Workshop Ciberseguridad LAN

Código: SEG-009

Propuesta de Valor: SEGURIDAD INFORMÁTICA

Duración: 16 Horas

Este curso tiene por objetivo instruir y ampliar los conocimientos ante las amenazas y ciberataques informáticos que ponen en riesgo a las redes corporativas de modo que puedan ser mitigadas poniendo en práctica arquitecturas y tecnologías de seguridad a fin de identificar, gestionar, diseñar y posicionar dispositivos de seguridad dentro de la red de comunicaciones.

Se desarrollarán laboratorios y actividades prácticas que ayudarán en un mejor entendimiento de los temas abordados en el curso.

Más información: AQUÍ

Reserve su plaza: AQUÍ

AUDIENCIA

Candidatos para este curso:

- Administradores de redes y sistemas.
- Consultores/Especialistas en Seguridad.
- Técnicos de soporte del área de sistemas y comunicaciones.
- Cualquiera que participe en operaciones de red.

PRE REQUISITOS

- Los participantes deben tener un nivel esencial de redes, manejo y configuración de dispositivos de redes.
- Además de fundamentos relacionados a seguridad informática.

OBJETIVOS

- Instruir y ampliar los conocimientos ante las amenazas y ciberataques informáticos que ponen en riesgo a las redes corporativas de modo que puedan ser mitigadas poniendo en práctica arquitecturas y tecnologías de seguridad a fin de identificar, gestionar, diseñar y posicionar dispositivos de seguridad dentro de la red de comunicaciones.

CERTIFICACIÓN DISPONIBLE

- Certificación emitida por COGNOS.

CONTENIDO

1. NOCIONES DE LA CIBERSEGURIDAD Y CIBERCRIMEN

1.1. ACTUALIDAD, INCIDENTES REGISTRADOS E IDENTIFICACION DE LOS ACTORES DEL CIBERCRIMEN.
1.2. ACTUALIDAD, INCIDENTES REGISTRADOS E IDENTIFICACION DE LOS ACTORES DEL CIBERCRIMEN.
1.3. DEFINICION DE CONCEPTOS Y ELEMENTOS DE SEGURIDAD DENTRO DE LA RED CORPORATIVA.
1.4. GENERALIDADES DE LOS PROTOCOLOS DE SEGURIDAD BASADA EN NIVELES DE APLICACION, TRANSPORTE, RED Y ENLACE DE DATOS.

2. CONTRAMEDIDAS ANTE ATAQUES INTERNOS

2.1. IDENTIFICAR LAS AMENAZAS Y VULNERABILIDADES ANTE ATAQUES INTERNOS HACIA LA LAN.
2.2. IDENTIFICAR LOS MECANISMOS MINIMOS NECESARIOS ANTE ATAQUES INTERNOS HACIA LA LAN.
2.3. METODOS DE CONFIGURACION RELACIONADOS A LA SEGURIDAD INTERNA DE UNA RED
2.4. APLICABILIDAD DE MEDIDAS BASICAS DE SEGURIDAD A NIVEL CAPA 1 Y 2 DEL MODELO OSI.

3. PROTEGIENDO EL PERIMETRO DE LA EMPRESA

3.1. IDENTIFICAR LAS AMENAZAS Y VULNERABILIDADES FRENTE ATAQUES DESDE INTERNET.
3.2. IDENTIFICAR LOS MECANISMOS NECESARIOS PARA ASEGURAR EL FIREWALL.
3.3. METODOS DE CONFIGURACION RELACIONADOS A LA SEGURIDAD PERIMETRAL DE UNA RED.
3.4. APLICABILIDAD DE MEDIDAS BASICAS DE SEGURIDAD PERIMETRAL BASADA EN FIREWALLS.
3.5. APLICABILIDAD DE MEDIDAS DE SEGURIDAD PARA SERVICIOS PUBLICADOS HACIA INTERNET.

4. MANEJO DE RIESGO Y GESTION DE AMENAZAS

4.1. CONOCER METODOS Y HERRAMIENTAS DEL MERCADO PARA IDENTIFICAR AMENAZAS EN LA RED.
4.2. CASO DE ESTUDIO RELACIONADO AL ASEGURAMIENTO DE UNA RED CORPORATIVA.
4.3. APLICAR MEJORES PRACTICAS DE GESTION PARA CONTRARRESTAR INCIDENTES DE SEGURIDAD.

BENEFICIOS

- Al finalizar el curso, usted tendrá solidos conocimientos ante las amenazas y ciberataques informáticos que ponen en riesgo a las redes corporativas de modo que puedan ser mitigadas poniendo en práctica arquitecturas y tecnologías de seguridad a fin de identificar, gestionar, diseñar y posicionar dispositivos de seguridad dentro de la red de comunicaciones.