tópicos clave de derecho informático
5.2. Marco legal mexicano
5.3. Leyes y regulaciones internacionales
5.4. Marcos de referencia
5.5. Delitos cibernéticos
5.6. Prácticas básicas en el dominio tecnológico
5.7. Peritaje informático e informática forense
5.8. Estudio de caso: Firma electrónica avanzada y tribunal digital en el PJ – México
5.9. Práctica: Identificar los apartados del marco de referencia elegido y los controles definidos en el módulo 3

Módulo VI. Prácticas de prevención y respuesta

6.1. Gobernanza
6.2. Protecciones físicas
6.3. Mantenimiento de Inventarios, CMDB, tickets
6.4. Control del acceso y protección de identidad
6.5. Protección de las zonas de seguridad de red
6.6. Protección contra la exfiltración de datos (DLP)
6.7. Plan de respaldos y recuperación
6.8. Análisis de logs, SIEM, SOAR, OSINT, etc.
6.9. Threat Hunting
6.10. Taller: Reglas de firewall
6.11. Tecnologías móviles
6.12. Acceso remoto y teletrabajo
6.13. Protección de las aplicaciones
6.14. Desarrollo seguro de aplicaciones
6.15. Concientización y capacitación a usuarios
6.16. Caso de estudio o taller: Simulación Phishing

Módulo VII. Ciberseguridad en sistemas de control industrial

7.1. Zonas de seguridad
7.2. Seguridad física
7.3. Tráfico de planta vs. Tráfico de T. I.
7.4. Vulnerabilidades conocidas
7.5. Análisis de logs, SIEM
7.6. Estándar ISA/IEC-62443
7.7. LAB: aplicación de zonas de seguridad en una red OT

Módulo VIII. Ciberseguridad e Inteligencia Artificial

8.1. Aprovechando la IA en CS
8.2. Riesgos de la IA a la ciberseguridad
8.3. Riesgos hacia la IA
8.4. Riesgos de privacidad
8.5. OWASP Top 10 for LLM Applications
8.6. MITRE ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)
8.7. Taller: Prompt injection

Módulo IX. Cíber espionaje, inteligencia y ataques de nación

9.1. Mecanismos de ciber espionaje
9.2. Grupos auspiciados por gobiernos (nation – state)
9.3. Desinformación y orientación de opinión
9.4. Estudio de caso: Stuxnet
9.5. Estudio de caso: Petya, WannaCry, NotPetya
9.6. Estudio de caso: Salt Typhoon

Módulo X. Diseñando un programa de Ciberseguridad para la organización

10.1. Evaluar la situación actual
10.2. Formalización
10.3. Riesgos, Respuesta, Recuperación
10.4. Educación a los usuarios
10.5. Selección de herramientas
10.6. Apoyo de terceros y proveedores
10.7. Estructurar líneas de acción y tareas específicas
10.8. Revisión y actualización continua

Requisitos de Ingreso

No se requieren conocimientos previos, cualquier interesado en ingresar puede hacerlo.

- La fecha de inicio está sujeta a cambios sin previo aviso.
- La apertura e inicio del programa está sujeta a reunir el grupo mínimo de 12 participantes.
- Capacidad máxima del grupo: 21 participantes

Requisitos de Acreditación

Haber cumplido con el 80% de asistencia.

Detalles del Programa

Fecha de Inicio: 03 de septiembre de 2025
Fecha de Fin: 28 de enero de 2026
Horario: Miércoles de 6pm a 10pm
Duración: 76 horas
Inversión: $27,507 MXN

Promociones*

Inscripción Anticipada: $1,500 MXN de descuento
Egresado: 10% de descuento
Grupo de 2 personas:** 10% de descuento
Grupo de 3 a 4 personas:** 15% de descuento
Grupo de 5 personas o más:** 20% de descuento

***** no acumulables
****** grupos pertenecientes a la misma empresa

Formas de Pago

Depósito Bancario:
Realizarlo en BBVA Bancomer a nombre de Instituto Educativo del Noroeste A.C. en la cuenta 0443028674

Transferencia Bancaria:
BBVA Bancomer
012020004430286743

CAMPUS MEXICALI

Diplomado en Ciberseguridad

Mayores Informes

Promotor: Lic. Adriana Osornio

Tel: (686) 149 6462

Email: adriana.osornio@cetys.mx

CETYS UNIVERSIDAD | Educación Continua