

## Servicio de Asesoramiento en CiberSeguridad (Básico)

Este plan está diseñado para ayudar a las pymes que no cuentan con una protección básica o bien tienen protección, pero no cuentan con un plan de ciberseguridad adecuado a su actividad.

Subvención de  
**6.000€**

- Evaluar la seguridad actual de la empresa, identificando sus activos y datos más críticos.
- Asegurar la continuidad del negocio ante posibles incidentes de seguridad, minimizando interrupciones.
- Crear un plan detallado de respuesta ante brechas de seguridad, con protocolos específicos para ciberataques.
- Diseñar una estrategia de ciberseguridad a medida para la empresa a corto y medio plazo.
- Cumplir con las normativas de protección de datos y estándares de seguridad de la información.
- Preparar la documentación inicial para implementar un Sistema de Gestión de Seguridad de la Información (SGSI", nos basaremos en la ISO 27001 y el ENS media-alta).
- Desarrollar y aplicar un caso práctico de ciberseguridad adaptado al negocio.
- Identificar oportunidades de uso de la inteligencia artificial en ciberseguridad.

### Diagnóstico Inicial (Documento 1)

**Se va a realizar un Análisis de Vulnerabilidades para conocer la situación actual de la empresa frente a riesgos, identificando los activos y datos más valiosos para la actividad de la empresa.** Va a incluir:

- Inventario y recopilación de información de los sistemas y fuentes a evaluar.
- Auditoria de los activos identificados y pruebas de penetración (pentesting).
- Listado de vulnerabilidades detectadas y dispositivos y servicios vulnerables.

### Resultados (Documento 2)

**Plan de Protección del Negocio:** Elaboración de un plan que cubra las necesidades en la organización mediante la definición de una Política de Seguridad que defina las medidas a implementar.

- Gestión de usuarios. Autenticación, política de contraseñas fuertes.
- Protección del correo electrónico / servidores /end points.
- Copias de Seguridad con mecanismos específicos anti ransomware
- Actualización y parcheo periódico de software

**Plan de continuidad de negocio:** Elaboración de un plan de continuidad de negocio enfocado en personas y sistemas de protección y restablecimiento de procesos y servicios críticos ante eventos de interrupción o desastre. Debe incluir:

- Gestión ante incidentes de seguridad
- Gestión de vulnerabilidades.
- Medidas de respuesta y recuperación

### Caso de Uso (Documento 3)

**Diagrama AS-S:** sobre el cual se representen los elementos de los sistemas de información de los que dispone la organización y como se relacionan entre si

**Resultados de las pruebas de pentesting:** reporte de las pruebas realizadas que incluya un resumen, metodología utilizada, hallazgos e impacto.