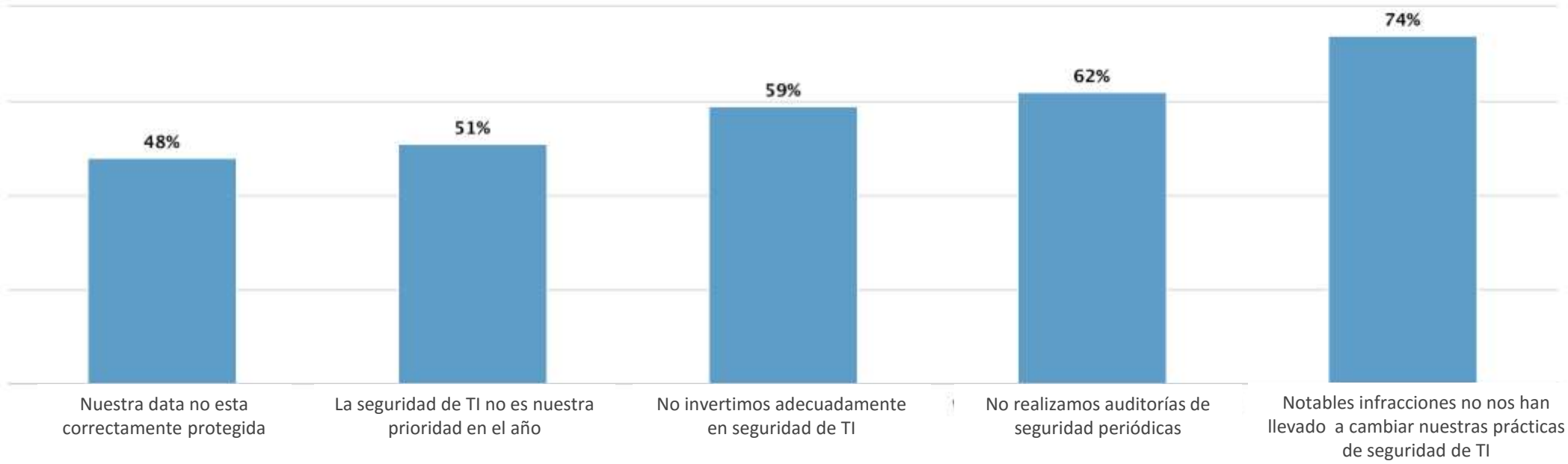
Kingston Technology

Como minimizar los riesgos en el transporte de información

Seguridad, organizaciones en riesgo

Percepciones de seguridad (Porcentaje de aquellos que seleccionaron “de acuerdo” o “muy de acuerdo)



Reporte de estado de las TI de Spiceworks (800 profesionales de TI)

Las compañías tienen sus razones para proteger los datos

Las organizaciones gastan millones tratando de evitar violaciones de datos.

Para entes gubernamentales	Financiero	Responsabilidad social	Protección de activos
• Más de 32 directivas para proteger globalmente los datos personales	• El costo promedio por violación datos es de $6,5 millones	• Las personas esperan que sus datos personales estén protegidos.	• La propiedad intelectual y los secretos de la compañía puede ser una ventaja competitiva.

1. 80% de las empresas no cuentan con una sistema para prevenir virus o malware por USBs.
2. El 50% de las empresas reconocen haber perdido USBs con información confidencial.
3. Sólo el 5% de las empresas en LATAM exigen el uso de contraseñas y encriptación de USBs.
4. Las compañías que comprometen información pierden hasta el 20% de sus clientes.

Seguridad de la información

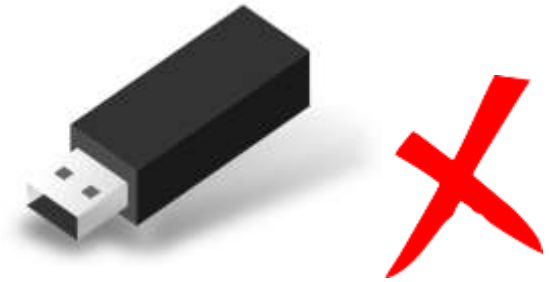
Antivirus Administrador de punto final ✓

