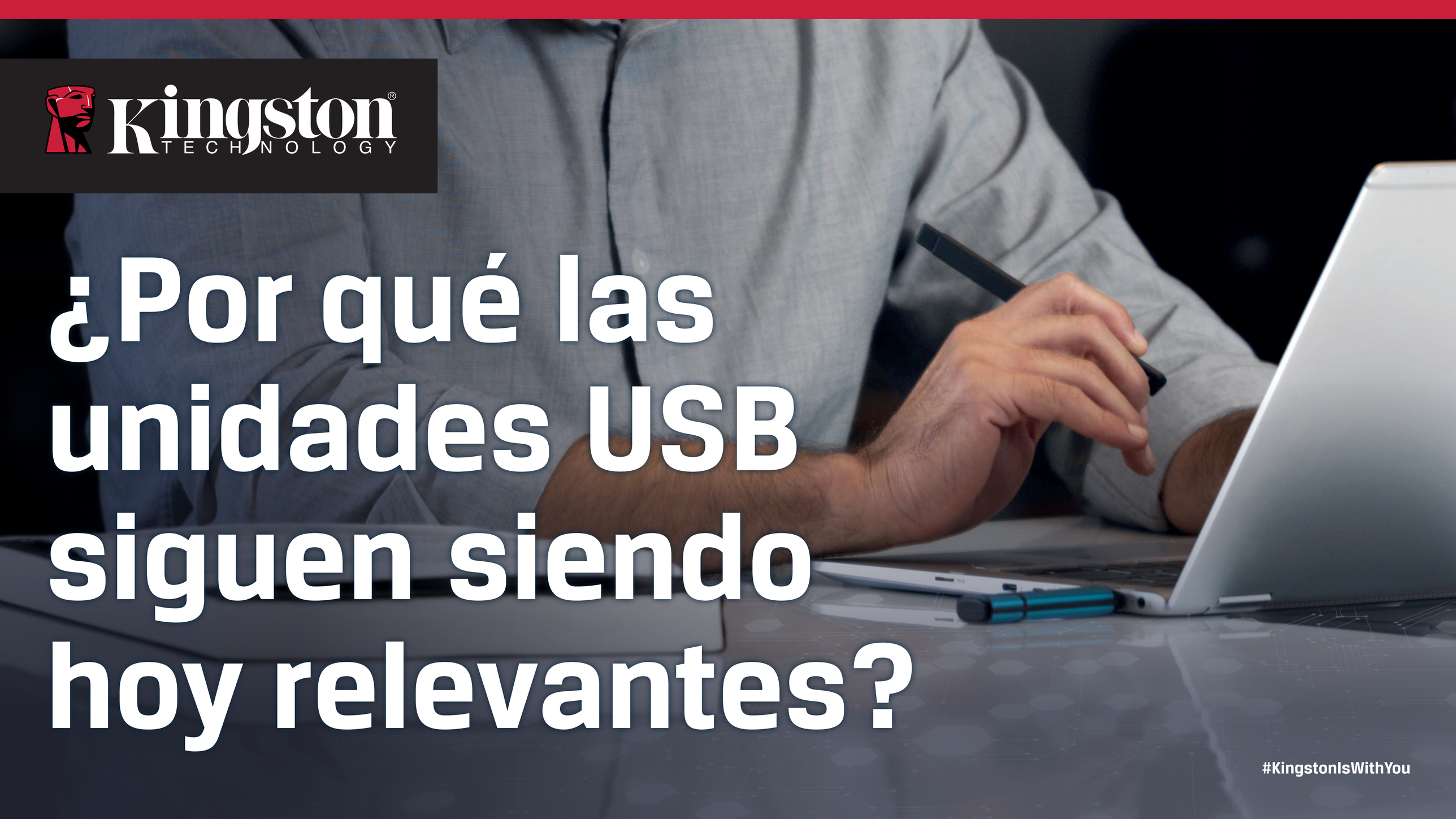


¿Por qué las unidades USB siguen siendo hoy relevantes?

#KingstonIsWithYou

¿Por qué las unidades USB siguen siendo hoy relevantes?

