

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)
- ✓ Procesador I5 o equivalente
- ✓ 250 Gb de espacio libre en el disco

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

Especialidades Formativas de Ciberseguridad Seleccionadas para impartir:

CÓDIGO	ESPECIALIDAD	HORAS
IFCT135PO	Ciberseguridad para usuarios	10
IFCT104	Ciberseguridad para microempresas.	15
IFCT102	Ciberseguridad en el Teletrabajo	15
ELEM02	Ciberseguridad en Instalaciones Industriales	35
IFCT89	Seguridad en internet y dispositivos móviles	36
IFCT124	Respuesta a incidentes de seguridad	86
IFCT050PO	Gestión de la Seguridad Informática en la Empresa	100

Ver fechas al final del documento

Contenidos Formativos de cada Especialidad

IFCT135PO: 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.

REQUISITOS ESPECÍFICOS:

- ✓ 4 Gb de Memoria RAM

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

CONTENIDOS FORMATIVOS:

- INTRODUCCIÓN A LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN.
 - Conceptos de seguridad en los sistemas.
 - Clasificación de las medidas de seguridad.
 - Requerimientos de seguridad en los sistemas de información.
 - Principales características.
 - Confidencialidad.
 - Integridad.
 - Disponibilidad.
 - Otras características.
 - Tipos de ataques.
- CIBERSEGURIDAD.
 - Concepto de ciberseguridad.
 - Amenazas más frecuentes a los sistemas de información.
 - Tecnologías de seguridad más habituales.
 - Gestión de la seguridad informática.
- SOFTWARE DAÑINO.
 - Conceptos sobre software dañino.
 - Clasificación del software dañino.
 - Amenazas persistentes y avanzadas.
- Ingeniería social y redes sociales.
- SEGURIDAD EN REDES INALÁMBRICAS.
- HERRAMIENTAS DE SEGURIDAD.
 - Medidas de protección.
 - Control de acceso de los usuarios al sistema operativo.
 - Permisos de los usuarios.
 - Registro de usuarios.
 - Autenticación de usuarios.
 - Gestión segura de comunicaciones, carpetas y otros recursos compartidos.
 - Gestión de carpetas compartidas en la red.
 - Tipos de accesos a carpetas compartidas.
 - Compartir impresoras.
 - Protección frente a código malicioso.
 - Antivirus.
 - Cortafuegos (firewall).
 - Antimalware.

IFCT104: Ciberseguridad para microempresas.

15 horas

DESTINATARIOS:

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

REQUISITOS ESPECÍFICOS:

- ✓ 8 Gb de Memoria RAM

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.

IFCT102: Ciberseguridad en el Teletrabajo

15 horas

DESTINATARIOS: Trabajadores que utilicen el ordenador como herramienta de trabajo y tengan pocos conocimientos de seguridad informática, que estén teletrabajando o con la posibilidad de hacerlo en algún momento.

No recomendable para responsables de informática o perfiles más técnicos.

REQUISITOS ESPECÍFICOS:

- ✓ 8 Gb de Memoria RAM

OBJETIVO GENERAL: Conocer y comprender las amenazas y circunstancias que pueden derivar en incidentes de seguridad en situación de teletrabajo.

CONTENIDOS FORMATIVOS:

Módulo 1: Ciberseguridad en el Trabajo – 15 horas

- Definición de los métodos de acceso remoto.
- Contextualización del teletrabajo
- Identificación de las principales amenazas para los terminales de teletrabajo.
- Identificación de las principales medidas para prevenir amenazas. Recopilación de evidencias.

- Seguridad en el acceso en remoto.
- Seguridad en los equipos de trabajo.
- Seguridad en dispositivos móviles.
- Técnicas y recursos para el análisis de los datos.
- Protección de datos en los terminales de teletrabajo.
- Utilización de Copias de seguridad en dispositivos de teletrabajo.

ELEM02: Ciberseguridad en Instalaciones Industriales

35 horas

DESTINATARIOS: Trabajadores responsables de informática o con perfil técnico.

