GUÍA CIBERSEGURIDAD

¿Qué es?

La ciberseguridad busca la protección de la información digital de autónomos y empresas 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 tenemos, 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 interno y qué aspectos debemos mejorar.

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

Estrategia Integral de Autónomos

FREMM
Federación Regional de Empresarios del Metal Murcia

Región de Murcia
Consejería de Empresa, Economía Social y Autónomo
Dirección General de Autónomos, Trabajo y Economía Social

Diez puntos imprescindibles para ser Ciberseguro

PRIMERO

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.

SEGUNDO

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.

TERCERO

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.

CUARTO

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.

QUINTO

Actualizaciones

De los sistemas de información, para mantener un nivel adecuado de la ciberseguridad.

SEXTO

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

SÉPTIMO

Información en tránsito.

Uso de dispositivos móviles, comunicaciones inalámbricas...

OCTAVO

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.

NOVENO

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.

DÉCIMO

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.