Resultados de la encuesta exclusiva de 2014

Amenazas de seguridad y filtraciones de datos de IT

Percepción frente a realidad: es hora de volver a calibrarlas

Crecimiento empresarial basado en la seguridad.
kaspersky.com/business

#securebiz

KASPERSKY lab

Índice

Acerca del Informe Global de Riesgos de IT

Ahora en su 4.º año, **el Informe Global de Riesgos de IT de Kaspersky Lab** recopila las percepciones de los profesionales de IT de todo el mundo. Realizado por especialistas investigadores de B2B International y analizado por los equipos expertos de investigación e información de amenazas de Kaspersky, el informe es un análisis esencial de las actitudes y estrategias predominantes del sector en lo que se refiere a la seguridad de IT. También sirve como una referencia en el sector para ayudar a las empresas a comprender el tipo y nivel de amenazas de seguridad a las que se enfrentan.

¿Por qué se recomienda leer este informe?

- **Recopila conclusiones globales y referencias cruzadas del sector**
- **Le ofrece información en exclusiva sobre los puntos de vista, las opiniones y las estrategias de los profesionales de IT de todo el mundo**
- **Le ayuda a comparar su seguridad de IT con la de otros compañeros del sector**

Informe Global de Riesgos de IT 2014

Resumen ejecutivo

Resumen de la encuesta:

- **3900 encuestados**
- **27 países**
- **Periodo de abril de 2013 a mayo de 2014**
- **Encuesta a profesionales de IT con un "buen conocimiento actualizado" de los problemas de IT**

Durante 2013 y 2014, el tema de la seguridad de IT se ha intensificado pasando a ser de una mera "preocupación" a una "noticia mundial", donde las fugas de datos, el espionaje corporativo y el cibercrimen aparecen con frecuencia en los titulares. Pero, ¿qué está sucediendo realmente detrás de toda la publicidad y de qué modo le afecta personalmente?

Los mercados mundiales comienzan a recobrar una mejor salud económica y las consideraciones estratégicas a largo plazo son de nuevo el tema principal en las salas de juntas. El renovado interés en el crecimiento, que deja a un lado el hecho de simplemente sobrevivir al próximo ejercicio, ha provocado un cambio en las prioridades, y ahora se presta más atención a las estrategias de gestión de riesgos. Pero estas estrategias solo son eficaces cuando se construyen a partir de una comprensión precisa del panorama actual de las amenazas.

Una de las cosas más interesantes que se resalta en la encuesta de este año es lo que hemos comenzado a llamar **"las carencias en la percepción"**. Es decir, la diferencia entre nuestra percepción de lo que está sucediendo y la realidad.

Durante 2013 y 2014, Kaspersky Lab detectó alrededor de 315 000 muestras maliciosas diariamente. De las empresas encuestadas, solo el **4 %** fue capaz de afirmar con precisión esta cifra. De hecho, el **91 %** de los encuestados infravaloró esta cifra y el **70 %** calculó que había menos de 10 000 amenazas diarias. Un grave error de cálculo.

Pero esto es solo una parte de la historia. El **94 %** de las empresas ha experimentado alguna forma de amenaza a la seguridad externa y, sin embargo, solo el **68 %** ha aplicado antimalware en sus estaciones de trabajo y únicamente el **44 %** utiliza soluciones de seguridad para sus dispositivos móviles.

El 94 % de las empresas ha experimentado alguna forma de amenaza a la seguridad externa

¿Cómo se puede solucionar esto? Tenemos que volver a calibrar nuestra percepción del sector a fin de comprender mejor las amenazas. Y no solamente las brechas de seguridad visibles, sino también los riesgos de seguridad diarios y continuos.

Unas de las grandes preocupaciones son el control y la integración de los dispositivos móviles en las prácticas normales de trabajo y la seguridad relativa a la virtualización. No obstante, solo el **34 %** de los encargados de tomar decisiones de IT comprende claramente las soluciones de seguridad virtual disponibles y el **46 %** de las empresas cree que sus soluciones de seguridad convencionales ofrecen una protección adecuada.

