DIPLOMA

Otorgado a:

VICENTE BURGOS MUÑOZ

Por la realización del curso de modalidad Teleformacion

EXPERTO EN CIBERSEGURIDAD

Impartido por el Centro Europeo de Formación NALLAM, realizado entre los días 05/03/2018 y 16/05/2018, con un total de 100 horas, Teleformacion con los contenidos que se especifican al dorso, quedando registrado con el número 01458/28468/417880

A 16 de Mayo de 2018

El Alumno/a,

Centro formador,

NALLAM FORMACIÓN

Knowledge with— NALLAM

Contenidos Impartidos:

TEMA 1. GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

o Introducción a la seguridad de la información

o Gestión de la seguridad de la información Principios básicos Factores críticos de éxito

o Normativas y estándares de seguridad Organizaciones: ISO, ISACA, NIST, IEC Estándares: COBIT, ISO/IEC 27000, ITIL Evolución de las normas de seguridad

o ISO 27002: Código de buenas prácticas para la gestión de la seguridad de la información Política de seguridad de la información Organización de la seguridad de la información Gestión de activos Seguridad de los RRHH Conformidad Control de acceso Seguridad física y ambiental Adquisición, desarrollo y mantenimiento de los sistemas de información Gestión de las comunicaciones y operaciones Gestión de incidencias en la seguridad de la información Gestión de la continuidad del negocio

o COBIT COBIT y el gobierno TI Estructura de COBIT: Dominios y procesos Marco de trabajo de COBIT

o Derecho TIC Protección de datos de carácter personal: LOPD Retención de datos: LRD SSI y comercio electrónico: LSSI Propiedad intelectual: LPI Firma electrónica: LFE Esquema Nacional de Seguridad (ENS)

o Cuerpo normativo Estructura del cuerpo normativo Publicación y difusión del cuerpo normativo: Políticas, normas y procedimientos

TEMA 2. ADMINISTRADOR SEGURIDAD PERIMETRAL

o Seguridad de la información

Principios y objetivos de la seguridad de los sistemas de información: Autenticidad, Confidencialidad, Integridad de la Información.

Aplicación de la criptografía a la seguridad de la información.

Técnicas para el cifrado de información confidencial. Certificados Digitales, Gestión de PKI (Public Key Infraestructure Aplicación de la Firma digital.

Proceso e implicaciones de la Facturación electrónica.

o Autenticación y Gestión de identidades

Políticas y procedimientos de seguridad para los procesos de autenticación. Autenticación de dos factores, utilización de tarjetas criptográficas (smart-card logon). Sistemas de Single Sign On (SSO). Autenticación remota de usuarios, utilización de servidores de autenticación RADIUS. Acceso remoto a la red interna mediante conexiones VPN.

o Seguridad perimetral

Diseño y definición de modelos para el establecimiento del perímetro de seguridad. Configuración de políticas y reglas de filtrado de cortafuegos.

Configuración segura de servidores y servicios sobre la DMZ.

Comunicaciones seguras a servicios internos a través de conexiones IPSEC. Establecimiento de túneles "cifrados" para conexión entre delegaciones. (Túneles IPSEC).

Establecimiento de túneles VPN mediante el protocolo SSLAcceso seguro mediante SSL a servidores Web y servidores de Correo.

o Seguridad en redes inalámbricas Configuración de dispositivos inalámbricos : Punto de acceso.Tarjetas inalámbricas. Autenticación WPA2 basada en Radius: Elementos necesarios. Servidor RADIUS. Directorio Activo. Certificados. Configuración de la autenticación PEAP.

o Seguridad en portátiles y sistemas móviles Seguridad física/lógica para el control de acceso: Seguridad de inicio en sistemas Windows y Linux. Seguridad de contraseñas. Sistemas de autenticación biométricos.

Cifrado de la información confidencial: Cifrado simétrico mediante contraseña única. Cifrado asimétrico mediante llave publica/privada (GPG). Herramientas para repositorio de contraseñas.

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) Medidas de seguridad en smartphones y tablets: Seguridad dispositivo. Seguridad aplicaciones instaladas.

TEMA 3. TÉCNICAS DE INTRUSIÓN - INFORMÁTICA FORENSE

Herramientas usadas por los atacantes.

o Scanners - Descripción de la metodología para buscar vulnerabilidades y herramientas

o Exploits - Descripción sobre exploits y los distintos tipos y herramientas.

o Rootkits - Descripción de rootkits en el mundo Linux y en el mundo Windows y ejemplos

Análisis forense.

o Metodología de Analisis forense y consideraciones legales - Copia de evidencias y herramientas:

o Localización de información en Windows - Principales repositorios de información en sistemas Windows

o Localización de información en Linux - Descripción de los principales repositorios de información en sistemas Linux

o Identificación de rootkits - Búsqueda de rootkits en Windows y Linux y sus herramientas

Herramientas para los administradores.

o Aplicación de bastionado en sistemas operativos - Descripción del proceso de fortificación de un sistema.

o Alarmas en tiempo real - Descripción de los SIEM

o Honeypots - Descripción de una honeypot.

*Objetivos:

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.

Este curso te da la formación necesaria para realizar las pruebas siguientes:

- CCS-G emitida por la Agencia de Certificaciones Ciberseguridad.
- CCSP-AP emitida por la Agencia de Certificaciones Ciberseguridad.
- CISA
- CISSP
- CISM
- CHFI
- GCFA