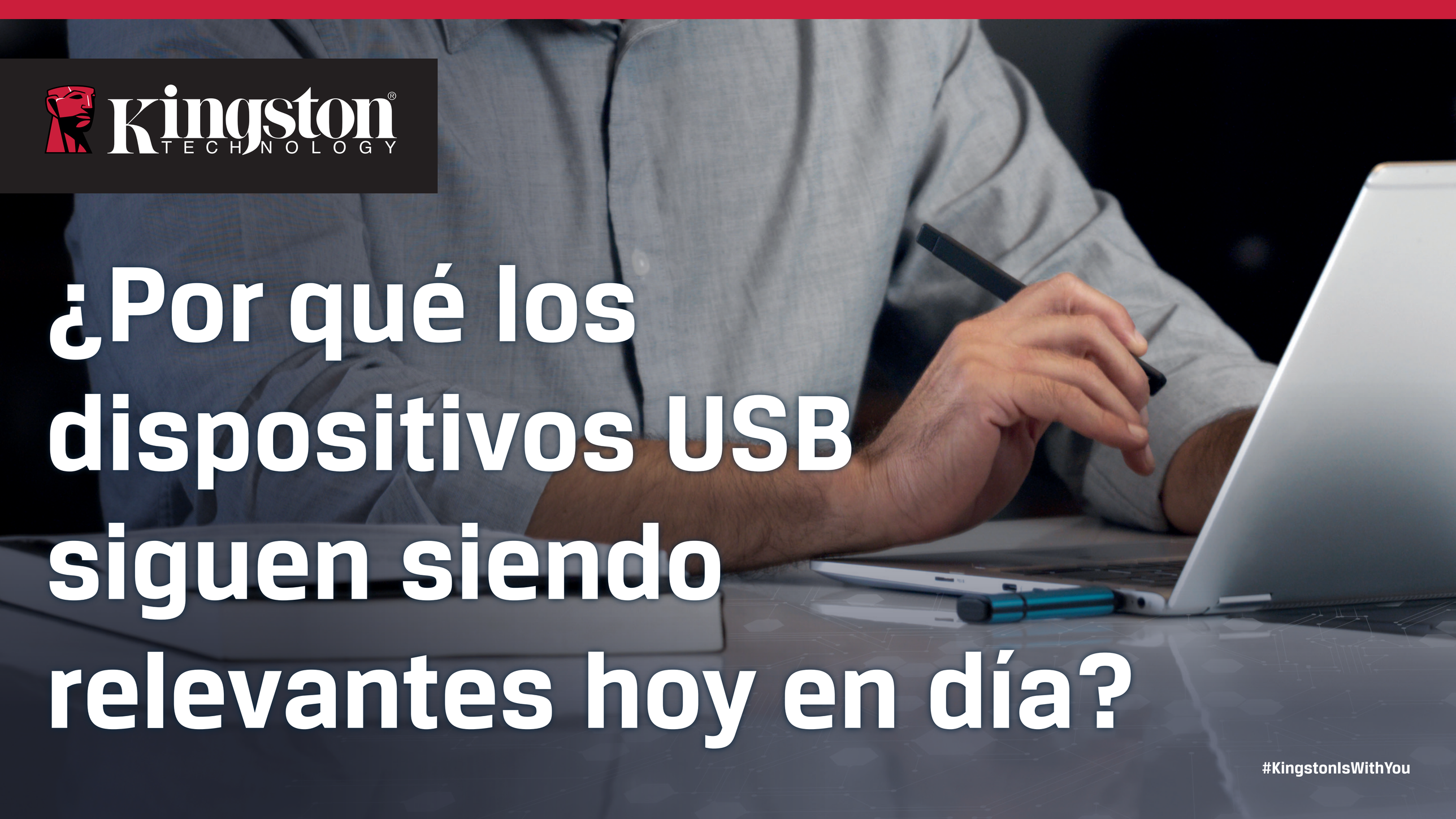

Kingston
TECHNOLOGY
¿Por qué los dispositivos USB siguen siendo relevantes hoy en día?
#KingstonIsWithYou

¿Por qué los dispositivos USB siguen siendo relevantes hoy en día?