REQUISITOS ESPECÍFICOS:

- ✓ 8 Gb de Memoria RAM

OBJETIVO GENERAL: Confeccionar y gestionar redes industriales a través de recursos tecnológicos, estableciendo conexiones remotas seguras que doten de seguridad a las comunicaciones entre los diferentes equipos que componen una instalación automatizada, en el contexto de la Industria 4.0.

CONTENIDOS FORMATIVOS:

Módulo 1: Ciberseguridad en instalaciones industriales – 35 horas

- Identificación de las características de la industria 4.0:
 - Redes industriales.
 - Entornos IT y OT.
 - Datos relevantes.
 - Interacción entre máquinas e instalaciones.
 - Conexiones remotas.
- Confección y gestión de redes industriales seguras:
 - Conceptos generales en ciberseguridad industrial.
 - Vulnerabilidades y amenazas que se pueden sufrir en entornos industriales
 - Ataques hacker en una red OT
 - Ataques hacker en una infraestructura crítica
 - Contramedidas para fortificar las redes y protocolos industriales.
 - Recomendaciones y consejos prácticos que permitan fortificar los sistemas y redes.
- Aplicación de la normativa y estándares en ciberseguridad:
 - Noción y objetivos de los estándares de ciberseguridad
 - Principales normas y estándares relacionados:
 - ISO/IEC 27001 y 27002
 - NERC
 - NIST
 - ISO 15408
 - ISO/IEC 27032
 - Estándares europeos en ciberseguridad
 - Estrategia de la Comisión Europea para el mercado único digital
 - Reglamento General de Protección de Datos
 - Directiva NIS
 - Asociación Española de Normalización (UNE)
 - Políticas de seguridad efectivas.
 - Noción de políticas de seguridad
 - Ámbitos de actuación de las políticas de seguridad
 - Implementación de una política de seguridad efectiva.

IFCT89: Seguridad en internet y dispositivos móviles

36 horas

DESTINATARIOS: Trabajadores que utilicen el ordenador como herramienta de trabajo y tengan pocos conocimientos de seguridad informática, que estén teletrabajando o con la posibilidad de hacerlo en algún momento.

No recomendable para responsables de informática o perfiles más técnicos.

REQUISITOS ESPECÍFICOS:

- ✓ Conexión de banda ancha a internet.

OBJETIVO GENERAL: Obtener los conocimientos adecuados para identificar los elementos, dentro de una red o dispositivos móviles, susceptibles de ser atacados, así como los diferentes tipos de ataque que pueden sufrir, como la omnipresencia de la tecnología en nuestro entorno afecta a nuestra privacidad o qué medidas de actuación se pueden acometer para minimizar el riesgo.

CONTENIDOS FORMATIVOS:

Módulo 1: 2 horas

- INTRODUCCIÓN:
 - Comprensión de la ciberseguridad.
 - Los riesgos, tipos y alcance.
 - Vectores de ataque tipos e impacto.
 - Medidas de prevención y actuación ante posibles ataques
 - Revisión del contexto futuro de la ciberseguridad.
 - Actividades de autoevaluación para fortalecer los conocimientos adquiridos por el alumno.

Módulo 2: 4 horas

- CIBERSEGURIDAD. CONCEPTOS BÁSICOS
 - ¿Qué es la Ciberseguridad?.
 - ¿Por qué aplicar la ciberseguridad?
 - ¿Cómo impacta la ciberseguridad en Internet y los dispositivos móviles?
 - Actividad de evaluación de los conocimientos adquiridos por el alumno.

Módulo 3: 16 horas

- RIESGOS, TIPOS Y VECTORES DE ATAQUE
 - Qué es un riesgo y los elementos de un sistema susceptibles de ser protegidos.
 - Tipos de riesgos.
 - Conceptos básicos de vectores de ataque.
 - Tipos de vectores de ataque (Phishing, malware, social engineering y medidas de actuación).
 - Vectores de ataque: medidas de prevención y actuación generales.
 - Vectores de ataque: medidas de prevención y generales en la gestión de redes conectadas o no a la Red: Cortafuegos, segmentación, monitorización, detección, registro y encriptación.
 - Vectores de ataque: medidas de actuación específicas para los dispositivos móviles.
 - Actividad de evaluación de los conocimientos adquiridos por el alumno.

