3.3

CRIPTOGRAFÍA

CRIPTOGRAFÍA - ¿POR QUÉ CIFRAR LA INFORMACIÓN?

- Una de las máximas de la seguridad informática es la confidencialidad
- En el siglo XXI el valor está en los datos
- No queremos revelar información relevante de nuestro negocio ni de nuestros usuarios
- LOPD

CRIPTOGRAFÍA

- Todas las funciones criptográficas empleadas deben implementarse en un sistema de confianza
- Proteger los "*secretos maestros*" de accesos no autorizados
- Manejar el sistema ante errores de los módulos criptográficos
- Todos los números, nombres de archivo, GUIDs y cadenas que deban ser aleatorios/as y no adivinables, serán generados con un módulo testeado y aprobado que cumpla con ese requisito

CRIPTOGRAFÍA

- Los módulos criptográficos utilizados deben ser compatibles con FIPS 140-2 o algún estándar similar
- Debe establecerse una política y un proceso para la gestión de claves criptográficas