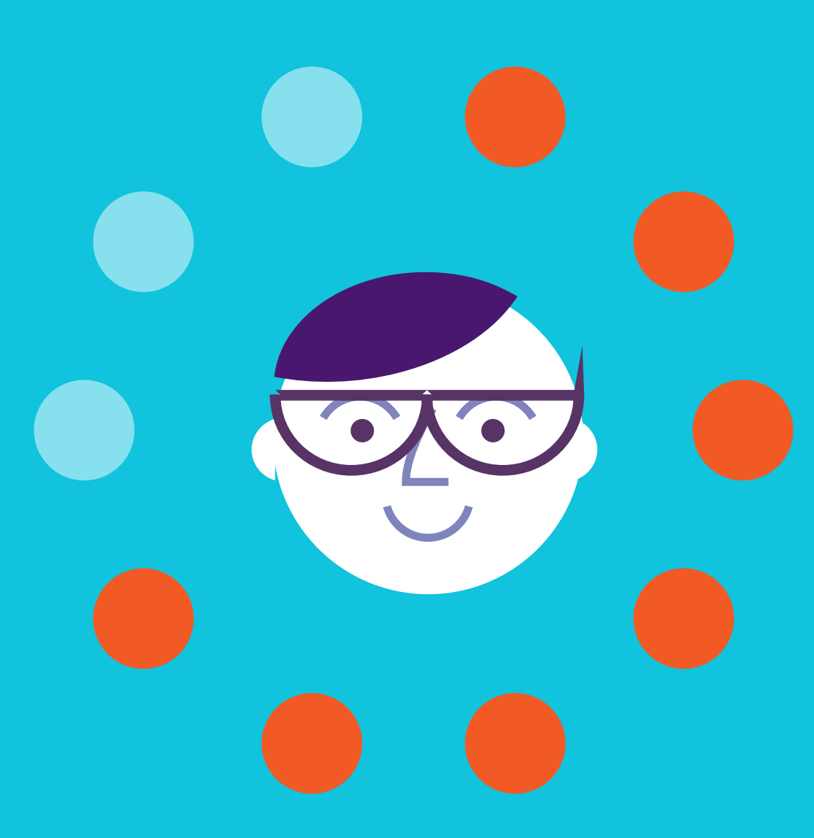
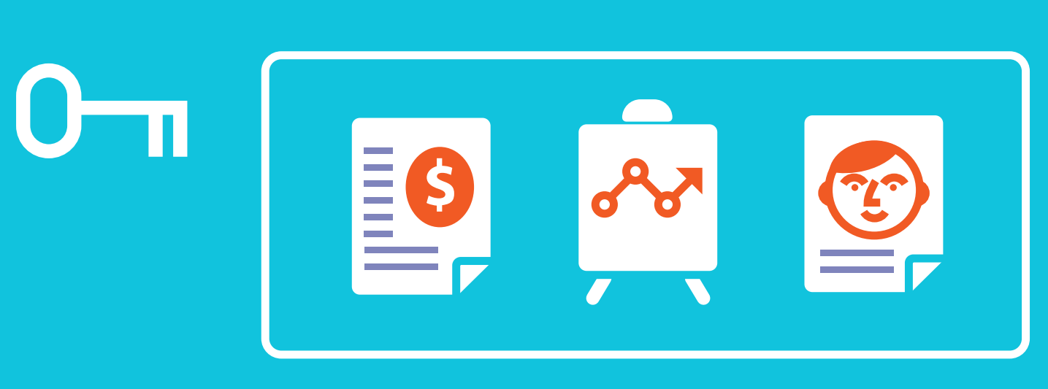
5 pasos para determinar si los empleados deberían ser su principal preocupación para la seguridad de datos corporativos