Prólogo y contenido

En la era digital actual, donde el 60% de todos los datos corporativos globales se almacenan en la nube[1], discutir sobre la relevancia de una tecnología de almacenamiento que se acerca a los treinta años de edad puede parecer un poco extraño. Sin embargo, desde su introducción, este producto básico de almacenamiento ha evolucionado y continúa haciéndolo.

Ya pasaron los días en que los dispositivos USB eran simplemente un medio estándar para conectar archivos, dispositivos y aplicaciones. Las soluciones actuales no solo cuentan con una velocidad de transferencia muy mejorada, sino que también proporcionan medios portátiles seguro y confiables que son obligatorios en muchas situaciones. Pero ¿cómo siguen siendo relevantes los dispositivos USBs, cuando las soluciones de almacenamiento en la nube aparentemente pueden ofrecer muchos de los mismos beneficios?

Dentro de este eBook debatiremos dónde pertenecen los dispositivos flash USB en medio de un paisaje dominado por la nube. Con el apoyo de información clave de algunos de los principales expertos de la industria, exploraremos cómo las organizaciones de hoy en día están utilizando dispositivos USB y debatiremos su lugar entre el encriptado basado por software, los entornos de almacenamiento independiente y la seguridad de datos de punto final.

Tabla de contenidos	Páginas

¿Por qué los dispositivos USB siguen siendo relevantes hoy en día?

Colaboradores

Este eBook ha sido creado en conjunto de tres expertos en la industria de TI y tecnologías emergentes.

Rafael Bloom

Rafael ha desarrollado su carrera en puestos senior de Productos Tecnológicos, Comunicaciones de Marketing y Desarrollo Comercial. Su práctica de asesoría se enfoca en los nuevos desafíos organizacionales, de productos y de comunicaciones en cambios tecnológicos y regulatorios. Este trabajo altamente diverso implica experiencia en materia de gobernanza de la información y cumplimiento por diseño, privacidad de datos y tecnologías emergentes como AdTech, Móviles y 5G, IA y Machine Learning.

Tomasz Surdyk

Con más de 24 años de experiencia en seguridad de TI en el área gubernamental, Tomasz es una figura líder cuando se trata de seguridad de la información, datos personales y ciberseguridad. En su pasado, ha inspeccionado sistemas y redes de TIC que procesan información clasificada y datos personales en la administración pública, y tiene autorización de seguridad para la OTAN y la UE. Desde hace varios años es propietario de una compañía especializada en la implementación de soluciones seguras aumentando la seguridad de la información de las empresas y los datos personales.

David Clarke

David es reconocido como uno de los 10 principales influencers por Thompson Reuter "Los 30 líderes de opinión y pensadores más influyentes en las redes sociales, en gestión de riesgos, cumplimiento y tecnología de la regulación en el Reino Unido" y está en la lista de los 50 mejores expertos globales de Kingston Technology. En el pasado, David ocupó varios puestos de gestión de seguridad, como Jefe global en la Ejecución de servicios de seguridad y Jefe de infraestructura de seguridad para las empresas Global FTSE 100.

El auge de los dispositivos flash USB

Cuando el primer dispositivo Universal Serial Bus (USB) apareció en el mercado hace más de veinte años, su compatibilidad colectiva fue un cambio de juego en el campo de la tecnología informática. Con la posibilidad de hacer que las operaciones en múltiples dispositivos sean ampliamente accesibles para las masas, el USB pronto evolucionó, ofreciendo una transferencia de datos significativamente más rápida, un puerto USB 3.0, e incluso mayores capacidades con el lanzamiento del primer dispositivo flash USB en 2000.

Desde entonces, la tecnología ha recorrido un largo camino en términos de almacenamiento de datos móviles y necesidades de seguridad. El enfoque está en la generación actual de dispositivos USB que están diseñados con casos de uso muy específicos en mente. Desde una perspectiva empresarial, el aumento del trabajo remoto e híbrido, el uso de servicios en la nube y las preocupaciones de ciberseguridad están impulsando la necesidad de soluciones más efectivas. Además, los requisitos normativos exigen que los datos se almacenen en conformidad. Estas presiones a menudo se ven agravadas por sistemas distribuidos y complejos que pueden ejecutarse "in situ" y en la nube.

