Cursos de Ciberseguridad GRATUITOS

DESTINATARIOS: autónomos y trabajadores de pequeñas y medianas empresas.

MODALIDAD: Aula Virtual. Comunicación directa y en tiempo real del docente y los alumnos.

NÚMERO MÁXIMO DE ALUMNOS POR CURSO: 20

REQUISITOS BÁSICOS: WEBCAM y MICRÓFONO (OBLIGATORIOS)

PLAZO DE INSCRIPCIÓN: Abierta (hasta completar un máximo de 20 personas por curso)

Especialidades Formativas de Ciberseguridad Seleccionadas para impartir:

CÓDIGO	ESPECIALIDAD	HORAS
IFCT149PO	Seguridad en el comercio electrónico	20
IFCT0024	Ciberseguridad para usuarios	10
IFCT104	Ciberseguridad para microempresas	15

IFCT121	Ciberseguridad. Riesgos y amenazas en la red	10
IFCT103	Ciberseguridad: prevención, análisis y respuesta a incidentes de seguridad	49
IFCT050PO	Gestión de la Seguridad Informática en la Empresa	100

Ver fechas al final del documento

CONTENIDOS FORMATIVOS DE CADA ESPECIALIDAD

IFCT149PO: Seguridad en el comercio electrónico

20 horas

DESTINATARIOS: Trabajadores pertenecientes a empresas del convenio/sector de servicios a las empresas.

OBJETIVO GENERAL: Conocer las medidas de seguridad aplicables a la protección de datos de carácter personal; analizando los métodos, sistemas y protocolos de seguridad para minimizar los riesgos y fraudes en las transacciones online, así como los aspectos jurídicos, legales y fiscales que se aplican al comercio electrónico y los diferentes métodos de pago online seguros.

CONTENIDOS FORMATIVOS:

- SEGURIDAD Y PROTECCIÓN DE DATOS
  - Seguridad en las TI
    - Contexto de la seguridad de la información
    - Qué es la seguridad de la información
    - Situación ideal de la seguridad de la información
    - Situación real de la seguridad de la información
    - En qué consiste la gestión de la seguridad
    - Decálogo de seguridad de la información
  - Accesos al sistema
    - Arquitectura de seguridad
    - Firewall o cortafuegos
    - Otros elementos de protección
  - Seguridad en las redes
    - Hacking. Seguridad IP
    - Seguridad en redes inalámbricas
    - Seguridad en redes móviles
  - Seguridad en Internet
    - Introducción
    - Requisitos de seguridad en el comercio electrónico
    - Causas de los problemas de seguridad
    - Perfil del amenazante y técnicas de ataque
- ASPECTOS JURÍDICOS EN EL COMERCIO ELECTRÓNICO
  - Introducción a la LOPD
    - Un derecho fundamental
    - Necesidad de proteger los datos personales
  - Ámbito de aplicación
    - Marco legal
  - Procedencia de los datos de carácter personal
    - Recogida de datos
    - Principio de consentimiento
    - Otros procedimientos de recogida de datos
    - Recogida de datos de fuentes de acceso público
    - Principio de calidad de los datos
    - Deber de secreto
  - Comercio Electrónico
  - LSSICE
    - Introducción
    - Marco Legal
    - A quién se aplica
    - Conceptos básicos
    - Obligaciones para las empresas que realizan comercio electrónico

- Recomendaciones de seguridad como usuario de Internet
- Malware

- Registro de protección de datos
  - Documento de seguridad
  - Responsables
  - Determinación del nivel de seguridad

- Niveles de seguridad
  - Niveles de seguridad y tipos de ficheros
  - Medidas de seguridad del nivel básico
  - Medidas de seguridad del nivel medio
  - Medidas de seguridad del nivel alto
  - Cuadro Resumen.