Prólogo y contenido

En la era digital de nuestros días, en la que el 60% del total de los datos corporativos globales están almacenados en la nube[1], podría parecer un tanto extraño hablar sobre la relevancia de una tecnología de almacenamiento que hoy se aproxima a su trigésimo cumpleaños. Sin embargo, desde su aparición este componente del almacenamiento ha evolucionado, y continúa haciéndolo.

Lejanos están los días en que las unidades USB eran simplemente un medio estándar de conectar archivos, unidades y aplicaciones. Las soluciones actuales no solamente se caracterizan por unas velocidades de transferencia ante impensables, sino que además son soportes portátiles fiables y seguros, de uso imprescindible en muchas situaciones. Pero, ¿en qué medida las unidades USB siguen siendo relevantes, en un momento en que las soluciones de almacenamiento en la nube pueden ofrecer, aparentemente, las mismas ventajas?

En este libro electrónico hablaremos de dónde encajan las unidades Flash USB en un paisaje dominado por la nube. Con la asistencia de las aportaciones de los mejores líderes del sector, analizaremos cómo las organizaciones actuales utilizan las unidades USB y debatiremos su espacio dentro del cifrado basado en software, los entornos de almacenamiento independientes y la protección de datos en puntos terminales.

Índice	Páginas
Colaboradores	3
El surgimiento de las unidades Flash USB	4
Almacenamiento portátil que satisface la creciente demanda	5-6
Cifrado: basado en hardware y basado en software	7-8
La creciente necesidad de proteger los datos sensibles	9
Protección de los datos financieros sensibles	10
Acceso seguro a los datos sanitarios de pacientes	11
La unidad USB en un futuro de almacenamiento en la nube	12-13
Resumen y Acerca de Kingston	14

¿Por qué las unidades USB siguen siendo hoy relevantes?

Colaboradores

Este libro electrónico ha sido compilado con tres expertos en TI y en tecnologías emergentes.

Rafael Bloom

La carrera de Rafael ha transcurrido en funciones de experto en productos tecnológicos, comunicaciones de marketing y desarrollo de negocio. Su especialización en materia de asesoramiento se centra en nuevos retos en materia de organización, productos y comunicaciones, así como en los cambios normativos. Esta actividad tan diversificada incluye especialización en gobernanza de los datos y cumplimiento normativo sobre diseño, privacidad de los datos y tecnologías emergentes, como AdTech, móviles y 5G, IA y aprendizaje automático.

Tomasz Surdyk

Con más de 24 años de experiencia en seguridad informática en las administraciones públicas, Tomasz es un reconocido experto en protección de la información, datos personales y ciberseguridad. En el pasado inspeccionaba sistemas y redes ICT que procesan información clasificada y datos personales en las administraciones gubernamentales, y tiene acreditación de seguridad de la OTAN y de la UE. Durante varios años fue propietario de una empresa especializada en la implementación de soluciones seguras para reforzar la protección de datos empresariales y personales.

David Clarke

David está considerado uno de los 10 principales influentes según la lista "30 principales líderes de pensamiento y pensadores sobre redes sociales, gestión de riesgos, cumplimiento normativo y tecnología regulatoria más influyentes del Reino Unido" de Thompson Reuter, y en la lista de 30 principales expertos globales de Kingston Technology. En el pasado, David ocupó diversas posiciones de gestión de seguridad, como jefe global de prestación de servicios de seguridad y jefe de infraestructura de seguridad de empresas multinacionales incluidas en el índice FTSE 100.

El surgimiento de las unidades Flash USB

Cuando, hace más de veinte años, apareció en el mercado la primera unidad Universal Serial Bus (USB, Bus serie universal), su compatibilidad colectiva fue un factor que cambió las normas del juego en el campo de la tecnología informática. Con la posibilidad de permitir el acceso de las masas a múltiples operaciones de dispositivos, muy pronto USB evolucionó, posibilitando transferencias de datos significativamente más rápidas, un puerto USB 3.0 e incluso mayores posibilidades que acompañaron el lanzamiento de la primera unidad Flash USB en 2000.

