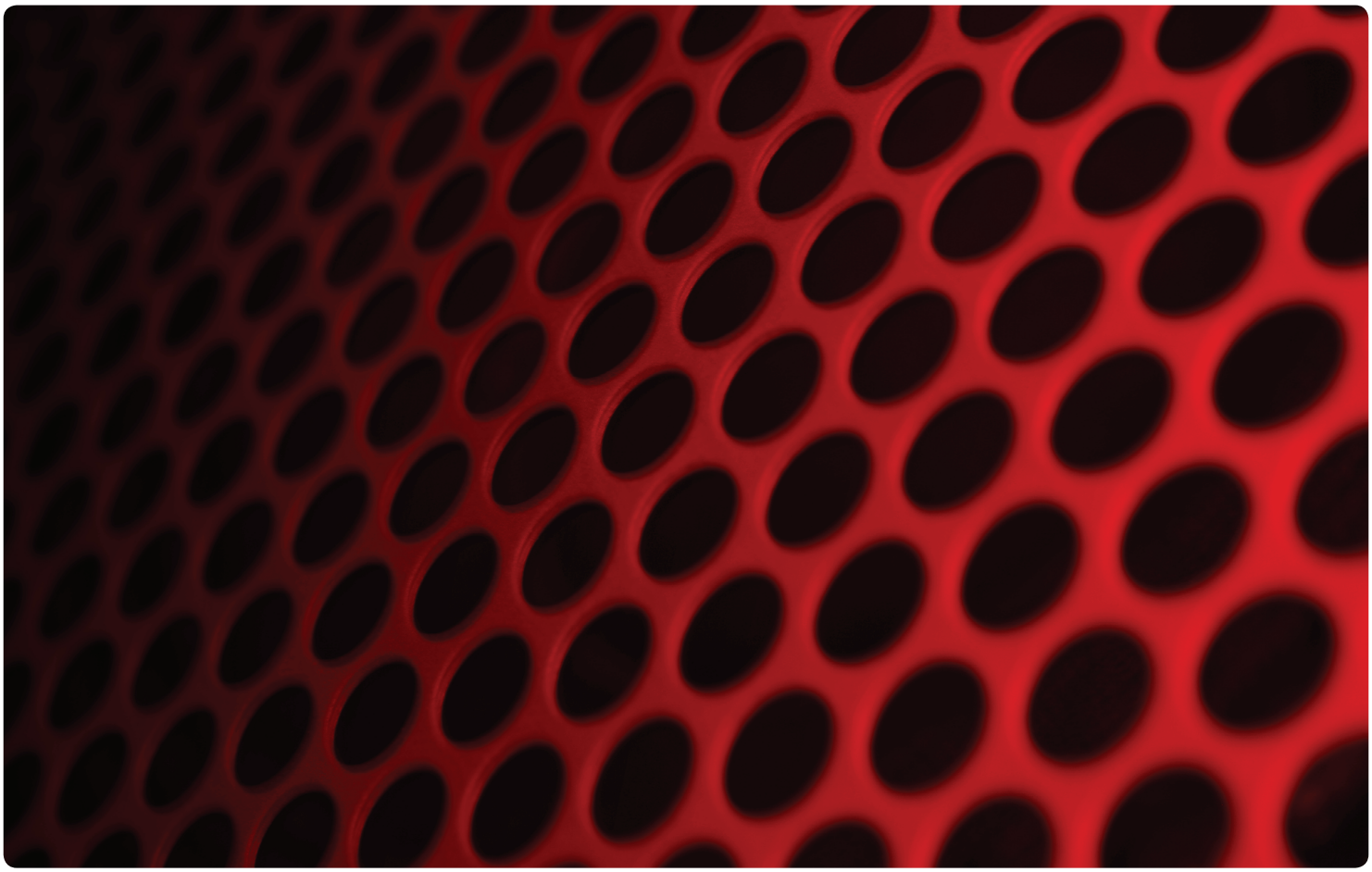
Riesgo de vulneraciones de datos

Cómo prevenirlas de conformidad con el RGPD de la UE



Introducción

La forma de trabajar cotidiana ha cambiado radicalmente y, por consiguiente, también los métodos de trabajo tradicionales: gracias a los soportes de almacenamiento móviles, podemos acceder a nuestros datos prácticamente en todo momento y desde cualquier lugar, y trabajar con ello dondequiera que estemos. Nos beneficiamos de esta **disponibilidad permanente** de información empresarial, y podemos crear **versiones para el trabajo móvil**, o copias de seguridad, optimizando así nuestros propios horarios de trabajo y, en última instancia, recortando efectivamente las operaciones.