El impacto **estimado** de las infracciones de datos para pequeñas y medianas empresas (pymes) se redujo en un **12 %**, al pasar de **46.000€ a 41.000€** estadounidenses, pero el impacto estimado de las grandes empresas aumentó en un **14 %**, de **de 600.000€ a 680.000€** estadounidenses, pero podría tratarse de un problema de percepción. Las grandes empresas son de mayor tamaño y están mejor equipadas para detectar las infracciones, mientras que las pequeñas y medianas empresas (pymes) pueden no saber cuándo han sido el objetivo de un ataque.

No obstante, este impacto no es tan simple como se podría pensar. El **87 %** de las empresas que sufrieron pérdidas de datos necesitaron servicios profesionales adicionales de algún tipo y casi la mitad (**47 %**) sufrieron grandes costes adicionales. El año pasado, el "daño típico" medio (contratación de servicios profesionales, aumento del tiempo de inactividad y pérdida de oportunidades comerciales) para las pymes por un suceso grave fue de 35 000 dólares estadounidenses. Para las grandes empresas, esta cifra fue de 690 000 dólares estadounidenses.

El impacto que las filtraciones de datos pueden tener en la confianza y la reputación también fue muy evidente. El **82 %** de las empresas podría considerar la posibilidad de interrumpir su relación con una institución financiera si sufriera una filtración, mientras que un **27 %** no piensa que los bancos estén haciendo lo suficiente para proteger su información financiera.

El 82 % de las empresas podría considerar la posibilidad de interrumpir su relación con una institución financiera si sufriera una filtración

No obstante, hay una división en la percepción de quién es, en última instancia, el responsable de proteger las transacciones financieras. Solo el **35 %** de los clientes piensa que las instituciones financieras son las principales responsables, mientras que el **85 %** de las instituciones financieras afirmó que ellas mismas sentían que eran las responsables.

Entonces, ¿quién lleva razón? El caso es que las empresas están haciendo grandes progresos, pero también lo está haciendo el sector del cibercrimen. Aunque existen las herramientas para que las empresas se protejan a sí mismas, la mayoría de las empresas todavía adopta un enfoque reactivo a la seguridad de IT. Necesitan ser más proactivas y dejar de infravalorar la diversidad, cantidad y sofisticación de las amenazas actuales. Expresado de forma sencilla, las soluciones antivirus tradicionales ya no son suficientes.

Las empresas necesitan reconocer el reto del problema que se les avecina. La construcción de una defensa a varios niveles contra las amenazas planteadas por los factores "humanos", la utilización cada vez más habitual de varios dispositivos y la aparición de nuevas tecnologías ahora es fundamental porque ninguna empresa dispone de los recursos humanos suficientes para gestionar todos los factores.

Es el momento de volver a calibrar seriamente la percepción y gestión de los problemas de seguridad. Las empresas tienen que ser más proactivas y no bajar la guardia, y necesitan formarse a sí mismas, o se arriesgarán a convertirse en la próxima gran noticia de seguridad de IT.

Expresado de forma sencilla, las soluciones antivirus tradicionales ya no son suficientes

Informe Global de Riesgos de IT 2014

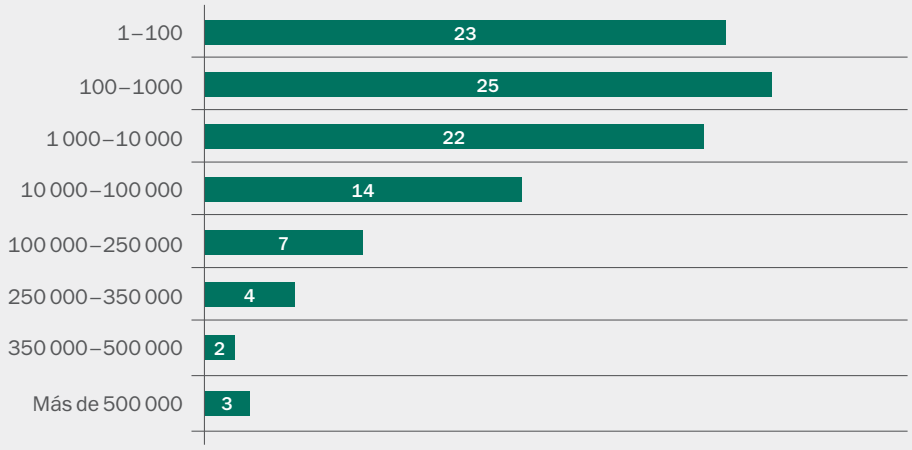
1 Percepción frente a realidad: ¿cómo podemos mejorar las carencias?