Desde entonces, la tecnología ha avanzado muchísimo en lo que respecta al almacenamiento de datos móviles y necesidades de seguridad. Hoy ponemos el foco en la actual generación de unidades USB, diseñadas teniendo en mente situaciones de uso muy específicas. Desde una perspectiva empresarial, el aumento del trabajo a distancia e híbrido, el uso de servicios en la nube y las inquietudes relativas a la ciberseguridad han planteado la necesidad de soluciones más efectivas. Junto con ello, los requisitos normativos exigen que los datos sean almacenados cumpliendo una serie de obligaciones. Estas presiones suelen complicarse por sistemas distribuidos y complejos que pueden ejecutarse "in situ" y en la nube.

Luego tenemos la cuestión del incremento de volúmenes de datos estructurados y no estructurados, como documentos, correos electrónicos, fotos, vídeos y metadatos... todo lo cual aumenta la complejidad de las necesidades de almacenamiento empresarial.

Entonces, si el almacenamiento en la nube podría resolver muchos de estos retos, ¿qué relevancia tienen las unidades USB en el actual panorama empresarial?

> **Mucha gente piensa que las unidades USB están obsoletas o son triviales debido a su uso en el pasado, y las consideran dispositivos más o menos anticuados, de bajo rendimiento y bajo nivel de seguridad.**
> **- Rafael Bloom**

Almacenamiento portátil que satisface la creciente demanda

Los patrones de uso de las unidades USB como un medio de almacenamiento portátil han decaído, siendo reemplazados por el empleo de unidades USB de alto rendimiento para copias de seguridad locales, personales y seguras, con una capa adicional de protección y confidencialidad de datos. Esto puede ser muy importante para los datos sensibles al cumplimiento normativo, como registros de RR.HH., datos financieros, historiales médicos, protección de propiedad intelectual (PI) y la información personalmente identificable (IPI). Además, esta generación de dispositivos incorpora una rápida transferencia de datos y capacidades de almacenamiento, copia de seguridad y protección que pueden utilizarse para:

- Información normativa que tiene que entregarse en mano
- Documentos legales y financieros que tienen que entregarse e imprimirse dentro o fuera de las instalaciones
- Cualquier entorno potencialmente hostil en el cual el secuestro de datos (o ransomware) puede ser una amenaza real
- Transferencia a sistemas de impresión en casos en que no se permite el acceso a redes

A la vanguardia de los proveedores de unidades USB cifradas, Kingston Technology se ha mantenido al ritmo de la evolución de la demanda con el lanzamiento de soluciones como la unidad Kingston IronKey™ S1000. Esta unidad USB cifrada, la mejor de su categoría, combina su compatibilidad con las normas más estrictas con su capacidad de proteger datos confidenciales mediante el cifrado XTS-AES de 256 bits y la incorporación de un criptochip separado con sólidas protecciones contra intrusiones. Además, cuenta con homologación FIPS 140-2 de Nivel 3. Esto significa que el gobierno de EE.UU. ha validado su efectividad en tanto que componente de hardware criptográfico, lo cual la hace ideal para organizaciones que necesitan una seguridad añadida en materia de protección de datos.

Estas unidades USB cifradas por hardware ofrecen soluciones centralizadas y seguras para la administración de dispositivos, tanto si los datos están en la nube como localmente. Además, un almacenamiento de datos cifrado compatible con la normativa y que resulta fácil de utilizar sin necesidad de software libera valiosos recursos de TI, ofreciendo soluciones diseñadas para una implementación rápida y eficiente.

Almacenamiento portátil que satisface la creciente demanda

Las copias de seguridad y el archivado son otro ejemplo de uso de unidades USB para proteger activos digitales a largo plazo, y de manera independiente de servicios de nube externos. Aunque es verdad que en la nube pueden manejarse fácilmente voluminosas transferencias de datos, la PI confidencial puede ser lo bastante sensible como para que convenga guardarla en una unidad USB cifrada segura, que puede almacenarse y protegerse alejada de Internet.

Siempre habrá circunstancias en que una organización necesite que los datos estén lógica y físicamente bajo su control, en especial cuando se utilizan unidades cifradas. Y existen casos en que el almacenamiento en HDD/SSD no puede cifrarse. El uso de unidades USB cifradas externas, como el Kingston IronKey D300S, resuelve este problema. Esta unidad Flash USB incorpora cifrado por hardware compatible con la Norma de cifrado avanzado (AES, por sus cifras en inglés) de 256 bits, que es un tipo de cifrado en bloque capaz de encriptar bloques de datos de 128 bits. Y en caso de que fuese necesario cifrar datos más allá de ese límite, AES utilizará el modo de cifrado de bloques XTS, capaz de ofrecer una protección de datos mejor y más sólida que los modos anteriores.

