Educación Continua

TECNOLÓGICO DE MONTERREY

Diplomado

Tecnologías de Ciberseguridad

Duración 128 horas

Objetivo general:
Proveer las bases teóricas y prácticas de todas las áreas técnicas de la ciberseguridad, con el objetivo de contar con todos los elementos para implementar una estrategia de seguridad dentro de una organización. Esto involucra identificar los diferentes servicios y mecanismos necesarios para construir un sistema informático operacional seguro que este alineado con los objetivos de la organización.

Beneficio:
1. Conocer todos los conceptos técnicos relacionados con Ciberseguridad
2. Contar con los elementos suficientes para que el personal a cargo de los sistemas de información de una organización pública o privada pueda entender e implementar una estrategia de ciberseguridad.

Dirigido a:
Ingenieros en informática
Personal de ambientes financieros en las áreas operativas
Programa dirigido a profesionales que trabajen en el área de sistemas de información, desarrollo, operaciones, redes y telecomunicaciones, administración de riesgos, auditoria de TI, control interno y de cumplimiento.

Requisito:
Conocimientos básicos de computación.
Licenciatura en sistemas, telecomunicaciones, actuaria.

Contenido:

Módulo 1 Introducción a ciberseguridad.

Presentar al usuario el diplomado, así como un panorama general de la seguridad Informática, en el cual se expliquen los conceptos básicos de la seguridad Informática, así como todo lo relacionado con el tópico de control de acceso.

Temario

1. Antecedentes y conceptos de seguridad informática.
2. Estadísticas relacionadas a la seguridad informática.
3. Opciones académicas
4. Certificaciones y estándares en seguridad informática.
5. Control de acceso.
6. Etapas del control de acceso.
7. Mecanismos de autenticación.
8. Tipos de control de acceso.
9. Control centralizado de acceso.

10. Control descentralizado de acceso.
11. Single Sign On.
12. Identity management

Duración del módulo: 8 horas

Módulo 2 Seguridad perimetral.

CConocer los principios básicos de la esteganografía, la criptografía y el criptoanálisis. Comprender cómo se pueden utilizar estos conceptos para asegurar los activos de una organización.

Temario

1 Introducción.
2 Definición y componentes del perímetro de seguridad.
3 Anatomía de ataques a las redes informáticas
4 Importancia de la seguridad a nivel red
5 Firewalls
6 Firewalls basados en software y en hardware (appliances)
7 VPNs
8 Servidores AAA

Duración del módulo: 8 horas

Módulo 3 Criptología.

Conocer los principios básicos de la esteganografía, la criptografía y el criptoanálisis. Comprender cómo se pueden utilizar estos conceptos para asegurar los activos de una organización.

Temario

1 Introducción a la criptografía
2 Criptografía y criptoanálisis
3 Conceptos básicos de criptografía.
4 Criptografía clásica: transposición y sustitución.
5 Máquinas criptográficas.
6 Criptografía moderna.
7 Criptografía simétrica de bloques.
8 Criptografía simétrica de flujo.
9 Criptografía asimétrica.
10 Diffie-Hellman.
11 Introducción a la teoría de números.
12 El criptosistema RSA.
13 Los algoritmos hash.
14 La firma digital.
15 Códigos de autenticación de mensaje.
16 Certificados digitales y autoridades certificadoras.
17 Infraestructura de llave pública.
18 Ciclo de vida de una llave.
19 Criptoanálisis.
20 Introducción a la esteganografía
21 Cifrado de correo electrónico.
22 Cifrado de dispositivos de almacenamiento.
23 Práctica de laboratorio de cifrado

Duración del módulo: 16 horas

Módulo 4 Seguridad nodal.

Conocer los diversos paradigmas de operación de los Sistemas de Detección de Intrusos (IDS) y de los Sistemas de Prevención de Intrusos. El participante conocerá las ventajas y desventajas de operación de esta tecnologí

Temario

1 El problema de la definición de las intrusiones.
2 Definición de la tecnología de IDS.
3 Definición de la tecnología de IPS.
4 Paradigmas para el uso de un IDS.
5 Paradigmas de correlación de datos.
6 Paradigmas de operación dependiendo de la fuente de los datos.
7 Engañando a los IDS: ataques y defensas.

Duración del módulo: 4 horas

Módulo 5 Seguridad es sistemas operativos unix .

Conocer las características principales de los diferentes sistemas Unix. Definir una lista de mejores prácticas para fortalecer un sistema operativo Unix.

