9. **Registro de actividad.** La monitorización permite prever y detectar las situaciones anómalas, de riesgo y posibles fallos de seguridad antes de que ocurra un incidente de seguridad.

10. **Continuidad de negocio.** Protege los principales procesos de negocio a través de un conjunto de tareas que permitan a la organización recuperarse tras un incidente grave en un plazo de tiempo que no comprometa su continuidad. De esta forma se garantiza una respuesta planificada ante cualquier fallo de seguridad.

En quién me apoyo

Para el asesoramiento: en la OAP de FREMM.
Para el desarrollo: en profesionales. Consulta el listado de habilitadores en la web de la OAP FREMM.
Para la financiación: consulta a la OAP FREMM sobre las líneas de ayuda existentes.

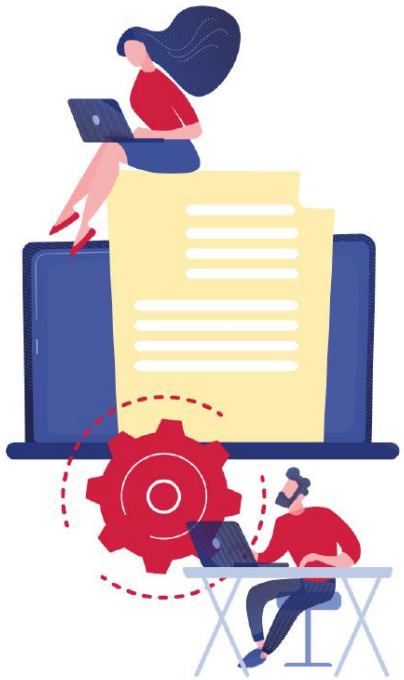
OAP FREMM
C/. del Metal, 4 30009 Murcia
Teléfono: 968931502/00/01
oap@fremm.es

Las Oficinas Acelera pyme puestas en marcha en toda España por Red.es, entidad pública adscrita al Ministerio de Asuntos Económicos y Transformación Digital a través de la Secretaría de Estado de Digitalización e Inteligencia Artificial, cuentan con un presupuesto global de 8 millones de euros, de los cuales Red.es aportará 6,3 y las entidades beneficiarias el resto. Las actuaciones están cofinanciadas con fondos FEDER de la Unión Europea, en el marco del Programa Operativo Pluriregional de España FEDER 2014-2020 (POPE) bajo el lema "Una manera de hacer Europa".

CIBERSEGURIDAD

https://oap.fremm.es/

Los ataques y amenazas de ciberseguridad no distinguen nombre o tamaño de empresa, simplemente persiguen sustraer, bloquear secuestrar uno de los activos más valiosos para las compañías: los datos.



En el año 2.017 las empresas españolas tuvieron pérdidas por valor de 14.000 millones de euros a causa de los ciberdelitos.

Fondo Europeo de Desarrollo Regional

"Una manera de hacer Europa"

CIBERSEGURIDAD

¿Qué es?

La ciberseguridad busca la protección de la información digital de la empresa que está presente en los sistemas interconectados. Está comprendida dentro de la seguridad de la información.

Principales ventajas

Conocer y emplear buenas prácticas en redes sociales, e-mail, website y demás entornos online, evitará posibles amenazas e incidentes de seguridad que, de suceder, pueden suponer grandes y graves pérdidas económicas, parada de los negocios, robo de datos sensibles (personales o de negocio) y, en definitiva, pérdida de confianza de los clientes y quebranto de la reputación, que finalmente se traducirán en disminución de resultados o desaparición de un negocio, incluso posibles problemas legales por daños o pérdidas económicas.

Por dónde empiezo

Para ver el nivel de ciberseguridad que hay en nuestra empresa, podemos recurrir al autodiagnóstico anónimo que está disponible en la web del **Instituto Nacional de Ciberseguridad (Incibe)**. Como resultado de este ejercicio, conoceremos el estado en seguridad de la información, qué riesgos de ciberseguridad amenazan el funcionamiento de la empresa y qué aspectos debemos mejorar.

Saber dónde falla la seguridad tecnológica de la empresa es un buen comienzo, así podemos precisar el diseño de nuestras acciones (https://www.incibe.es/protege-tu-empresa/conoces-tus-riesgos).

Diez pasos imprescindibles para ser una pyme CIBERSEGURIDAD

1. **Política y normativa**. Analiza tu estado de seguridad y define a dónde quieres llegar. Establece una normativa interna (compromisos) y cumple con la normativa obligatoria relacionada con la protección de datos y con los sistemas informáticos que la tratan.

2. **Control de acceso**. Identifica quién puede acceder a dónde y para hacer qué. Define procedimientos para la gestión de contraseñas, alta/baja de usuarios y sus permisos.

3. **Copias de seguridad**, que son la salvaguarda básica para proteger la información. Dependiendo del tamaño y necesidades de la empresa, los soportes, frecuencia y procedimientos para realizar las copias pueden ser distintos. El soporte escogido dependerá del sistema de copia seleccionado, de la fiabilidad que sea necesaria y de la inversión que deseemos realizar.

4. **Protección antimalware** a la totalidad de los equipos y dispositivos corporativos (incluidos móviles, USB, y discos duros portátiles), para prevenir, detectar y contener cualquier tipo de amenaza a la que se vea expuesta la organización.

5. **Actualizaciones** de los sistemas de información, para mantener un nivel adecuado de la ciberseguridad.

6. **Seguridad de la red**. Se deben establecer pautas básicas para mantenerla protegida frente a posibles ataques o intrusiones (incluidas las redes wifi).

7. **Información en tránsito**. Uso de dispositivos móviles, comunicaciones inalámbricas...

8. **Gestión de soportes**. Se necesitan infraestructuras de almacenamiento flexibles y soluciones que protejan y resguarden la información y se adapten a los rápidos cambios del negocio y las nuevas exigencias del mercado, garantizando el rápido retorno de la inversión efectuada.