Sin embargo, la movilidad de los datos tiene una importante desventaja. La pérdida o extravío de las unidades USB supone un severo riesgo. El **72%** del total de las empresas que respondieron a una encuesta* manifestaron que ya no podían encontrar unidades USB individuales. Se trata de algo especialmente grave, ya que el 25% de las empresas encuestadas guardaban en dichas unidades **datos sensibles**. Dichas vulneraciones de datos socavan la **confianza de los clientes** en las empresas y, por consiguiente, llevan aparejada no solo la pérdida de la buena imagen, sino también importantes costes. Estas cifras no incluyen los riesgos derivados de la publicación o uso delictivo de los datos.

Los legisladores han reaccionado al creciente riesgo de las vulneraciones de datos. A partir de mayo de 2018, el **Reglamento general de protección de datos de la Unión Europea** (RGPD UE) obligará a las empresas a asumir sus responsabilidades en mucha mayor medida. Entre otras cosas, podrán imponerse graves penalizaciones en caso de incumplimiento de las cláusulas obligatorias.

En el presente informe técnico encontrará:

- Todo lo que necesita saber acerca de la movilidad y las vulneraciones de datos
- Todo lo que exige el RGPD UE y cómo tienen que actuar las empresas para ajustarse a la nueva normativa
- Todo lo que puede hacer específicamente las vulneraciones de datos

ÍNDICE

* Encuesta realizada por Kingston Technology en 2016 en Alemania (número de respuestas: 200)

El RGPD UE está basado en la prevención

El Reglamento General de Protección de Datos de la Unión Europea (RGPD UE) sustituye los reglamentos nacionales en materia de protección de datos, y entrará en vigor el 25 de mayo de 2018, tras un período de transición de dos años. El principal objetivo del RGPD UE es mejorar **la protección de los datos y los derechos fundamentales de los ciudadanos de la UE.**

El RGPD UE no solamente se aplica a las empresas europeas, sino también a todas las organizaciones que ofrecen productos y servicios (incluyendo los gratuitos) a ciudadanos de la UE y que para ello registran sus datos personales. El RGPD UE no diferencia entre grandes, medianas o pequeñas empresas. Ese es el motivo por el cual la protección de datos debería ser un asunto examinado a fondo en todas las organizaciones que recogen, tratan y almacenan datos personales.

El objetivo de proteger los datos personales está respaldado por significativas sanciones: las vulneraciones de la protección de datos, contra las que no se hayan adoptado medidas adecuadas, podrán ser sancionadas con hasta el **4% de la facturación anual consolidada de la empresa, o hasta 20 millones de euros.**

Además, todas las vulneraciones de la protección de datos deberá comunicarse a la autoridad supervisora y a las personas afectadas por ello. Además de las penalizaciones financieras, las consecuencias pueden ser extremadamente graves para una empresa en términos de reputación, confianza de los clientes y ventas.

Estas medidas tienen por objeto garantizar que las vulneraciones de datos se eviten en todo lo que sea posible. Su intención es reducir al mínimo la divulgación de datos personales y a promover que las organizaciones adopten medidas preventivas. Sin embargo, la UE es consciente de que la protección absoluta de los datos no es viable. Por ello, la nueva directiva pretende conseguir **la mayor prevención posible.**