Temario

1 Historia de Unix.
2 Tipos de Unix.
3 Elementos principales de Unix.
4 Seguridad y Unix.
5 Autenticación en Unix.
6 Los sistemas de archivos.
7 Los archivos de inicialización.
8 Monitoreo del sistema.
9 Bitácoras en Unix.
10 Los servicios de red.
11 Los comandos r.
12 Calendarización tareas.
13 El RPC: Remote Procedure Call.
14 Servicio de nombres, mensajería y ftp.
15 NFS: Network File System.
16 El servidor X Windows.

Duración del módulo: 12 horas

Módulo 6 Seguridad en ambientes mainframes.

Conocer las ventajas y desventajas desde el punto de vista de seguridad de los sistemas operativos basados en Win32 y Win64 de Microsoft.

Temario

1 Orígenes e Historia.
2 Básicos Win32 y NT.

3 Arquitectura de Seguridad de Windows 2000.
4 Arquitectura de Seguridad de Windows XP.
5 Arquitectura de Seguridad de Windows 2003.
6 Arquitectura de Seguridad de Windows Vista.
7 Arquitectura de Seguridad de Windows 2008.
8 Arquitectura de Seguridad de Windows 7.

Duración del módulo: 4 horas

Módulo 7 Seguridad en bases de datos.

Conocer el funcionamiento y características de los dispositivos que conforman una red inalámbrica. Definir la arquitectura, y mejores prácticas, de una red inalámbrica que proporciona funcionalidad y seguridad a una organización.

Temario

1 Introducción a tecnologías inalámbricas.
2 El protocolo IEEE 802.11.
3 Antenas.
4 Wired Equivalent Privacy (WEP).
5 Wifi Prrotected Access (WPA/WPA2).
6 WARDriving.
7 Atacando WEP.
8 Atacando WPA.
9 Ataques explotando clientes.
10 Esquemas de defensa para redes inalámbricas.

Duración del módulo: 4 horas

Módulo 8 Seguridad en aplicaciones y desarrollo de sistemas.

Conocer los fundamentos de diseño y tecnologías de seguridad relacionadas con sistemas tipo mainframes.

Temario

1 Introducción a la seguridad en mainframes.
2 Breve historia de los mainframes y su arquitectura.
3 La seguridad en los mainframes, historia y funcionalidad buscada.
4 Como se lleva la seguridad en mainframe, administración y definiciones.
5 Otros elementos de seguridad del sistema operativo.
6 Operación y administración.
7 Elementos de auditoría a la seguridad en mainframes.
8 Auditoría de la seguridad.

Duración del módulo: 4 horas

Módulo 9 Metodologías de pruebas de penetración.

Conocer el funcionamiento de las herramientas más utilizadas en Ciberseguridad

Temario

1 Introducción.
2 Escaneo de puertos TCP/UDP: Nmap.

3 Firewalls
4 Detectores de intrusos
5 Sniffers
6 Software para inyección de paquetes
7 Crackeo de contraseñas en línea y fuera de línea

Duración del módulo: 4 horas

Módulo 10 Seguridad en aplicaciones Web.

Conocer los equipos que conforman las redes de conmutación no directamente conectadas donde se intercambia actualmente más del 90% de los envíos. Caracterizar los ataques que pasan a través de estos equipos intermedios, de los ataques que sufren los mismos y de las soluciones que pueden implementarse para evitar dichos ataques.

Temario

1 Introducción
2 Caracterización de dispositivos intermedios.
3 Equipos intermedios de capa I
4 Seguridad física.
5 Equipos intermedios de capa II
6 PVSTP y puertos de confianza.
7 ACLs
8 Soluciones generales a ataques
9 Equipos Intermedios de capa III
10 Equipos Intermedios multicapas.

Duración del módulo: 4 horas

Módulo 11 Seguridad en sistemas operativos Windows.

Conocer lo que es una prueba de penetración y las principales metodologías.

Temario

1. Definición de una prueba de penetración
2. Metodología OWASP
3. NIST 800-115
4. Open-Source Security Testing Metodology (OSSTM)
5. Penetration Testing Execution StandardPTES
6. Reportes

Duración del módulo: 12 horas

Módulo 12 Seguridad en redes inalámbricas.

Conocer los puntos a tomar en cuenta para diseñar e implementar una aplicación segura, basada en las mejores prácticas propuestas por el proyecto OWASP.

