



Financiado por  
la Unión Europea  
NextGenerationEU



Plan de Recuperación,  
Transformación y Resiliencia



JUNTA DE  
EXTREMADURA

Cámara  
Cáceres

# ANEXO III

CATÁLOGO DE ESPECIALIDADES FORMATIVAS Y MÓDULOS



## **ESPECIALIDAD FORMATIVA - POSICIONAMIENTO EN LA WEB PARA EL EMPRENDIMIENTO.**

### **MÓDULO 1 - CÓMO POSICIONAR PÁGINAS WEB CUANDO SE EMPRENDE UN NEGOCIO**

#### **1.1. Posicionamiento en buscadores de empresas de nueva creación.**

##### **1.1.1. Buscadores y directorios.**

##### **1.1.2. Relevancia de los resultados.**

##### **1.1.3. Tráfico cualificado.**

##### **1.1.4. Técnicas penalizables de posicionamiento.**

#### **1.2. Palabras clave.**

##### **1.2.1. La importancia de las palabras clave.**

##### **1.2.2. Analizar el tráfico que recibe el sitio web.**

#### **1.3. ¿Dónde utilizar las palabras clave?**

##### **1.3.1. Dominio y URL.**

##### **1.3.2. El título de la página. Encabezados y texto de la página.**

##### **1.3.3. Las etiquetas meta.**

### **MÓDULO 2 - ENLACES Y MARCADORES SOCIALES**

#### **2.1. Enlaces (I).**

##### **2.1.1. Enlaces internos.**

##### **2.1.2. Conseguir enlaces externos. Alta en directorios.**

#### **2.2. Enlaces (II).**

##### **2.2.1. Marcadores sociales. Intercambio de enlaces.**

##### **2.2.2. Enlaces que penalizan.**

##### **2.2.3. Mapa del sitio (Sitemap).**

#### **2.3. Contenidos difíciles de posicionar cuando se crea una empresa.**

##### **2.3.1. Imágenes.**

##### **2.3.2. Flash. Alternativas actuales**

##### **2.3.3. El archivo robots.txt .**

### **MÓDULO 3 - EL EMPRENDEDOR COMO ANALISTA WEB: CÓMO DISEÑAR UNA WEB Y MEDIR EL TRÁFICO CON GOOGLE ANALYTICS**

#### **3.1. Diseño y Usabilidad de la página Web del nuevo negocio Online.**

##### **3.1.1. Pasos previos al diseño web: dominio, hosting, etc.**

##### **3.1.2. Cómo elegir un proveedor para un diseño web a medida.**

##### **3.1.3. Prácticos: Aplicaciones de software disponibles.**

##### **3.1.4. Caso real: Virtual Shop.**

##### **3.1.5. Estructura del negocio online: BackOffice y Frontoffice.**

##### **3.1.6. Caso Real: Concepción de un negocio online.**

##### **3.1.7. Caso práctico resuelto.**

#### **3.2. Gestión de Blog Corporativo.**

##### **3.2.1. Cómo adecuar los contenidos para fidelizar al cliente.**

##### **3.2.2. El Blog en la estrategia online: Facebook Connect, etc.**

##### **3.2.3. Cómo crear un blog con Blogger, paso a paso.**

##### **3.2.4. Cómo crear un blog con Wordpress, paso a paso.**

##### **3.2.5. Caso práctico resuelto.**

### **MÓDULO 4- MARKETING 3.0**

#### **4.1. Marketing 3.0.**

##### **4.1.1. Value Management: Prepararse para el Marketing 3.0.**

##### **4.1.2. Co-Creation: El cliente como creador del producto.**



- 4.1.3 Comunidades 3.0: Comunicación Cliente-Cliente.
- 4.1.4. Creación de campañas de Comunicación en la Web Semántica.
- 4.1.5. Ejemplo Real: Nuestra marca y su ADN social.
- 4.1.6. Ejercicio Práctico: Crear una estrategia de Marketing dinámica 3.0