Powered by EndpointProtector.com

1 Verifique a qué documentos tienen acceso los empleados

Documentos financieros, bases de datos de clientes, planes de marketing



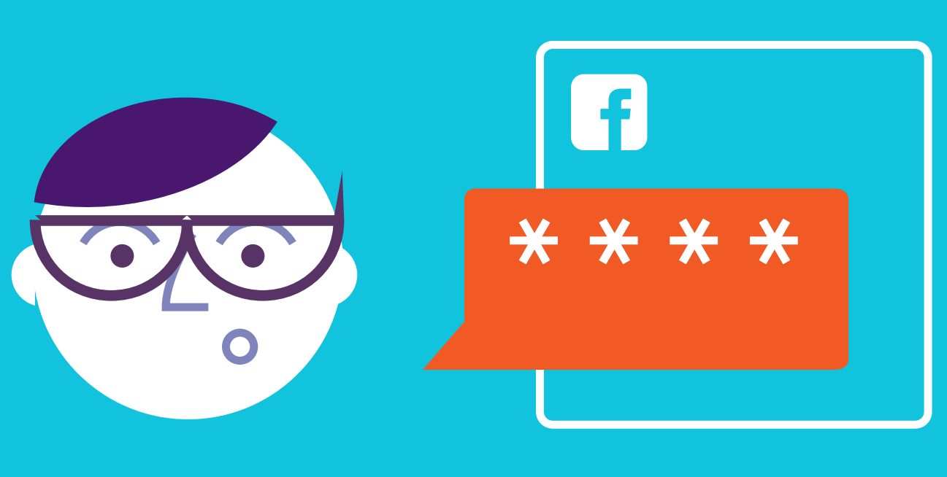


7 de cada 10

empleados tienen acceso a los archivos confidenciales y los utilizan en su trabajo diario

6 de cada 10 empleados desconocen qué archivos son confidenciales

4 de cada 10



empleados le podrían contar un incidente de un compañero que ha publicado información confidencial en las redes sociales o en otros lugares donde no debería estar

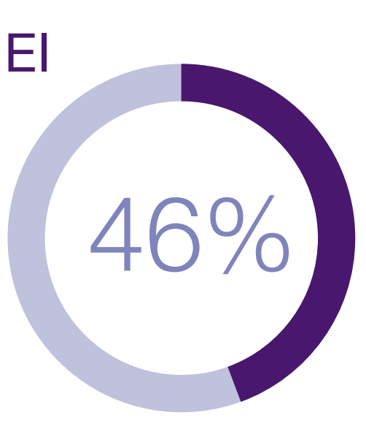
2 Observe qué herramientas utilizan los empleados para compartir archivos:

Skype, Dropbox, Outlook, dispositivos USB

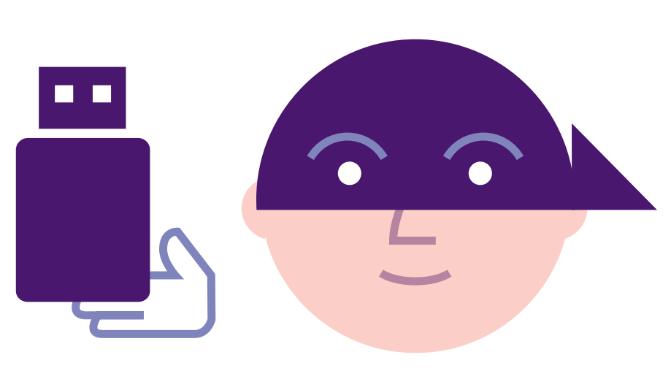
El 90%

de los empleados utilizan Outlook para compartir archivos con compañeros de trabajo, colaboradores y otros destinatarios

El



de los empleados copian archivos del trabajo a ordenadores personales o se conectan en remoto a la red corporativa para continuar el trabajo en su domicilio