> En mi opinión, las unidades Flash USB siguen utilizándose y son parte integral de la protección de datos. Se utilizan, entre otras cosas, para transferir información rápidamente entre dispositivos, así como para su almacenamiento y protección adecuados.
> - Tomasz Surdyk

Cifrado: basado en hardware y basado en software

Observando cómo se cifran los datos, podría alegarse que el cifrado mediante hardware resulta más fácil de administrar, y es más seguro, que el cifrado por software. Esto se debe a que el proceso de cifrado se mantiene independiente del resto del sistema anfitrión, lo cual dificulta muchísimo interceptarlo y quebrarlo. El software de administración centralizado a nivel de dispositivo permite controlar las unidades a través de conexiones de la LAN de la intranet y de Internet, y es una excelente herramienta para:

- Establecer y forzar políticas de uso individual y/o grupal de USB cifradas
- Auditar la actividad de archivos para un mejor seguimiento de los movimientos de datos a/desde la organización
- Ejecutar copias de seguridad a distancia de contenidos para el transporte de datos críticos
- Desactivar a distancia dispositivos en caso de que una unidad USB se extravíe o quede comprometida
- Ejecutar restablecimientos remotos de contraseñas si sus usuarios las han olvidado

Si las unidades autorizadas se administran correctamente de esta manera, se reduce al mínimo el riesgo de que los datos sensibles sean copiados y compartidos. Por otra parte, las actuales unidades USB con cifrado por hardware ofrecen diversas funciones de protección adicionales que impiden que personas distintas de sus destinatarios lean, o accedan a, archivos y mensajes.

> **Creo que el cifrado por hardware es mejor que el cifrado por software. Las diferencias entre los métodos de cifrado por hardware y por software son significativas en lo que respecta a la vulnerabilidad a ataques de fuerza bruta. En el caso de los dispositivos cifrados por hardware, no es fácil sucumbir a esos ataques.**
>
> - Tomasz Surdyk

Cifrado: basado en hardware y basado en software

Si bien las empresas podrían considerar el cifrado basado en software por motivos de coste, se trataría de una decisión corta de miras. Las soluciones basadas en software comparten los recursos de cifrado del dispositivo anfitrión con otros programas, por lo cual son tan seguras como lo es dicho equipo. Además, a menudo se requieren actualizaciones de dicho software que, de no ejecutarse, dejan los datos en situación de vulnerabilidad. Las unidades USB cifradas por software pueden ser objeto de ataques de fuerza bruta ilimitados para adivinar la contraseña, y no tienen medios para resistir ataques de diccionario basados en software, que pueden intentar combinaciones de millones de caracteres en breves períodos de tiempo.