## **ESPECIALIDAD FORMATIVA: SEGURIDAD INFORMÁTICA Y FIRMA DIGITAL**

### **MÓDULO 1 - FIRMA ELECTRÓNICA / FIRMA DIGITAL**

- 1. Introducción a la Firma Electrónica y Firma Digital
  - 1.1 Definición de firma electrónica y firma digital.
  - 1.2 Diferencias entre firma electrónica y firma digital.
  - 1.3 Importancia y aplicaciones en la era digital.
    - 1.1 Marco Legal y Normativo
      - 1.1.1 Legislación internacional y nacional relacionada con la firma electrónica y firma digital.
      - 1.1.2 Requisitos legales para la validez de una firma electrónica y firma digital.
    - 1.2 Tecnologías y Métodos de Implementación
      - 1.2.1 Tecnologías subyacentes en la firma electrónica y firma digital.
      - 1.2.2 Métodos de implementación de firma electrónica y firma digital.
      - 1.2.3 Certificados digitales y autoridades de certificación.
    - 1.3 Seguridad y Confianza en la Firma Digital
      - 1.3.1 Principios de seguridad en la firma digital.
      - 1.3.2 Amenazas y riesgos asociados a la firma digital.
      - 1.3.3 Estrategias para garantizar la confianza en la firma digital.
    - 1.4 Aplicaciones y Casos de Uso
      - 1.4.1 Uso de la firma electrónica y firma digital en transacciones financieras.
      - 1.4.2 Firma digital en contratos y documentos legales.
      - 1.4.3 Integración de la firma digital en procesos empresariales y administrativos.
    - 1.5 Implementación Práctica
      - 1.5.1 Configuración y uso de herramientas para la generación de firma digital.
      - 1.5.2 Proceso de firma digital en documentos electrónicos.
      - 1.5.3 Verificación de la autenticidad de una firma digital.
    - 1.6 Consideraciones Éticas y Sociales
      - 1.6.1 Impacto de la firma digital en la privacidad y seguridad de los datos.
      - 1.6.2 Aspectos éticos de la firma electrónica y firma digital.
      - 1.6.3 Implicaciones sociales de la adopción masiva de la firma digital.
    - 1.7 Futuras Tendencias y Desarrollos
      - 1.7.1 Avances tecnológicos en el campo de la firma electrónica y firma digital.
      - 1.7.2 Tendencias emergentes en regulaciones y estándares de firma digital.
      - 1.7.3 Posibles aplicaciones futuras y su impacto en la sociedad y los negocios.
    - 1.8 Evaluación y Certificación
      - 1.8.1 Evaluaciones prácticas y teóricas para medir el conocimiento adquirido.
      - 1.8.2 Certificación de competencias en firma electrónica y firma digital.
    - 1.9 Conclusiones y Recomendaciones
      - 1.9.1 Resumen de los principales conceptos aprendidos.
      - 1.9.2 Recomendaciones para la implementación segura y efectiva de la firma electrónica y firma digital.
      - 1.9.3 Reflexión sobre el futuro de la firma digital en un mundo cada vez más digitalizado.

### **MÓDULO 2 - TIPOS DE CERTIFICADOS**



## 2. Tipos de certificados:

- 2.1. Certificados de Servidor (SSL: Capa de zócalos seguro)
- 2.2. Microsoft Server Gated Cryptography Certificates (Certificados de CGC-una extensión del protocolo SSL- ofrecida por Microsoft).

- 2.3. Certificados Canalizadores.
- 2.4. Certificados de Correo Electrónico.
- 2.5. Certificados de Valoración de páginas WEB.
- 2.6. Certificados de Sello, Fecha y Hora

## MÓDULO 3 - SISTEMAS DE SEGURIDAD EN LA EMPRESA

### 3. Sistemas de seguridad en la empresa.

- 3.1. Sistemas pasivos y reactivos.
- 3.2. Suplantación o spoofing:
  - 3.2.1. SET (Secure Electronic Transaction).
  - 3.2.2. PGP (Enterprise Security).
  - 3.2.3. SSL (Secure Socket Layout).