> **Existe una creciente brecha entre lo que las empresas creen que es el panorama actual de amenazas y lo que en realidad es. Es lo que llamamos las "carencias de percepción". Demuestra que las empresas, independientemente de su tamaño, infravaloran tremendamente tanto la cantidad como la gravedad de las amenazas a las que enfrentan.**
>
> Costin Raiu, equipo de análisis e investigación global, Kaspersky Lab

Como responsable de la toma de decisiones de IT, usted es también el responsable de los sistemas comerciales críticos y la infraestructura. Protege a su empresa contra las amenazas, evita la pérdida de datos y se asegura de que todo funciona de manera óptima. Y la mayor parte del tiempo, lo consigue. Pero, ¿qué hay de las ocasiones en que no lo consigue? ¿Qué ocurre con los problemas que no detecta?

A veces necesita realizar un análisis de la realidad para obtener ayuda, así como ajustar su percepción, a fin de reflejar la naturaleza siempre cambiante y en desarrollo de las amenazas a las que se enfrenta. El **91 %** de los responsables de la toma de decisiones empresariales infravalora el número de muestras de amenazas detectadas diariamente, y solo el **4 %** tiene una idea exacta de la cantidad real que existe. Es más, la mayoría de nosotros infravalora drásticamente esta cifra, con un **70 %** que cree que son menos de 10 000 las nuevas muestras que se descubren diariamente. La cifra real, según ha detectado Kaspersky Lab, es de 315 000 nuevas muestras.

Número percibido de muestras de malware nuevo detectadas diariamente (%)



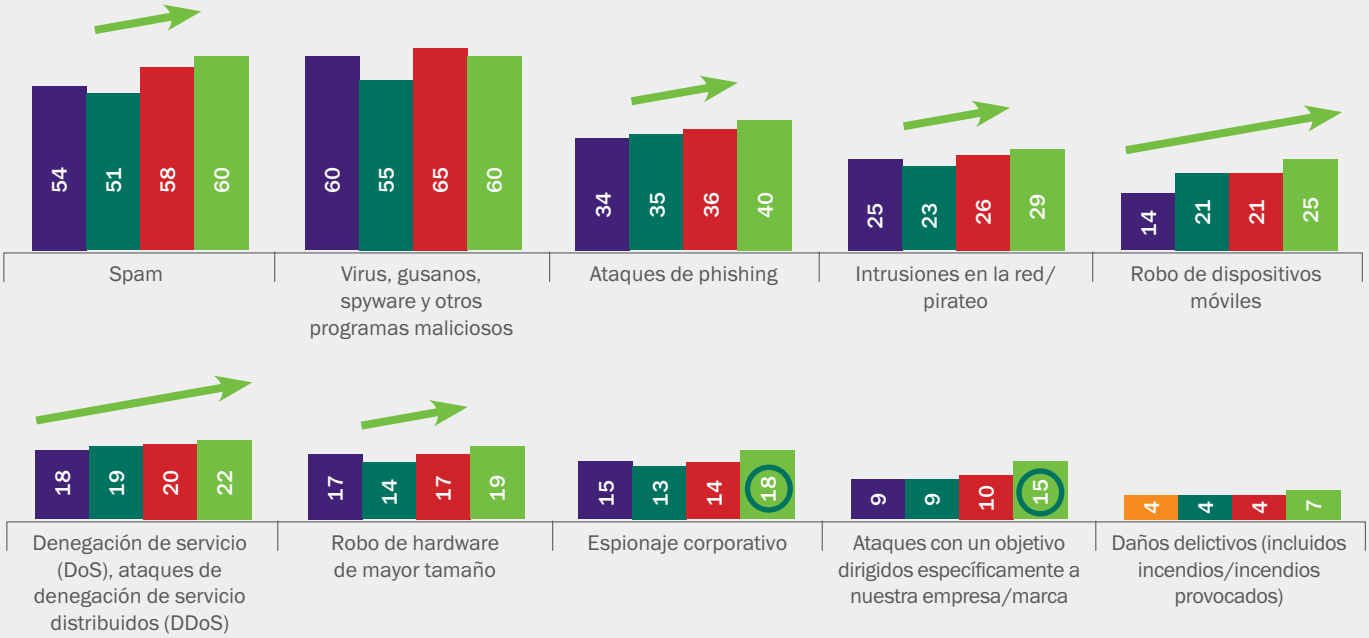
Sorprendentemente, pese a infravalorar el número de amenazas, los participantes en la encuesta informaron de la percepción de un aumento en el número de ciberataques anuales durante los últimos 4 años. Este podría ser el caso de muchas empresas que piensan que se ha producido un aumento de las amenazas relacionadas con ellas, pero que no tienen una idea clara de la situación general.