Luego está la cuestión del aumento de los volúmenes de datos estructurados y no estructurados, tales como documentos, correos electrónicos, fotos, videos y metadatos, todo lo cual se suma a la complejidad de las necesidades de almacenamiento empresarial en evolución.

Pero si el almacenamiento en la nube puede responder a muchos de estos desafíos, ¿qué relevancia tienen los dispositivos USB en el panorama empresarial actual?

> **Muchas personas piensan que los dispositivos USB son anticuados o triviales debido a su uso en el pasado como dispositivos más o menos desechables, de bajo rendimiento y baja seguridad. - Rafael Bloom**

Almacenamiento portátil que satisface la evolución de la demanda

Si bien los patrones más antiguos de uso de los dispositivos USB como medio para el almacenamiento portátil se han desvanecido, el uso de dispositivos USB de alto rendimiento ha surgido para realizar copias de seguridad locales personales y seguras con una capa adicional de protección de datos y confidencialidad. Esto puede ser muy importante para los datos sensibles al cumplimento de la normatividad, como los registros de recursos humanos, los datos financieros, los registros sanitarios, la seguridad de la propiedad intelectual (IP) y toda la información personal identificable (PII). Además, esta generación de dispositivos viene con capacidades de transferencia rápida de datos, almacenamiento, respaldo y seguridad que se pueden utilizar para:

- Información reglamentaria que necesita ser entregada a mano
- Documentos legales y financieros que deben entregarse e imprimirse en el sitio o fuera del sitio
- Cualquier entorno potencialmente hostil donde el ransomware pueda ser una amenaza
- Transferencia a sistemas de impresión donde no se permite el acceso a la red

Los principales proveedores de USB encriptados Kingston Technology han seguido el ritmo de la evolución de la demanda con el lanzamiento de soluciones como el Kingston IronKey™ S1000. Este dispositivo USB encriptado, el mejor de su clase, cumple con las normas más estrictas y cuenta con la capacidad de proteger los datos confidenciales mediante el encriptado XTS-AES de 256 bits junto con un criptochip independiente que cuenta con sólidas protecciones antimanipulación. Asimismo, cuenta con certificación FIPS 140-2 de nivel 3. Esto significa que ha sido validado formalmente por el gobierno de EE. UU. por su efectividad como una pieza de hardware criptográfico, lo que lo hace ideal para las organizaciones que necesitan mayor tranquilidad cuando se trata de protección de datos.

Estos dispositivos USB encriptados por hardware ofrecen soluciones centralizadas de administración de dispositivos seguros, ya sea que sus datos estén basados en la nube o "in-situ". El almacenamiento de datos encriptados que cumple con la normatividad y que es fácil de usar sin necesidad de software también libera un valioso tiempo de TI, ofreciendo soluciones diseñadas para una implementación rápida y eficiente.

Almacenamiento portátil que satisface la evolución de la demanda

La copia de seguridad y el archivado es otro ejemplo en el que los dispositivos USB se pueden utilizar para proteger los activos digitales a largo plazo e independientemente de los servicios en la nube de terceros. Si bien es cierto que las grandes transferencias de datos se manejan fácilmente en la nube, la IP patentada aún puede ser lo suficientemente sensible como para que valga la pena almacenarla en un dispositivo USB encriptado y seguro, que se puede almacenar lejos del Internet y con total seguridad.

Entonces siempre habrá circunstancias en las que una organización necesite que los datos estén lógica y físicamente bajo su control, especialmente cuando se utilizan dispositivos encriptados. Y hay casos en los que el almacenamiento en un disco duro/SSD no se puede encriptar. El uso de dispositivos USB encriptados externos resuelve este problema, como el Kingston IronKey D300S. Este dispositivo flash USB cuenta con el encriptado por hardware XTS 256-bit estándar de encriptación avanzada (AES), que es un tipo de encriptado por bloques que puede encriptar bloques de datos de 128 bits. Y cuando existe la necesidad de encriptar datos más allá de esto, AES utilizará el modo de encriptado de bloque XTS que es capaz de proporcionar una mejor y más fuerte protección de datos que los modos anteriores.

