SECURITY [SNAPSHOT]

Mobile Device Management:

Más allá del BYOD

KASPERSKY lab

Dispositivos Móviles: Riesgos y Recompensas

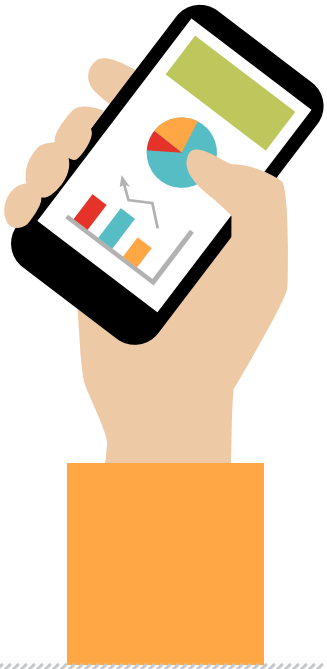
48% de los negocios están preocupados por el uso inapropiado que hacen los empleados al momento de compartir datos de la compañía a través de dispositivos móviles que traen al trabajo.[1]

54% de los negocios han tenido sus datos expuestos por culpa de empleados que pierden sus dispositivos.[1]

48% de los incidentes de ciberseguridad fueron el resultado directo del descuido de algún empleado, incluso más que por el robo de dispositivos, el cual registró un 37% de incidentes.[1]

54% de compañías no se sienten bien protegidas al momento de compartir datos a través de dispositivos móviles.[2]

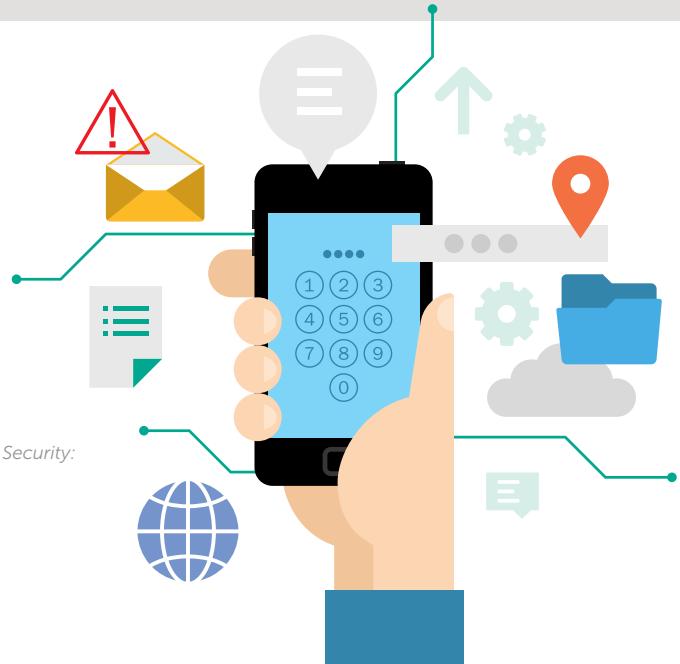
53% de compañías no se sienten bien protegidas en caso de la pérdida física de dispositivos móviles.[2]



La tecnología móvil está cambiando, no solo en cómo trabajamos, sino en cómo nos comprometemos con los clientes. La forma en que hacemos negocios ha cambiado fundamentalmente, con laptops haciendo el papel esencial como oficinas móviles, y con la ayuda de todos los dispositivos, desde tablets hasta teléfonos. Más y más compañías están respondiendo a la necesidad de una movilidad más amplia. La política empresarial de Bring Your Own Device (BYOD) satisface a los empleados y reduce costos.

La otra parte de esto es que las mismas funciones que hacen a los dispositivos tan importantes para los empleados, también los hacen atractivos para los cibercriminales. Debido a esto, el 51% de empresas están de acuerdo en que el aumento en la cantidad de dispositivos utilizados en sus organizaciones, hacen más difícil el control de la seguridad en esos dispositivos.

Por esta razón, el administrador de dispositivos móviles ahora hace mucho más que solo permitir a los empleados traer sus propios dispositivos. Se trata de tener su red completa segura con los dispositivos móviles, para balancear lo que los empleados necesitan para hacer su trabajo con lo que la compañía necesita para mantener sus datos seguros.



1. Kaspersky Lab´s *The Human Factor in IT Security: How Employees are Making Businesses Vulnerable from Within*
2. *Corporate IT Security Risks Survey 2016* from Kaspersky Lab and B2B International IT Security Risks Survey 2016

Elegir la Solución de Seguridad Móvil Correcta

No hay duda de que cada vez más compañías se enfrentan a la necesidad de contar con una solución de seguridad móvil, pero la tarea de implementar nuevas políticas de seguridad y tecnología, o incluso actualizaciones, puede ser abrumador.

