DIPLOMADO EN SEGURIDAD EN REDES MICROSOFT®

Hackers, virus, panes. ¿Cuáles son los conocimientos de seguridad que un **CSO (Chief Security Officer)** debe desarrollar y adoptar para prevenirse contra el bombardeo de éstas y de otras amenazas de la red? Las respuestas están en el **Diplomado en Seguridad en Redes Microsoft®**, con el cual actualizarás tus conocimientos sobre el manejo de herramientas avanzadas de protección, blindaje de sistema operativo, **VPNs**, **Firewalls** y seguridad perimetral.

DIRIGIDO A:

Gerentes y directores del área de **telecomunicaciones, Informática**, especialistas en **TI**, proveedores de **Internet**, administradores, encargados de **seguridad**, profesionales de las áreas de **computación, sistemas y comunicaciones** que deseen actualizar sus conocimientos e implementar seguridad en sus servicios de Intranet y seguridad perimetral.

BENEFICIOS:

- El participante conocerá las nuevas herramientas y la evolución de los ataques cibernéticos.
- Conocerá los nuevos esquemas de seguridad empresarial.
- Ser reconocido como un especialista en la demandada actividad de seguridad en redes.
- Tomar control de la seguridad en redes complejas.
- Obtener un puesto de mayor responsabilidad y remuneración.
- Mantener una ventaja competitiva dentro del mercado laboral.
- Aumentar tu productividad y ser reconocido como un especialista en seguridad Microsoft®.

INCLUYE:

- Instalaciones adecuadas
- Material y manuales de cursos
- Instructores Certificados

- Box lunch y Servicio de cafetería continua
- Estacionamiento
- Registro **STPS**

MÓDULO 1 TIPS Y BLINDAJE DEL SISTEMA OPERATIVO

Objetivo: Proveer al participante bases sólidas en la administración de la seguridad del **sistema operativo**, el uso de herramientas de búsqueda de vulnerabilidades, sistemas de detección de intrusos, análisis de registros, además de revisar las últimas técnicas de ataques mediante **troyanos, puertas traseras, ataques a passwords (crackers) o secuestro de sesiones** en donde se analiza cómo funciona y las medidas de protección necesarios para evitarlos.

Dirigido a: Directores y gerentes del área de **Telecomunicaciones**, profesionales de las áreas de computación, informática, sistemas y comunicaciones que deseen tener un sistema operativo robusto.

Requisitos: Conocimientos de administración en **Windows®**.

Duración: 20 hrs.

TEMARIO:

Identificando los riesgos de Seguridad

- Identificando los riesgos para datos
- Identificando los riesgos para servicios
- Identificando trucos potenciales
- Introducción a los estándares de Seguridad Comunes
- Planeando una red segura

Introducción a la seguridad de Windows 2000®

- Introducción a las características de seguridad
- Autenticación de las cuentas de usuarios
- Acceso seguro a los recursos
- Introducción a las tecnologías de encriptación
- Encriptación de datos almacenados y Transmisión

- Revisión a las tecnologías de **PKI**

Planeación de los accesos administrativos

- Determinando el modelo administrativo apropiado
- Estrategias para el diseño de grupos
- Planeando del acceso local
- Planeando el acceso remoto

Planeación de las cuentas de usuarios

- Diseñando políticas de cuentas y políticas de grupos
- Planeando la creación de cuentas y su ubicación
- Planeando la delegación de la autoridad
- Auditando las cuentas de usuarios

Planeación de la seguridad en Computadoras Windows 2003®

- Introducción
- Planeación de la seguridad Física
- Evaluando requerimientos de seguridad
- Diseñando la configuración de plantillas de seguridad
- Evaluando la configuración de la seguridad

Seguridad en recursos de impresión y archivos

- Examinando la seguridad del sistema de archivos
- Protegiendo los recursos a través de **DACL**
- Encriptando datos con **EFS**
- Auditando los accesos a los recursos
- Respaldos seguros y Procedimientos de restauración
- Protegiendo datos de Virus

Canales seguros de Comunicación

- Introducción
- Evaluar riesgos
- Diseño de la seguridad en capa aplicación
- Diseño de la seguridad en la capa de Network
- Desarrollando estrategias para la Encriptación del tráfico de red
-

Extendiendo la red a los Socios de la empresa

- Introducción
- Proveyendo el acceso a socios
- Uso de Aplicaciones seguras para los socios
- Conexiones seguras para los socios remotos
- Estructurando el AD para la administración de cuentas de socios
- Autenticación de socios desde dominios de confianza

Desarrollando un plan de seguridad

- Introducción
- Diseñando un plan de seguridad
- Definiendo los requerimientos de seguridad
- Administrando el plan de seguridad

MÓDULO 2

CONFIGURACIÓN DE REDES PRIVADAS VIRTUALES (VPNS) CON WINDOWS 2003/2008®

Objetivo: Proveer al participante los conocimientos y herramientas necesarios para diseñar e implementar **Redes Privadas Virtuales (VPNs)** utilizando protocolos de seguridad (**IPSec, PPTP, L2TP**) bajo ambiente **Windows®**.

Dirigido a: Directores y gerentes del área de **Telecomunicaciones, Informática**, profesionales de las áreas de computación, sistemas y comunicaciones que deseen implementar seguridad en redes corporativas a través de **VPNs**.

Requisitos: Conocimientos de **Windows®** y redes **TCP/IP**.

Duración: 20 hrs.