VPN ✓

Seguridad en la nube ✓

Firewall ✓

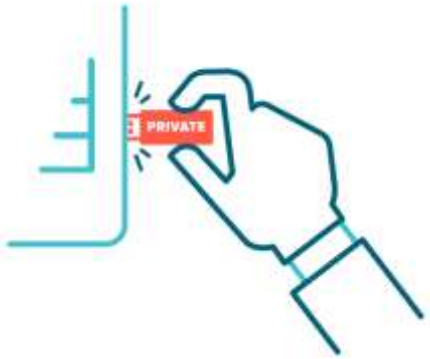
ACL VLAN ✓



Información en memorias USB

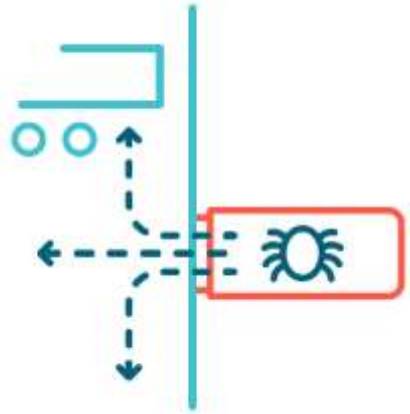
Los 4 mayores riesgos

Alguien que accidentalmente pierde una memoria USB



Una memoria USB llena de información es robada

Un usuario en quien confiamos esconde información en un USB

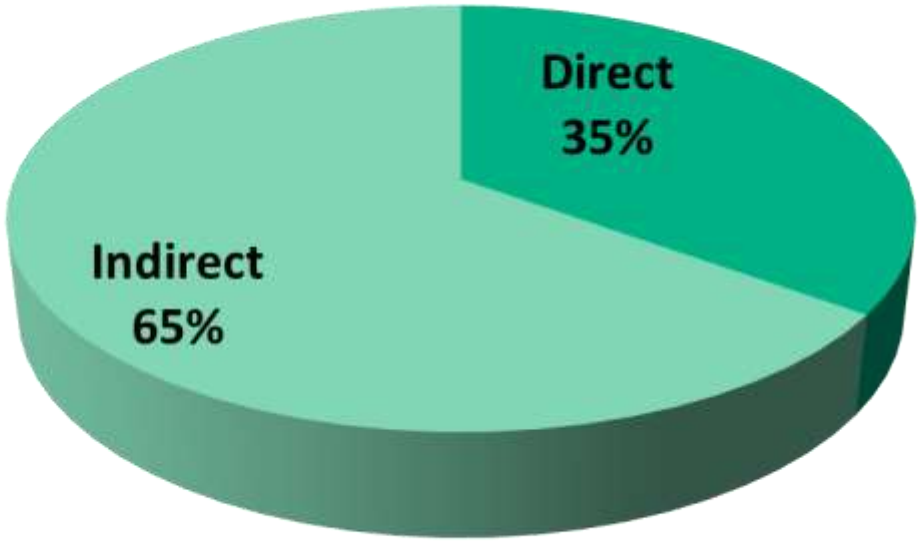


Alguien en la organización encuentra un USB y lo conecta por curiosidad*.

*48% de los usuarios abre al menos un archivo.

Detalle de los costos de las violaciones de datos

- Publicidad negativa
- Rotación de clientes
- Pérdida de oportunidades de negocios*
- Adquisición de nuevos clientes
- Disminución del fondo de comercio
- Empleados improductivos



- Investigación
- Honorarios legales
- Multas/Juicios
- Protección de la identidad
- Costos de notificación
- Reemplazar/contratar nuevo personal

Muchas empresas han perdido información en USBs

Algunas empresas ya están protegidas…

Deloitte. EY Volkswagen HARLEY-DAVIDSON MOTOR COMPANY

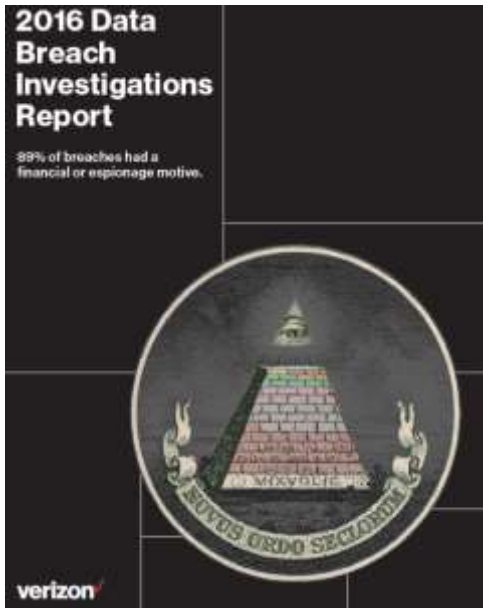
Información gubernamental fue a dar a un bar

