Ciberseguridad Básica (30 horas)

MÓDULO 1: Fundamentos de la Ciberseguridad (15 horas)

UF1: Conceptos básicos y amenazas digitales (7 horas)

- Definición y objetivos de la ciberseguridad.
- Principales amenazas: malware, phishing, ransomware, ingeniería social.
- Consecuencias de los ataques para la empresa y la persona emprendedora.
- Buenas prácticas en el uso de contraseñas y autenticación.
- Aplicación práctica: identificación de correos sospechosos y análisis de enlaces.

UF2: Protección de dispositivos y redes (8 horas)

- Seguridad en ordenadores, smartphones y tablets.
- Configuración básica de antivirus y firewalls.
- Redes seguras: Wi-Fi, VPN y cifrado de datos.
- Actualizaciones y parches de software como medida preventiva.
- Aplicación práctica: configuración segura de un dispositivo y de una red Wi-Fi.

MÓDULO 2: Gestión de la información y seguridad digital (15 horas)

UF1: Protección de datos y privacidad (7 horas)

- Legislación básica: RGPD y obligaciones para emprendedores.
- Tipos de datos personales y confidenciales.
- Copias de seguridad (backup) y almacenamiento seguro en la nube.
- Aplicación práctica: creación de copias de seguridad y uso de almacenamiento cifrado.

UF2: Ciberseguridad en la actividad empresarial (8 horas)

- Protección de sitios web y comercio electrónico.
- Correo corporativo y riesgos asociados.
- Seguridad en redes sociales corporativas: configuración de privacidad, autenticación en dos pasos, control de accesos y prevención de phishing.
- Buenas prácticas de publicación y gestión de reputación digital.
- Identificación y gestión de incidentes de seguridad y plan básico de respuesta.

- Aplicación práctica: configuración segura de perfiles y páginas de empresa; simulación de ataques de ingeniería social en redes sociales.