> En mi opinión, los dispositivos flash USB se siguen utilizando y son una parte integral de la seguridad de los datos. Se utilizan, entre otros: para transferir rápidamente información entre dispositivos, así como para su almacenamiento y protección adecuados.
> - Tomasz Surdyk

Encriptación: Basado en hardware versus basado en software

Observando cómo se encriptan los datos, se puede argumentar que el encriptado basado en hardware es más fácil de administrar y más seguro que el encriptado basado en software. Esto se debe a que el proceso de encriptado se mantiene separado del resto del sistema huésped, por lo que es mucho más difícil de interceptar o romper. La administración centralizada a nivel de dispositivo permite el control de dispositivo sobre las conexiones LAN de intranet e Internet, y puede ser una excelente herramienta para:

- Establecimiento y aplicación de políticas de uso de USB individuales y/o grupales encriptadas
- Auditar la actividad de los archivos para realizar un mejor seguimiento de los datos a medida que se mueven dentro y fuera de su organización
- Proporcionar respaldo de contenido remoto para el transporte de datos críticos
- Desactivar remotamente dispositivos cuando se pierde o se pone en peligro un USB
- Realizar restablecimiento de contraseña remotos cuando está se olvida

Cuando los dispositivos autorizados se gestionan correctamente de esta manera, se minimiza el riesgo de que se copien y compartan datos confidenciales. Además, los dispositivos USB modernos encriptados por hardware ofrecen una gran cantidad de funciones de seguridad adicionales que ayudan a evitar que cualquier persona que no sea el destinatario previsto acceda o lea archivos y mensajes.

> **Creo que el encriptado por hardware es mejor que el encriptado por software. Las diferencias entre los métodos de encriptado por hardware y software son significativas en términos de vulnerabilidad a los ataques de fuerza bruta. En el caso de los dispositivos encriptados por hardware, no es fácil sucumbir a tales ataques. - Tomasz Surdyk**

Encriptación: Basado en hardware versus basado en software

Si bien las empresas pueden considerar el encriptado basado en software debido al costo, esto puede ser un poco miope. Las soluciones basadas en software comparten los recursos de encriptado del dispositivo huésped con otros programas, por lo que solo es tan seguro como el equipo y a menudo requieren actualizaciones de software que, si no se mantienen, lo dejarán vulnerable. Los dispositivos USB encriptados por software pueden estar sujetos a ataques de fuerza bruta ilimitados para adivinar la contraseña, y no tienen medios para resistir ataques de diccionario basados en software, que pueden probar millones de combinaciones de caracteres en períodos cortos de tiempo.