Basta con escribir en Google "información confidencial USB", y aparecerán casos como:

- Gobierno de Gran Bretaña
- Milicia de Estados Unidos
- CEMEX
- Hospitales
- Consejo de planeación familiar de Filadelfia

http://netmedia.info/articulos.php?id_art=8642&id_sec=31

Mercado



When we zoom in on just confirmed breaches, the numbers are less astronomical and we see industries such as Accommodation and Retail accounting for a more significant percentage of breaches (as opposed to incidents). This is unsurprising as they process information which is highly desirable to financially motivated criminals.

Industry	Total	Small	Large	Unknown
Accommodation (72)	362	140	79	143
Administrative (56)	44	6	3	35
Agriculture (11)	4	1	0	3
Construction (23)	9	0	4	5
Educational (61)	254	16	29	209
Entertainment (71)	2,707	18	1	2,688
Finance (52)	1,368	29	131	1,208
Healthcare (62)	166	21	25	120
Information (51)	1,028	18	38	972
Management (55)	1	0	1	0
Manufacturing (31-33)	171	7	61	103
Mining (21)	11	1	7	3
Other Services (81)	17	5	3	9
Professional (54)	916	24	9	883
Public (92)	47,237	6	46,973	258
Real Estate (53)	11	3	4	4
Retail (44-45)	370	109	23	238
Trade (42)	15	3	7	5
Transportation (48-49)	31	1	6	24
Utilities (22)	24	0	3	21
Unknown	9,453	113	1	9,339
Total	64,199	521	47,408	16,270

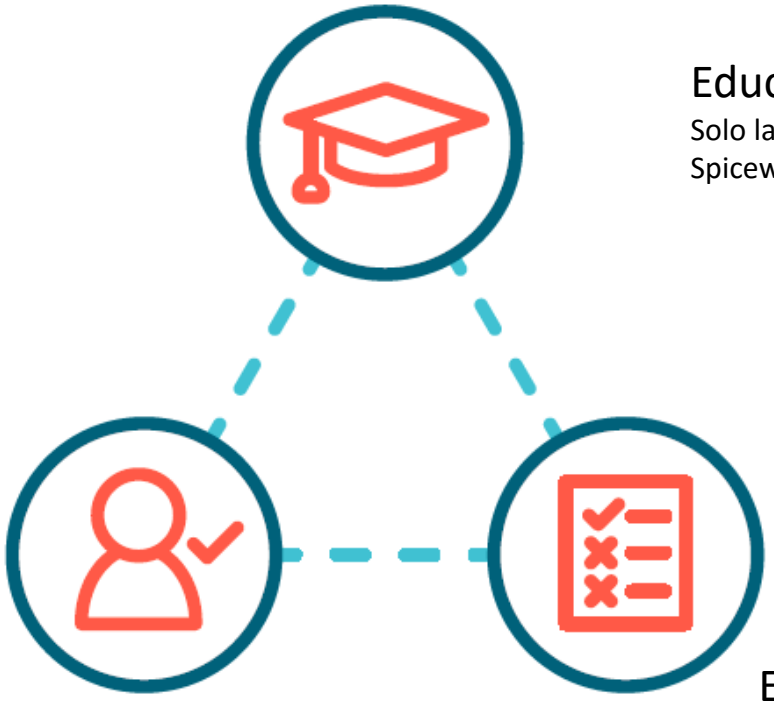
(Página. 4)

Table 1.
Number of security incidents by victim industry and organization size, 2015 dataset.

¿Qué deben hacer las organizaciones?

Políticas de restricción de uso.

Políticas documentadas y comunicadas consistentemente. Un 80% tiene políticas.
19% deja que toda la empresa las utilice
Solo 10% permite solo USBs encriptados



Educación al usuario.

Solo la mitad de los encuestados por Spiceworks educa a los usuarios.

Ejecución de las políticas

Es más eficiente si son automatizadas y sistematizadas
Y no cuando se confía en el honor o responsabilidad del usuario.

Opciones de políticas a ser consideradas por las organizaciones

Bloqueo de puertos USB

+ Seguridad definitiva
- Limita flexibilidad al empleado
- Costos/ entrenamiento para otros sistemas de transferencia de datos

Uso de USBs Encriptados

+ Flexibilidad para los empleados
+ Seguridad de datos
+ Punto final manejable
- Inversión de Hardware

Provee:

- **Seguridad organizacional**
- **Seguridad física**
- **Gobernación del riesgo**
- **Control de acceso**
- **Continuidad del negocio**
- **Conformidad con estándares**

Gestione amenazas y maneje riesgos

Kingston cubre cada uno de los niveles de sus necesidades empresariales.