No importa el tamaño de su organización, existen ciertos factores que necesite considerar primero. Recomendamos aproximarse al problema desde cuatro puntos diferentes del panorama de Mobile Device Management, MDM:

- Usuarios
- Dispositivos
- Programas
- Infraestrutura

Dado que el 40% de negocios informan que los empleados esconden los incidentes de seguridad cuando ocurren, es importante empezar con el punto más débil de cualquier plan de seguridad, sus **usuarios**. Haga las siguientes preguntas a sus empleados:

- ¿Cómo suelen hacer uso de sus dispositivos?
- ¿A qué datos necesitan acceder?
- ¿Cuáles son las necesidades de los diferentes departamentos?
- ¿Qué privilegios deberían tener los empleados en su red?
- ¿Quién puede hacer qué y dónde?
- ¿Qué harían si les robaran o perdieran un dispositivo?

¿Qué se aprendió?

Como siempre, es importante saber cómo sus empleados usan sus dispositivos. Las personas del área de ventas pueden tener necesidades completamente diferentes que las del departamento de finanzas. Al entender quién hace qué y dónde, podrá empezar a tener la idea de su panorama móvil completo.

Al observar los **dispositivos**, existen otras consideraciones, tales como:

- ¿Qué tipo de dispositivos necesitan usar con más frecuencia los empleados? ¿Qué tipo de dispositivos permitirá?
- ¿Cómo se presentará cada dispositivo móvil?
- ¿Qué restricciones de seguridad necesitará reforzar para estar a la altura de las necesidades empresariales de su organización?

¿Qué se aprendió?

Los dispositivos que permite dentro de su organización, determinarán una gran parte de su política de seguridad. Asegúrese de que estos no solo reflejen las necesidades de los empleados, sino lo que el consumidor probablemente necesite.

Después de determinar los problemas relacionados a sus usuarios, es importante salir y buscar **programas**:

- ¿Qué aplicaciones y programas necesitan sus empleados para hacer su trabajo?
- ¿Cuáles son los programas o aplicaciones riesgosas que quiere bloquear?ser bloqueados?

¿Qué se aprendió?

No siempre puede tener lo que quiera. Es importante que tenga el equilibrio entre lo que sus empleados quieren utilizar y lo que mantiene a su organización segura. Bloquear algunas aplicaciones y programas por completo será una parte necesaria para la seguridad de su estructura.

Y es entonces cuando es momento de ver el panorama completo de toda su **infraestructura**:

- ¿Cómo gestionará y apoyará el departamento de TI a las necesidades móviles?
- ¿Qué flexibilidad necesita para construir y permitir más dispositivos y más aplicaciones y servicios que no aún no se han inventado?

¿Qué se aprendió?

El cambio es una de las constantes en el panorama de TI. Asegúrese de construir suficiente flexibilidad en su plan para darle entrada al crecimiento y cambio inevitable, tanto dentro de su organización, como en el mundo de la tecnología.