Los análisis de riesgo predictivos ayudan

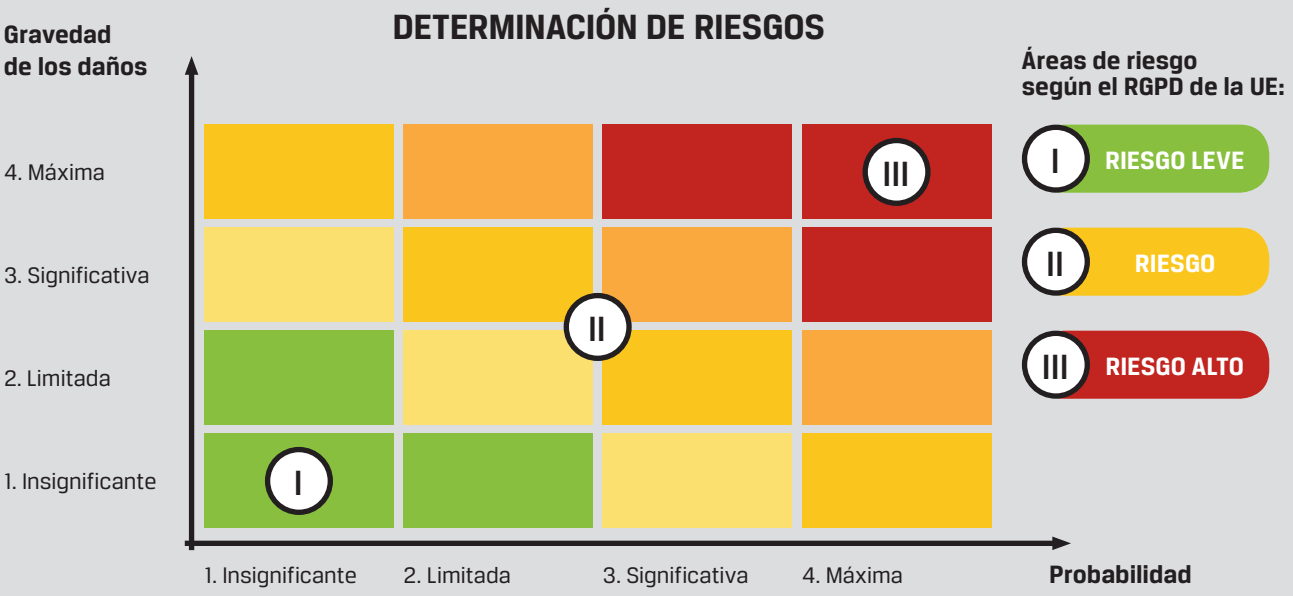
Para prevenir las vulneraciones de la protección de datos, es necesario saber dónde pueden producirse. Por consiguiente, es necesario identificar y analizar los potenciales riesgos. Todas las áreas de una organización en que se manipulen datos habrán de examinarse exhaustivamente. ¿Dónde se recogen los datos personales? ¿Cómo se tratan y almacenan?

El RGPD UE exige este análisis de riesgos. Deben considerarse la probabilidad y la severidad de los posibles daños. El **Responsable de protección de datos** puede utilizar esta información para adoptar las medidas específicas pertinentes.

Una **matriz de riesgo** puede contribuir a identificar los potenciales riesgos del almacenamiento de datos. Esta matriz señala dónde es necesario adoptar medidas. Con ella es posible localizar perfectamente cada potencial riesgo y determinar su gravedad. Los tres grupos de riesgos —Bajo, Medio y Alto— indican la necesidad de medidas necesarias para proteger la seguridad.

El Artículo 32 apartado 1 del RGPD UE estipula:

"Teniendo en cuenta el estado de la técnica, los costes de aplicación y la naturaleza, el alcance, el contexto y los fines del tratamiento, así como los
riesgos de probabilidad y gravedad variables para los derechos y libertades de las personas físicas,el responsable y el encargado del tratamiento aplicarán medidas técnicas y organizativas apropiadas para garantizar un nivel de seguridad adecuado al riesgo[.]"



Un **panorama general exhaustivo** de todas las ubicaciones en las que se guardan datos personales facilita el análisis, ya que indica con exactitud dónde se requieren las actuaciones más urgentes. Los **motivos** de la evaluación de riesgos pueden consultarse directamente en las columnas de causas de riesgo, probabilidad y alcance de los daños. De este modo, los riesgos podrán eliminarse efectivamente, como parte de unos preparativos óptimos de cara a la fecha clave del 24 de mayo de 2018.

El RGPD UE propone estas medidas de seguridad

El objetivo fundamental del RGPD UE para el tratamiento de los datos personales es "garantizar un nivel de seguridad adecuado al riesgo" (Artículo 32, apartado 1). Tras la realización del análisis de riesgos, deben adoptarse las consiguientes medidas apropiadas de una parte, y garantizar la protección de la otra.