- Derechos de los afectados
  - Concepto de afectado o interesado
  - Deber de ser informado
  - Consentimiento
  - Derechos de las personas
  - Algunos inconvenientes de utilizar una pasarela de pago

- Tarjetas de créditos: banda magnética, tarjetas inteligentes y multiservicio
  - ¿Qué es una tarjeta de crédito?
  - Banda magnética
  - Tarjetas inteligentes y multiservicio

- 3D Secure
  - ¿Qué es el 3D Secure?
  - Procedimiento
  - El sistema tradicional basado en el CVV no es suficiente
  - Pagos en 3D Secure
  - Cómo se realizan los pagos en 3D Secure
  - La autenticación
  - Responsabilidad

- Internet Mobile Payment
  - El Pago por móvil
  - Internet Mobile Payment
  - Servicios ofrecidos por las operadoras telefónicas

- Modelos de negocio de los diferentes actores
  - Modelos de negocio y Actores del Comercio electrónico
  - Diferentes enfoques del negocio online
  - Principales actores del comercio electrónico en España

- Workflow y funcionamiento de un sistema de pago a través de móvil
  - Obligaciones si hacen publicidad por vía electrónica

- LISI
  - Introducción
  - Aspectos más destacables
  - Comunicaciones con usuarios y contratos online

- SEGURIDAD EN LOS MEDIOS DE PAGO ON-LINE
  - Sistemas de pago no integrados
    - Sistemas de pago no integrados
    - Paypal
  - Sistemas de pago integrados - pasarelas de pago
    - ¿Qué es una pasarela de pago?
    - Cómo funciona una pasarela de pago
    - Pasarelas de pago vs. el pago tradicional con tarjeta de crédito

- PAGOS Y TRIBUTACIÓN
  - Sistema de pago
    - Introducción
    - Métodos tradicionales u off-line
    - Métodos de pago online
    - Costes en la instalación de las formas de pago
    - Seguridad en los medios de pago
  - Dinero electrónico
    - Concepto de dinero electrónico
    - Clasificaciones
    - Ejemplos de sistemas basados en tarjetas
    - Ejemplo de sistemas basados en software
  - Protocolos de seguridad
    - Introducción
    - Protocolos más usados
    - Secure Socket Layer (SSL)
    - Secure Electronic Transaction (SET)
  - Firma electrónica
    - Concepto
    - Proceso de firma reconocida
    - Utilidad
    - Elementos
    - Tipos de firmas
    - Dispositivos externos de firma electrónica
  - Certificados y entidades de certificación
    - Certificado electrónico
    - Tipos de certificados electrónicos

- Tecnologías aplicables al pago móvil
- WorkFlow o Flujo de datos
- Variantes de pago por referencia
- Ejemplo de proceso de pago por móvil: servicio de taxi
- Plataformas de pago por móvil
- Situación mundial del pago por móvil

- Clases de certificados electrónicos
- Entidades emisoras de certificados

- Imposición directa e indirecta
  - Introducción
  - Imposición directa sobre el comercio electrónico
  - Imposición indirecta
- Fiscalidad transnacional
  - Soberanía fiscal
  - Calificación de las rentas
  - Establecimiento permanente
  - Imposición directa

IFCT0024: Ciberseguridad para usuarios

10 horas

DESTINATARIOS:
Trabajadores que no tengan ningún conocimiento de Ciberseguridad.
Curso básico si se quiere seguir adquiriendo más conocimientos sobre Ciberseguridad.

OBJETIVO GENERAL: Valorar la necesidad de la gestión de la seguridad en las organizaciones, distinguiendo las principales amenazas a los sistemas de información e identificando las principales herramientas de seguridad y su aplicación en cada caso.

