Tecnológico de Monterrey | Educación Continua

THE LEARNING GATE

Certificación

CYBERSECURITY ANALYST

Desarrolla una visión completa de la seguridad informática: gestión de riesgos, protección y operación eficiente.

¿Qué son las **certificaciones?**

En la actualidad, las empresas le dan mayor valor a las competencias, habilidades y resultados de aprendizaje que derivan de actividades no necesariamente ligadas con un título profesional o grado.

Ante este escenario mundial, el Tecnológico de Monterrey ha creado **CERTIFICACIONES** accesibles, flexibles y eficaces que te permiten ser proactivo en la elección de habilidades y conocimientos que necesitas acreditar y comprobar.

Los reconocimientos se te otorgan al concluir satisfactoriamente un programa, demostrando que has obtenido los conocimientos, pero sobre todo, que puedes aplicarlos en los ámbitos laboral y/o personal, a través de un proyecto real.

Beneficios:

- Sirven para demostrar a potenciales empleadores tus conocimientos, competencias, habilidades y resultados de aprendizaje.
- Tú defines el perfil de tu proyecto para certificarte, en función de las competencias que deseas aplicar y de la organización en la que colaboras.
- Son independientes y complementarias a los títulos formales de grados académicos del Tecnológico de Monterrey.
- Son acumulables, ya que pueden sumarse para obtener una certificación de mayor especialización, o pueden otorgar créditos académicos para acreditar materias de Posgrado.
- Al concluir cada una, recibirás una insignia digital, con autenticación Blockchain, prácticamente infalsificable, que podrás compartir en redes sociales y medios digitales.

Objetivo de la **Certificación Cybersecurity Analyst**

Reconocer a los participantes que han contribuido a estructurar una visión holística de las responsabilidades en seguridad de la información. Esto abarca áreas clave como la gestión de seguridad informática, la gestión de riesgos informáticos, y la implementación y operación de medidas de seguridad, todo con el objetivo de garantizar que la infraestructura de la organización sea sólida y apoye la continuidad del negocio.

¿Qué hace único a **este programa?**

Con esta certificación podrás demostrar las competencias de:

- Information Security Management
- IT Risk Management
- Information Security Development
- Information Security Operation

Dato sobre retorno de inversión

El estudio más reciente de “Panorama de Amenazas para América Latina” revela que, de junio de 2022 a julio de 2023, se registraron 286 millones de bloqueos de intentos de phishing, lo que representa un aumento del **617%** en comparación con los 12 meses anteriores y un promedio de 544 ataques por minuto. Los sectores de gobierno y finanzas han sido los más afectados por tales ataques, al igual que los internautas*.

**Estudio “Panorama de Amenazas para América Latina” elaborado por la empresa multinacional de ciberseguridad y antivirus, Kaspersky.*

Objetivo

Con este programa podrás desarrollar una comprensión integral de las diversas responsabilidades asociadas con la seguridad de la información, incluyendo aspectos como la seguridad informática, la gestión de riesgos informáticos, la implementación y operación efectiva de la seguridad informática.

Dirigido a

Este programa es ideal para ingenieros y profesionales con afinidad por los sistemas computacionales, que cuenten con conocimientos en procesos y soporte técnico, y al menos un año de experiencia en el campo.

The Learning Gate

Modelo Flex

Para ti, que te gusta aprender a tu propio ritmo y tomar tus propias decisiones.

Sesión de onboarding personal.

Comienza y termina tu Certificación de acuerdo con tu ritmo y tu propia agenda.

Elige el Certificado de Competencias o Microcertificado que se adapte mejor a tus intereses.

Mantén completa flexibilidad en tu aprendizaje.

CERTIFICACIÓN

Cybersecurity Analyst

150 horas | 4 microcertificados | 11 módulos

Onboarding: Inicia tu Certificación

MICROCERTIFICADOS	Information Security Management	IT Risk Management	Information Security Development	Information Security Operation
MÓDULOS	Threats, Attacks and Vulnerabilities	Risk Mitigation Controls	Security Architecture	Security Operations and Monitoring
	Vulnerability Assessment and Penetration Testing Methods and Tools	Applying Appropriate Risk Strategies	Security Architecture Implementation Model	Incident Response and Forensics Procedures
	Compliance and Assessment	Business Continuity and Disaster Recovery Concepts		
	Governance, Compliance Frameworks and Legal Considerations			

Temario

Onboarding: Inicia tu Certificación

Identificarás el ecosistema de aprendizaje de la plataforma The Learning Gate con la finalidad de sacar el mayor provecho, alcanzando el éxito en tu nuevo viaje de aprendizaje.

1. Bienvenida
2. Tu Certificación
3. Pilares para el éxito
4. Navegación TLG
5. Comunidad

Microcertificado

Information Security Management

Módulo 1 | Threats, Attacks and Vulnerabilities

10 horas

Te familiarizarás con los diversos tipos de amenazas, ataques y vulnerabilidades que pueden comprometer una arquitectura de TI.

1. Conceptos generales
2. Amenazas y vulnerabilidades
3. Ataques y controles
4. Tipos y fuentes de inteligencia
5. Contensión

Módulo 2 | Vulnerability Assessment and Penetration Testing Methods and Tools

10 horas

Adquirirás conocimiento sobre los métodos y herramientas especializadas para llevar a cabo análisis de vulnerabilidades y ejecutar pruebas de penetración eficaces.

1. Importancia de la exploración de vulnerabilidad
2. Security Content Automation Protocol (SCAP)
3. Fuentes de información
4. Pruebas de penetración
5. Herramientas de seguridad

Módulo 3 | Compliance and Assessment

10 horas

Aprenderás a verificar el cumplimiento de los controles de seguridad establecidos en la arquitectura de TI de tu organización.

