CONVOCATORIA CURSOS GRATUITOS TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

SECTOR OTROS SERVICIOS

ZigaNetworks

www.ziganetworks.com

¿Quiénes pueden participar en los cursos?

El sector Otros servicios incluye los siguientes colectivos profesionales:

- Empresas de Peluquería, Institutos de Belleza, Gimnasios y Similares.
- Empresas de seguridad privada.
- Empresas de servicio doméstico.
- Empleados de fincas urbanas
- Empresas de servicios funerarios
- Empresas de limpieza, lavado y planchado de ropa.

Podrán participar:

- ***Trabajadores, Autónomos del R.G. de los sectores arriba mencionados*** que estén dados de alta en las empresas de esos sectores a la fecha de inicio de la formación.

- ***Desemplead@s*** (disponen del 30% del total de plazas), único requisito disponer en vigor de la tarjeta de demandante de empleo.

*NOTA IMPORTANTE: Un trabajador@ podrá hacer en esta Convocatoria o un curso superior a 120 horas o en su defecto varios cursos que no sumen más de 120 horas.

Colectivos prioritarios para Inscribirse

- Mujeres
- Personas con discapacidad
- Personas con baja cualificación (normalmente suelen ser los que en su nómina aparecen los grupos de cotización 06,07 y 010 por ejemplo)
- Mayores de 45 años
- Trabajadores con contrato a tiempo parcial o temporal.
- Trabajadores de Pymes (contra más pequeñas sean las empresas mejor)

Documentación a aportar

- Anexo I Original–hoja de participante-
- Fotocopia DNI del alumn@ o en su en su defecto tarjeta de la S.S. o vida laboral actualizada.
- Cabecera de la nómina (sin datos económicos) del mes vigente al inicio del curso para los trabajadores por cuenta ajena y para los autónomos (último recibo pago del mismo a la S.S.)

Plazo de ejecución de los cursos

1 Año desde la fecha de aprobación

PLAZAS LIMITADAS POR RIGUROSO ORDEN DE LLEGADA DE DOCUMENTACIÓN.

Cursos Subvencionados

Nombre Curso	Modalidad	Horas	Plazas Totales
IFCT 101PO PLANIFICACIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA	TELEFORMACIÓN	80	30

PROGRAMAS FORMATIVOS:

IFCT101PO PLANIFICACIÓN DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA

Objetivos

Planificar la seguridad informática en la empresa

Contenidos

U.D.1. DEBILIDADES, AMENAZAS Y ATAQUES

● OBJETIVO ESPECÍFICO: DEFINICIÓN DE SEGURIDAD INFORMÁTICA, LOS OBJETIVOS Y CONOCER LAS AMENAZAS EXISTENTES EN EL ENTORNO INFORMÁTICO. IDENTIFICAR LAS ACTIVIDADES FRAUDULENTAS, AMENAZAS Y ATAQUES QUE PUEDE SUFRIR CUALQUIER SISTEMA ANTE LAS ACCIONES ENGAÑOSAS DEL EXTERIOR. SE PRETENDE ANALIZAR EL PAPEL DE LOS INTRUSOS Y/O ATACANTES.

1.1. Tipos de atacantes
1.1.1. RECONOCIMIENTO DE SISTEMAS
1.1.2. DETECCIÓN DE VULNERABILIDADES
1.1.3. ROBO DE INFORMACIÓN
1.1.4. MODIFICACIÓN DE CONTENIDOS ANTERIORMENTE ENVIADOS
1.2. Motivaciones del atancante
1.3. Metodología de un atancante determinado
1.4. Vulnerabilidades y ataques comunes
1.5. Herramientas de hacking Y PHISING
1.5.1. DEFINICIÓN DE HACKING Y PHISING
1.5.2. TIPOLOGÍA DE HERRAMIENTAS DE HACKING Y PHISING
1.6. Ingeniería social
1.7. Prevención de ataques
1.7.1. EVALUAR REGULARMENTE LAS VULNERABILIDADES DEL ENTORNO
1.7.2. COMPROBAR CON REGULARIDAD TODOS LOS SITEMAS Y DISPOSITIVOS DE RED.
1.7.3. ESTABLECER PROGRAMAS DE FORMACION SOBRE SEGURIDAD PARA EL PERSONAL DE LA EMPRESA.
1.7.4. MANTENER EL SISTEMA OPERATIVO Y NAVEGADORES ACTUALIZADOS
1.7.5. PROTEGER LAS CONTRASEÑAS
1.7.6. UTILIZAR ANTIVIRUS POTENTES QUE ANALICE TODAS LAS DESCARGAS
1.7.7. DESCONFIAR DE LOS CORREOS DE REMITENTES DESCONOCIDOS
1.7.8. NO ABRIR FICHEROS SOSPECHOSOS, ETC.
1.8. Respuesta a contingencias

U.D.2. ADMINISTRACIÓN DE LA SEGURIDAD EN REDES

● OBJETIVO ESPECÍFICO: MINIMIZAR ERRORES, FRAUDES Y PÉRDIDAS EN LOS SISTEMAS DE INFORMACIÓN DE LAS EMPRESAS, ASÍ COMO A SUS CLIENTES, PROVEEDORES Y OTRAS PARTES INTERESADAS.