CONTENIDOS FORMATIVOS:

- Aproximación a la seguridad en sistemas de información.
- Asimilación de conceptos de seguridad en los sistemas:
  - Clasificación de las medidas de seguridad.
  - Conocimiento acerca de los requerimientos de seguridad en los sistemas de información.
  - Identificación de principales características.
  - Confidencialidad.
  - Gestión de la integridad.
  - Comprensión de la disponibilidad.
  - Identificación de otras características.
  - Identificación de tipos de ataques.
- Conocimiento del ámbito de la Ciberseguridad para usuario:
  - Comprensión del concepto de ciberseguridad.
  - Identificación de amenazas más frecuentes a los sistemas de información.
  - Utilización de tecnologías de seguridad más habituales.
  - Gestión de la seguridad informática.
- Identificación de softwares dañinos:
  - Asimilación de conceptos sobre software dañino.
  - Clasificación del software dañino.
  - Identificación de amenazas persistentes y avanzadas.
  - Prevención sobre la ingeniería social y redes sociales.
- Gestión de la seguridad en redes inalámbricas
- Aplicación de herramientas de seguridad:
  - Aplicación de medidas de protección.
  - Control de acceso de los usuarios al sistema operativo.
  - Gestión del permiso de los usuarios.

- Gestión del registro de usuarios.
- Autentificación de usuarios.
- Gestión segura de comunicaciones, carpetas y otros recursos compartidos.
- Gestión de carpetas compartidas en la red.
- Identificación de tipos de accesos a carpetas compartidas.
- Procedimiento para compartir impresoras.
- Protección frente a código malicioso.
- Configuración del Antivirus.
- Configuración del Cortafuegos (firewall).
- Aplicación del Antimalware.

IFCT104: Ciberseguridad para microempresas

15 horas

DESTINATARIOS: Trabajadores con conocimientos básicos de Ciberseguridad (aconsejable haber hecho antes el curso de Ciberseguridad para Usuarios).

OBJETIVO GENERAL: Conocer, comprender y analizar los riesgos de seguridad más habituales en una microempresa.

CONTENIDOS FORMATIVOS:

Módulo 1: Ciberseguridad para microempresas – 15 horas

- Contextualización de la ciberseguridad en la microempresa.
  - Conoce a tu enemigo.
  - Conócete a ti mismo.
- Utilización de técnicas y recursos para el análisis de datos. Recopilación de evidencias.
  - Uso seguro de las nuevas tecnologías en la empresa.
- Identificación de las principales medidas para prevenir amenazas.
  - Seguridad en la nube.
  - Seguridad en dispositivos móviles y redes wifi.
  - Relación segura con proveedores y clientes.
- Desarrollo de una política de prevención de incidentes de seguridad en la microempresa
  - Legislación y normativa de seguridad.
  - Incidentes de seguridad.
  - Auditoría de sistemas.
  - Prevención y protección.

IFCT121: Ciberseguridad. Riesgos y amenazas en la red

10 horas

DESTINATARIOS:
Trabajadores que ya tengan conocimientos de Ciberseguridad.

OBJETIVO GENERAL: Concienciar a los usuarios de los posibles riesgos que pueden afectarle a nivel individual y de empresa, así como facilitarles una serie de "buenas prácticas" que puedan aplicar, no sólo en su espacio de trabajo, sino también en su vida personal.

CONTENIDOS FORMATIVOS:

- Conocimientos avanzados sobre nuestra identidad digital.
  - Capacidad de identificación personal en el ámbito digital.
  - Conocimiento sobre la protección de nuestra identidad digital.
  - Conocimiento sobre los derechos asociados a la identidad digital.
  - Conocimiento avanzado de los aspectos de navegación segura por internet.
  - Capacidad de identificación y uso de protocolos seguros en internet.
  - Conocimiento avanzado sobre el proceso de reporte y comunicación de ciberincidentes.
- Conocimiento de las ciberamenazas y aplicación de técnicas de defensa.
  - Conocimiento de los incidentes de seguridad (robo, filtrado y secuestro de información) y sus características.
  - Capacidad para la implementación de las estrategias de protección contra los ciberataques.
  - Capacidades para aplicar técnicas de defensa en el ciber-entorno.
  - Capacidad para minimizar los daños causados por los posibles ciberincidentes.
- Conocimiento avanzado de los lenguajes de programación en ciberseguridad.
  - Conocimiento del lenguaje común de los ciberriesgos.
  - Conocimiento de los principales lenguajes de programación orientados a la ciberseguridad.
  - Conocer los lenguajes que utilizan los hackers.
- Detección, análisis y anticipación a los riesgos de seguridad.
  - Conocimiento sobre las vulnerabilidades y riesgos de seguridad informática.
  - Detección, análisis y anticipación a los riesgos de seguridad.
  - Conocimiento sobre los comportamientos que ponen en riesgo nuestra seguridad en entornos digitales.
  - Capacidad de detección incipiente de los riesgos y minimización de los efectos de los daños producidos en la seguridad digital.
- Implementación de buenas prácticas en entorno digital.
  - Capacidad de búsqueda y localización de información sobre buenas prácticas en las entidades oficiales de gestión de la ciberseguridad (CCN-CERT o INCIBE).
  - Capacidad de implementar buenas prácticas en el entorno digital, a través del conocimiento de los principales mecanismos de protección (gestión segura de contraseñas, gestión y control de los sistemas antivirus, control de accesos y aplicaciones críticas, etc.).
  - Capacidad de identificación y clasificación de la información que se maneja en entorno digital y aplicación de las medidas necesarias para su protección, que se plasmará en distintas políticas de seguridad informática.

IFCT103: Ciberseguridad: prevención, análisis y respuesta a incidentes de seguridad

49 horas

DESTINATARIOS: Trabajadores con destreza general a nivel informático (manejo de ficheros y carpetas en Windows) y que tengan autorización para crear máquinas virtuales en el equipo que utilicen.

OBJETIVO GENERAL: Conocer y comprender las nociones fundamentales de ciberseguridad que permitan prevenir y dar respuesta a los incidentes de seguridad.

CONTENIDOS FORMATIVOS:

Módulo 1: Ciberseguridad: prevención, análisis y respuesta a incidentes de seguridad – 49 horas

- Conocimiento del Gobierno de Seguridad de una organización.
  - Gobierno de la Seguridad
  - Cumplimiento de las normas de seguridad
- Identificación de las acciones preventivas que se deben planificar para evitar incidentes.
  - Amenazas y análisis de riesgos
- Recolección de evidencias tras un ataque.
  - Identificación de diferentes tipos de ataques e incidentes que pueden darse en una empresa.
  - Utilización de técnicas y recursos para el análisis de datos.
- Creación de un plan de respuesta ante incidentes
  - Respuesta a incidentes de seguridad.
  - Criptografía.
  - Plan de recuperación ante desastres.
- Práctica de hacking ético

IFCT050PO: Gestión de la Seguridad Informática en la Empresa

100 horas

DESTINATARIOS: Trabajadores responsables de informática o con perfil técnico.

OBJETIVO GENERAL: Gestionar la seguridad informática en la empresa.

CONTENIDOS FORMATIVOS:

- INTRODUCCIÓN A LA SEGURIDAD
  - Introducción a la seguridad de información.
  - Modelo de ciclo de vida de la seguridad de la información.
  - Confidencialidad, integridad y disponibilidad. Principios de protección de la seguridad de la información.
  - Políticas de seguridad.
  - Tácticas de ataque.
  - Concepto de hacking.
  - Árbol de ataque.
  - Lista de amenazas para la seguridad de la información.
  - Vulnerabilidades.
  - Vulnerabilidades en sistemas Windows.
  - Vulnerabilidades en aplicaciones multiplataforma.
  - Vulnerabilidades en sistemas Unix y Mac OS.
  - Buenas prácticas y salvaguardas para la seguridad de la red.
  - Recomendaciones para la seguridad de su red.