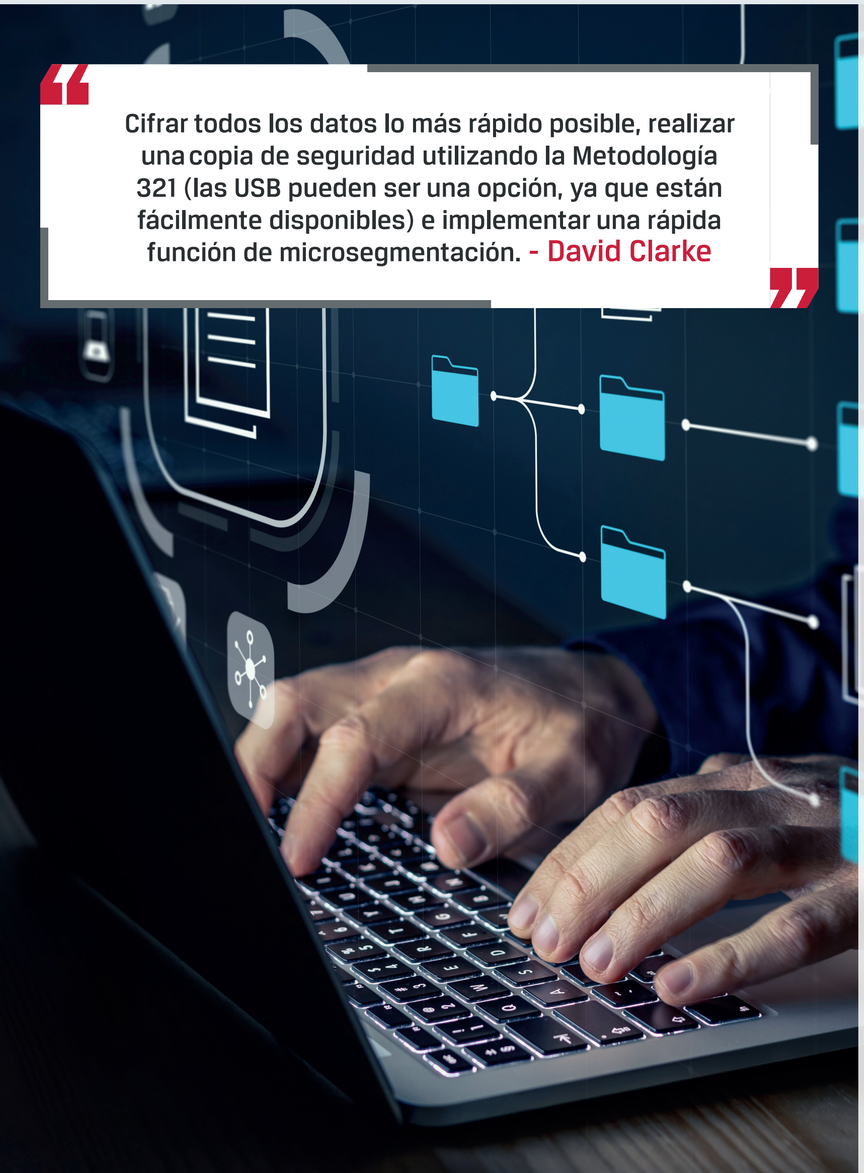
Como si esto fuese poco, el cifrado por software también es cifrado extraíble. Un empleado con una unidad cifrada por software puede copiar los datos, formatear la unidad y, de ese modo, eliminar el cifrado. Después podrá volver a copiar los archivos de datos y utilizar la unidad sin el engorro de tener que autenticarla en diferentes plataformas y sistemas operativos.

Como ya hemos dicho, con el cifrado basado en hardware, el "cifrado" físico —y el consiguiente almacenamiento de datos— es independiente del sistema anfitrión. Esto garantiza una capa adicional de defensa en caso de que los sistemas se viesen comprometidos.

Esto no puede pasarse por alto, en especial en sectores tales como el financiero, el sanitario y las administraciones públicas. Esto se debe a que regulaciones tales como la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) de EE.UU. y las Normas de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI DSS) suelen incluir estrictos requisitos en materia de cifrado de información sensible.

En última instancia, el cumplimiento de estas normas utilizando sólidos dispositivos cifrados por hardware evitará a las organizaciones onerosas multas y pleitos, por no hablar del tremendo daño reputacional. Aunque las unidades cifradas por hardware pueden resultar más costosas que las económicas unidades USB, en caso de una vulneración se podrían pagar fácilmente centenares de unidades con solo unas pocas horas de honorarios jurídicos.

La creciente necesidad de proteger los datos sensibles



> Cifrar todos los datos lo más rápido posible, realizar una copia de seguridad utilizando la Metodología 321 (las USB pueden ser una opción, ya que están fácilmente disponibles) e implementar una rápida función de microsegmentación. - David Clarke

A la hora de proteger datos sensibles contra extravíos y robos, toda organización tiene la obligación de asegurarse de que sus dispositivos dispongan de las funciones de seguridad adecuadas. También es importante considerar que, aunque existen muchísimas ciberamenazas en continua evolución, el nivel de madurez digital y la capacidad de administración de datos en sus propios terminales por parte de los usuarios siguen siendo un destacado factor de riesgo si no se abordan. Las amenazas interiores, que incluyen la pérdida del control de los datos o de los dispositivos de almacenamiento USB, la transmisión de datos fuera de un entorno seguro, el uso de unidades USB no cifradas y el compartir contraseñas, pueden ser resultado de falta de debida diligencia de parte de los usuarios finales. Todo ello puede evitarse con una capacitación adecuada, con formación y con las soluciones de unidades USB correctas.

