Alerta de USB:
Proteja sus datos

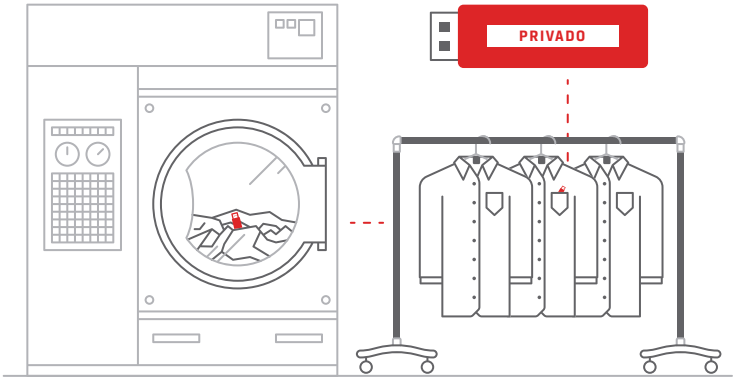
Mientras que por un lado las unidades USB han revolucionado las transferencias de datos, por el otro representan graves riesgos para la seguridad. Por su extraordinaria portabilidad, las unidades USB pueden portarse y aparecer en cualquier lado, desde los bolsillos de una chaqueta hasta aparcamientos, poniendo en riesgo los datos. ¿Cómo puede un departamento de TI abordar estos riesgos sin prohibir completamente el uso de unidades USB, con los inconvenientes que ello supone?

¿Qué es lo peor que puede ocurrir?

Las unidades USB suponen diversos riesgos:

PÉRDIDA

Cada año, unas **22.000 unidades USB** acaban en las lavanderías[1]



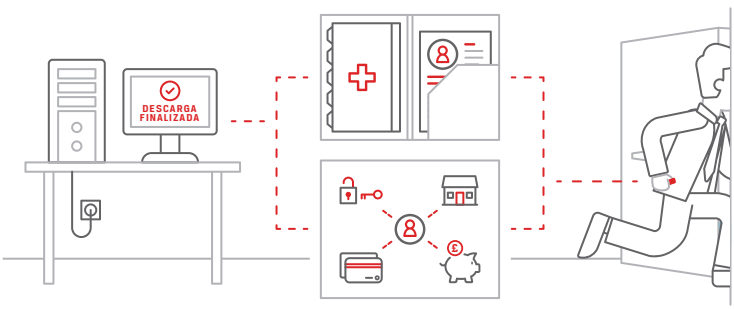
HALLAZGO

El 48% de las personas que encuentran unidades USB las enchufan y abren al menos un archivo[4]

ROBO

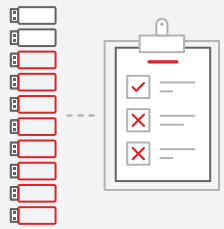
Una unidad USB que contenía datos sensibles de **pacientes** se perdió en Urgencias de un hospital[2]

Un empleado insatisfecho utilizó una unidad USB para robar información bancaria **de unas 30.000 personas**[3]



¿Cómo resuelven los profesionales informáticos los problemas de seguridad que plantean las unidades USB?

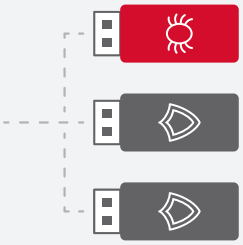
Una encuesta realizada por Spiceworks entre profesionales informáticos llegó a la conclusión de que, aunque la mayoría de las organizaciones conocen los problemas de seguridad que plantean las unidades USB, muchas no necesariamente los han resuelto.[5]



El 80% de las organizaciones tienen políticas en materia de USB

Las más habituales: limitan el uso de las unidades USB a empleados o departamentos específicos