- **USB encriptado para almacenamiento de datos con cumplimiento al 100%**
- **Simple, fácil de usar, no necesita otros dispositivos o softwares.**
- **Diseñado para un despliegue rápido y eficiente**

Regulaciones Globales

- Implementación y aplicación de estándares de seguridad cibernética y de datos para proteger la información sensible.

Malware / Intrusión / Elemento humano

- El malware es una manera de infectar computadoras y redes para obtener, manipular y controlar sistemas y datos. El usuario no se entera.

Dispositivos USB

El uso de USBs no encriptados derivados de Bring Your Own Device (BYOD) y freebies aleatorios.

Por qué un USB Encriptado de Kingston

- **30 años** de **Liderazgo en** Tecnología, **Innovación** y **Confiabilidad**
- El líder mundial en dispositivos de almacenamiento USB encriptados por hardware, de seguridad basada en hardware mejorada, y administrados
- Diseñado para proteger datos altamente confidenciales que requieren de una seguridad hermética, estos dispositivos cumplen con las directivas específicas de agencias como TAA y FIPS.
- Los sectores del gobierno, empresarial, de salud, educación, financiero y de consumo confían en Kingston.

Línea de productos USB encriptados

Kingston te mantiene en conformidad

Seguridad personal • SMB / Seguridad profesional • Grado militar de alta gama

USB encriptado DataTraveler

DT2000

DTVP30

DTVP30AV

DTVP30DM
DT4000G2DM

IRONKEY™

IKS3000/ IKS300M
IKS1000B/ IKS1000E

Los dispositivos USB encriptados se integran con la seguridad de punto final.

A través de la gestión de punto final, las compañías pueden poner en lista blanca a los dispositivos USB aprobados por la compañía para asegurarse de que los usuarios utilicen siempre encriptación.

KASPERSKY lab

intel Security

Symantec.