Felizmente, el RGPD UE también proporciona información específica sobre cuán exhaustivas deben ser las medidas de protección de los datos sensibles. El Artículo 32, apartado 1, también especifica que estas medidas deberán incluir también, entre otros: "[...] la **seudonimización** y el **cifrado** de los datos personales". Por consiguiente, ambos procedimientos pueden aplicarse a las medidas de protección compatibles con el RGPD UE.

Por seudonimizar los registros de datos personales se entiende la sustitución de los nombres **por códigos numéricos aleatorios** y la clave se almacena en una **tabla maestra**. Este proceso se caracteriza por la importante ventaja de que puede automatizarse totalmente. Sin embargo, la tabla maestra tiene que estar disponible en todo momento, y no puede extraviarse ni sobrescribirse. Asimismo, es fundamental que no siempre sea necesario un nombre para identificar a la persona correspondiente. Por ejemplo, su identidad también podrá determinarse por su sexo, fecha de nacimiento y lugar de residencia. Por consiguiente, persiste un **riesgo residual**.

El cifrado es otra medida de seguridad recomendada por el RGPD UE. Los datos —en cualquier estado y en todo momento de la transmisión— deben estar cifrados.

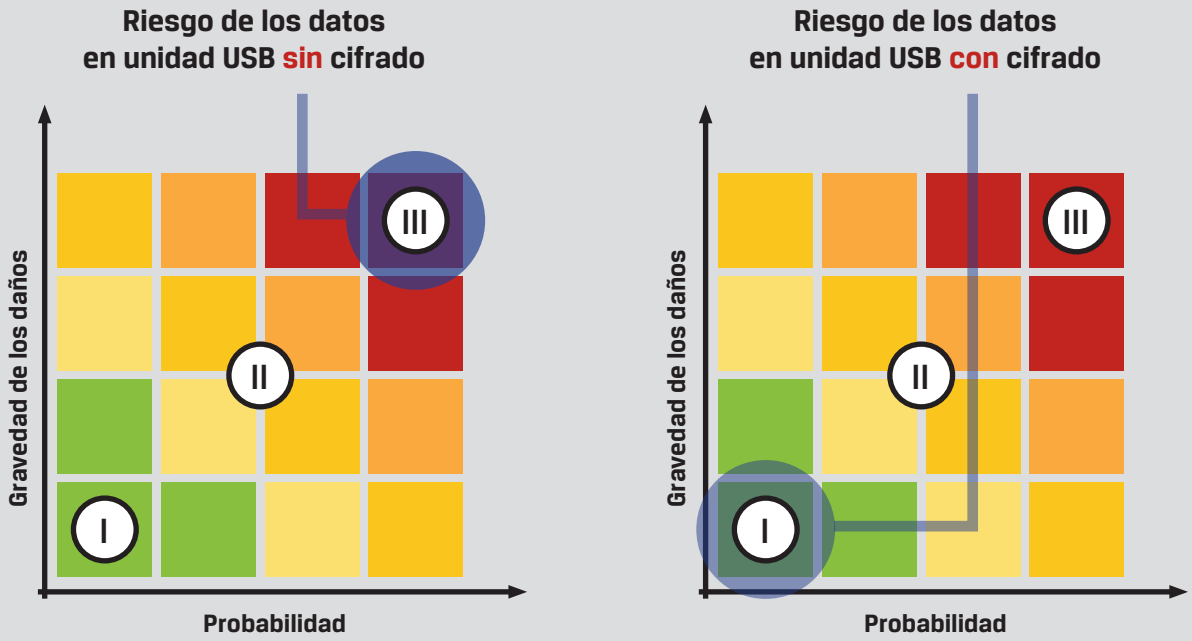
Las **certificaciones voluntarias de los fabricantes, como FIPS 197 o 140 – Nivel 3**, son la marca de los cifrados de alta calidad. Esto garantiza un cierto estándar de seguridad que, en el futuro, jugará un papel cada vez más importante como evidencia en el contexto del RGPD UE.

