



Cursos Funcionales

Curso I: Formación Security Officer Modulo I

Descripción:

Este modulo permitirá al estudiante enfocarse en las tareas y el conocimiento con los que debe contar el Gerente de Seguridad de información para administrar de forma efectiva la seguridad de información dentro de una organización.

Contenido:

1. Conceptos de seguridad de Información
2. Gobierno de seguridad de Información
3. Gerencia de Seguridad de Información
4. Sistema de Gestión de Seguridad de Información
5. Analisis de Brechas
6. Norma ISO 27001 e ISO 27002, dominios y su interpretación
7. Modelo PDCA para la implantación de un SGSI
 - a. Fase de Planificación para la implantación de un SGSI
 - b. Fase de Desarrollo para la implantación de un SGSI
 - c. Fase de Chequeo y monitoreo en la implantación de un SGSI
 - d. Fase de Retroalimentación y Mejora continua en la gestión de un SGSI
8. Roles y responsabilidades organizacionales de la gestión de Seguridad

Curso II: Formación Security Officer Modulo II

Descripción:

Este curso permitirá al estudiante enfocarse en el conocimiento técnico básico necesario para que el gerente de seguridad pueda conocer las tecnologías de seguridad y la mejor forma de sacarle el máximo rendimiento en la organización.

Contenido

1. Firewalls
2. Administración de cuentas de usuarios
3. Detección y Prevención de Intrusos
4. Antivirus
5. Infraestructura de llave publica (PKI)
6. Capa de Socket Segura (SSL)
7. Single Sign On (SSO)
8. Biometria
9. Encriptación
10. Acceso remoto
11. Firma digital
12. Intercambio electrónico de datos (EDI) y Transferencia Electrónica de Fondos (EFT)
13. Redes privadas virtuales
14. Transferencia electrónica segura
15. Forense
16. Tecnologías de Monitoreo



Curso III: Cobit y Auditoria.

Descripción:

El aprendizaje y conocimiento de la metodología COBIT, cubre tres grandes campos de la empresa ya que se orienta al cumplimiento de los objetivos empresariales, a la organización y operación de la Unidad de Sistemas de acuerdo a estándares y normas de reconocimiento internacional y finalmente a la Auditoria Interna, ya que incluye guías para realizar auditorias informáticas, sin embargo el gerente de seguridad debe conocer también su ámbito de aplicación e implementación pues los conceptos de seguridad de información y controles que se derivan tienen un impacto importante en las actividades relacionadas a la seguridad de información.

Contenido

1. Presentación General del COBIT 4.0 / 4.1
2. Introducción a las Directrices de Auditoria.-
3. Planeación y organización
4. Adquisición e Implementación
5. Entrega y Soporte
6. Monitoreo y Evaluación
7. Taller de Elaboración de Programas de Trabajo COBIT

Curso IV: Análisis y gestión de Riesgos

Descripción:

Este curso permite al participante comprender la importancia de la administración y análisis de riesgos como una herramienta para satisfacer las necesidades de negocio, así como también proporciona una metodología para el análisis y gestión de riesgos.

Contenido

1. Definición y Objetivo del análisis y la gestión del riesgo
2. Administración eficaz de riesgos de seguridad de información
3. Implementación de la administración de riesgos
4. Procesos de administración de riesgos
5. Amenazas
6. Vulnerabilidades
7. Riesgos
8. Impacto
9. Controles y Contramedidas
10. Clasificación de activos de información



Curso V: BCP/DRP (Business Continuity Plan/Disaster Recovery Plan)

Descripción:

Este curso brinda al participante el conocimiento necesario para la preparación y desarrollo de un Plan de Continuidad / Plan de recuperación de desastres.

Contenido

1. Planeamiento de la continuidad del negocio/recuperación de desastres
2. Casos de desastres y otras interrupciones
3. Análisis de impacto sobre el negocio
4. Objetivos de punto de recuperación y objetivo de tiempo de recuperación
5. Estrategias y alternativas de recuperación
6. Desarrollo del BCP y DRP
7. Organización y asignación de responsables
8. Componentes de un plan de continuidad
9. Métodos de recuperación de desastres de las redes de telecomunicación
10. Métodos de recuperación de desastres del servidor
11. Pruebas del plan

Curso VI: Legislación Informática y Pericia Electrónica

Descripción:

Este curso permitirá al participante identificar y Caracterizar las etapas de un Peritaje Informático Forense, y la relación intrínseca entre éstas y el Marco Legal Vigente, comprender exhaustivamente los Procedimientos técnicos a seguir en la Identificación / Adquisición, Preservación, Análisis y Presentación de la Evidencia Digital, identificar y Seleccionar las Herramientas Forenses adecuadas para su utilización en cada etapa.