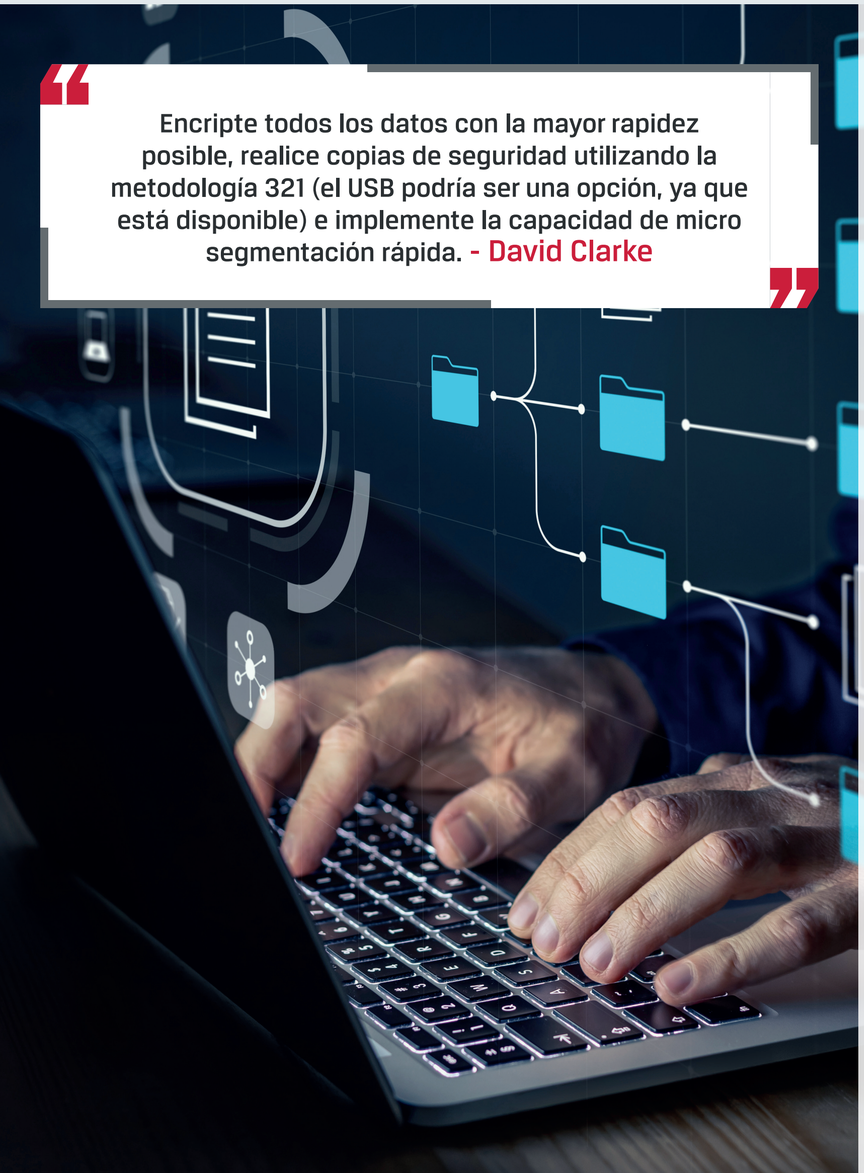
Asimismo, el encriptado por software también es un encriptado removible. Cualquier empleado con un dispositivo encriptado por software puede copiar los datos, formatear el dispositivo USB y se eliminar el encriptado. Luego pueden copiar los archivos de datos y utilizar el dispositivo sin las molestias de autenticarse en diferentes plataformas y sistemas operativos.

Como mencionamos anteriormente, con el encriptado basado en hardware, el "encriptado " físico - y el posterior almacenamiento de datos - se produce independientemente del sistema huésped. Esto garantiza una capa adicional de defensa, si los sistemas alguna vez se vieran comprometidos.

Esto no se puede pasar por alto, particularmente para aquellos en industrias como las financieras, la atención médica y el gobierno. Esto se debe a que las regulaciones como la Ley de portabilidad y responsabilidad del seguro médico (HIPAA) y el Estándar de seguridad de datos de la industria de tarjetas de pago (PCI DSS) a menudo cuentan con requisitos estrictos con respecto al encriptado de información confidencial.

Cumplir con estas regulaciones mediante el uso de dispositivos encriptados por hardware en última instancia, ayudará a las organizaciones a evitar multas costosas, demandas y daños a la reputación potencialmente paralizantes. Si bien los dispositivos encriptados por hardware pueden ser más costosas que los dispositivos USB básicos más baratos, los costos legales de una violación de datos pueden pagar fácilmente cientos de dispositivos en solo unas pocas horas de tarifas de consulta legal.

La creciente necesidad de proteger los datos confidenciales



> Encripte todos los datos con la mayor rapidez posible, realice copias de seguridad utilizando la metodología 321 (el USB podría ser una opción, ya que está disponible) e implemente la capacidad de micro segmentación rápida. - David Clarke

Cuando se trata de proteger datos confidenciales contra pérdida y robo, cada organización tiene la obligación de garantizar que sus dispositivos tengan las características de seguridad adecuadas. También es importante tener en cuenta que, si bien hay una miríada de amenazas cibernéticas en constante evolución, el nivel de madurez digital y las habilidades de gestión de datos de los usuarios siguen siendo un factor de riesgo prominente si no se abordan. La amenaza interna que incluye la pérdida del control de datos o de dispositivos de almacenamiento USB, la transmisión de datos fuera de un entorno seguro, el uso de dispositivos USB no encriptados y el intercambio de contraseñas pueden ser el resultado de una falta de diligencia por parte del usuario final. Todo lo cual se puede evitar con la formación, educación y las soluciones de dispositivo USB adecuadas.