SOPHOS

Lista blanca

- ID del Proveedor
- ID del producto
- Números de serie

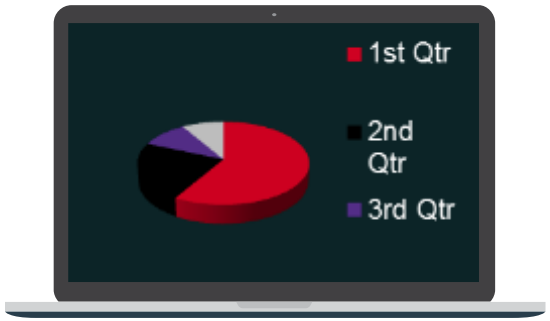
Kingston TECHNOLOGY

Encripción de datos en Laptops

6 veces más rápida

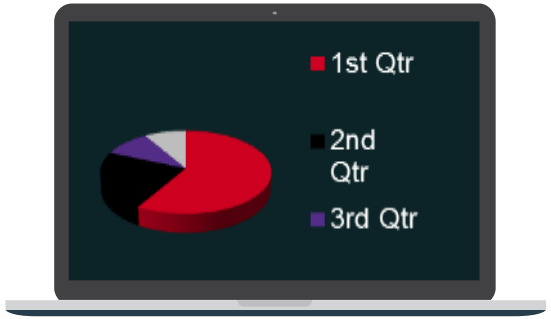
KC400/240G
Corporate class SSD

1 hora, 8 min*



Seagate 500GB
SATA3 16Mb
7200 rpm HDD

6+ hours*

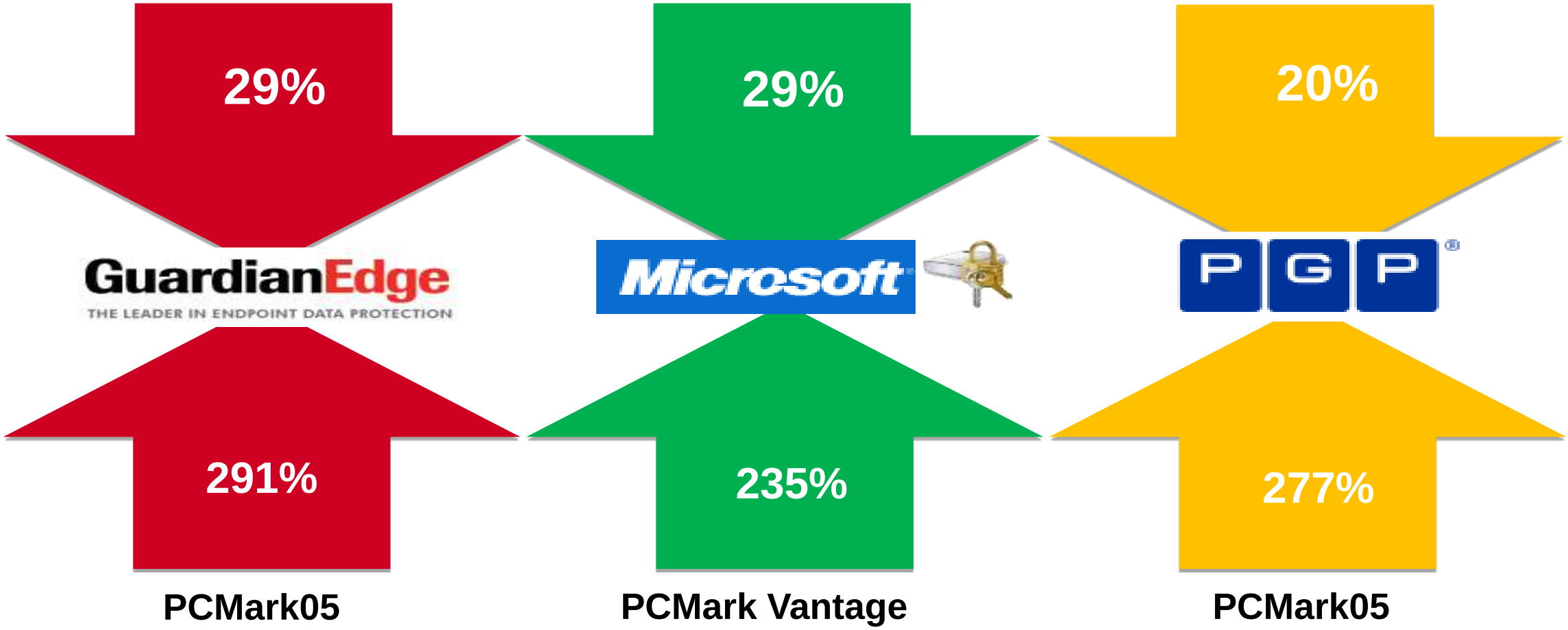


Computo personal

- Laptops encriptadas pierden 30% de desempeño
- PCs viejas adquieren nueva de 2 a 3 años más de vida
- Transporte de datos confidenciales

Deloitte.
HSBC
EY

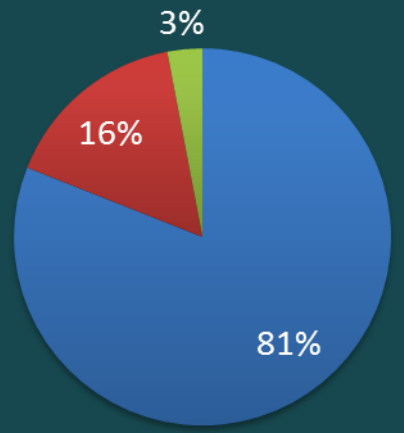
Recuperación en el desempeño perdido por criptografia de software (7200 RPM HDD vs. SSD)



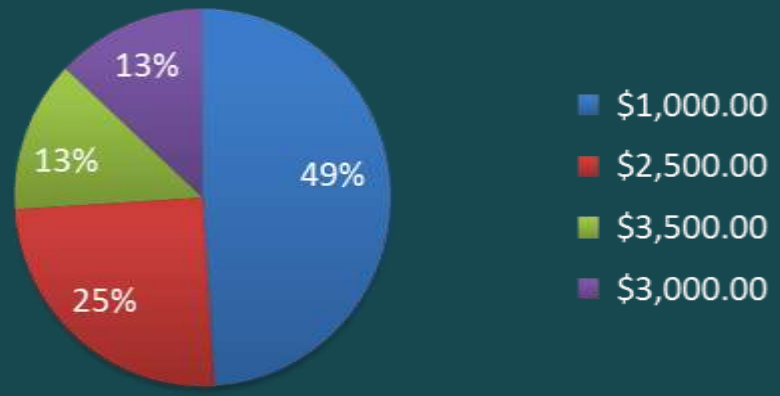
* Based on internal Kingston testing using Kingston V+100 vs. 7200 RPM HDD

