Junta de Castilla y León

RETO CASTILLA Y LEÓN
CIBERSEGURA

FUNDACIÓN ANCLAJE Y FORMACIÓN CASTILLA Y LEÓN

CURSOS CIBERSEGURIDAD

Destinatarios: Prioritariamente trabajadores de pequeñas y medianas empresas y autónomos

1. Ciberseguridad para usuarios (10 horas)
2. Ciberseguridad en Instalaciones Industriales (35 horas)
3. Seguridad Informática y Firma Digital (50 horas)
4. Ciberseguridad y Reglamento General de Protección de Datos (RGPD) aplicado al Comercio Electrónico (40 horas)
5. Gestión de la Ciberseguridad en Pymes. Comercio Electrónico Seguro (50 horas)
6. Gestión de la Seguridad Informática en la Empresa (100 horas)

MODALIDAD:

Plataforma online presencial

DURACIÓN:

2 horas y media

HORARIO:

TARDES: de Lunes a Jueves

*Excepto fiestas nacionales

De 16:00 a 18:30 h.

INSCRIPCIONES

Rellenar FORMULARIO en la página de la Fundación:

www.fafecyl.es

983 32 45 40

direccion.fafecyl@jcyl.es

1 Ciberseguridad para usuarios

10 horas

Fecha de Impartición: Opciones: del 6 al 9 de Septiembre o del 25 al 28 de Octubre

- **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.
    - o Principales características.
    - o Confidencialidad.
    - o Integridad.
    - o Disponibilidad.
    - o Otras características.
    - o 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.
    - o Permisos de los usuarios.
    - o Registro de usuarios.
    - o Autentificación de usuarios.
  - Gestión segura de comunicaciones, carpetas y otros recursos compartidos.
    - o Gestión de carpetas compartidas en la red.
    - o Tipos de accesos a carpetas compartidas.
    - o Compartir impresoras.
  - Protección frente a código malicioso.
    - o Antivirus.
    - o Cortafuegos (firewall).
    - o Antimalware.

2 Ciberseguridad en Instalaciones Industriales

35 horas

Fecha de Impartición: del 6 al 28 de Septiembre

- **Identificación de las características de la industria 4.0:**
  - Redes industriales.
  - Entornos IT y OT.
  - Datos relevantes.
  - Interacción entre maquinas 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:
    - o ISO/IEC 27001 y 27002
    - o NERC
    - o NIST
    - o ISO 15408
    - o ISO/IEC 27032
  - Estándares europeos en ciberseguridad
    - o Estrategia de la Comisión Europea para el mercado único digital
    - o Reglamento General de Protección de Datos
    - o Directiva NIS
  - Asociación Española de Normalización (UNE)
  - Políticas de seguridad efectivas.
    - o Noción de políticas de seguridad
    - o Ámbitos de actuación de las políticas de seguridad
    - o Implementación de una política de seguridad efectiva.

3 Seguridad Informática y Firma Digital

50 horas

Fecha de Impartición: del 16 de Septiembre al 21 de Octubre

- **Firma electrónica / firma digital.**

- **Tipos de certificados:**
  - Certificados de Servidor (SSL: Capa de zócalos seguro)
  - Microsoft Server Gated Cryptography Certificates (Certificados de CGC-una extensión del protocolo SSL-ofrecida por Microsoft).
  - Certificados Canalizadores.
  - Certificados de Correo Electrónico.
  - Certificados de Valoración de páginas WEB.
  - Certificados de Sello, Fecha y Hora

- **Sistemas de seguridad en la empresa.**
  - Sistemas pasivos y reactivos.
  - Suplantación o spoofing:
    - o SET (Secure Electronic Transaction).
    - o PGP (Enterprise Security).
    - o SSL (Secure Socket Layout).