2.1. Diseño e implantación de políticas de seguridad
2.1.1. ALCANCE DE LA POLÍTICA DE SEGURIDAD
2.1.2. OBJETIVOS DE LA POLÍTICA DE SEGURIDAD
2.1.3. RESPONSABILIDAD DE CADA UNO DE LOS SERVICIOS Y NIVELES DE LA ORGANIZACIÓN
2.1.4. RESPONSABILIDAD DE LOS USUARIOS
2.1.5. CONDICIONES MÍNIMAS PARA LA CONFIGURACIÓN DE LOS SISTEMAS
2.1.6. ACTUALIZACIONES DE LA POLÍTICA DE SEGURIDAD.

U.D.3. TECNOLOGÍAS CRIPTOGRÁFICAS

● OBJETIVO ESPECÍFICO: DISEÑAR E IMPLEMENTAR SISTEMAS SEGUROS DE ACCESO Y TRANSMISIÓN DE DATOS. DAR A CONOCER EL MANEJO DE USO E IMPLANTACIÓN DE TÉCNICAS CRIPTOGRÁFICAS EN LOS

SERVICIOS QUE LO REQUIEREN ATENDIENDO A ESPECIFICACIONES DE SEGURIDAD INFORMÁTICA. FAMILIARIZARSE CON LOS DISTINTOS TIPOS DE CERTIFICADOS DIGITALES EXISTENTES.

3.1. Encriptación simétrica
3.1.1. VENTAJAS E INCONVENIENTES
3.1.2. APLICACIONES
3.2. Encriptación asimétrica
3.2.1. VENTAJAS E INCONVENIENTES
3.2.2. APLICACIONES
3.3. Firmas digitales
3.3.1. DEFINICIÓN
3.3.2. INSTALACIÓN Y USO
3.3.3. CLASIFICACIÓN
3.3.4. FACTORES IMPLICADOS EN LA FIRMA
3.3.5. APLICACIONES
3.4. Certificados digitales
3.4.1. DEFINICIÓN
3.4.2. INSTALACIÓN Y USO
3.4.3. PROTECCIÓN DE LOS CERTIFICADOS
3.4.4. CERTIFICADOS VÁLIDOS
3.5. SSL/TLS. La herramienta de encriptación multiusos
3.5.1. DESCRIPCIÓN
3.5.2. FUNCIONAMIENTO
3.5.3. APLICACIONES
3.5.4. SEGURIDAD
3.6. Navegación segura: HTTPS
3.6.1. CARACTERÍSTICAS
3.6.2. DIFERENCIAS ENTRE HTTPS Y HTTP
3.6.3. LIMITACIONES

U.D.4. SISTEMAS DE AUTENTIFICACIÓN

● OBJETIVO ESPECÍFICO: LLEVAR A CABO EL PROCESO DE INTENTO DE VERIFICAR LA IDENTIDAD DIGITAL DEL REMITENTE DE UNA COMUNICACIÓN COMO UNA PETICIÓN PARA CONECTARSE. EL REMITENTE SIENDO AUTENTICADO PUEDE SER UNA PERSONA QUE USA UN ORDENADOR, UN ORDENADOR POR SÍ MISMO O UN PROGRAMA DEL ORDENADOR. MEDIANTE LA “AUTENTICACIÓN" PODRÁN ASEGURAR QUE LOS USUARIOS SON QUIEN ELLOS DICEN QUE ELLOS SON - QUE EL USUARIO QUE INTENTA REALIZAR FUNCIONES EN UN SISTEMA ES DE HECHO EL USUARIO QUE TIENE LA AUTORIZACIÓN PARA HACER ASÍ.

