SENDA GESTIÓN S.L
www.sendagestion.com
mperez@sendagestion.com
968204734

FORMACIÓN

Catálogo de Cursos

CODE 7 CIBERSEGURIDAD

Sector: INFORMATICA

CONVOCATORIA ABIERTA. Si está interesado en este curso, por favor, consulte las fechas.

Modalidad: ONLINE

Duración: 100.00 horas

Objetivos:

El objetivo general del curso es formar a profesionales en el ámbito de la ciberseguridad digital, en los elementos nuevos en esta área, profundizando en aspectos fundamentales propios de esta disciplina; pero no se restringe a los temas técnicos sino que también analiza el funcionamiento y estructuras de una empresa para responder de manera eficaz a las demandas y retos de la ciberseguridad, así como aspectos legales y regulatorios y revisión de estándares.
Aplicar medidas de seguridad con el fin de proteger los activos y procesos de la organización.
Diseñar una arquitectura de seguridad perimetral que garantice la seguridad y el control de acceso a los sistemas de información, así como garantizar la confidencialidad y el control de acceso a los equipos y dispositivos móviles y portátiles.
Aprender las técnicas y herramientas utilizadas por los atacantes, y conocer la manera correcta de actuar ante un ataque.

Contenidos:

1. MÓDULO 1. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN 1.1. Introducción a la seguridad de la información 1.2. Gestión de la seguridad de la información 1.2.1. Principios básicos de la seguridad de la información 1.2.2. Factores críticos de éxito 1.3. Normativas y estándares de seguridad 1.3.1. Organizaciones: ISO, ISACA, NIST, IEC 1.3.2. Estándares: COBIT, ISO/IEC 27000, ITIL 1.3.3. Evolución de las normas de seguridad 1.4. ISO 27002: Código de buenas prácticas para la gestión de la seguridad de la información 1.4.1. Políticas de seguridad de la información 1.4.2. Aspectos organizativos de la seguridad de la información 1.4.3. Seguridad ligada a los recursos humanos 1.4.4. Gestión de activos 1.4.5. Control de accesos 1.4.6. Cifrado 1.4.7. Seguridad física y ambiental 1.4.8. Seguridad en la operativa 1.4.9. Seguridad en las telecomunicaciones 1.4.10. Adquisición, desarrollo y mantenimiento de los sistemas de información 1.4.11. Relaciones con suministradores 1.4.12. Gestión de incidentes en la seguridad de la información 1.4.13. Aspectos de seguridad de la información en la gestión de la continuidad del negocio 1.4.14. Cumplimiento 1.5. COBIT 2019 Fundamentos introducción y principios 1.5.1. Introducción y principios de COBIT 2019 1.5.2. Sistema de gobierno y gestión 1.5.3. Objetivos de gobierno y gestión 1.6. Legislación relacionada con la seguridad de la información 1.6.1. Protección de datos que carácter personal: LOPDGDD 1.6.2. SSI y comercio electrónico: LSSI-CE 1.6.3. Propiedad intelectual: LPI 1.6.4. Ley de servicios electrónicos de confianza 1.6.5. Esquema nacional de seguridad (ENS) 1.7. Estructura, publicación y difusión del cuerpo normativo
www.nallam.es Tel. 902043289
2. MÓDULO 2. ADMINISTRACIÓN DE SEGURIDAD PERIMETRAL 2.1. Seguridad de la información 2.1.1. Principios y objetivos de la seguridad de los sistemas de información:

Autenticidad, Confidencialidad, Integridad de la información 2.1.2. Aplicación de la criptografía a la seguridad de la información 2.1.3. Técnicas para el cifrado de información confidencial 2.1.4. Certificados digitales, gestión de PKI (Public Key Infraestructure) 2.1.5. Aplicación de la firma digital 2.1.6. Proceso e implicaciones de la facturación electrónica 2.2. Autenticación y gestión de identidades 2.2.1. Políticas y procedimientos de seguridad para los procesos de autenticación 2.2.2. Autenticación de dos factores, utilización de tarjetas criptográficas (Smart-card logon) 2.2.3. Sistemas Single Sign On (SSO) 2.2.4. Autenticación remota de usuarios, utilización de servidores de autenticación RADIUS 2.2.5. Acceso remoto a la red interna mediante conexiones VPN 2.3. Acceso perimetral 2.3.1. Diseño y definición de modelos para el establecimiento del perímetro de seguridad 2.3.2. Configuración de políticas y reglas de filtrado de cortafuego 2.3.3. Configuración segura de servidores y servicios sobre DMZ 2.3.4. Comunicaciones seguras a servicios internos a través de conexiones IPSEC 2.3.5. Establecimiento de túneles “cifrados” para conexión entre delegaciones (túneles IPSEC) 2.3.6. Establecimiento de túneles VPN mediante el protocolo SSL. Acceso seguro mediante SSL a servidores Web y servidores de correo. 2.4. Seguridad de redes inalámbricas 2.4.1. Configuración de dispositivos inalámbricos: Punto de acceso y tarjetas inalámbricas 2.4.2. Autenticación WPA2 basada en RADIUS: Elementos necesarios, servidos RADIUS. Active directory. Certificados. Configuración de autenticación PEAP. 2.5. Seguridad en portátiles y dispositivos móviles 2.5.1. Seguridad física/lógica para el control de acceso: Seguridad de inicio en sistemas Windows y Linux. Seguridad de contraseñas. Sistemas de autenticación biométricos. 2.5.2. Cifrado de la información confidencial: Cifrado simétrico mediante contraseña única. Cifrado asimétrico mediante llave publica/privada (GPG). Herramientas para repositorio de contraseñas. 2.5.3. Control de dispositivos removibles, memorias, discos USB,… Riesgos en el uso de dispositivos de almacenamiento externos. Control de acceso y utilización de dispositivos externos (DEVICELOOK)
2.5.4. Medidas de seguridad en smartphones y tablets: Seguridad dispositivo. Seguridad aplicaciones instaladas.
www.nallam.es Tel. 902043289
3. MÓDULO 3. TÉCNICAS DE INTRUSIÓN – INFORMÁTICA FORENSE
3.1. Herramientas usadas por los atacantes
3.1.1. Scanners - Descripción de la metodología para buscar vulnerabilidades y herramientas
3.1.2. Exploits - Descripción sobre exploits y los distintos tipos y herramientas.
3.1.3. Rootkits - Descripción de rootkits en el mundo Linux y en el mundo Windows y ejemplos
3.2. Análisis forense
3.2.1. Metodología de Analisis forense y consideraciones legales - Copia de evidencias y herramientas
3.2.2. Localización de información en Windows - Principales repositorios de información en sistemas Windows
3.2.3. Localización de información en Linux - Descripción de los principales repositorios de información en sistemas Linux
3.2.4. Identificación de rootkits - Búsqueda de rootkits en Windows y Linux y sus herramientas
3.3. Herramientas para los administradores
3.3.1. Aplicación de bastionado en sistemas operativos - Descripción del proceso de fortificación de un sistema
3.3.2. Alarmas en tiempo real - Descripción de los SIEM
3.3.3. Honeypots - Descripción de una honeypot