Si los datos personales se cifran debidamente —el cifrado AES de 256 es la técnica más avanzada—, no podrán ser utilizados incluso en caso de resultar robados o vulnerados. La obligación de informar a las personas afectadas o de realizar un anuncio público, ya no es aplicable por cuanto o existe riesgo alguno.

No obstante, sigue siendo obligatorio notificar a la autoridad supervisora responsable.

Unidades USB cifradas en todo momento, en todo lugar: Kingston Technology

Según la encuesta antes mencionadas, las empresas que guardan datos personales en unidades USB no cifradas se exponen a un alto riesgo, por cuanto suelen extraviarse, ser robadas o perderse de algún otro modo. En este caso, los riesgos deberían evaluarse a nivel general, ya que la probabilidad y potencial gravedad de los daños pueden considerarse altos. En ambos casos se pueden reducir significativamente utilizando unidades USB cifradas, lo cual implica que el riesgo global podría clasificarse como "insignificante".



Con sus líneas de productos DataTraveler DTVP3.0 y DT4000G2 de una parte, y IronKey D300 y S1000, Kingston Technology ofrece diversas unidades USB que satisfacen las más altas normas de seguridad mencionadas. Los datos almacenados se mantienen 100% cifrados, y se protegen contra el acceso no autorizado mediante contraseñas complejas. Por ejemplo, tras 10 intentos fallidos de inicio de sesión, ya no será posible acceder a los datos.

Las unidades USB de Kingston se cifran de conformidad con la norma de seguridad **AES-256** en modo XTS. Este algoritmo está adaptado a las normas de seguridad vigentes. Las homologaciones con **FIPS 197** y **FIPS 140-2** garantizan que los datos se mantengan absolutamente protegidos, incluso en caso de extravío o robo. Por otra parte, las versiones DataTraveler 4000G2, IronKey D300 y IronKey S1000 incorporan también protección física contra la manipulación de conformidad con la norma FIPS 140-2. En alguna de sus unidades USB (DTVP3.0, DTVP3.0AV, DT4000G2 con administración y D300), Kingston también ofrece un programa de personalización mediante el cual es posible integrarlas en una solución de administración centralizada utilizando, por ejemplo, números de serie e ID de productos. También puede definirse el número máximo de intentos de introducción de contraseña.

Kingston Technology se ha aliado con **DataLocker** para poder incorporar soluciones de gestión a sus unidades USB cifradas. DataLocker aporta el programa de software SafeConsole y el sistema EMS (Enterprise Management System) para las unidades USB cifradas DataTraveler y IronKey de Kingston, lo cual permite administrar centralizadamente las unidades USB de su organización.

DataTraveler Vault Privacy 3.0 y DataTraveler 4000 G2 de Kingston se comercializan como versiones administradas (la administración es opcional), ambas compatibles con la administración centralizada mediante SafeConsole de DataLocker. También los modelos D300 y S1000 de IronKey se comercializan como versiones administradas, ambas compatibles con IronKey EMS de DataLocker.

Estas soluciones permiten ajustarse más fácilmente a los **requisitos de cumplimiento normativo**, además de proporcionar a los empleados **asistencia adicional**. Por ejemplo, mediante las funciones de restablecimiento remoto de contraseña o de detección automática de malware. También simplifican el cumplimiento de directrices de seguridad exhaustivas, porque permiten a los administradores de sistemas controlar con facilidad la totalidad de las unidades de la organización.

En caso de que se extraviase una unidad USB cifrada de Kingston, ello no supone automáticamente una incidencia de datos. De este modo, los soportes de almacenamiento móviles cifrados eliminan un conocido, y muchas veces subestimado, riesgo de seguridad para las empresas. El uso de unidades USB cifradas resuelve pequeñas, aunque peligrosas, lagunas de seguridad, **evitando vulneraciones de protección de datos de acuerdo con el RGPD UE.**

¿ALGUNA OTRA PREGUNTA?

No dude en ponerse en contacto con nosotros:

+44 (0) 1932 738888

EncryptedUSB@kingston.eu

www.kingston.com

El presente informe técnico fue creado por B2B Media Group GmbH en nombre de Kingston Technology Europe Co LLP y Kingston Digital Europe Co LLP.
http://www.b2bmg.de / kontakt@b2bmg.de