

PROGRAMA DE FORMACIÓN GREMIAL DESARROLLO SEGURO DE APLICACIONES

OBJETIVOS

- ▶ Este programa de formación tiene como objetivo homologar los conceptos y la visión respecto a los riesgos y mejores prácticas en el diseño y programación de aplicaciones (incluyendo aplicaciones móviles) dentro de las instituciones financieras, buscando que estén alineados a todos los requerimientos regulatorios.
- ▶ Dar a conocer las diversas técnicas, estándares y mejores prácticas de desarrollo seguro, que ayuden a reducir riesgos de incidentes por deficiencias o vulnerabilidades en códigos y aplicaciones

Los contenidos de este programa fueron elaborados por el Tecnológico de Monterrey. Asimismo, fueron revisados y aprobados por la Comisión de Ciberseguridad y la ABM.

Dirigido, entre otros, a:

- Diseño y desarrollo de sistemas / aplicaciones
- Áreas de infraestructura tecnológica
- Áreas de desarrollo y pruebas (QA),
- Personal de infraestructura y telecomunicaciones
- Personal de soporte a la producción

Duración del curso: 24 hrs.

TEMARIO

I. Seguridad en el ciclo de vida de desarrollo de software

El ciclo de vida de desarrollo de software.

- Referencia PCI SCL (Ciclo de vida de software).

Entendiendo la seguridad en aplicaciones, amenazas y ataques.

- PCI DSS, mantener el apego a mejores prácticas de desarrollo seguro.
 - Recopilación de requerimientos de seguridad.
 - Diseño y arquitectura de aplicaciones seguras.
 - Controles en aplicaciones en producción.
 - Controles en aplicaciones en desarrollo.
 - Estrategias para el desarrollo de aplicaciones.
 - Metodología de seguridad para el desarrollo de aplicaciones.
- Metodologías recomendadas por PCI DSS.
 - El rol del especialista de seguridad en el desarrollo de aplicaciones.
 - Determinación del nivel de riesgo aceptable en las aplicaciones.
 - Administración de cambios.
 - Administración de configuraciones.

3 hrs.



II. Fundamentos de la programación segura

Modelo de seguridad.

Modelado de amenazas.

Escenarios de ataque.

Prácticas de codificación segura (lenguaje Java):

- Validación de entradas
- Autenticación y autorización
- Materiales y herramientas criptográficas
- Administración de sesiones
- Manejo de errores.

Prácticas de uso seguro de bases de datos:

- Confidencialidad
- Integridad
- Disponibilidad

Pruebas estáticas y dinámicas de aplicaciones seguras (SAST & DAST)

Referencia PCI DSS Versión 4.0

5 hrs.



III. Seguridad en aplicaciones Web

Introducción a desarrollo de aplicaciones WEB

Seguridad en aplicaciones Web.

OWASP Top 10.

Ataques de autenticación y autorización.

Ataques de administración de sesiones.

Ataques lógicos de aplicaciones.

Validación de datos.

Ataques AJAX.

Revisión de código y pruebas de seguridad de aplicaciones web.

PCI DSS prueba de desarrollo seguro (escaneo).

3 hrs.



IV. Desarrollo seguro de Aplicaciones Móviles

Introducción a las aplicaciones móviles.

Amenazas y ataques de aplicaciones móviles.

El estándar de seguridad de aplicaciones móviles de la OWASP.

Requerimientos de arquitectura, diseño y modelado de amenazas.

Requerimientos de almacenamiento de datos y privacidad.

Requerimientos criptográficos.

Requerimientos de autenticación y administración de sesiones.

Requerimiento de redes y comunicaciones.

Requerimientos de arquitectura y

inicial. Requerimientos de interacción ambiental.

Requerimientos Calidad del código y requerimiento de configuración

Requerimientos de resiliencia contra ataques de ingeniería inversa.

Pruebas de aplicaciones móviles.

5 hrs.



V. Desarrollo seguro de APIs

4 hrs.



API REST y API SOAP.
Amenazas y ataques en el uso de APIs.
OWASP API Security Top 10.
Transferencia de datos a través de APIs.
Cifrado y firma de datos.
Autenticación y autorización.
Protocolo OAuth.
Herramientas de seguridad para APIs.
API Gateways.

4 hrs.



VI. DevSecOps-Desarrollo Seguridad y Operaciones

Introducción a DevOps
Conceptos base
Everything as Code
Infrastructure as Code
Integrando seguridad en CI/CD (Continuous Integration and Delivery)
Administración de vulnerabilidades en DevOps
Administración de artefactos
Administración de secretos usando Vault , Jenkins y Docker Secrets
Herramientas básicas
Seguridad en Contenedores
Seguridad en Máquinas Virtuales

***Coadyuva en el cumplimiento de los requisitos, en materia de capacitación, para la Certificación o Revalidación de la Certificación en PCI DSS.**

PORTAFOLIO DE SERVICIOS

- ▶ Curso con ejemplos prácticos y evaluaciones formativas.
- ▶ Gestión administrativa: registro de participantes, notificación de usuario y contraseña, seguimiento de avances y resultados por participante, reportes, etc.
- ▶ Emisión y administración de constancias electrónicas de acreditación de los participantes.
- ▶ Asesoría y seguimiento a través del Centro de Atención a Usuarios (CAU) de lunes a viernes de 9:00 a 18:00 horas.
- ▶ Minería de información.

ELEMENTOS DEL MODELO DE APRENDIZAJE



RAPID LEARNING



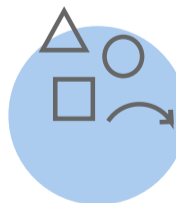
STORYTELLING



ENGAGEMENT LEARNING



VISUAL THINKING



GAMIFICACIÓN

CONTACTANOS:



Paola Navarro Ferrer
Tel. 55 5722-4358
educacioncontinua@abm.org.mx



Karen Guzmán Meza
Tel. 55 5722-4392
kgzman@abm.org.mx



Ana Lilia Ortega Angeles
Tel. 55 5722-4388
aortega@abm.org.mx