> La organización debería tener un mapa claro de sus datos, incluyendo los niveles de importancia y/o sensibilidad de todos ellos, y elaborar un plan que aborde primero los más importantes, sea mediante la retirada física de la conexión a ellos, u oscureciendo la fuente de datos. Es fundamental poder aislar rápidamente los sistemas afectados, y absolutamente vital contar con un plan documentado que haya sido debidamente practicado. - Rafael Bloom

La preplanificación y una estructura de comunicaciones bien comprobada juegan también un importante papel en hacer frente a amenazas potencialmente existenciales. Hoy en día, las ciberamenazas van apuntadas a los puntos débiles de las organizaciones.

El momento óptimo para elaborar un plan de USB cifradas es antes de tener efectivamente que demostrar que dispone de uno, mediante la incorporación de unidades Flash USB cifradas y de las políticas correspondientes, a la estrategia global de seguridad de su organización. No tener un plan preparado para las unidades USB cifradas, y no tener directrices, nos deja sin nada sobre lo que construir, y a la organización abierta a riesgos a todos los niveles, incluyendo el incumplimiento normativo (como el Reglamento General de Protección de Datos, RGPD, cuyo Artículo 32 manifiesta específicamente que los datos sensibles deben ser cifrados.

> Los usuarios procesan datos sensibles. No ser conscientes de ello incrementa la responsabilidad y afecta significativamente a la imagen y a la seguridad de la empresa. Para proteger los datos sensibles deben utilizase diversas soluciones de seguridad, incluyendo el cifrado de los datos. - Tomasz Surdyk

Protección de los datos financieros sensibles

Además de las implicaciones de seguridad, también existen normas de cumplimiento a las que deben atenerse las soluciones de almacenamiento y copia de seguridad de los datos. Algunas de estas prácticas, como la necesidad de administrar e imponer plazos de conservación de datos, son comunes y verticales, en tanto que otras (como la migración de datos empresariales a la nube) son tratadas de manera muy diferente.

En muchos verticales, como los servicios financieros, se han puesto en vigor normas que han hecho obligatoria la administración adecuada de los datos. En especial, los bancos se mostraron inicialmente reticentes a recurrir a terceros para el almacenamiento y las copias de seguridad, y muchos todavía insisten en controlar directamente toda su infraestructura de datos.

Por otra parte, las instituciones financieras están obligadas a cumplir una creciente lista de normas de protección de datos, como la Ley Sarbanes-Oxley (SOX) de EE.UU. y el Reglamento General de Protección de Datos (RGPD) de la Unión Europea. Sin embargo, a medida que crece el número de empleados móviles y de contratistas externos, también aumenta el riesgo de fuga de datos y de incumplimiento de los mandatos impuestos por las citadas leyes y normas.

Lo cierto es que las iniciativas de cumplimiento pueden verse comprometidas con sorprendente facilidad si los empleados omiten proteger sus identidades digitales y los espacios de trabajo portátiles, los registros de clientes y los datos financieros que portan consigo. Ese es el motivo por el cual muchas organizaciones han empezado a adoptar soluciones de seguridad móviles, como las unidades USB cifradas Kingston IronKey, con el objeto de proteger sus identidades y aplicaciones digitales dondequiera que sus empleados las lleven consigo.

> **Si consideramos el cambio de tendencia generalizado hacia una huella informática más distribuida y hacia la tremenda escalabilidad de la infraestructura de la nube, resulta fácil ver que la mayoría de los sectores, y sobre todo el grueso de las pymes, ya se desinteresan de administrar salas de servidores refrigeradas.**
> - Rafael Bloom

Acceso seguro a los datos sanitarios de pacientes

El sanitario es otro sector en el cual la protección de los datos es más importante que nunca. Los datos de los pacientes se encuentran en un riesgo aún mayor de ser robados. En 2021, las vulneraciones han dejado expuestos 45,67 registros de pacientes, el mayor total anual desde 2015[2]. En lo que respecta al almacenamiento y a la copia de seguridad de los datos, los de los pacientes constan de la información crítica y exhaustiva que permite a los prestadores de servicios sanitarios tratarlos de manera segura.

