Ejercicio 1

No cumplir con los principios generales.
No aplicar o contar con las medidas técnicas de seguridad insuficientes.

CaixaBank, es la segunda compañía española que mayor multa ha recibido por incumplir el Reglamento General de Protección de Datos. La entidad bancaria catalana ocupa el decimotercer lugar por la multa de 6 millones de euros que le impuso la Agencia Española de Protección de Datos por usar de forma ilícita los datos personales de sus clientes.

Vodafone, fue sancionada por saltarse la protección de datos y no frenar acciones comerciales cuando se les pedía. La sentencia subrayaba, además, que se tuvo en cuenta como agravante que la compañía había sido sancionada desde enero de 2018 en más de 50 ocasiones.

BBVA, fue sancionada con 5 millones de euros por usar la información personal de sus clientes sin su consentimiento.

Ejercicio 2

La Agencia de Protección de datos multa a una web por usar 'cookies' sin el consentimiento de sus usuarios.

Se interpuso ante la agencia Española de Protección de datos.

Se le impone una multa a la empresa sancionada de 5000€.

No me parece proporcionada, seguramente que la empresa sancionada haya ganado más dinero por la infracción cometida y pagar 5000€ no le suponga ningún esfuerzo.

Ejercicio 3

Utilizar protocolos seguros https para páginas web y pasarelas de pago. Asegurando de esta manera que la información va cifrada.

Utilizar un certificado válido y al día para la web y la tienda online. Garantizando así que las conexiones a la web empresarial son legítimas.

Actualizar el software de los servidores web, evitando así vulnerabilidades conocidas.

Cifrar la información sensible que se almacene en las bases de datos de la web.

Almacenar las contraseñas de los clientes cifradas y nunca enviarlas como texto plano.

Utilizar los sellos de confianza o distintivos que muestran el compromiso de la empresa con códigos éticos y la implantación de medidas de seguridad.

Usar sistemas de reputación por votos, permitiendo a los clientes valorar públicamente el servicio recibido.

Mantener los sistemas actualizados libres de virus y vulnerabilidades.

Concienciar a los empleados de la correcta utilización de los sistemas corporativos.

Utilizar redes seguras para comunicar con los clientes cifrando la información cuando sea necesario.

Incluir la información de los clientes en los análisis de riesgos anuales, realizar copias de seguridad periódicas y verificar sus procedimientos de restauración.

Implementar mecanismos correctos de autenticación, comunicar las contraseñas a los clientes de forma segura y almacenarlas cifradas, asegurando que solo él puede recuperarla y cambiarla.