> La organización debe tener un mapa claro de su información, incluido el nivel de importancia y/o sensibilidad de todos sus conjuntos de datos, con el plan abordando primero los datos más importantes, ya sea eliminando físicamente la conexión a los datos o haciendo que esa fuente de datos se oscurezca. Ser capaz de aislar rápidamente los sistemas afectados es clave, y una vez más, tener un plan documentado que haya practicado anteriormente es absolutamente vital. - Rafael Bloom

La planificación previa y una estructura de comunicaciones bien practicada también desempeñan un factor clave para hacer frente a una amenaza potencialmente existencial. Las amenazas cibernéticas actuales están destinadas a abordar los puntos débiles de las organizaciones.

El mejor momento para desarrollar un plan USB encriptado es antes de que sea realmente necesario, incorporando dispositivos y políticas USB encriptados en la estrategia de seguridad general de su organización. Al no tener un plan para los USB encriptados y no tener directrices, no tiene nada en qué basarse, y su organización está abierta al riesgo en todos los niveles, incluido el incumplimiento de las regulaciones, tales como el Reglamento general de protección de datos (GDPR), donde el artículo 32 establece específicamente que los datos confidenciales deben encriptarse.

> Los usuarios procesan datos confidenciales. Perder estos aumenta la responsabilidad y afecta significativamente la imagen y la seguridad de la empresa. Para proteger los datos confidenciales, se deben utilizar varias soluciones de seguridad, incluido el encriptado de datos. - Tomasz Surdyk

Asegurar datos financieros confidenciales

Junto con las implicaciones de seguridad, también hay estándares de cumplimiento que las soluciones de almacenamiento de datos y copias de seguridad deben cumplir. Algunas de estas prácticas, como la necesidad de gestionar y hacer cumplir los planes de retención de datos, son comunes en todos los sectores verticales, mientras que otras, como la migración de los datos de la empresa a la nube, se tratan de forma muy diferente.

En muchos sectores verticales, como el de los servicios financieros, han entrado en vigor normativas que han hecho obligatoria la gestión adecuada de los datos. Sobre todo, los bancos, inicialmente eran muy reticentes a usar terceros para el almacenamiento y copias de seguridad, y muchos todavía insisten en poseer toda su infraestructura de datos.

Las instituciones financieras también están obligadas a cumplir con una lista creciente de regulaciones y estándares de seguridad de datos, como la Ley Sarbanes-Oxley (SOX) y el Reglamento general de protección de datos (GDPR). Sin embargo, a medida que crece el número de empleados y contratistas móviles, también lo hace el riesgo de fuga de información y el incumplimiento de los mandatos impuestos por dichas leyes y normas.

La verdad es que los esfuerzos de cumplimiento pueden verse comprometidos con sorprendente facilidad si los empleados móviles no logran proteger sus identidades digitales, sus espacios de trabajo portátiles, y los registros de clientes y datos financieros que llevan. Es por eso que cada vez más organizaciones están avanzando hacia soluciones de seguridad móvil como los dispositivos USB encriptados Kingston IronKey, para proteger las identidades digitales y las aplicaciones sin importar dónde las lleven sus empleados.

> **Cuando se considera el cambio de tendencia general a una huella de TI más distribuida y la gran escalabilidad de la infraestructura de la nube, es fácil ver cómo la mayoría de las industrias, y la mayoría de las PYMEs, ya no se preocupan por la gestión de salas de servidores refrigerados. - Rafael Bloom**

Acceso seguro a los datos de salud del paciente

La atención médica es otra industria donde la seguridad de los datos es más importante que nunca. La información de los pacientes corre un riesgo aún mayor de ser robada, con violaciones que exponen 45,67 millones de registros de pacientes en 2021, el total anual más grande desde 2015[2]. Cuando se trata de almacenamiento de datos y copias de seguridad, los datos de los pacientes corresponden a la información médica crítica y completa que permite a los proveedores de atención médica tratar a sus pacientes de manera segura.