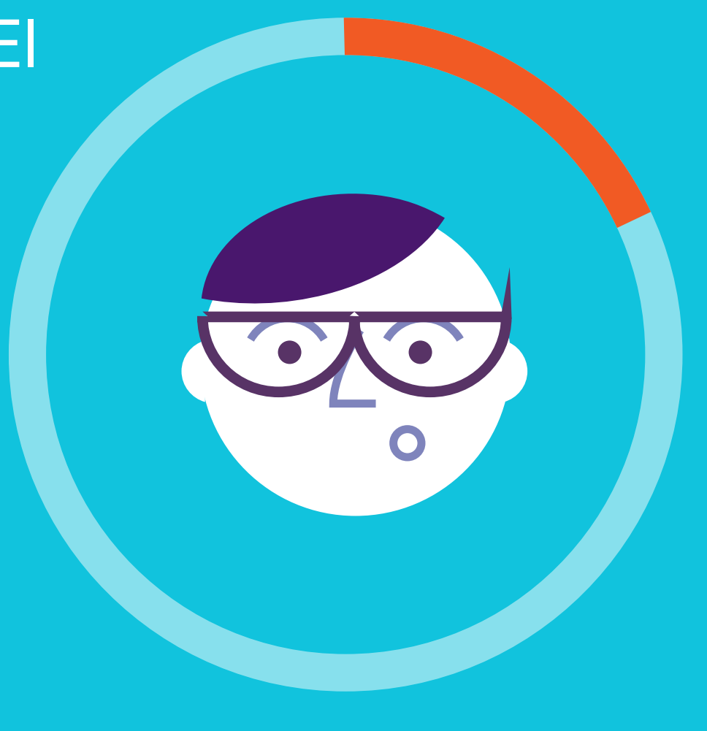


Las causas TOP 3

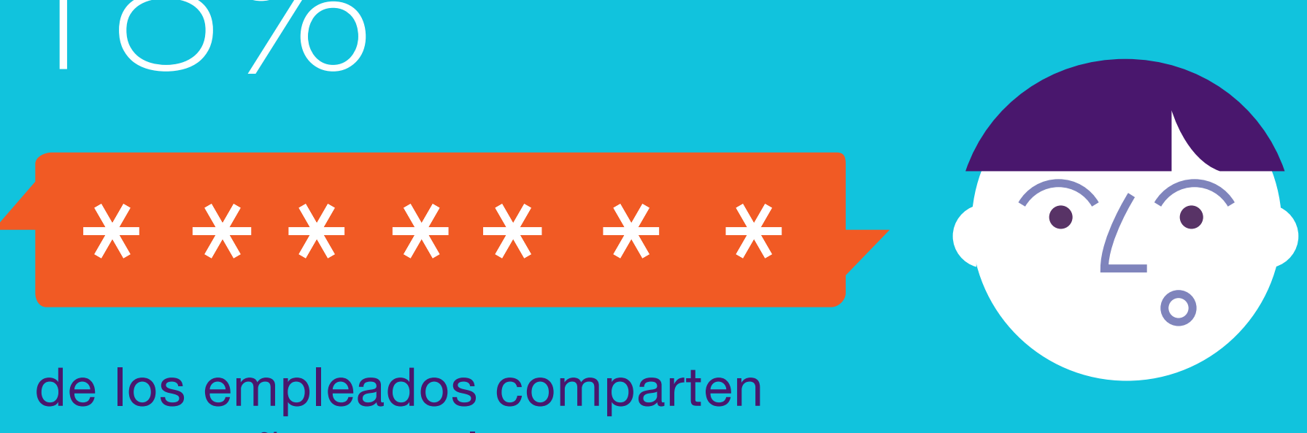
de las brechas de datos a nivel mundial incluyen dispositivos USB no cifrados perdidos o robados

3 Elabore un breve cuestionario para averiguar los conocimientos de los empleados con respecto a la seguridad de datos

El

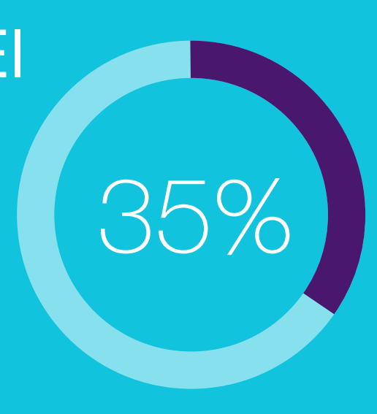


18%



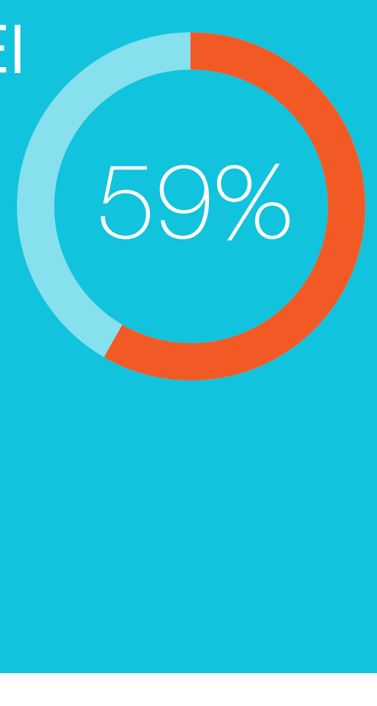
de los empleados comparten contraseñas con los compañeros de trabajo