Rompiendo el mito del precio del SSD

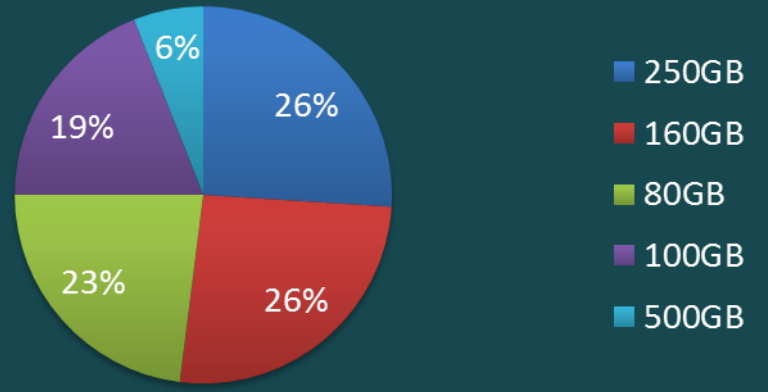
Capacidad promedio HDD en la empresa

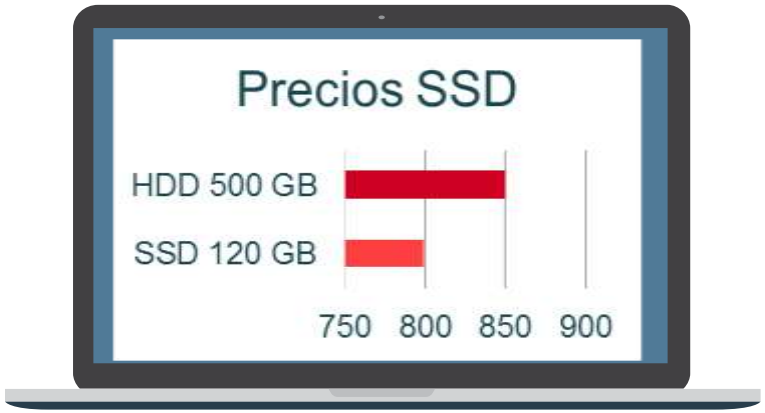


Calcula el precio de un SSD 120GB



Uso promedio del HDD





Resultados

- El 51% de los usuarios finales tienen una idea erronea del precio
- Un SSD de 120GB es más barato que un HDD de 500GB
- El 94% de los usuarios utilizan menos de 250GB de almacenamiento

El precio no es un problema!

Encuesta realizada por Kingston ene 2016 a 50 empresas.

Kingston TECHNOLOGY

SSD con encripción: UV500

x10

10X más rápido* que un disco duro

- Con increíble velocidad de lecutura y escritura el UV500 no solo aumenta el desempeño, sino que puede traer nueva vida a los sistemas viejos.

Ideal para desktop & notebooks

Viene en multiples factores de forma (2.5”/M.2/mSATA) para satisfacer un amplio número de sistemas. Es ideal para notebooks y sistemas de con espacio limitado.

Protección Encriptada

Proteja datos sensibles con soporte Encripción basada en hardware de 256-bit AES Hardware-based Encryption y TCG Opal 2.0.

GB

Multiples capacidades disponibles

- Disponible hasta en capacidades de 960GB
- Proporciona espacio suficiente para todos los archivos aplicaciones, videos y fotos
- Puede reemplazar un SSD de menor capacidad para satisfacer las necesidades de almacenamiento.

*Based on internal testing

Contactos de Kingston México

Colombia

Juan Jose Sandoval
Country Manager- Colombia
Cel.: +573185340738
Juan_sandoval@kingston.com

Corporativo de ventas

Gerardo Rocha
Gerente corporativo para Latinoamérica
Cel.: +5215539124280
Gerardo_rocha@kingston.com

Ingeniería

Ing. Armando Galván C.
Gerente de tecnología SSD
Tel Oficina. 01(55) 1105-0879
Armando_Galvan@kingston.com

Ing. Luis E. Pérez Plata
RAM Gerente de tecnología para Latinoamérica
Tel: 01 (55)1105-0564/65
Luis_perez@kingston.com