## **ESPECIALIDAD FORMATIVA: GESTION DE LA SEGURIDAD INFORMÁTICA EN LA EMPRESA**

### MÓDULO 1 - INTRODUCCIÓN A LA SEGURIDAD

#### 1. INTRODUCCIÓN A LA SEGURIDAD

- 1.1. Introducción a la seguridad de información.
- 1.2. Modelo de ciclo de vida de la seguridad de la información.
- 1.3. Confidencialidad, integridad y disponibilidad. Principios de protección de la seguridad de la información.
- 1.4. Políticas de seguridad.
- 1.5. Tácticas de ataque.
- 1.6. Concepto de hacking.
- 1.7. Árbol de ataque.
- 1.8. Lista de amenazas para la seguridad de la información.
- 1.9. Vulnerabilidades.
- 1.10. Vulnerabilidades en sistemas Windows.
- 1.11. Vulnerabilidades en aplicaciones multiplataforma.
- 1.12. Vulnerabilidades en sistemas Unix y Mac OS.
- 1.13. Buenas prácticas y salvaguardas para la seguridad de la red.
- 1.14. Recomendaciones para la seguridad de su red

### MÓDULO 2 - POLÍTICAS DE SEGURIDAD

- 2.1. Introducción a las políticas de seguridad.
- 2.2. ¿Por qué son importantes las políticas?
- 2.3. Qué debe de contener una política de seguridad.
- 2.4. Lo que no debe contener una política de seguridad.
- 2.5. Cómo conformar una política de seguridad informática.
- 2.6. Hacer que se cumplan las decisiones sobre estrategia y políticas.

### MÓDULO 3 - AUDITORIA Y NORMATIVA DE SEGURIDAD

- 3.1. Introducción a la auditoría de seguridad de la información y a los sistemas de gestión de seguridad de la información.
- 3.2. Ciclo del sistema de gestión de seguridad de la información.
- 3.3. Seguridad de la información. 3.4. Definiciones y clasificación de los activos.
- 3.5. Seguridad humana, seguridad física y del entorno.



- 3.6. Gestión de comunicaciones y operaciones.
- 3.7. Control de accesos.
- 3.8. Gestión de continuidad del negocio.
- 3.9. Conformidad y legalidad.

#### MÓDULO 4 - ESTRATEGIAS DE SEGURIDAD

- 4.1. Menor privilegio.
- 4.2. Defensa en profundidad.
- 4.3. Punto de choque.
- 4.4. El eslabón más débil.
- 4.5. Postura de fallo seguro.
- 4.6. Postura de negación establecida: lo que no está prohibido.
- 4.7. Postura de permiso establecido: lo que no está permitido.
- 4.8. Participación universal.
- 4.9. Diversificación de la defensa.
- 4.10. Simplicidad.

#### MÓDULO 5 - EXPLORACIÓN DE LAS REDES

- 5.1. Exploración de la red.
- 5.2. Inventario de una red. Herramientas del reconocimiento.
- 5.3. NMAP Y SCANLINE.
- 5.4. Reconocimiento. Limitar y explorar.
- 5.5. Reconocimiento. Exploración.
- 5.6. Reconocimiento. Enumerar.

#### MÓDULO 6 - ATAQUES REMOTOS Y LOCALES

- 6.1. Clasificación de los ataques.
- 6.2. Ataques remotos en UNIX.
- 6.3. Ataques remotos sobre servicios inseguros en UNIX.
- 6.4. Ataques locales en UNIX.
- 6.5. ¿Qué hacer si recibimos un ataque?

#### MÓDULO 7 - SEGURIDAD EN REDES INALÁMBRICAS

- 7.1. Introducción.
- 7.2. Introducción al estándar inalámbrico 802.11 – WIFI
- 7.3. Topologías.
- 7.4. Seguridad en redes Wireless. Redes abiertas.
- 7.5. WEP.
- 7.6. WEP. Ataques.
- 7.7. Otros mecanismos de cifrado.

#### MÓDULO 8 - CRIPTOGRAFÍA Y CRIPTOANÁLISIS

- 8.1. Criptografía y criptoanálisis: introducción y definición.
- 8.2. Cifrado y descifrado.
- 8.3. Ejemplo de cifrado: relleno de una sola vez y criptografía clásica.
- 8.4. Ejemplo de cifrado: criptografía moderna.
- 8.5. Comentarios sobre claves públicas y privadas: sesiones.