El

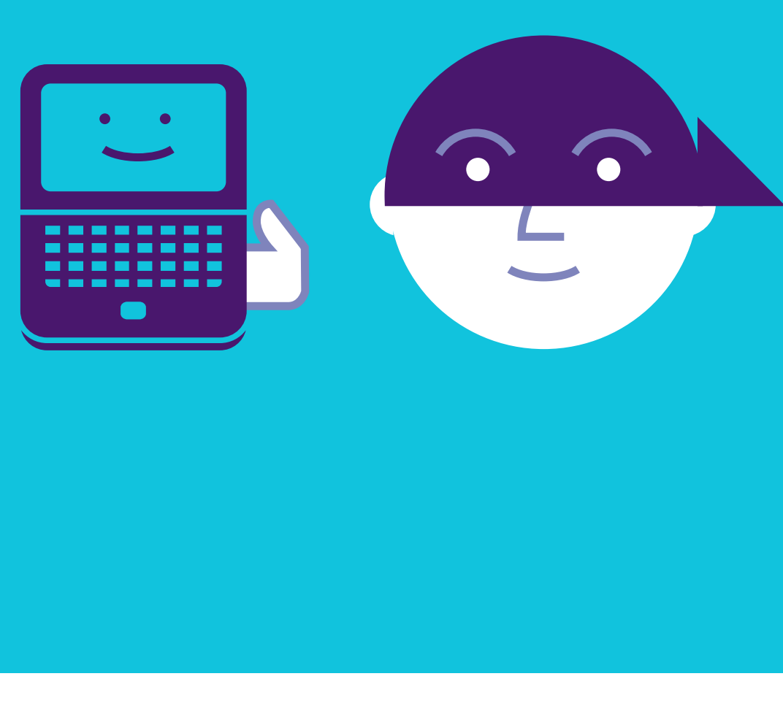


de los empleados creen que la seguridad de datos no es su responsabilidad

El

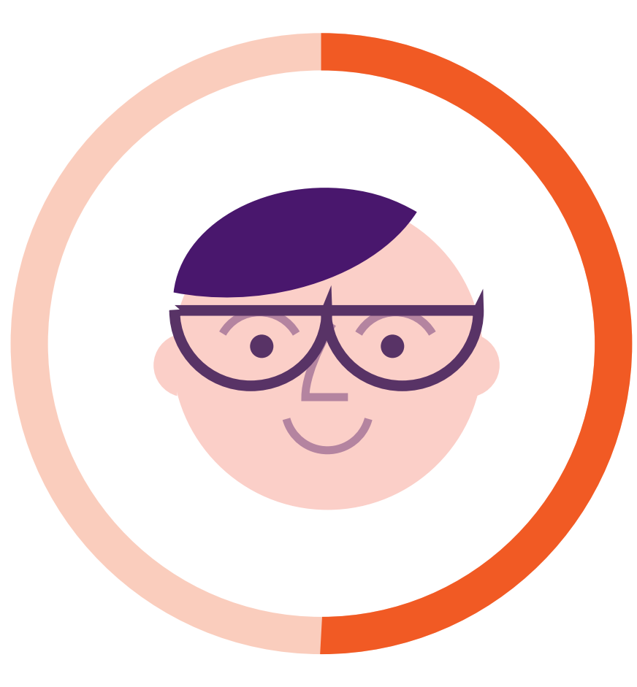


de los empleados piensan que la pérdida de un dispositivo móvil o un portátil con datos de la empresa no representa una gran amenaza



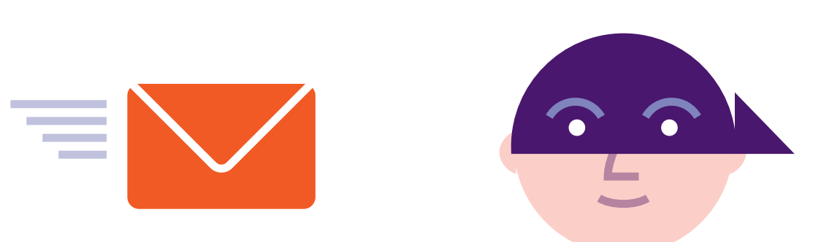
4 Determine si sus actuales herramientas de seguridad podrían detectar una fuga de datos

¿Puede usted detectar al empleado que envía un informe financiero a un destinatario sospechoso?