Contenido

1. Origen y Conceptos de las Ciencias Forenses.
2. Bases Doctrinarias y Técnicas. Cuándo, Dónde, Cómo, Qué, Quién, Por Qué.
3. La Pericia Forense Informática: Conceptos universalmente aceptados.
4. Marco Normativo Legal.
5. Entendiendo la Evidencia Digital. Evidencia y Medios. Los tiempos en el proceso de Identificación.
6. Mutabilidad de la Evidencia Digital. Evidencia Perdurable y Volátil. Formas de Identificación.
7. Evidencia Volátil: Identificación de la existencia. Monitoreos de Red. Formas de Adquisición.
8. Herramientas de uso común para la Identificación y Adquisición.
9. Casos Ejemplificadores. Ventajas e inconvenientes.
10. Fragilidad de la Evidencia Digital. Escena del Crimen, Contaminación y Nulidad de la Prueba.
11. Procedimientos para la Preservación de la Evidencia con conformidad legal. Flujograma.
12. De la Escena del Crimen a la Cadena de Custodia. Apagado y Retiro de Evidencia Digital.
13. La Documentación del Análisis Forense como base para la elaboración del Informe Pericial. Fundamentación Técnica.
14. Contenido de un Informe Pericial. Rubricado.



Curso VII: Liderazgo y gestión de Equipos

Descripción:

El participante de este curso podrá reconocer las fases de formación, tormenta, normalización y productividad de un equipo y cómo actuar en cada una de ellas desarrollar la habilidad de identificar los roles dentro de un equipo para poder utilizar las mejores capacidades de cada persona practicar el estilo de dirección apropiado a cada situación desarrollar habilidades para: delegar, tomar decisiones y resolver problemas comprender las características de un equipo eficaz: habilidades, objetivos comunes, implicación y responsabilidad, comunicación

Contenido

1. Dirigir y liderar
2. Grupo de trabajo y equipo de trabajo
3. etapas del desarrollo de un equipo
4. roles dentro de un equipo
5. liderazgo situacional y delegación
6. toma de decisiones
7. resolución de problemas
8. características de un equipo eficaz
9. desarrollo de las personas
10. motivación



Curso VIII: Técnicas de Ataque y Defensa

Descripción:

Este curso permitirá al alumno el conocimiento de las técnicas de ataque y defensa de infraestructuras de RED desde el punto de vista interno y externo.

Contenido

- 1 Footprint
- 2 Scanning
- 3 Enumeracion
- 4 Análisis de Vulnerabilidades
- 5 Obtención de Acceso
- 6 Escalamiento de Privilegios
- 7 Contramedidas

Curso IX: Análisis Forense Computacional

Descripción:

Este curso propone las metodologías y fundamentos necesarios para realizar análisis forense orientado hacia la seguridad de la información.

Contenido

1. De la Escena del Crimen a la Cadena de Custodia. Apagado y Retiro de Evidencia Digital.
2. Documentación del Proceso. Uso del Reloj Patrón. Time Stamping
3. Validación de la Prueba preservada: Checksum y Hash.
4. Casos especiales de Preservación de Evidencia Volátil. Preparación de la Escena. Recolección. Memory Dumps. Sniffers y Monitores. Process List & Tracking.
5. Evidencia Remota. Crawlers. Adquisición por Web. Web Dumpers. Wget.
6. Herramientas para la Preservación de la Evidencia Digital.
7. Requisitos Técnico-Legales para Analizar la Evidencia Digital.
8. Recreación Cronológica de hechos. Importancia de los Registros, la Documentación y el Uso del Reloj Patrón. Tiempo crítico de Cadena de Custodia en el almacenamiento de la Evidencia.
9. Preparación de Evidencia Analizable: Copias. Casos Especiales de Análisis Unico por Destrucción. Documentación del Proceso. Comprobación de identidad por Hashing o Checksums
10. Buceando en los Datos. Técnicas de Análisis. Revisión de Logs, Archivos Temporales, Swappings, Cachés, Recycleds, Spools y similares. Recuperación de Datos relevantes. Scaneo de los Medios por FileSystems o por Geometría Física.
11. Tipos comunes de datos: Mails, Imágenes, Documentos de Ofimática. Los Metadatos. Interpretación.
12. Variedad de Herramientas para el Análisis Forense de la Evidencia Digital.



Curso X: Seguridad Plataforma Linux

Descripción:

Este curso ofrece al estudiante las herramientas y el conocimiento adecuado sobre la plataforma Linux orientado al aseguramiento de este tipo de plataformas.

Contenido:

1. Manejo de usuarios y Filesystem.
2. Aseguramiento de la configuración base.
3. Administración y manejo de Firewall.
4. Administración y manejo de Proxy.
5. Detección y Prevención de Intrusos.
6. Blindaje de Aplicaciones.
7. Aseguramiento de servicios.
8. Administración y configuración de VPN.

Curso XI: Seguridad Plataforma Windows

Descripción:

Este curso ofrece al estudiante las herramientas y el conocimiento adecuado sobre la plataforma Windows orientado al aseguramiento de este tipo de plataformas.

Contenido:

1. Autenticación en profundidad.
2. Aseguramiento mediante roles y Grupos
3. Aseguramiento de servidores y servicios
4. Aseguramiento de IIS
5. Infraestructura de PKI

Curso XII: Auditoria de Seguridad de Plataformas tecnológicas



Descripción:

Este curso ofrece al estudiante las herramientas y el conocimiento adecuado sobre las metodologías de auditoría y seguridad sobre las plataforma tecnológicas.

Contenido:

1. Auditoria y seguridad de dispositivos de seguridad perimétrica
2. Firewall
3. IDS
4. IPS
5. Proxys