Esto podría incluir desde los archivos de registros sanitarios electrónicos (EHR, por sus siglas en inglés) de los pacientes, con historiales médicos, pruebas, fotografías e imágenes radiográficas, hasta archivos administrativos que incluyen nóminas, seguros de los pacientes y cuentas a pagar. Enfrentado a una creciente fuerza de trabajo móvil y a un mercado sanitario que está experimentando una importante agitación y transformación, no es de extrañar que a los prestadores de los servicios sanitarios les preocupe la protección de los datos.

> **Especialmente en un momento en que el secuestro de datos parece ser una ocupación muy fructífera, toda organización que maneje datos sensibles debería considerar cómo operar bajo presiones extremas.**
> **- Rafael Bloom**

Además, si no se prevén los riesgos y se cumplen mandatos estrictos, como la Ley de Portabilidad y Responsabilidad de Seguros de Salud (HIPAA) o la Ley de Tecnología de la Información de Salud Clínica y Económica (HITECH) podría conllevar costosas vulneraciones de datos, con el añadido de la pérdida de confianza de los pacientes, los colaboradores o las autoridades.

Con soluciones como la gama de unidades USB cifradas Kingtson IronKey, las organizaciones sanitarias pueden establecer políticas en materia contraseñas, uso de aplicaciones, recuperación, etc. a través de un puñado o de miles de unidades, desde una única consola. Los trabajadores móviles y de primera línea pueden ser empoderados para atender a más pacientes, con soluciones que evitan la necesidad de que instalen controladores u otros software para poder acceder de manera segura a sus datos almacenados. Por su parte, usuarios y administradores pueden bloquear los datos rápida y fácilmente, independientemente de dónde se encuentren.

La unidad USB en un futuro de almacenamiento en la nube

> **El almacenamiento de datos en la nube es el presente y el futuro. Yo todavía sostengo que lo más seguro es proteger físicamente los datos; es decir, utilizando unidades USB cifradas. Los usuarios no tienen pleno control sobre lo que ocurre en la nube. Sin embargo, sí tenemos control sobre los datos contenidos en unidades USB cifradas, que protegemos y almacenamos nosotros mismos. Aparte de nosotros, nadie más tiene acceso a estos soportes. - Tomasz Surdyk**

Ahora que las ventajas de las unidades USB quedan claras, ¿cuál será exactamente su papel en un futuro de almacenamiento en la nube?

Una década atrás existía una enorme demanda de unidades USB, en calidad de principal herramienta para almacenar y transferir datos cómodamente. Sin embargo, con el impacto de los nuevos modelos de trabajo híbridos y de los equipos cada vez más distribuidos, la nube hoy permite un acceso fácil y sencillo a la información almacenada desde numerosos dispositivos. Si bien las unidades Flash fueron otrora inmensamente populares debido a la comodidad que ofrecían para transportar archivos, hoy en día, los servicios de almacenamiento en la nube facilitan mejor la portabilidad de archivos.

Dicho esto, el almacenamiento en la nube todavía tiene muchas limitaciones. Se requiere conectividad de red, lo cual no solamente impone cómo y cuándo hacer copias de seguridad o transferir archivos, sino que además supone un problema de seguridad adicional. Cuando una empresa impone el uso de la nube, no necesariamente podrá controlar desde dónde se accede a los datos. Por consiguiente, el simple acto de acceder a una VPN utilizando una conexión wifi personal o pública, nos expone al riesgo de ser pirateados. Además, los servicios en la nube son muy atractivos para los ciberdelincuentes: hoy, la mayor parte del malware (el 61%) se envía mediante aplicaciones en la nube[3].