Módulo 4: 14 horas

- IMPLICACIONES EN LA CIBERSEGURIDAD DE LA EVOLUCIÓN DE LAS AMENAZAS ACTUALES Y DE LA ADOPCIÓN DE NUEVAS TECNOLOGÍAS
 - Gestión de ingentes cantidades de datos en sistemas cada vez más complejos.
 - La Inteligencia Artificial (IA) será un componente central de todos los sistemas de ciberseguridad.
 - La industria de la ciberseguridad se centrará en las amenazas de la guerra cibernética.
 - Habrá más crackers con los que lidiar.
 - Desarrollo del talento en ciberseguridad se vuelve esencial.
 - La tecnología heredada seguirá siendo un problema.
- Internet de las cosas (IoT).
- Supercomputación (Computación cuántica).
- Mayor uso de las redes autoadaptables.
- Generalización del uso de los Gestores de Seguridad para el Acceso a la Nube (Cloud Access Security Broker - CASB).
- Análisis de amenazas internas mediante sistemas UEBA (User and Entity Behavior Analytics).
- Implantación generalizada de autenticación multifactor física en entornos críticos.
- El Coronavirus (COVID-19) lo ha cambiado todo (Teletrabajo y la ciberresiliencia).
- Actividad de evaluación de los conocimientos adquiridos por el alumno.

IFCT124: Respuesta a incidentes de seguridad

86 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.

REQUISITOS ESPECÍFICOS:

- ✓ 8 Gb de Memoria RAM

OBJETIVO GENERAL: Identificar las características de los ataques informáticos, programar herramientas de detección, y reaccionar para detener el ataque (contener) y recuperar el funcionamiento de los procesos de negocio.

CONTENIDOS FORMATIVOS:

Módulo 1: 10 horas

- GESTIÓN DE RESPUESTA A INCIDENTES

- Descripción de un equipo de respuesta a incidentes
 - o Estructura organizativa
 - o Distribución de funciones y operación
- Organización de un equipo de respuesta a incidentes
 - o Creación de procedimientos, políticas y planes para respuesta a incidentes
- Identificación de servicios
 - o Servicios Reactivos
 - o Servicios Proactivos
 - o Gestión de la Ciberseguridad
- Relación de las fases en la respuesta a incidentes
 - o Detección del incidente

- o Análisis de datos e identificación del incidente
- o Contención y erradicación del incidente
- o Recuperación del incidente
- o Notificación del incidente por regulación
- Localización y contacto de los equipos de coordinación y respuesta a incidentes de ciberseguridad: CSIRTs
 - o Agencia de Ciberseguridad de Cataluña: modelos de interrelación y servicio
 - o Foros internacionales: FIRST, TERENA, Trusted Introducer
 - o Agentes nacionales: INCIBE, CCN-CERT, CNPIC
 - o Asociación nacional de equipos de respuesta a incidentes: CSIRT.ES

Módulo 2: 40 horas

- RECOGIDA DE DATOS Y GESTIÓN DE ALARMAS
 - Recopilación de datos significativos
 - Identificación de las fuentes de datos internas de un centro de operaciones de seguridad, mediante herramientas de monitorización de red y sistemas informáticos.
 - Identificación de fuentes de datos externas: Análisis de inteligencia del ataque (investigación, Threat Intelligence) e Inteligencia en fuentes abiertas (OSINT)
 - Recogida de evidencias digitales: búsquedas ciegas, preservación de la confidencialidad de los datos, preservación de la cadena de custodia y gestión de copias de seguridad.
 - Análisis de datos de intrusiones
 - Evaluación del impacto potencial de la intrusión y determinación del nivel de alerta correspondiente.
- Detección de intrusiones (IDS)
- Protección contra intrusiones (IPS)
- Gestión de datos
- Análisis forense: conocer las buenas prácticas de recogida de evidencias digitales, para mantener su validez en caso de realizarse una denuncia por los daños sufridos.
- Correlación de datos y generación de alarmas.
 - Gestión de logs de los diferentes sistemas y servicios
 - Sistemas de gestión de eventos de seguridad (SIEM)
 - Homogeneización de los datos. Filtrado y normalización de las fuentes.
 - Tratamiento de las alarmas: automatización de respuestas y comunicación del escenario del incidente.
 - Otras herramientas: Orquestación y Automatización (SOAR), Visualización de datos y Generación automática de informes.