#### MÓDULO 9 - AUTENTICACIÓN

- 9.1. Validación de identificación en redes.
- 9.2. Validación de identificación en redes: métodos de autenticación.
- 9.3. Validación de identificación basada en clave secreta compartida: protocolo.
- 9.4. Establecimiento de una clave compartida: intercambio de claves Diffie-Hellman.



- 9.5. Validación de identificación usando un centro de distribución de claves.
- 9.6. Protocolo de autenticación Kerberos.
- 9.7. Validación de identificación de clave pública.
- 9.8. Validación de identificación de clave pública: protocolo de interbloqueo.

## **ESPECIALIDAD FORMATIVA: INTERNET SEGURO**

### **MÓDULO 1 - INTRODUCCIÓN Y ANTIVIRUS**

#### **1. INTRODUCCIÓN Y ANTIVIRUS**

- 1.1. Introducción a la seguridad.
- 1.2. Introducción a la seguridad.
- 1.3. Antivirus. Definición de virus. Tipos de virus
- 1.4. Previo a instalar ningún programa.
- 1.5. Antivirus. Descarga e instalación.
- 1.6. Otros programas recomendados.
- 1.7. Herramientas de desinfección gratuitas.
- 1.8. Técnico. Ejemplo de infección por virus.
- 1.9. Anexo.
- 1.10. Referencias.
- 1.11. Tengo un mensaje de error ¿y ahora?
- 1.12. Monográficos.

### **MÓDULO 2 - ANTIVIRUS. CONFIGURACIÓN, UTILIZACIÓN**

- 2.1. Test de conocimientos previos.
- 2.2. Antivirus. Configuración.
- 2.3. Antivirus. Utilización.
- 2.4. Antivirus. Actualización.
- 2.5. Troyanos.
- 2.6. Pantalla típica de un troyano cuando estamos a punto de infectarnos.
- 2.7. Esquema de seguridad.
- 2.8. Técnico. Detalles del virus Sasser.
- 2.9. Anexo.
- 2.10. Referencias.

### **MÓDULO 3 - CORTAFUEGOS**

- 3.1. Test de conocimientos previos.
- 3.2. Cortafuegos. Definición.
- 3.3. Tipos de cortafuegos.
- 3.4. Concepto de puerto.
- 3.5. Tipos de cortafuegos.
- 3.6. Cortafuegos de Windows XP.
- 3.7. Cortafuegos de Windows 7.
- 3.8. Cortafuegos de Windows 8.
- 3.9. Limitaciones de los cortafuegos.
- 3.10. Descarga e instalación. Zonealarm.
- 3.11. Configuración.
- 3.12. Utilización.
- 3.13. Actualización.
- 3.14. Consola del sistema.
- 3.15. Otros programas recomendados.
- 3.16. Direcciones de comprobación en línea.
- 3.17. Esquema de seguridad.



3.18. Novedad. USB Firewall.

3.19. Técnico. Cómo funciona un IDS (sistema de detección de intrusos) Inalámbricas.

3.20. Anexo.

3.21. Referencias.

#### MÓDULO 4 - ANTIESPÍAS

4.1. Test de conocimientos previos.

4.2. Definición de módulo espía.

4.3. Tipos de espías.

4.4. Cookies.

4.5. SpyBot.

4.6. Malwarebytes.

4.7. Spywareblaster.

4.8. Descarga e instalación.

4.9. Técnico. Evidence Eliminator, amenaza para que lo compres.

4.10. Anexo.

4.11. Referencias.

4.12. Glosario.

#### MÓDULO 5 - ANTIESPÍAS. CONFIGURACIÓN, UTILIZACIÓN

5.1. Test de conocimientos previos.

5.2. Configuración.

5.3. Utilización.

5.4. Actualización.

5.5. Otros programas recomendados.

5.6. Direcciones de comprobación en línea.

5.7. Cómo eliminar los programas espía de un sistema (Pasos).

5.8. Esquema de seguridad.

5.9. Kaspersky admite que están saturados de peligros en la red.

5.10. "Apple está 10 años detrás de Microsoft en materia de seguridad informática".