4 Ciberseguridad y Reglamento General de Protección de Datos (RGPD) aplicado al Comercio Electrónico

40 horas

Fecha de Impartición: del 13 de Septiembre al 7 de Octubre

MÓDULO 1: 30 horas

Reglamento General de Protección de Datos (RGPD) en proyectos de comercio electrónico

- **Determinación de los aspectos clave del comercio electrónico (e-commerce):**
  - Aproximación al nuevo paradigma del entorno digital
  - Conceptos básicos del comercio electrónico
  - Identificación de las posibilidades y aplicaciones prácticas del comercio electrónico
  - Aplicación de las garantías legales en proyecto de e- commerce.
  - Identificación de las principales plataformas tecnológicas para desarrollar un ecommerce.

- **Identificación de los elementos necesarios para afrontar con garantías la adaptación al Reglamento General de Protección de Datos en proyectos de ecommerce.**
  - Marco jurídico aplicable: principales novedades en el ámbito legislativo.
  - Conceptos teóricos básicos de la normativa protectora de datos de carácter personal aplicado al comercio electrónico: datos de carácter personal; tratamiento de datos; figuras del tratamiento de datos; tipos de tratamiento de datos; categoría de datos; transferencias de datos (internacionales/ transfronterizas).
  - Tratamiento de los datos conforme a las bases de legitimación: el consentimiento como elemento clave.
  - Obligaciones del responsable del tratamiento.
  - Obligaciones del encargado del tratamiento.

4 Ciberseguridad y Reglamento General de Protección de Datos (RGPD) aplicado al Comercio Electrónico

40 horas

- **Comprensión de los aspectos legales básicos que tienen que ser respetados por un servicio de venta online**
  - Ley de Servicios de la Sociedad de la Información (LSSI): ámbito de aplicación, principales obligaciones para plataformas de servicios online y régimen sancionador
  - Régimen jurídico de las comunicaciones comerciales, ofertas y concursos por vía electrónica.
  - Uso de cookies y tecnologías similares: tipología y obligaciones
  - Contratos por vía electrónica: obligaciones previas e información posterior a la contratación.
  - Terceros de confianza: servicios de confianza electrónica.

- **Exposición de las obligaciones en materia de consumidores y usuarios.**
  - Información previa a la celebración del contrato
  - Factura electrónica
  - Entrega de los bienes
  - Información post-contractual
  - Derecho de desistimiento

4 Ciberseguridad y Reglamento General de Protección de Datos (RGPD) aplicado al Comercio Electrónico

40 horas

MÓDULO 2: 10 horas — Ciberseguridad en el Comercio Electrónico

- **Identificación de las ciberamenazas y formas de fomentar la ciberseguridad en el comercio electrónico.**
  - Principales riesgos, amenazas y vulnerabilidades
  - Análisis de las Medidas de protección
  - Buenas prácticas para mejorar la confianza de los clientes

- **Determinación de las medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado.**
  - Necesidad de llevar a cabo un análisis de amenazas y riesgos potenciales
  - Evaluaciones de impacto en materia de protección de datos
  - Plan de acción para tratar los riesgos detectados

- **Actuación ante un incidente de seguridad.**
  - Detección y comunicación en punto de notificación establecido
  - Fases para la gestión y tratamiento de incidentes de seguridad
  - Obligación de notificación a la autoridad de control y usuarios en caso de que el incidente afecte a datos personales
  - Ejemplos de incidentes de seguridad

5 Gestión de la Ciberseguridad en Pymes. Comercio Electrónico Seguro

50 horas

Fecha de Impartición: del 2 de Noviembre al 9 de Diciembre

MÓDULO 1: 20 horas Introducción a la Ciberseguridad

- **Identificación de los conceptos básicos de ciberseguridad y su relación con la seguridad**
  - Definición y alcance de la ciberseguridad
  - Áreas de actuación de la ciberseguridad
  - Ubicación de la ciberseguridad
  - Dimensiones de la seguridad y garantías que ofrece
  - Implementación de las dimensiones
  - Protección de la información

- **Relación entre las amenazas y las vulnerabilidades reconociendo sus efectos en los sistemas**
  - Ingeniería social
  - Vulnerabilidades en la autenticación
  - Malware y botnets
  - Seguridad en el perímetro de las redes
  - Riesgos de seguridad
  - Incidentes de seguridad