Esto podría incluir todo, desde archivos de registros electrónicos de salud (EHR) de los pacientes, los cuales contienen historias clínicas, exámenes fotografías e imágenes radiográficas, hasta archivos administrativos que incluyen registros de nómina, información del seguro del paciente y cuentas por pagar. Enfrentados a una creciente fuerza laboral móvil y a un mercado global de atención médica que está experimentando una gran agitación y transformación, no es de extrañar que los proveedores de atención médica de hoy estén preocupados por la seguridad de los datos.

> **Dado que el ransomware en particular es una especie de industria en crecimiento, todas las organizaciones que manejan datos confidenciales deben considerar cómo operar bajo una presión extrema. - Rafael Bloom**

Además, el no anticipar los riesgos y no cumplir con mandatos estrictos como la Ley de portabilidad y responsabilidad del seguro médico (HIPAA) o la Ley de tecnología de información de salud para la salud económica y clínica (HITECH) podría resultar en una costosa filtración de datos de atención médica, lo que puede sacudir aún más la confianza del paciente, socio o regulador.

Con soluciones como la gama de dispositivos USB encriptados de Kingston IronKey, las organizaciones de atención médica pueden establecer políticas para contraseñas, uso de aplicaciones, recuperación y más, en un puñado de dispositivos o miles de ellos, desde una sola consola. Los trabajadores móviles y de primera línea pueden ser empoderados para apoyar a más pacientes, con soluciones fáciles de usar que eliminan la necesidad de que los empleados instalen controladores u otro software, con el fin de acceder de forma segura a sus datos almacenados. Mientras los usuarios y administradores pueden bloquear datos de forma fácil y rápida, sin importar a dónde vayan.

El dispositivo USB en un futuro conjunto con el almacenamiento en la nube

> **El almacenamiento de datos en la nube es el presente y el futuro. Continuó argumentando que proteger físicamente los datos, por ejemplo, mediante el uso de dispositivos USB encriptados, es lo más seguro. Los usuarios no tienen control total sobre lo que sucede en la nube. Sin embargo, tenemos control sobre los datos en los dispositivos USB, que aseguramos y almacenamos nosotros mismos. Aparte de nosotros, nadie tiene acceso a estos medios. - Tomasz Surdyk**

Ahora que los beneficios de los dispositivos USB son claros, ¿cuál es exactamente su papel en un futuro de almacenamiento en la nube?

Hace una década, dispositivos USB tenían una gran demanda como la herramienta principal para almacenar y transferir datos de manera conveniente. Sin embargo, con el impacto de nuevos modelos de trabajo híbridos y equipos de trabajo cada vez más distribuidos, la nube ahora proporciona acceso rápido y simple desde muchos dispositivos a la información almacenada. Mientras que los dispositivos flash fueron alguna vez inmensamente populares debido a la comodidad única que ofrecían para el transporte de archivos. Hoy en día, los servicios de almacenamiento en la nube ofrecen una mayor facilidad de portabilidad de archivos.

Dicho esto, todavía hay muchas limitaciones cuando se trata de almacenamiento en la nube. Se requiere conectividad de red, que no solo dicta cómo y cuándo se pueden realizar copias de seguridad o transferir archivos, sino que agrega una preocupación de seguridad adicional. Cuando una empresa exige el uso de la nube, no es necesariamente capaz de controlar desde dónde se accede a los datos. Por lo tanto, el simple acto de acceder a una VPN utilizando una conexión Wi-Fi personal o pública abre el riesgo de ser hackeado. Además, los servicios en la nube son muy atractivos para los agentes de amenazas, ya que la mayoría de los programas maliciosos (61%) se distribuyen ahora a través de aplicaciones en la nube[3].