5.11. Anexo.

5.12. Referencias

#### MÓDULO 6 - ACTUALIZACIÓN DEL SISTEMA OPERATIVO

6.1. Test de conocimientos previos.

6.2. WindowsUpdate.

6.3. Configuraciones de Windows Update.

6.4. Módulos espía en Windows XP.

6.5. SafeXP.

6.6. Objetos (o complementos) del Internet Explorer.

6.7. Navegadores alternativos.

6.8. Anexo.

6.9. Referencias.

#### MÓDULO 7 - NAVEGADOR SEGURO. CERTIFICADOS

7.1. Test de conocimientos previos.

7.2. Navegador seguro.

7.3. Certificados.

7.4. Anexo. Tarjetas criptográficas y Token USB.

7.5. Técnico. ¿Qué es un ataque de denegación de servicio (Ddos)?

7.6. Anexo.

7.7. Referencias.

7.8. Anexo. DNI electrónico (eDNI).



## MÓDULO 8 - CORREO SEGURO

- 8.1. Test de conocimientos previos.
- 8.2. Correo seguro.
- 8.3. Correo anónimo.
- 8.4. Técnico. Correo anónimo.
- 8.5. Hushmail.
- 8.6. Esquema de seguridad.
- 8.7. Anexo.
- 8.8. Referencias. MÓDULO 9 - SEGURIDAD EN LAS REDES P2P

- 9.1. Test de conocimientos previos.
- 9.2. Seguridad en las redes P2P.
- 9.3. Peerguardian.
- 9.4. Seguridad al contactar con el Proveedor de Internet.
- 9.5. Checkdialer.
- 9.6. Esquema de seguridad.
- 9.7. Técnico. Usuarios P2P prefieren anonimato a velocidad.
- 9.8. España se posiciona como uno de los países del mundo con más fraudes en Internet.
- 9.9. Esquema de funcionamiento de una red.
- 9.10. Anexo.

## MÓDULO 10 - COMPROBAR SEGURIDAD

- 10.1. Test de conocimientos previos.
- 10.2. Microsoft Baseline Security Analyzer.
- 10.3. Comprobaciones on-line de seguridad y antivirus.
- 10.4. Técnico. Comprobar seguridad de un sistema Windows XP.
- 10.5. Anexo.
- 10.6. Referencias.

## MÓDULO 11- VARIOS

- 11.1. Test de conocimientos previos.
- 11.2. Copias de seguridad.
- 11.3. Contraseñas.
- 11.4. Control remoto.
- 11.5. Mensajería electrónica.
- 11.6. Privacidad y anonimato.
- 11.7. Boletines electrónicos.
- 11.8. Listas de seguridad.
- 11.9. Compras a través de Internet.
- 11.10. Banca electrónica.
- 11.11. Enlaces y noticias sobre seguridad informática.
- 11.12. Anexo. Navegador Firefox.
- 11.13. Agenda de control.
- 11.14. Técnico. PandaLabs descubre un nuevo troyano Briz que permite el control remoto del ordenador y realizar estafas online.
- 11.15. Técnico. Seguridad en Linux.
- 11.16. Seguridad inalámbrica (Wifi).
- 11.17. Referencias.



## **ESPECIALIDAD FORMATIVA: CIBERSEGURIDAD PARA USUARIOS**

### **MÓDULO 1 - INTRODUCCIÓN A LA SEGURIDAD EN SISTEMAS DE INFORMACIÓN**

- 1.1. Conceptos de seguridad en los sistemas.
- 1.2. Clasificación de las medidas de seguridad.
- 1.3. Requerimientos de seguridad en los sistemas de información.
  - 1.3.1. Principales características.
  - 1.3.2. Confidencialidad.
  - 1.3.3. Integridad.
  - 1.3.4. Disponibilidad.
  - 1.3.5. Otras características.
  - 1.3.6. Tipos de ataques.

### **MÓDULO 2 - CIBERSEGURIDAD**

- 2.1. Concepto de ciberseguridad.
- 2.2. Amenazas más frecuentes a los sistemas de información.
- 2.3. Tecnologías de seguridad más habituales.
- 2.4. Gestión de la seguridad informática.