4.1. Tecnologías de identificación
4.2. RAP y CHAP
4.2.1. FUNCIONAMIENTO
4.2.2. DIFERENCIAS
4.2.3. CARACTERÍSTICAS
4.3. RADIUS
4.3.1. DEFINICIÓN DEL SERVIDOR RADIUS
4.3.2. CARACTERÍSTICAS
4.3.3. FUNCIONAMIENTO
4.3.4. APLICACIONES
4.4. El protocolo 802.1X.
4.5. La suite de protocolos EAP: LEAP, PEAP. EAP-TLS
4.6. Sistemas biométricos
4.6.1. DEFINICIÓN
4.6.2. FUNCIONAMIENTO
4.6.3. VENTAJAS E INCONVENIENTES
4.6.4. PROCESO DE AUTENTIFICACIÓN E IDENTIFICACIÓN BIOMÉTRICA
4.6.5. PRINCIPALES APLICACIONES DE LA BIOMETRÍA

U.D.5. REDES VIRTUALES PRIVADAS

● OBJETIVO ESPECÍFICO: ADQUIRIR LA COMPETENCIA GENERAL PARA PODER CONFIGURAR REDES PRIVADAS VIRTUALES (VPN) GARANTIZANDO LA SEGURIDAD. CONOCER Y MANEJAR ELEMENTOS NECESARIOS PARA CREAR VPNS QUE PERMITAN ASEGURAR ACCESOS SEGUROS.

5.1. Beneficios y características
5.2. IP Sec
5.2.1. DEFINICIÓN
5.2.2. MODOS DE PROPORCIONAR SEGURIDAD:
- 5.2.2.1. MODO TRANSPORTE

- 5.2.2.2. MODO TUNEL
5.2.3. PROTOCOLOS DE SEGURIDAD
5.3. VPNs con SSL-TLS
5.3.1. DEFINICIÓN
5.3.2. TIPOLOGÍAS
5.3.2. INSTALACIÓN
5.3.3. AUTENTICACIÓN
5.3.4. PRINCIPALES PROBLEMAS

U.D.6. FIREWALLS

● OBJETIVO ESPECÍFICO: ADQUIRIR CONOCIMIENTOS MÁS AVANZADOS SOBRE CORTAFUEGOS O FIREWALL, DE QUE SE COMPONE, COMO FUNCIONA Y SUS DIFERENTES TIPOLOGÍAS. APRENDER A DETECTAR RIESGOS Y COMO A TRAVÉS DEL CORTAFUEGOS PODER MITIGAR, FRENAR E INCLUSO ELIMINAR SU ATAQUE. EL OBJETIVO PRINCIPAL ES EVITAR EL MANEJO DE UN SISTEMA O UN GRUPO DE SISTEMA QUE DECIDE PUEDE ACCEDER DESDE EL EXTERIOR DE UNA RED PRIVADA , QUIENES PUEDEN EJECUTAR ESTOS SERVICIOS Y TAMBIÉN QUE SERVICIOS PUEDEN UTILIZAR LOS USUARIOS DE LA INTRANET HACIA EL EXTERIOR.

6.1. Arquitectura de Firewalls
6.2. Filtrado de paquetes sin estados
6.2.1. DESCRIPCIÓN
6.2.2. VULNERABILIDADES
6.2.3. APLICACIONES
6.3. Servidores Proxy
6.3.1. CARACTERÍSTICAS
6.3.2. VENTAJAS E INCONVENIENTES
6.3.3. APLICACIONES
6.3.4. TIPOLOGÍAS
6.4. Filtrado dinámico o “stateful”
6.4.1. DESCRIPCIÓN
6.4.2. VULNERABILIDADES
6.4.3. APLICACIONES
6.5. Firewalls de siguiente generación
6.6. Funciones avanzadas

U.D.7. DETECCIÓN Y PREVENCIÓN AUTOMATIZADA DE INTRUSIONES (IDS-IPS)

● OBJETIVO ESPECÍFICO: ESTABLECER IN SISTEMA DE PREVENCIÓN DE INTRUSOS, MEDIANTE LA INSTALACIÓN DE SOFTWARE QUE EJERZA EL CONTROL DE ACCESO A UNA RED PARA PROTEGER LOS SISTEMAS DE ATAQUES Y ABUSOS.

7.1. Arquitectura de sistemas IDS
7.2. Herramientas de software
7.3. Captura de intrusos con Honeypots
7.3.1. DESCRIPCIÓN
7.3.2. FUNCIONAMIENTO
7.3.3. CENTRALIZACIÓN DE LA INFORMACIÓN
7.3.4. CLASIFICACIÓN DE LOS HONEYPOTS
7.3.5. VENTAJAS E INCONVENIENTES

administracion@ziganetworks.com

www.ziganetworks.com

FINANCIA

GOBIERNO DE ESPAÑA
MINISTERIO DE EMPLEO Y SEGURIDAD SOCIAL
SERVICIO PÚBLICO DE EMPLEO ESTATAL