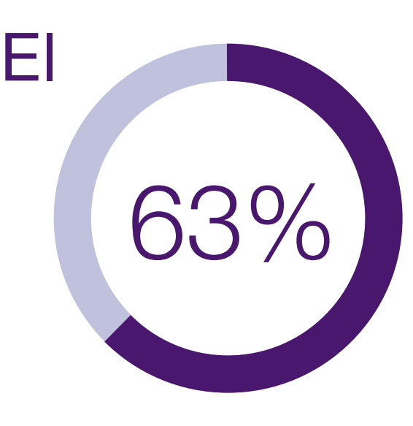
El 50%

de los empleados han enviado correos electrónicos a la persona equivocada



¿Qué pasa si los usuarios copian y pegan los datos confidenciales en Google Drive?

El



de las empresas no han podido establecer con certeza cómo ocurrió la pérdida de datos antes de implementar una solución Data Loss Prevention (DLP)

¿Sabe cuántos empleados sincronizan su correo electrónico corporativo con su móvil personal?

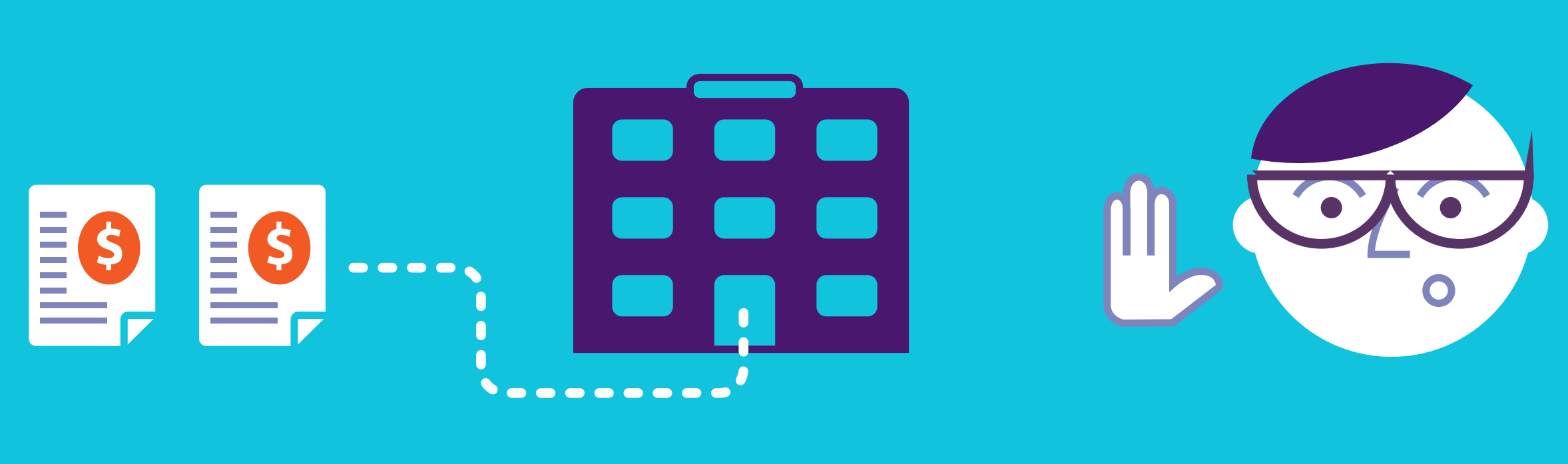
El 68%

prefiere sincronizar su correo electrónico corporativo para estar al día con las cuestiones urgentes

5 Averigüe cómo identificar los perjuicios financieros y otros daños derivados de las fugas de datos

¿Podría su empresa cubrir esos costes?

El



de los clientes potenciales no trabajarían con una compañía que ha sufrido una fuga de datos reciente

$4.8 millones es la multa más alta establecida para una fuga de datos que infringió la regulación HIPAA *

$3.5 millones es el coste medio de una brecha de datos *

Fuente: Investigación CoSoSys en clientes con una media de 500 equipos de las siguientes regiones: USA, LATAM, Europa y Asia
*http://www.hhs.gov/news/press/2014pres/05/20140507b.html
**http://www.darkreading.com/attacks-breaches/ponemon-cost-of-a-data-breach-rose-to-$35m-in-2013/d/d-id/1251019