ASOCIACIÓN DE BANCOS DE MÉXICO

EDUCACIÓN CONTINUA ABM

PROGRAMA DE FORMACIÓN GREMIAL
DESARROLLO SEGURO DE APLICACIONES

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

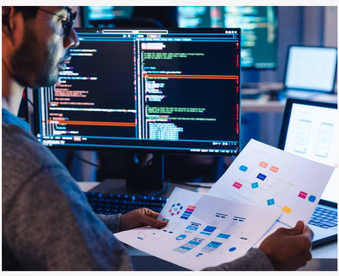
Objetivos:

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.

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



Temario

I. SEGURIDAD EN EL CICLO DE VIDA DE DESARROLLO DE SOFTWARE

Duración aproximada: 3 horas.

1.1 El ciclo de vida de desarrollo de software.
1.1.1 Referencia PCI SCI. (Ciclo de vida de software).Asimismo, fueron revisados y aprobados por la Comisión de Ciberseguridad de la ABM.
1.2 Entendiendo la seguridad en aplicaciones, amenazas y ataques.
1.2.1 **PCI DSS, mantener el apego a mejores prácticas de desarrollo**
1.2.1.1 Diseño y arquitectura de aplicaciones seguras.
1.2.1.2 Controles en aplicaciones en producción.
1.2.1.3 Controles en aplicaciones en desarrollo.
1.2.1.4 Estrategias para el desarrollo de aplicaciones.
1.2.1.5 Metodología de seguridad para el desarrollo de aplicaciones.
1.2.2 **Metologías recomendadas por PCI DSS.**
1.2.2.1 El rol del especialista de seguridad en el desarrollo de aplicaciones. Determinación del nivel de riesgo aceptable en las aplicaciones.
1.2.2.2 Administración de cambios.
1.2.2.3 Administración de configuraciones.

II. FUNDAMENTOS DE LA PROGRAMACIÓN SEGURA

Duración aproximada: 5 horas.

2.1 Modelo de seguridad.
2.2 Modelado de amenazas.
2.3 Escenarios de ataque.
2.4 Prácticas de codificación segura (lenguaje Java):
2.4.1 Validación de entradas
2.4.2 Autenticación y autorización
2.4.3 Materiales y herramientas criptográficas
2.4.4 Administración de sesiones
2.4.5 Manejo de errores.
2.5 Prácticas de uso seguro de bases de datos:
2.5.1 Confidencialidad
2.5.2 Integridad
2.5.3 Disponibilidad
2.6 Pruebas estáticas y dinámicas de aplicaciones seguras (SAST &
2.6.1 Referencia PCI DSS Versión 4.0

III. SEGURIDAD EN APLICACIONES WEB

Duración aproximada: 3 horas.

3.1 Introducción a desarrollo de aplicaciones Web
3.2 Seguridad en aplicaciones Web.
3.3 OWASP Top 10.
3.4 Ataques de autenticación y autorización.
3.5 Ataques de administración de sesiones.
3.6 Ataques lógica de aplicaciones.
3.7 Validación de datos.
3.8 Ataques AJAX.
3.9 Revisión de código y pruebas de seguridad de aplicaciones Web
3.10 PCI DSS prueba de desarrollo seguro (escaneo).

IV. DESARROLLO SEGURO DE APLICACIONES MÓVILES

Duración aproximada: 5 horas.

4.1 Introducción a las aplicaciones móviles.
4.2 Amenazas y ataques de aplicaciones móviles
4.3 El estándar de seguridad de aplicaciones móviles de la OWASP.
4.3.1 Requerimientos de arquitectura, diseño y modelado de amenazas.
4.3.2 Requerimientos de almacenamiento de datos y privacidad.
4.3.3 Requerimientos criptográficos.
4.3.4 Requerimientos de autenticación y administración de sesiones.
4.3.5 Requerimientos de redes y comunicaciones.
4.3.6 Requerimientos de arquitectura y inicial.
4.3.7 Requerimientos de interacción ambiental.
4.3.8 Requerimientos Calidad del código y requerimiento de configuración.
4.4 Requerimientos de resiliencia contra ataques de ingeniería inversa.
4.5 Pruebas de aplicaciones móviles.

V. DESARROLLO SEGURO DE APIS

Duración aproximada: 4 horas.

5.1 API REST y APLI SOAP.
5.2 Amenazas y ataques en el uso de APIs.
5.3 OWASP API Security Top 10.
5.4 Transferencia de datos a través de APIs.
5.4.1 Cifrado y firma de datos.
5.5 Autenticación y autorización.
5.5.1 Protocolo OAuth.
5.6 Herramientas de seguridad de APIs.
5.6.1 API Gateways.

VI. DevSecOps-DESARROLLO SEGURIDAD Y OPERACIONES

Duración aproximada: 4 horas.

6.1 Introducción de DevOps.
6.2 Conceptos base.
6.3 Everything as Code.
6.4 Infrastructure as Code.
6.5 Integrando seguridad en CI/CD (Continuous Integration
6.6 Administración de vulnerabilidades en DevOps.
6.7 Administración de artefactos.
6.8 Administración de secretos usando Vault, Jenkins y Dockers Secrets
6.9 Herramientas básicas.
6.10 Seguridad de Contenedores.
6.11 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, aplicaciones por módulo y evaluación final.
- Gestión administrativa: registro de participantes, notificación de usuarios y contraseña, seguimiento de avances y resultados por participante, reportes, etc.
- Emisión y administración de constancias electrónicas de acreditación de los participantes.
- Minería de información.
- Asesoría y seguimiento a través del Centro de Atención a Usuarios

Nueva modalidad adaptativa

Al inicio de cada módulo, tendrás la oportunidad de presentar una evaluación diagnóstica que te permitirá exentar los temas que ya conozcas, para que solo tomes aquellos que necesites reforzar, lo cual redunda en un menor tiempo de navegación y una mejor experiencia.

Elementos del modelo de aprendizaje

RAPID LEARNING

VISUAL THINKING

STORYTELLING

ENGAGEMENT LEARNING

GAMIFICACIÓN

Alan Correa Rosales
Tel. 55 5722-4389
acorrea@educacioncontinua-abm.com.mx

Luis Antonio Ramírez Mendoza
Tel. 55 5722-4397
lramirez@abm.org.mx

Karen Daniela Guzmán Meza
Tel. 5722-4392
kguzman@abm.org.mx

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