Soporte Técnico

Soporte_CN@kingston.com Tel. 018000219694

Kingston Technology

Productos con encriptación

Línea de productos Encriptados DataTraveler

Lower Cost → Most Secure

	Locker+ G3	Vault Privacy 3.0	2000	4000G2
				
Encriptado	Encriptado por hardware	Encriptado por hardware AES de 256 bits	Encriptado por hardware AES de 256 bits	Encriptado por hardware AES de 256 bits
Característica	Software USBtoCloud™	Modo de encriptado en bloques XTS	SO independiente	Modo de encriptado en bloques XTS
FIPS	n/r	FIPS 197	FIPS 197 (aplicación)	FIPS 140-2 Nivel 3
Capacidades	8GB a 64GB	4GB a 64GB	16GB a 32GB	4GB a 64GB
Anti-Virus	Disponible a través de USBtoCloud™	SKUs anti-virus disponibles	n/r	n/r

DT Locker+G3: Protección de datos personales fácil de usar

USB 3.0	Lectura*	Escritura*
8GB	80MB/seg	10MB/seg
16GB	135MB/seg	20MB/seg
32GB	135MB/seg	40MB/seg
64GB	135MB/seg	40MB/seg

- **Encriptación basada en hardware** — Lo mejor en seguridad personal, para mantener protegida la información.
- Facilidad de uso – no es necesaria la instalación de aplicaciones
- Protección de avanzada mediante contraseña
  - Contraseña compleja
  - Se bloquea después de 10 intentos
- **Ahora con Software USBtoCloud** , que incluye respaldo de archivos a Google Drive, Amazon S3, Microsoft OneDrive, Dropbox, Box, OneDrive para Business o ShareFile.
- **Anti-Virus disponible a través de USBtoCloud™**
- Carcasa metálica duradera
- USB 3.0, compatible con USB 2.0
- Funciona de forma intercambiable con sistemas Mac y Windows**
- Garantía de 5 años
- Capacidades de 8 a 64GB
- Programa de co-logo personalizable

***Basado en pruebas realizadas internamente.**

**** USBtoCloud sólo trabaja con Windows**

DataTraveler 2000: Memoria con teclado

USB 3.0	Lectura*	Escritura*
16GB	120MB/seg	20MB/seg
32GB	135MB/seg	40MB/seg
64GB	135MB/seg	40MB/seg

*** Velocidades USB 2.0: 30MB/seg (lectura), 20MB/seg (escritura)**

- **100% de encriptado por hardware**
  - Encriptación 256-bit AES por Hardware
  - Modo de encriptado en bloques XTS
- **Independiente del Sistema Operativo**
- Se bloquea y reformatea después 10 intentos de intrusión
- Sistema de auto-bloqueo, cuando el USB se desconecta. Opción configurable de solo lectura
- Protección contra propagación de virus
- **Certificación FIPS-197**
- USB 3.0, compatible con USB 2.0
- Carcasa resistente al agua
- Capacidad de 16 a 64GB

DataTraveler Vault Privacy: Potente seguridad para la empresa

USB 3.0	Lectura*	Escritura*
4GB	80MB/seg	12MB/seg
8GB	165MB/seg	22MB/seg
16GB	165MB/seg	22MB/seg
32GB	250MB/seg	40MB/seg
64GB	250MB/seg	85MB/seg

* Velocidades USB 2.0: 30MB/seg lectura, 20MB/seg escritura (4GB: 30MB/seg lectura, 12MB/seg escritura

+ SKU's administrados no soportan Linux

- 100% Encriptado por hardware
  - **Encriptación AES de 256 bits basada en hardware**
  - Modo de encriptación en bloques **XTS**
- El dispositivo se bloquea y reformatea luego de 10 intentos de intrusión
- Uso obligatorio de contraseña compleja
- Modo de sólo lectura seleccionable por el usuario
  - Protección contra la difusión de virus
- **FIPS -197**
- **USB 3.0,** compatible con USB 2.0
- Resistente carcasa metálica a prueba de agua
- Soporte para SO Windows, Mac y Linux
- Programa Co-Logo Personalizable
- Garantía de 5 años
- Capacidades de 4, 8, 16, 32, 64GB
- **SKU Anti-Virus: DTVP30AV**
- **Solución administrada – DTVP30M-R**

Memorias USB administrables

SAFECONSOLE®

Los USBs con administración centralizada permiten a las organizaciones fácil y rápidamente establecer un centro de comandos para inventariar, auditar y controlar los dispositivos USB.

