# 6.1 Seguridad digital

La seguridad digital consiste en el uso seguro y responsable de la tecnología. Para ello hay que tener en cuenta diferentes áreas.

## Principales áreas de seguridad digital

En primer lugar, la protección de los dispositivos digitales es fundamental. Los ordenadores, teléfonos o tabletas deben protegerse frente a virus, hackeos y otros peligros. Para ello, se recomienda mantener actualizados los sistemas operativos y antivirus, así como realizar copias de seguridad.

También es imprescindible la protección de los **datos personales y de la privacidad**. Es conveniente guardar y compartir información de forma segura, no publicando datos no identificables en la red y comprobando el uso de sitios web seguros. También es importante saber identificar los mensajes sospechosos para evitar fraudes que pretendan robar datos.

Para garantizar la **protección de la salud y el bienestar** es necesario un uso equilibrado de la tecnología. Controlar el tiempo que se pasa en el uso de los dispositivos y tomar medidas de protección frente a mensajes nocivos. También se hace hincapié en el posible uso de la tecnología digital para ayudar a personas mayores o con necesidades especiales.

La protección del **medio ambiente** exige un uso responsable de la tecnología. La reducción del consumo energético, la correcta gestión de los residuos electrónicos y la elección de dispositivos respetuosos con el medio ambiente son actividades recomendables.

## Seguridad de datos, información y conocimiento

Por último, hay que profundizar en la definición de seguridad, ya que garantizar la seguridad de la información y del conocimiento es imprescindible en cualquier empresa u organización. Es necesario velar por la confidencialidad, integridad y disponibilidad de la información, desarrollando políticas de seguridad y la gestión de riesgos. Definiciones de los aspectos de seguridad aquí mencionados:

**Confidencialidad de la información**: Garantizar que la información esté a disposición exclusiva de las personas autorizadas, evitando accesos no autorizados.

**Integridad de la información**: Asegurarse de que los datos son exactos y fiables, evitando modificaciones o manipulaciones no autorizadas.

**Acceso a la información**: Garantizar la disponibilidad y disponibilidad de la información cuando sea necesario, asegurando el correcto funcionamiento de los sistemas.

## Grupo de seguridad de la información de la empresa

Para trabajar la seguridad digital dentro de la empresa es conveniente que exista un Grupo de Seguridad de la Información; una unidad integrada en el organigrama de la empresa. Su función fundamental es gestionar y proteger la seguridad de los datos, información y conocimiento de la empresa. Para ello, realiza diversas actividades que garanticen la protección de los activos digitales de la empresa.

- En primer lugar, debe llevar a cabo el desarrollo de las **políticas de seguridad**, estableciendo directrices y normas para la protección de la información. Además, debe realizar un inventario de activos que permita la identificación y control de los sistemas de información, datos y recursos tecnológicos de la empresa.
- **La gestión de riesgos** también es responsabilidad de este grupo. Esto supone analizar y minimizar los factores que pueden poner en peligro la seguridad de la información. Para ello, estableciendo medidas de protección tecnológicas y organizativas, como cortafuegos, sistemas de cifrado o controles de acceso.
- Además, debe llevar a cabo **acciones de sensibilización y formación** para garantizar el conocimiento y cumplimiento de los protocolos de seguridad por parte del personal. Por otro lado, realiza la gestión de los hechos, es decir, respondiendo rápida y eficazmente ante violaciones de seguridad o ciberataques.
- Finalmente, debe realizar **auditorías de seguridad** para comprobar el correcto funcionamiento de las medidas de protección de la información establecidas y proponer mejoras. Así, el Grupo de Seguridad de la Información actualiza y refuerza permanentemente la protección de la información de la empresa.

## Conclusión

La seguridad digital es **responsabilidad de todos** y para ello debemos adoptar hábitos seguros. En el uso de la tecnología es imprescindible garantizar la protección de los dispositivos, la privacidad de los datos personales, la salud, el medio ambiente y la seguridad de las empresas. Para ello es necesario aplicar actualizaciones, protocolos de seguridad y gestión de riesgos de forma continua, lo que permite reforzar la seguridad digital y minimizar los riesgos

*(última actualización 20/05/2025)*