> **Quizá sería sensato considerar qué ocurre cuando la nube no está disponible, los escenarios en los cuales los datos deben estar 100% disponibles, y dónde el almacenamiento a largo plazo podría conllevar una vulnerabilidad. - David Clarke**

La unidad USB en un futuro de almacenamiento en la nube

Por otra parte, el cifrado de USB puede hacerse mediante el hardware del dispositivo, o bien mediante software. El cifrado por hardware, sin necesidad de software, es el método más eficaz de protección de ciberataques. Se trata de una solución excelente y nada complicada de protegernos contra vulneraciones de datos, además de satisfacer estrictas normas de protección de datos para ayudar a las organizaciones a gestionar de manera fiable los riesgos y a reducir riesgos.

Por cuanto son autocontenidas, las unidades USB cifradas mediante software no requieren un elemento de software en el ordenador anfitrión. El hecho de que no exista una vulnerabilidad del software también elimina la posibilidad de ataques de fuerza bruta, de espionaje y a la memoria. Además, las unidades USB con cifrado basado en software se exponen al riesgo de que cualquier usuario pueda desactivar el cifrado formateando la unidad en cualquier ordenador y utilizándola para guardar datos sensibles de manera no protegida.

Por su parte, las unidades USB con cifrado de hardware son soportes físicos excepcionales para proteger los datos. Permiten establecer criterios de acceso a los datos por parte de un usuario o administrador, y pueden integrarse con las soluciones de terminales locales existentes. Esto las convierte en una solución práctica y económica para muchos escenarios en los que el almacenamiento en la nube no funcionaría, o no sería una solución tan eficaz. Esto puede ocurrir cuando los datos que deben almacenarse proceden de dispositivos que no están conectados a una red, o tienen que mantenerse privados o que sea necesario acceder a los mismos fuera de línea.

> **Si pensamos en que los datos pueden ser 'calientes' o 'fríos', en función de su nivel de utilidad cotidiana para una organización, sería mucho más eficiente poner los datos 'fríos' en la nube, y apoyarse más en el almacenamiento en USB localizadas para los datos 'calientes', en caso de que la continuidad operativa y el alto rendimiento sean elementos importantes para una organización o para una función o proceso crítico en particular. - Rafael Bloom**

Resumen

Aunque no podemos predecir la llegada de una futura innovación, lo que está a nuestro alcance es ofrecer una línea galardonada de unidades USB que incorporan una gama dinámica de soluciones cifradas para todos los niveles de requisitos de protección de datos móviles. Desde unidades USB con teclado alfanumérico como sencilla protección de PIN y homologación FIPS 140-2 de Nivel 3 para el nivel más alto de cifrado junto con protecciones antimanipulación, hasta tecnología SuperSpeed USB 3.1 altamente segura, los productos Kingtson IronKey han sido diseñados para resolver sus problemas de datos con unidades USB que posibilitan un transporte de datos potente y eficaz, y soluciones de almacenamiento de datos móviles.

Nuestro equipo de expertos especializados está a su disposición en todas las fases de su proyecto de almacenamiento de datos, ofreciéndole un apoyo fiable a la hora de ayudarle a encontrar la solución de almacenamiento adecuada para sus necesidades.

Tenemos las aptitudes y las capacidades técnicas para ayudarle a mantener segura la información confidencial y cumplir las nuevas normas, tanto si lo que pretende preparar un plan de USB cifradas como identificar las mejoras unidades USB para su empresa o establecer e imponer políticas de seguridad. Ofreciendo un servicio altamente personalizado, nos comprometemos a facilitarle productos que promuevan sus prioridades de almacenamiento digital y permitirle mantenerse al ritmo de la asombrosa velocidad a la que está avanzando el mundo empresarial.

Acerca de Kingston

Con más de 35 años de experiencia, Kingston cuenta con los conocimientos necesarios para identificar y resolver sus retos de datos móviles, facilitando a sus empleados trabajar con seguridad desde cualquier lugar sin comprometer a su organización.

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

©2022 Kingston Technology Europe Co LLP y Kingston Digital Europe Co LLP, Kingston Court, Brooklands Close, Sunbury-on-Thames, Middlesex, TW16 7EP, Reino Unido.
Tel: +44 (0) 1932 738888 Fax: +44 (0) 1932 785469. Reservados todos los derechos. Todos los nombres de empresas y marcas registradas son propiedad de sus respectivos dueños.

#KingstonIsWithYou