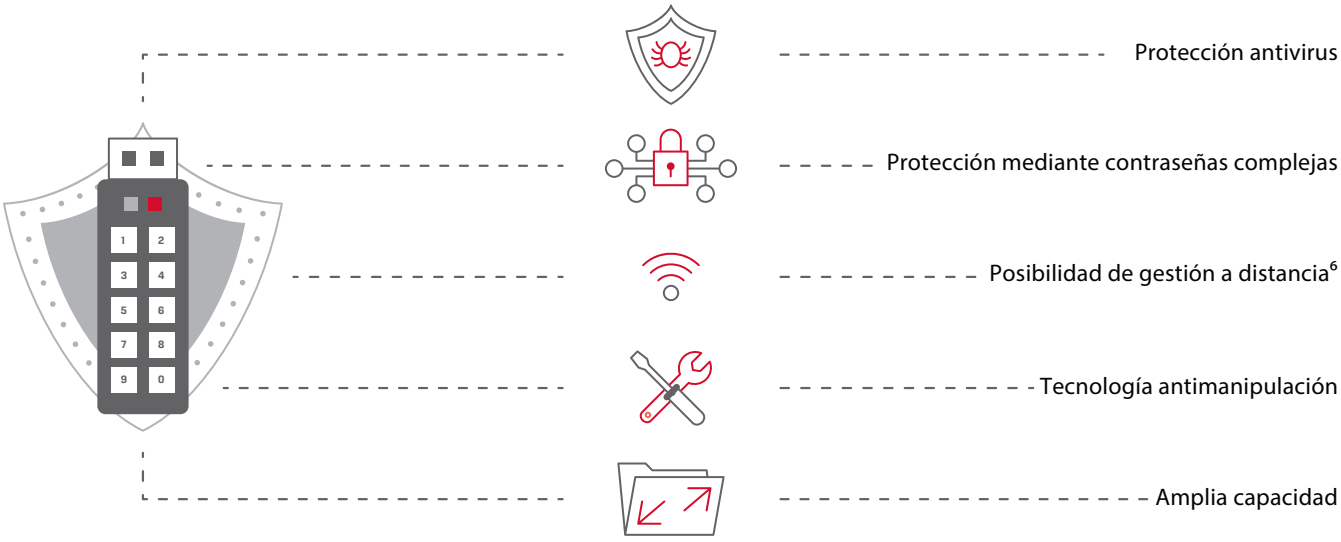
< 20% de las organizaciones que han implantado estas políticas obligan a usar unidades USB cifradas



Con todo, **una tercera parte** de los encuestados han experimentado amenazas o vulneraciones de la seguridad con estas unidades durante el último año.

Las unidades USB cifradas nunca revelan sus secretos.

Las unidades USB cifradas pueden ser potentes herramientas para resolver los habituales problemas de seguridad de los datos, contribuyendo a su protección y a la compatibilidad con:



Protéjase con Kingston.

Las unidades USB cifradas IronKey de Kingston han sido diseñadas para proteger incluso los datos más sensibles, aplicando las más estrictas normas y protocolos de seguridad implementados por organismos gubernamentales, prestadores de servicios médicos e instituciones financieras.

Fuentes:
1. Steve Bush, "22,000 USB sticks go to the dry cleaners" [22.000 unidades USB acaban en las lavanderías]; ElectronicsWeekly.com, 14 de enero de 2016. www.electronicsweekly.com/news/business/information-technology/22000-usbs-sticks-go-to-the-dry-cleaners-2016-01/
2. Taya Flores, "IU Health Arnett reports missing patient info" [IU Health Arnett denuncia la pérdida de datos de pacientes], JConline, 5 de enero de 2016. www.jconline.com/story/news/2016/01/05/iu-health-arnett-reports-missing-patient-info/78300400/
3. Tom Brant, "Report: FDIC Employees Caused Repeated Security Breaches" [Informe: Empleados de la FDIC provocaron repetidas vulneraciones de datos], PC Magazine, 15 de julio de 2016. www.pcmag.com/news/346179/report-fdic-employees-caused-repeated-security-breaches
4. Elie Bursztein, "Concerns about USB security are real: 48% of people do plug-in USB drives found in parking lots" [Los temores por la seguridad de las unidades USB están fundamentados: el 48% de la gente abre las unidades USB que encuentra en los aparcamientos], Elie.net, abril de 2016. www.elie.net/blog/security/concerns-about-usb-security-are-real-48-percent-of-people-do-plug-in-usb-drives-found-in-parking-lots
5. Encuesta de Spiceworks a 300 responsables de toma de decisiones informáticas en EE.UU., Canadá y Europa, encargada por Kingston, febrero de 2017.
6. Para ofrecer soluciones para la gestión de sus unidades USB cifradas, Kingston Digital ha establecido una alianza con DataLocker. www.kingston.com/us/usb/encrypted_security/management-solutions

Kingston TECHNOLOGY