1. Importancia de la privacidad y protección dentro del programa de seguridad e información y cumplimiento
2. Leyes y regulaciones en protección de datos
3. Riesgos de la información y controles de protección
4. Revisión y selección frameworks
5. Políticas, procedimientos y controles

Módulo 4 | Governance, Compliance Frameworks and Legal Considerations

10 horas

Descubrirás cómo implementar un gobierno eficaz de ciberseguridad, familiarizándote con los marcos de referencia para el cumplimiento y las consideraciones legales pertinentes en tu organización.

1. Security controls
2. Regulations, standards frameworks and organizational policies
3. Privacy
4. Security concerns associated with integrating diverse industries
5. Understanding regulations, accreditations, standards and legal considerations

Microcertificado

IT Risk Management

Módulo 5 | Risk Mitigation Controls

10 horas

Te capacitarás en el uso de controles efectivos para la mitigación de riesgos de ciberseguridad.

1. Introducción al desarrollo seguro de sistemas
2. Contexto de vulnerabilidades en sistemas
3. Principales vectores de ataque en sistemas
4. Cacería de amenazas
5. Aplicación de controles para la mitigación de riesgos en sistemas

Módulo 6 | Applying Appropriate Risk Strategies

10 horas

Desarrollarás una comprensión completa de la estrategia necesaria para mitigar eficazmente los riesgos asociados con la ciberseguridad.

1. Apreciación de riesgos
2. Técnicas de gestión de riesgos
3. Ciclo de vida de la gestión de riesgos
4. Monitoreo de riesgos
5. Políticas de seguridad, buenas prácticas y problemáticas

Módulo 7 | Business Continuity and Disaster Recovery Concepts

10 horas

Adquirirás conocimientos sobre los aspectos clave para garantizar la continuidad del negocio y la elaboración de planes de recuperación ante desastres.

1. Introducción a planes de recuperación del desastre y continuidad del negocio
2. Prácticas profesionales para la gestión de la continuidad del negocio (BCM)
3. Análisis de impacto al negocio (BIA) y estrategias de continuidad del negocio
4. Pruebas, programas de concienciación y entrenamiento
5. Manejo de crisis

Microcertificado

Information Security Development

Módulo 8 | Security Architecture

10 horas

Identificarás los controles esenciales que debe incorporar la arquitectura de seguridad en una infraestructura de TI, con el fin de minimizar los riesgos de seguridad de manera efectiva.

1. Enterprise security architecture
2. Secure application development & deployment
3. Advanced network design
4. Network management and monitoring tools
5. Cybersecurity resilience

Módulo 9 | Security Architecture Implementation Model

10 horas

Explorarás a detalle cómo se implementa la arquitectura de seguridad en la infraestructura de TI, lo que te permitirá comprender su despliegue y funcionamiento efectivo.

1. Investigación de soluciones tecnológicas
2. Selección de soluciones tecnológicas
3. Diseño de la arquitectura de seguridad
4. Implementación de la arquitectura de seguridad
5. Mantenimiento de la arquitectura de seguridad

Ⅳ Microcertificado

Information Security Operation

Módulo 10 | Security Operations and Monitoring

10 horas

Obtendrás una comprensión integral de todos los elementos involucrados en la operación y el monitoreo efectivo de la seguridad informática.

1. Identificación de los sistemas de operación y monitoreo de la organización
2. Herramientas para el monitoreo y la operación de la seguridad de la organización
3. Implementación de operación y monitoreo
4. Automatización de la operación y monitoreo
5. Operación y monitoreo de la seguridad informática

Módulo 11 | Incident Response and Forensics Procedures

10 horas

Te capacitarás en la implementación de mecanismos robustos para responder a incidentes y llevar a cabo procedimientos forenses de manera efectiva.

1. Introduction to incident response and digital forensic
2. Incident handling and response process: part 1
3. Incident handling and response process: part 2
4. Digital forensic process: part 1
5. Digital forensic process: part 2

Pondrás en práctica los conocimientos y competencias obtenidos a través del desarrollo de un **Proyecto Integrador de Dominio Autónomo (PIDA)**, que te permitirá obtener la Certificación.

Certificación

150
Horas

110
Horas
Certificado de Competencias

+

40
Horas
Proyecto Integrador de Dominio Autónomo (PIDA)

¿Cómo demostrarás **tu aprendizaje?**

MODELO PIDA

(Proyecto Integrador de Dominio Autónomo)

Al terminar el **Certificado de Competencias,** obtendrás una insignia **Oro.**

Al terminar la **Certificación,** obtendrás una insignia **Diamante.**

Estas insignias están respaldadas por **tecnología Blockchain**, lo que fortalecerá tu currículum digital y te permitirá demostrar tus habilidades de manera rápida y segura en plataformas digitales.

¿Por qué somos el mejor aliado para tu desarrollo profesional?

- Mejor universidad privada de México, QS University Rankings 2024.
- Top 4 de las mejores universidades de Latinoamérica, según QS University Rankings: Latin America 2024.
- Universidad #2 de las mejores universidades de Latinoamérica, según QS World University Rankings: Latin America and The Caribbean 2024.
- Universidad #5 en México en la opinión de los empleadores QS Graduate Employability Rankings 2024.
- Top 4 de las mejores universidades de Latinoamérica, según Times Higher Education's (THE) Latin America University Rankings 2023.

Tecnológico de Monterrey | Educación Continua

THE LEARNING GATE

Descubre más sobre tu programa

www.maestriasydiplomados.tec.mx

Haz contacto

800 800 2114 | educacion.continua@itesm.mx