Temario

1 Proceso de código seguro
2 Modelado de riesgos
3 Mitigación de riesgos
4 La base del código seguro

5 Criterios de OWASP
6 OWASP Top Ten

Duración del módulo: 4 horas

Módulo 13 Seguridad en dispositivos móviles y telefonía.

Conocer los aspectos relacionados con la seguridad en base de datos y datawarehouse, así como las herramientas y módulos de seguridad de las bases de datos y datawarehouse más utilizadas en la industria

Temario

1 Tipos de bases de datos.
2 Características de los DBMS´s.
3 Arquitecturas de los DBMS´s.
4 Lenguajes de los DBMS´S.
5 Seguridad en base de datos.
6 Modelos de seguridad.
7 Confidencialidad en las bases de datos.
8 Integridad en las bases de datos.

Duración del módulo: 4 horas

Módulo 14 Computación forense.

Conocer los aspectos relacionados con la seguridad en aplicaciones en producción, desarrollo, y las metodologías y herramientas para analizar, diseñar, e implementar controles en el ciclo de vida del desarrollo de aplicaciones

Temario

1 Controles en aplicaciones en producción.
2 Controles en aplicaciones en desarrollo.
3 CMM.
4 Sistemas expertos.
5 Redes neurales.
6 Control del proyecto.
7 Control del producto
8 Principios de auditoría.
9 Estrategias para el desarrollo de aplicaciones.
10 Metodología de seguridad para el desarrollo de aplicaciones.
11 El rol del especialista de seguridad en el desarrollo de aplicaciones
12 Determinación del nivel de riesgo aceptable en las aplicaciones.
13 Acreditación y Certificación.
14 Conversión de las aplicaciones.
15 Administración de cambios
16 Administración de configuraciones.

Duración del módulo: 4 horas

Módulo 15 Sistemas de detección y prevención de intrusiones.

Conocer las características principales del software malicioso, así como las amenazas de este tipo de software. Implementar las contramedidas necesarias para mitigar el riesgo provocado por el software malicioso.

Temario

1 Introducción
2 Historia
3 Clasificación extensa.
4 Funcionamiento del software malicioso
5 Daños que un virus puede generar.
6 Análisis de software malicioso (Ingeniería Inversa)
7 Depuración en contra de desensamble
8 Detección y frenado

Duración del módulo: 4 horas

Módulo 16 Gestión de la seguridad de la información.

Conocer las características de los dispositivos móviles, las vulnerabilidades y amenazas de este tipo de dispositivos. Comprender las mejores prácticas para definir políticas para el uso seguro de dispositivos móviles.

Temario

1 Dispositivos móviles
2 Almacenamiento móvil
3 Seguridad dispositivos almacenamiento móvil.
4 Bluetooth
5 Smartphones
6 BYOD
7 Seguridad en sistemas de telecomunicaciones
8 Telefonía fija
9 Voz sobre IP

Duración del módulo: 8 horas

Módulo 17 Software malicioso.

Conocer qué es y para qué sirve el cómputo forense. Comprender la metodología de aplicación del cómputo forense.

Temario

1 Definición y principios.
2 Necesidad de investigación.
3 Tipos de análisis forense.
4 Los 4 pasos del proceso forense.
5 Preparándose para el incidente
6 La respuesta al incidente.
7 Importancia de la evidencia.
8 Cadena de custodia.
9 Manejo de evidencia.
10 Errores técnicos.
11 Respuesta en vivo.
12 Ejecución de análisis forense.
13 Búsqueda de evidencia en diversas plataformas y sistemas operativos.
14 Cómputo forense vs. análisis forense clásico

Duración del módulo: 4 horas

Módulo 18 Tendencias Ciberseguridad.

.

Temario

1. Estado actual de la ciberseguridad
2. Evolución de la ciberseguridad
3. La academia y la ciencia de la ciberseguridad
4. Ataques computacionales del futuro
5. Dispositivos y medidas de seguridad del futuro

Duración del módulo: 4 horas

Módulo 19 Herramientas de seguridad.

Conocer todos los aspectos relacionados con la administración de la seguridad de la información, a fin de poder elegir las mejores opciones tecnológicas para implementar los controles definidos como resultado de esta administración.

Temario

1. El oficial de seguridad de la información
2. Arquitectura de seguridad
3. Métricas de la seguridad de la información

1 Políticas de seguridad
2 Compliance
3 Seguridad en las operaciones
4 BCP & DRP
5 Legislación
6 Análisis de riesgos
7 Auditoría seguridad información

Duración del módulo: 16 horas