Introducción a la Infraestructura de Red

- Identificando métodos de acceso remoto
- Introducción a la Infraestructura de Red y Configuración del laboratorio
- Rehabilitación de contraseñas para **ruteadores**
- Configuración de la Intranet: segmentos **IP** y protocolos de **ruteo**

Introducción a las VPNs

- Qué son las **VPNs**
- Requerimientos básicos
- Conceptos de tunneling
- Repaso al Protocolo **PPP**
- Protocolo **PPTP**
- Protocolo **L2TP**
- Túnel con **IPSec**
- Encriptación Simétrica y qué es **PKI**
- Soporte **RAS**

Configuración de Redes Seguras utilizando IPSec

- Introducción a **IPSecurity**
- Implementación **IPSec**
- Utilizando **IPSec** como modo de Transporte
- Utilizando **IPSec** como Túnel
- Creando políticas de seguridad con **IPSec**
- Seleccionando un esquema de encriptación
- Probando la asignación de políticas **IPSec**
- Optimizando el rendimiento para **IPSec**

Configurando los servicios de Acceso Remoto

- Examinando el servicio **RRAS**
- Operación **VPNs**
- Configurando conexiones de entrada
- Configurando conexiones de salida
- Configuración Multilink
- Configurando Protocolos de Autenticación
- Integrando el servicio **RRAS** con **DHCP**

Soporte al servicio de Acceso Remoto a través de la Red

- Examinando las políticas de acceso remoto
- Creando políticas de acceso remoto
- Identificando problemas de Acceso Remoto
- Identificando problemas del hardware de comunicaciones
- Identificando problemas en líneas de comunicaciones
- Identificando problemas de configuración

Utilizando servicios de autenticación

- Introducción al **IAS**
- Propósito del **RADIUS**
- Instalando y configurando **IAS**

MÓDULO 3

IMPLEMENTACIÓN DE FOREFRONT THREAT MANAGEMENT (TMG) GATEWAY 2010®

Objetivo: Ofrece los conocimientos y habilidades para diseñar e implementar el acceso a Internet, acceso remoto y soluciones de protección de correo utilizando Microsoft Forefront Threat Management Gateway (TMG) 2010®.

Dirigido a: Arquitectos, consultores, técnicos y Ventas Profesionales involucrados en el diseño, implementación, operación o soluciones de seguridad.

Requisitos: Conocimientos de administración en **Windows®**.

Duración: 14 hrs.

TEMARIO:

Información general Forefront Threat Management Gateway (TMG) 2010®

- Introducción a **Forefront TMG®**
- Instalación y Configuración Inicial
- Conceptos básicos de configuración

Secure Web Gateway

- Información general de **Secure Web Gateway**
- Inspección **HTTPS**
- Filtrado de **URL**
- Protección contra malware
- Prevención de intrusiones

La puerta de acceso remoto

- Resumen de la puerta de enlace de acceso remoto
- Publicando Non-HTTP Server
- Publicación en la Web
- Conectividad de red privada virtual (VPNs)

Retransmisión de correo seguro

- Información general de retransmisión de correo seguro
- Componentes de la solución
- Configuración de Protección SMTP

Consideraciones de diseño y el despliegue de Forefront (TMG) 2010®

- Consideraciones de diseño lógico
- Escalabilidad y disponibilidad
- Configuración del cliente
- Opciones de migración

MÓDULO 4 — TÓPICOS AVANZADOS DE SEGURIDAD EN REDES MICROSOFT®

Objetivo: Enseñar al participante a utilizar nuevas herramientas y técnicas avanzadas de seguridad con el fin de enfrentar las nuevas amenazas y riesgos que representa que su **LAN** esté conectado a **Internet**. Y al mismo tiempo garantizar la disponibilidad y **performance** de las aplicaciones críticas de su red.

Dirigido a: Directores y gerentes del área de **Informática**, **telecomunicaciones**, profesionales de las áreas de computación, sistemas y comunicaciones que deseen aprender cómo defenderse proactivamente de los ataques de los endiablados **hackers**.

Requisitos: Conocimientos de administración en **Windows®**.

Duración: 20 hrs.

TEMARIO:

Herramientas de evaluación de la seguridad

- Evaluación de la configuración de seguridad
- Consola Configuración y análisis de seguridad
- Utilidad de Línea de comandos **Secedit.exe**
- Evaluación de la seguridad

Microsoft® Baseline Security Analyzer

- Uso de **MBSA**

Herramientas de terceros

- Barrido de puertos
- Puertos comunes de Windows®
- Determinar puertos abiertos en el equipo local

- Determinar los puertos abiertos en un equipo remoto
- Opciones **Host Discovery**

Seguridad de la LAN y pruebas de penetración

- Evaluar la seguridad de la red
- Tipos de evaluaciones de seguridad
- Búsqueda de vulnerabilidades y penetración
- Auditoría de seguridad IT
- Cómo realizar evaluaciones de seguridad
- Evaluación de seguridad
- Realización de pruebas de penetración
- Troubleshooting en problemas descubiertos

Herramientas para la Administración de la seguridad

- Analizando la Seguridad de la Red
- Instalación **Retina Network Security Scanner**
- Manejo de Retina

Escáner para detectar Recursos Compartidos y permisos

- Instalando **Dumpsec**
- Permisos **Sharing**
- Permisos **NTFS**
- Permisos **Registry**

Detección de Intrusos

- Clasificación de los **IDS**

AirSnare

Instalación AirSnare

NetCat

Ataques a Windows y Prevención

- Las contraseñas débiles anulan la seguridad fuerte
- Ataque de diccionario: **LC4**
- Para abrir la aplicación

Asterwin

Herramientas Adicionales

Trout / Whois

Rpcdump

Firmas Digitales

- Introducción a la Criptografía
- Encriptación de Claves Públicas
- Autenticación de claves Públicas
- Firmas Digitales
- Autoridades de Certificación

Implementación de Certificate Authority, CA

Instalando el Servicio de Certificados

- Instalación de Componentes
- Creando un CA subordinado
- Instalando un certificado desde un archivo
- Listas de Revocación de certificado