EL NUEVO

LA UE **R**EGLAMENTO **G**ENERAL DE **P**ROTECCIÓN DE **D**ATOS (EU RGPD)

¿QUÉ ES EL RGPD?

Es un nuevo reglamento cuyo objetivo es **reforzar** los derechos individuales a la protección de datos dentro de la Unión Europea.

Sustituye a la directiva de 1995 y está diseñado para garantizar la futura **protección de datos** dentro de la Unión Europea mientras se unifican varias leyes nacionales.

El RGPD también se aplicará a las organizaciones **externas a la UE** que procesen datos de ciudadanos de la Unión.

¿Cuándo se aplicarán dichos cambios?

2016 Adopción del nuevo reglamento. Las empresas disponen de **2 años** para cumplir con el reglamento

2018 Implementación completa y **cumplimiento estricto** del RGPD de la UE

A partir del **2018**, las empresas deberán utilizar medidas de seguridad de vanguardia para la protección de los datos personales

En caso de vulneración de los datos personales, las empresas se enfrentarán a sanciones de hasta el 4% de sus ingresos anuales o 20 millones de € (cualquiera que sea mayor) y deberán notificárselo a su autoridad nacional de control

Estudios

El coste medio de una vulneración de los datos personales se ha incrementado en un 23% desde el 2013

€3.7m El coste medio de una vulneración de los datos personales para organizaciones de mayor tamaño de la UE

Los costes más elevados se producen en

LOS SECTORES **SANITARIO, EDUCATIVO** Y **FINANCIERO**

5 Pasos para cumplir con el **RGPD**

1 Conocimiento
Comprenda el nuevo reglamento y lo que significa

2 Evaluación
Comprenda quién hace uso y tiene acceso a los datos

3 Política
Defina su estrategia para el flujo de datos

4 Tecnología
Considere diferentes opciones de gestión de punto final y cifrado de hardware

5 Educación
Asegúrese de que su personal conozca el RGPD y realice las prácticas recomendadas en las políticas de protección de datos

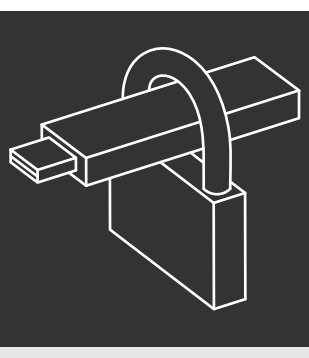
UN PEQUEÑO USB PUEDE PROVOCAR MUCHOS PROBLEMAS

Los empleados que sacan datos de la oficina incrementan el riesgo de que los mismos se vean expuestos a **mayores peligros.**

De hecho, podría conllevar a que la empresa corriera con **elevadas sanciones**, además de tener que hacerse cargo de los costes de recuperación y un posible desastre en cuanto a las RR. PP.

Recuerde que esto se puede aplicar tanto a los datos que **necesite** proteger como a los que **quiera** proteger.

El cifrado es la mejor forma de estar seguro.
Los productos cifrados de Kingston minimizan los riesgos que supone traspasar datos entre unidades USB y garantizan que sus datos más importantes y confidenciales estén protegidos.



¿Lo sabía?

Si se pierde o se roba un USB, pero los datos que contiene están **cifrados**, se trata de una

VULNERACIÓN DE LA SEGURIDAD

no de una vulneración de los datos personales y, por tanto, puede que no haya que informar sobre ello.

Unidades USB de Kingston y IronKey

Unidades USB cifradas	DataTraveler 2000	DataTraveler Vault Privacy	IronKey D300	IronKey S1000
Seguridad	XTS	XTS	XTS	XTS
Certificación	FIPS 197, IP57	FIPS 197	FIPS 140-2 nivel 3	FIPS 140-2 nivel 3 MIL-STD-810F
Crypto Chip	-	-	-	✓
Modelo Managed	-	✓ (SafeConsole de DataLocker)	✓ (EMS de DataLocker)	✓ (EMS de DataLocker)
Modelo antivirus	-	✓	-	-

También disponible en versión antivirus
Este modelo presenta una protección antivirus de ESET de fácil implementación que protege el contenido de la unidad frente a los virus, software espía, troyanos, gusanos, rootkits, adware y otras amenazas que se diseminan por Internet. El motor antivirus ESET NOD32® proporciona alertas inmediatas. Esta protección antivirus no requiere instalación alguna e incluye una licencia preactivada de cinco años.

Personalizable
Personalice las unidades en una variedad de formas, como la contraseña doble, los números de serie, el cologo, el número de intentos de introducción de contraseña, la longitud mínima de contraseña y el identificador de producto personalizado para cumplir con los requisitos de TI corporativos internos.

www.kingston.com/encrypted

Dé un pequeño aunque **importante** paso en su lista de tareas para la implementación del RGPD invirtiendo en el **cifrado AES de 256 bits basado en hardware**

Fuentes
Ponemon Institute: Estudio sobre el coste de la Pérdida de Datos 2015 - Análisis Global (2015 Cost of Data Breach Study Global Analysis)
Comisión Europea: Reforma de las leyes de protección de datos de la UE (http://ec.europa.eu/justice/data-protection/reform/index_en.htm)