1.2. ¿Qué queremos proteger?

La seguridad informática pretende **proteger recursos** valiosos de una organización. En un sistema informático lo que queremos proteger son sus activos, es decir, los recursos que forman parte del sistema y que podemos agrupar en:

- **Hardware**: elementos físicos del sistema informático, tales como procesadores, electrónica y cableado de red, medios de almacenamiento (cabinas, discos, cintas, DVDs,...).
- **Software**: elementos lógicos o programas que se ejecutan sobre el hardware, tanto si es el propio sistema operativo como las aplicaciones.
- **Datos**: comprenden la información lógica que procesa el software haciendo uso del hardware. En general serán informaciones estructuradas en bases de datos o paquetes de información que viajan por la red.
- **Otros**: fungibles, personas, infraestructuras,.. aquellos que se 'usan y gastan' como puede ser la tinta y papel en las impresoras, los soportes tipo DVD o incluso cintas si las copias se hacen en ese medio, etc.

De ellos los mas críticos son los datos, el hardware y el software. Es decir, los datos que están almacenados en el hardware y que son procesados por las aplicaciones software.

El activo mas crítico son los datos. El resto se puede reponer con facilidad pero los datos no.

La empresa debe tener una buena política de copias de seguridad y ser capaz de reponerlos en el estado mas próximo al momento en que se produjo la pérdida.

Si la empresa no es capaz de reponer dichos datos, le conllevaría de pérdida de tiempo y dinero.

Para ello se establecen **planes de seguridad** que garantizan los tres principios establecidos con anterioridad. Estos nos ayudan a identificar **vulnerabilidades** e implementar planes de contingencia adecuados.