Módulo 3: 24 horas

- RECOMENDACIONES DE BUENAS PRÁCTICAS Y MARCO REGULADOR
 - Interpretación, selección y aplicación de las herramientas y los estándares internacionales y nacionales de detección y respuesta a incidentes de ciberseguridad
 - MITRE ATT&CK
 - SIGMA (Security Management Services)
 - SIEM (OSSIM)
 - IDS (SNORT)
 - RTIR
 - OTRS
 - LUCIA
 - Clasificación de normativas de protección de datos personales
- RGPD de la UE (Reglamento General de Protección de Datos Europeo)
- LOPD-GDD (Ley Orgánica de protección de datos y garantía de derechos digitales española)
- Adecuación al Esquema Nacional de Seguridad
 - Metodología de análisis y gestión de los riesgos (MAGERIT)
 - Herramientas de análisis, evaluación y gestión de riesgos (PILAR)
- Aplicación de la Directiva NIS
 - Proveedores de servicios esenciales
 - Impacto en las empresas suministradoras
- Definición de los principios de la ética profesional
 - En la respuesta a incidentes
 - En la captura y custodia de evidencias

Módulo 4: Desarrollo de una respuesta a un incidente de ciberseguridad – 12 horas

- Extracción de información:
 - De una fuente de datos de tráfico en una red corporativa.
 - De fuentes OSINT
 - Selección de los parámetros para la detección y generación de alarmas relevantes.
- Gestión de la respuesta a un incidente de seguridad informática.
- Automatización de los procesos de detección de intrusiones:
 - Integración de fuentes de datos en una herramienta SIEM
 - Identificación de fuentes de cooperación para optimización de la respuesta a un incidente de ciberseguridad.
 - Planificación de actuaciones y procedimientos
 - Resolución de un ciber-incidente

IFCT050PO: Gestión de la Seguridad Informática en la Empresa

100 horas

DESTINATARIOS: Trabajadores responsables de informática o con perfil técnico.

REQUISITOS ESPECÍFICOS:

- ✓ 8 Gb de Memoria RAM

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.
- **CRİPTOGRAFÍA Y CRİPTOANÁLISIS.**
 - 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

(La semana del 5 al 9 de diciembre será "no lectiva")

IFCT135PO Ciberseguridad para usuarios	10 h.	► Del 12 al 16 de Septiembre	► Del 19 al 26 de Septiembre
		► Del 3 al 7 de Octubre	► Del 21 al 28 de Noviembre
		9:00h a 11:00h de lunes a viernes	16:30h a 18:30h de lunes a jueves
IFCT104 Ciberseguridad para Microempresas	15 h.	Del 24 de Octubre al 8 de Noviembre 16:30h a 18:30h de lunes a jueves	
IFCT102 Ciberseguridad en el Teletrabajo	15 h.	Del 9 al 18 de Noviembre 9:00h a 11:00h de lunes a viernes	
ELEM02 Ciberseguridad en Instalaciones Industriales	35 h.	Del 19 de Septiembre al 19 de Octubre 16:30h a 18:30h de lunes a jueves	
IFCT89 Seguridad en Internet y dispositivos móviles	36 h.	Del 14 de Noviembre al 20 de Diciembre 16:30h a 18:30h de lunes a jueves	
IFCT124 Respuesta a incidentes de seguridad	86 h.	Del 12 de Septiembre al 29 de Noviembre 16:30h a 18:30h de lunes a jueves	
IFCT050PO Gestión de la Seguridad Informática en la Empresa	100 h.	Del 19 de Septiembre al 22 de Diciembre 16:30h a 18:30h de lunes a jueves	

**PARA INSCRIBIRTE RELLENA EL [FORMULARIO](#) QUE TIENES
EN NUESTRA PÁGINA WEB**