- Reinicio de contraseña de forma remota
- Políticas de contraseña
- Auditoria de dispositivos
- Administración de estado de dispositivo
- Geolocalización y Geofencing

•Los SKUs administrables de Kingston (DT4000G2DM & DTVP30DM) soportan la última versión de SafeConsole.
•Los USB funcionan sin SafeConsole, puede implementarlo posteriormente.

IRONKEY™

IronKey S1000
Disponible en modelos Básico y Empresarial*

- Con resistencia y durabilidad de grado militar, fabricado con una carcasa **de aluminio anodizado** y rellena de epoxi, el dispositivo aguantará incluso bajo las situaciones más demandantes.
- **Administración por llave de encriptación** con Criptochip incluido
- **Firmware firmado digitalmente** que lo hace inmune a BadUSB
- **Cuenta con la validación FIPS 140-2 Nivel 3**, con encriptación AES de 256 bits basado en hardware en modo XTS.
- *Servicio de administración empresarial - IronKey EMS por DataLocker

IronKey D300
Disponible en modelos Estándar y Administrado

- **Carcasa de Zinc** y sello de protección contra alteraciones en epoxi para seguridad física, el dispositivo aguantará incluso bajo las situaciones más demandantes.
- **Firmware firmado digitalmente** que lo hace inmune a BadUSB
- **Cuenta con la validación FIPS 140-2 Nivel 3**, con encriptación AES de 256 bits basado en hardware en modo XTS.
- Rápida transferencia de datos que usa la última tecnología NAND Flash y de controladores
- *Servicio de administración empresarial - IronKey EMS por DataLocker

Modelos Empresariales y Administrados

Despliegue fácil y flexible

Crea un centro de comando virtual

Se asegura que los dispositivos involucrados no comprometan los datos

DATALOCKER®
SIMPLY SECURE

SUPERSPEED USB CERTIFIED

TAA COMPLIANT

FIPS Level 3 Certified 140-2

Kingston TECHNOLOGY

DataTraveler Vault Privacy 3.0 con Anti-Virus ESET

- **NOD 32** el motor de AV provisto será ESET
    - Potente utilidad antivirus que evita que los virus, troyanos y otra clase de malware se propague a través del USB.
- Solución fácil de implementar y pre-activada en fábrica
- Carga automáticamente cuando el usuario autentifica correctamente el dispositivo
- El ícono en la bandeja de sistema avisa a los usuarios de las amenazas
- **USB 3.0** compatible con USB 2.0
- Capacidades de 4, 8, 16, 32, 64GB
- ESET: compatible con Windows (XP, Vista, 7, 8)
- Licencia por 5 años
- **Número de parte: DTVP30AV/xxGB**

IronKey S1000

Capacidad	S1000 Básico	S1000 Empresarial
4GB	IKS1000B/4GB	IKS1000E/4GB
8GB	IKS1000B/8GB	IKS1000E/8GB
16GB	IKS1000B/16GB	IKS1000E/16GB
32GB	IKS1000B/32GB	IKS1000E/32GB
64GB	IKS1000B/64GB	IKS1000E/64GB
128GB	IKS1000B/128GB	IKS1000E/128GB

- Encriptación por hardware al 100%
  - Encriptación AES de 256 bits basada en hardware
  - Modo de encriptado en bloques XTS
- Validado para FIPS 140-2 Nivel 3
  - Certificado #2320
- USB 3.0, compatible a la inversa con USB 2.0
- Después de 10 intentos fallidos el dispositivo se puede auto-destruir o reiniciar, dependiendo de la selección del usuario.
- Modo de sólo lectura seleccionable por el usuario
  - Protección contra la difusión de virus
- Resistente carcasa de aluminio anodizado a prueba de agua
- Soporte para SO Windows, Mac y Linux
- Garantía de 5 años
- Capacidades de 4 a 128GB
- Lectura Máx.: 400 MB/segundo; Escritura Máx.: 300 MB/segundo
- Los dispositivos básicos pueden actualizarse a grado Empresarial.

Empresarial - Administrado

Reduce Riesgos

•Proteja los datos de forma eficiente y económica mediante la administración de políticas de uso y encriptación, restricciones de contraseña y más desde una consola central.

Administración segura

•Asistencia remota de restablecimiento de contraseña.
•Gestión de políticas a nivel individual
•Bloquear, deshabilitar o destruir un dispositivo borrando cada bloque de datos del dispositivo comprometido, haciéndolo inutilizable.