- POLÍTICAS DE SEGURIDAD.
  - Introducción a las políticas de seguridad.
  - ¿Por qué son importantes las políticas?
  - Qué debe de contener una política de seguridad.
  - Lo que no debe contener una política de seguridad.
  - Cómo conformar una política de seguridad informática.
  - Hacer que se cumplan las decisiones sobre estrategia y políticas.
- AUDITORIA Y NORMATIVA DE SEGURIDAD.
  - Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.
  - Ciclo del sistema de gestión de seguridad de la información.
  - Seguridad de la información
  - Definiciones y clasificación de los activos.
  - Seguridad humana, seguridad física y del entorno.
  - Gestión de comunicaciones y operaciones.
  - Control de accesos.
  - Gestión de continuidad del negocio.
  - Conformidad y legalidad.
- ESTRATEGIAS DE SEGURIDAD.
  - Menor privilegio.
  - Defensa en profundidad.
  - Punto de choque.
  - El eslabón más débil.
  - Postura de fallo seguro.
  - Postura de negación establecida: lo que no está prohibido.
  - Postura de permiso establecido: lo que no está permitido.
  - Participación universal.
  - Diversificación de la defensa.
  - Simplicidad.
- EXPLORACIÓN DE LAS REDES.
  - Exploración de la red.
  - Inventario de una red. Herramientas del reconocimiento.
  - NMAP Y SCANLINE.
  - Reconocimiento. Limitar y explorar.
  - Reconocimiento. Exploración.
  - Reconocimiento. Enumerar.
- ATAQUES REMOTOS Y LOCALES.
  - Clasificación de los ataques.
  - Ataques remotos en UNIX.
  - Ataques remotos sobre servicios inseguros en UNIX.
  - Ataques locales en UNIX.
  - ¿Qué hacer si recibimos un ataque?
- SEGURIDAD EN REDES INALÁMBRICAS
  - Introducción.
  - Introducción al estándar inalámbrico 802.11 – WIFI
  - Topologías.
  - Seguridad en redes Wireless. Redes abiertas.
  - WEP.
  - WEP. Ataques.
  - Otros mecanismos de cifrado.
- CRIPTOGRAFÍA Y CRIPTOANÁLISIS.
  - Criptografía y criptoanálisis: introducción y definición.
  - Cifrado y descifrado.
  - Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.
  - Ejemplo de cifrado: criptografía moderna.
  - Comentarios sobre claves públicas y privadas: sesiones.
- AUTENTICACIÓN.
  - Validación de identificación en redes.
  - Validación de identificación en redes: métodos de autenticación.
  - Validación de identificación basada en clave secreta compartida: protocolo.
  - Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.
  - Validación de identificación usando un centro de distribución de claves.
  - Protocolo de autenticación Kerberos.
  - Validación de identificación de clave pública.
  - Validación de identificación de clave pública: protocolo de interbloqueo.

FECHAS DE IMPARTICIÓN

IFCT149PO **Seguridad en el Comercio Electrónico**	**20 h.**	**Del 11 al 26 de Noviembre** 16:30h a 18:30h de lunes a jueves	
IFCT0024 **Ciberseguridad para usuarios**	**10 h.**	▸ **Del 14 al 18 de Octubre** 9:00h a 11:00h de lunes a viernes	▸ **Del 4 al 11 de Noviembre** 16:30h a 18:30h de lunes a jueves
IFCT104 **Ciberseguridad para Microempresas**	**15 h.**	▸ **Del 21 al 31 de Octubre** 16:30h a 18:30h de lunes a jueves	
IFCT121 **Ciberseguridad. Riesgos y amenazas en la red**	**10 h.**	▸ **Del 7 al 14 de Octubre** 16:30h a 18:30h de lunes a jueves	
IFCT103 **Ciberseguridad: Prevención, análisis y respuesta a incidentes de seguridad.**	**49 h.**	**Del 7 de Oct. al 18 de Nov.** 16:30h a 18:30h de lunes a jueves	
IFCT050PO **Gestión de la Seguridad Informática en la Empresa**	**100 h.**	**Del 23 de Sept. al 18 de Dic.** 16:00h a 18:00h de lunes a jueves	

PARA INSCRIBIRTE RELLENA EL FORMULARIO QUE TIENES EN NUESTRA PÁGINA WEB