- **Identificación de los mecanismos de defensa a implementar en las redes privadas**
  - Defensa en profundidad y la DMZ
  - Antimalware
  - Contraseñas
  - Control de acceso
  - Controles para definir una red segura
  - Sistemas de detección de ataques
  - Recuperación de los sistemas ante un ciberataque

- **Utilidad de la correlación de eventos en la prevención e investigación de incidentes**
  - Eventos y tipos
  - Eventos de los sistemas de seguridad
  - Criticidad de los eventos
  - Tratamiento de los eventos para su automatización
  - Soluciones de automatización. El SIEM

- **Identificación de las medidas de seguridad en las redes inalámbricas y dispositivos móviles**
  - La conexión inalámbrica y las redes
  - Configuración de seguridad de las WLAN
  - Medidas de seguridad en el router
  - Amenazas en los terminales móviles

5 Gestión de la Ciberseguridad en Pymes. Comercio Electrónico Seguro

50 horas

- **Caracterización de los mecanismos de protección de la información**
  - Fuga de la información
  - Gestión de la fuga de información
  - Métodos de copia de seguridad
  - Restauración de los datos

- **Reconocimiento de los sistemas biométricos y aplicaciones**
  - Técnicas biométricas
  - Aplicaciones de la biometría
  - Gestión de riesgos en biometría

- **Identificación de los servicios que se implementan en la nube**
  - Cloud computing
  - Seguridad en la nube
  - Servicios de seguridad en la nube

- **Caracterización de los diferentes tipos de ciberataques**
  - Categorías de los ciberataques
  - Ataques para obtener información
  - Ataques a nivel de red
  - Ataques de monitorización
  - Ataques de autenticación
  - Ataques de denegación de servicio

- **Introducción de la ciberseguridad en la empresa**
  - Seguridad en la empresa
  - Causas de los ataques en la empresa
  - Revisión de ciberseguridad en la empresa
  - Pilares de una estrategia de ciberseguridad
  - Roles en ciberseguridad
  - Controles de seguridad a establecer en una organización

- **Identificación del usuario como elemento de ciberseguridad en la empresa**
  - Rol del usuario en el puesto de trabajo
  - Protección del puesto de trabajo
  - Acceso remoto y teletrabajo
  - Escritorio virtual

5 Gestión de la Ciberseguridad en Pymes. Comercio Electrónico Seguro

50 horas

MÓDULO 2: 30 horas — Aplicación de la Ciberseguridad en las PYMES

- **Detección de necesidades de protección y seguridad en las empresas**
  - Clasificación de la información empresarial
  - Medidas de protección de la información
  - Almacenamiento seguro de la información
  - Eliminación de los datos. Borrado seguro
  - Conservación de la información
  - Almacenamiento extraíble

- **Desarrollo de planes y políticas de seguridad en una empresa**
  - Plan director de seguridad
  - Políticas de seguridad dirigidas a los componentes de la empresa
  - Normas y procedimientos técnicos

- **Utilidad de los planes de continuidad de negocio en la empresa**
  - Análisis y gestión de riesgos
  - Plan de continuidad de negocio
  - Plan de contingencia
  - Auditorías de seguridad

- **Necesidad de un plan de recuperación de desastres en la empresa**
  - En plan de recuperación de desastres
  - Guía de desarrollo de un plan de recuperación de desastres

- **Introducción a la seguridad en el comercio electrónico**
  - Identidad digital y reputación empresarial
  - Cliente online y su protección
  - Redes sociales y la empresa
  - Fraude online
  - Protección de la web

- **Aplicación de medidas de ciberseguridad en redes inalámbricas y dispositivos móviles**
  - Formas de ataque y métodos de seguridad en las redes inalámbricas
  - Sistemas de gestión de dispositivos móviles de la empresa
  - Estrategia BYOD

- **Caracterización de la tecnología IoT en la empresa 10**
  - IoT en la empresa en la actualidad y en el futuro.
  - Riesgos de seguridad
  - Recomendaciones de seguridad

6 Gestión de la Seguridad Informática en la Empresa — 100 horas

Fecha de Impartición: del 30 de Septiembre al 16 de Diciembre

- **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.

- **Auditoría 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.

6 Gestión de la Seguridad Informática en la Empresa

100 horas

- **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.