> **Tal vez sea prudente considerar lo que sucede cuando la nube no está disponible, los escenarios donde los datos deben estar 100% disponibles y donde el almacenamiento a largo plazo podría crear una vulnerabilidad. - David Clarke**

El dispositivo USB en un futuro conjunto con el almacenamiento en la nube

Por otro lado, el encriptado USB se puede realizar a través del hardware del dispositivo o del software. El encriptado sin software y centrado en el hardware es el medio más efectivo para brindar protección contra los ataques cibernéticos. Es una solución excelente y sencilla para proteger contra violaciones de datos, y puede cumplir con los estrictos estándares de cumplimiento con la máxima seguridad en la protección de datos para ayudar a las organizaciones a gestionar con confianza las amenazas y reducir los riesgos.

Al ser autosuficientes, los dispositivos USB encriptados por hardware no requieren un elemento de software en la computadora huésped. Ni la vulnerabilidad del software dará pie la posibilidad de ataques de fuerza bruta, rastreo y hash de memoria. Los dispositivos USB encriptados por software también se enfrentan al riesgo de que cualquier usuario pueda deshabilitar el encriptado formateando el dispositivo en cualquier computadora y use el dispositivo para almacenar datos confidenciales de manera desprotegida.

Los dispositivos USB encriptados por hardware también ofrecen un medio físico excepcional para mantener los datos seguros. Permiten que los criterios de acceso a la información sean establecidos por un usuario o administrador, y pueden integrarse con soluciones locales de punto final existentes. Esto los convierte en una solución conveniente y rentable para muchos escenarios donde el almacenamiento en la nube no funcionaría o no sería una solución tan efectiva. Esto puede ser cuando los datos necesitan ser almacenados desde dispositivos que no están conectados a la red, que necesitan ser privados, o que requieren acceso cuando están fuera de línea.

> **Si pensamos que los datos son 'fríos' o 'calientes' dependiendo de su nivel de utilidad diario para una organización, entonces podría ser más eficiente poner datos 'fríos' en la nube y apoyarse más en el almacenamiento USB localizado para datos 'calientes', si la continuidad operativa y el alto rendimiento es lo más importante para la organización, o para una función o proceso crítico para el negocio en particular.**
>
> - Rafael Bloom

Resumen

Si bien no podemos predecir la llegada de innovaciones futuras, lo que podemos ofrecer es un galardonado portafolio de dispositivos USBs que ofrecen una gama dinámica de soluciones encriptadas para todos los niveles de requisitos de protección de datos móviles. Desde los dispositivos USB que cuentan con un teclado alfanumérico para una protección de PIN fácil de usar; hasta con la certificación FIPS 140-2-Level 3 para el más alto nivel de encriptado junto con protecciones antimanipulación; hasta la tecnología SuperSpeed USB 3.1 que no compromete la seguridad, los productos Kingston IronKey están diseñados para satisfacer sus desafíos de datos, con dispositivos USB que prometen soluciones potentes y efectivas de transporte de datos y almacenamiento de datos móviles.

Nuestro equipo especializado de expertos está listo para ayudarle en cada paso de su viaje en el almacenamiento de datos, ofreciendo un par de manos confiables cuando se trate de ayudarlo a encontrar la solución de almacenamiento adecuada para satisfacer sus necesidades.

Tenemos las habilidades y la capacidad técnica para ayudarlo a mantener segura la información confidencial y cumplir con la nueva normatividad, ya sea que esté buscando crear un plan USB encriptado, identificar los mejores dispositivos USB para su negocio, o establecer y aplicar políticas de seguridad. Al ofrecer un servicio altamente personalizado, nos comprometemos a ofrecer productos que respalden sus prioridades de almacenamiento de datos, permitiéndole seguir el ritmo de la velocidad sin precedentes a la que se mueve el mundo empresarial.

Acerca de Kingston

Con 35 años de experiencia, Kingston tiene los conocimientos necesarios para identificar y resolver sus desafíos en materia de datos móviles, lo que facilita que su personal desempeñe su trabajo de forma segura sin poner en peligro 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

#KingstonIsWithYou