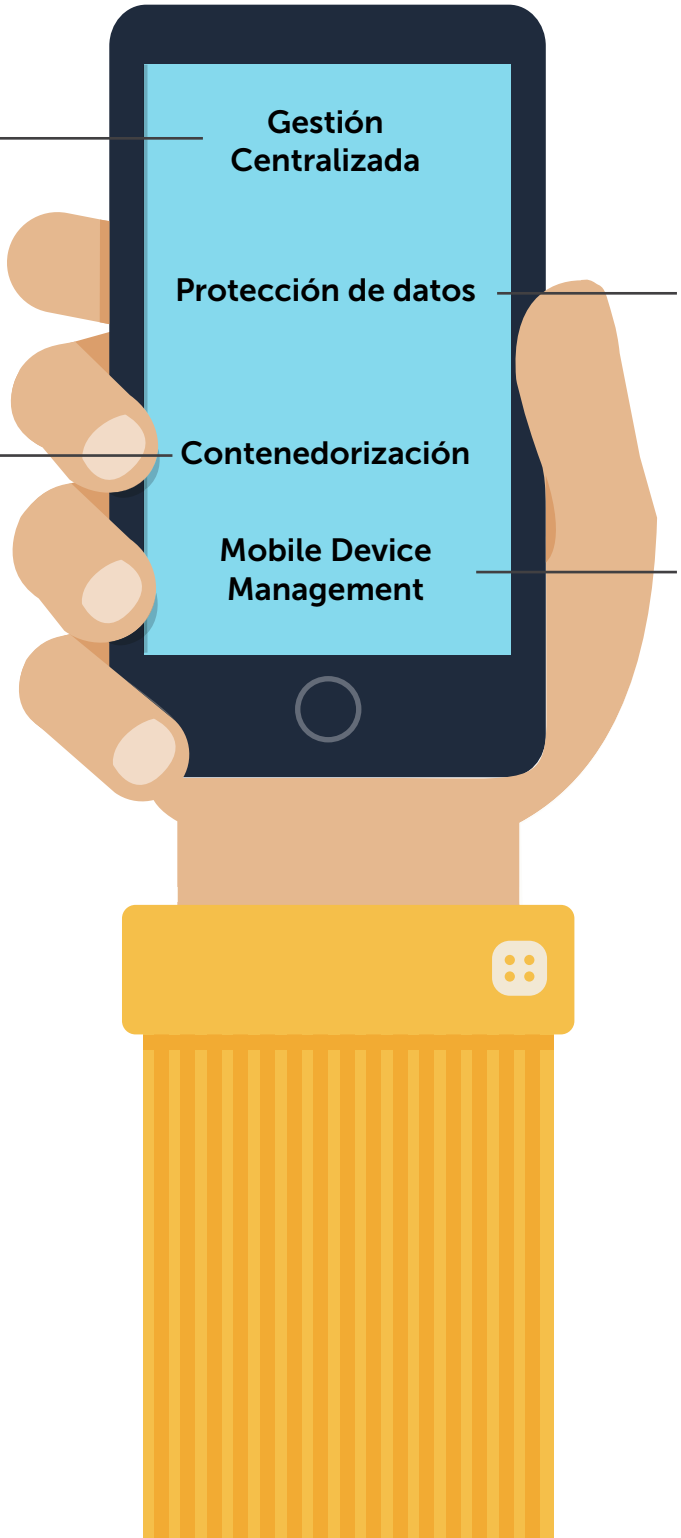
Kaspersky Security for Mobile

Kaspersky Security for Mobile asegura que los dispositivos dentro de su red estén seguros, sin importar dónde estén, protegiéndolos contra malware móvil en constante evolución. Nuestra **solución** le permite ganar visibilidad y control de los smartphones y tablets en su entorno de una forma rápida y sencilla, desde una ubicación central y con una disrupción mínima.

Ventajas de nuestro producto de Mobile Device Management:

Kaspersky Security for Mobile le permite gestionar sus dispositivos móviles desde la misma consola, al igual que otras plataformas endpoint: Kaspersky Security Center o Kaspersky Endpoint Security Cloud. Ver datos en los dispositivos, crear, gestionar políticas de empresa, enviar comandos a dispositivos y ejecutar informes, todo desde una consola central de gestión sencilla.

La contenedorización activa la separación de datos personales y del negocio en un mismo dispositivo. Los datos del negocio se almacenan en contenedores protegidos que pueden ser cifrados, protegidos con contraseña, y asegurados contra malware. La limpieza selectiva facilita a la política de BYOD.



Protección de los datos personales y corporativos del usuario. De ser necesario, las medidas de respuesta de emergencia pueden usarse para prevenir que los dispositivos comprometidos no accedan a los datos de la compañía, o incluso bloquearlos de forma remota.

Configura y activa el uso de contraseñas, cifrado, Bluetooth y cámara, como también políticas grupales para Android, iOS y Windows Phone. Ejecuta informes en el dispositivo y las aplicaciones instaladas. La integración con todo lo mejor en plataformas de gestión de dispositivo móvil, permite el lanzamiento y control de forma remota "Over the Air" (OTA) para la gestión y el uso fácil de los dispositivos soportados.

True Cybersecurity for Business

El enfoque de True Cybersecurity de Kaspersky Lab combina la seguridad multicapa con el aprendizaje automático y la inteligencia sobre amenazas asistida por la nube para proteger contra amenazas que pueda enfrentar su negocio. True Cybersecurity no solo previene ataques, sino que también predice, detecta y actúa rápidamente, asegurando al mismo tiempo, la continuidad de su organización.

Descargue ya su Prueba Gratis >

Únase a nosotros

- Síganos en Facebook
- Síganos en Twitter
- Síganos en LinkedIn
- Síganos en YouTube
- Lea nuestro Blog

Acerca de Kaspersky Lab

Kaspersky Lab es una de las compañías de ciberseguridad de más rápido crecimiento en el mundo y la más grande como propiedad privada. La compañía se encuentra entre los cuatro principales proveedores mundiales de soluciones de seguridad para usuarios finales (IDC, 2014). Desde 1997, Kaspersky Lab ha sido un innovador en ciberseguridad y ofrece soluciones efectivas de seguridad digital e inteligencia contra amenazas para grandes empresas, PyMES y consumidores. Kaspersky Lab es una compañía internacional que opera en 200 países y territorios alrededor del mundo, proporcionando protección a más de 400 millones de usuarios a nivel global. Lee más en latam.kaspersky.com

Contacte hoy a Kaspersky Lab para saber más acerca de Kaspersky Endpoint Security for Business y nuestras otras soluciones y servicios de seguridad TI:
latam.kaspersky.com/small-to-medium-business-security/contact-us

latam.kaspersky.com
#truecybersecurity