

Un plan de implantación incluye varios programas. En uno de ellos, se encuentra: Objetivo: asegurar la confidencialidad alta de los datos de usuario, que forman parte del servicio de “puesto de trabajo en red”. Los datos se guardan en carpetas de datos proporcionadas por el sistema operativo. Salvaguarda 1: restringir el uso de los puertos USB, para evitar la evasión de información de los datos, que se guardan en carpetas de datos del sistema de ficheros En base exclusivamente a esta información, se pide: Determinar los sistemas implicados en el plan de implantación, según la clasificación MAGERIT de división en capas. Analizar los requisitos de seguridad de cada sistema implicado. Enunciar la salvaguarda a aplicar en términos de activo, amenaza, riesgo y contramedida

## SOLUCIÓN

### Informe de insuficiencias

Sistemas implicados. Según el enfoque de MAGERIT de división en capas:

CAPA 4 (Servicio): servicio de puesto de trabajo en red.

CAPA 3 (Información): datos de usuario de red.

CAPA 2 (Aplicaciones): sistema operativo con carpetas de datos.

CAPA 1 (Soporte): Estación de trabajo con puerto USB, persona.

Análisis de los requisitos de seguridad. Según el enfoque de dependencia jerárquica entre activos, los requisitos que se indican son C = alta, y se propagan hacia los activos inferiores, acumulándose a su valor propio (que es nulo, al no tener otra información en el enunciado):  
Servicio de puesto de trabajo en red: C = alta.

Datos de usuario: C = alta.

Sistema operativo con carpetas de datos: C = alta.

Estación de trabajo, persona: C = alta.

Describir las medidas a aplicar. Activo: “información”.

Amenaza: “evasión de información”. Riesgo: alto en la confidencialidad. Salvaguarda: restringir puerto USB.