### **MÓDULO 3 - SOFTWARE DAÑINO**

- 3.1. Conceptos sobre software dañino.
- 3.2. Clasificación del software dañino.
- 3.3. Amenazas persistentes y avanzadas.
- 3.4. Ingeniería social y redes sociales.

### **MÓDULO 4 - SEGURIDAD EN REDES INALÁMBRICAS**

- 4.1. Seguridad en redes inalámbricas

### **MÓDULO 5 - HERRAMIENTAS DE SEGURIDAD**

- 5.1. Medidas de protección.
- 5.2. Control de acceso de los usuarios al sistema operativo.
  - 5.2.1. Permisos de los usuarios.
  - 5.2.2. Registro de usuarios.
  - 5.2.3. Autenticación de usuarios.
- 5.3. Gestión segura de comunicaciones, carpetas y otros recursos compartidos.
  - 5.3.1. Gestión de carpetas compartidas en la red.
  - 5.3.2. Tipos de accesos a carpetas compartidas.
  - 5.3.3. Compartir impresoras.
- 5.4. Protección frente a código malicioso.
  - 5.4.1. Antivirus.
  - 5.4.2. Cortafuegos (firewall).
  - 5.4.3. Antimalware.

## **ESPECIALIDAD FORMATIVA: MEDIOS ELECTRÓNICOS**

### **MÓDULO 1 - INTRODUCCIÓN A GOOGLE DRIVE Y SUS HERRAMIENTAS COLABORATIVAS**

- 1.1 Funcionalidades y ventajas de Google Drive.
- 1.2 Creación y configuración de una cuenta de Google Drive.
- 1.3 Navegación y organización de archivos en Google Drive.
- 1.4 Compartir archivos y carpetas de forma colaborativa.
- 1.5 Colaboración en tiempo real en documentos, hojas de cálculo y presentaciones.
- 1.6 Configuración de permisos de acceso y edición en Google Drive.
- 1.7 Gestión de versiones de documentos colaborativos.



## MÓDULO 2 - GMAIL, MEET Y CALENDAR

- 2.1 Funcionalidades principales de Gmail y su integración con Google Drive.
- 2.2 Organización y gestión de correos electrónicos en Gmail.
- 2.3 Programación y gestión de reuniones virtuales con Google Meet.
- 2.4 Integración de Google Calendar con Gmail para la gestión eficiente de eventos y citas.
- 2.5 Configuración de recordatorios y notificaciones en Google Calendar.
- 2.6 Uso de la función de programación de envío en Gmail.

## MÓDULO 3 - DOCUMENTOS

- 3.1 Creación, edición y formato de documentos de texto en Google Docs.
- 3.2 Herramientas de colaboración en tiempo real en Google Docs.
- 3.3 Uso de plantillas y complementos para documentos en Google Docs.
- 3.4 Comentarios y sugerencias colaborativas en documentos en Google Docs.
- 3.5 Configuración de permisos de visualización y edición en documentos compartidos en Google Docs.
- 3.6 Exportación e impresión de documentos desde Google Docs.

## MÓDULO 4 - HOJAS DE CÁLCULO

- 4.1 Creación, edición y formato de hojas de cálculo en Google Sheets.
- 4.2 Funciones y fórmulas básicas en Google Sheets.
- 4.3 Gráficos y visualizaciones de datos en Google Sheets.
- 4.4 Colaboración en tiempo real en hojas de cálculo en Google Sheets.
- 4.5 Importación y exportación de datos en Google Sheets.
- 4.6 Configuración de permisos de acceso y edición en hojas de cálculo compartidas en Google Sheets.

## MÓDULO 5 - PRESENTACIONES Y FORMULARIOS

- 5.1 Creación, edición y formato de presentaciones en Google Slides.
- 5.2 Incorporación de imágenes, videos y animaciones en presentaciones en Google Slides.
- 5.3 Diseño de diapositivas y transiciones en Google Slides.
- 5.4 Colaboración en tiempo real en presentaciones en Google Slides.
- 5.5 Creación y personalización de formularios en Google Forms.
- 5.6 Uso de formularios para la recopilación de datos y respuestas en Google Forms.
- 5.7 Análisis de respuestas y generación de informes en Google Forms