Las empresas de todos los tamaños han informado de un aumento de los niveles de spam, phishing y ataques DDoS como áreas de preocupación. El espionaje corporativo y los ataques con un objetivo también aumentan. El número de empresas que denuncian ataques concretos destinados directamente a ellas ha aumentado en un **5 %** desde 2013, y ahora es de un **15 %**.

Por lo tanto, ¿qué hay detrás de todas estas amenazas?

Amenazas externas experimentadas

El 94 % de las empresas ha experimentado alguna forma de amenaza externa. También existe la aparición de algunas tendencias claras, tales como el aumento constante de los ataques de denegación de servicio, en los últimos cuatro años.



% de las empresas que experimentan cada evento

2011 (n=1408) 2012 (n=2376) 2013 (n=1912) 2014 (n=2119)

Interanual bastante mayor

Un gran error es el de considerar que el malware es algo específico e independiente, en lugar de algo que está realmente integrado en los ciberataques. Aunque las denuncias de ataques de malware en realidad disminuyeron entre 2013 y 2014, siguen siendo las amenazas más habituales y peligrosas para la seguridad de IT. El phishing, los ataques DDoS y los ataques con un objetivo están todos conectados por el uso de malware cada vez más sofisticado.

Y aunque ya se están adoptando una serie de medidas de seguridad, todavía hay grandes lagunas en los sistemas de seguridad de IT, independientemente del tamaño de la empresa.

A pesar de la naturaleza de la amenaza que representa el malware, solo el **68 %** de las empresas implementa software antimalware en sus estaciones de trabajo, solo el **42 %** utiliza las soluciones de seguridad móvil, y solo el **52 %** de todas las empresas encuestadas con regularidad revisa o actualiza el software, una de las tareas más importantes para evitar los ataques de malware o las filtraciones de datos.

En el mejor de los casos, esto sugiere que las empresas solo están parcialmente protegidas; una lectura más crítica sugiere que, lamentablemente, no están preparadas para las amenazas a las que se enfrentan.

Entonces, ¿cómo pueden las empresas mejorar las carencias? A través de una mejor comprensión de la verdadera naturaleza de estas amenazas y de la implementación y el mantenimiento efectivos de soluciones de seguridad específicas.

2 Las amenazas más sofisticadas requieren protección a varios niveles

Actualmente, las empresas de todo el mundo se enfrentan a amenazas de seguridad cada vez más complejas. Y, por desgracia, la solución ya no pasa por un solo producto o enfoque que pueda protegerlas contra todo tipo de malware, virus o programas maliciosos. Una política basada en "talla única" carece del alcance y la capacidad para la protección de las empresas de ataques diversos a su infraestructura de IT.

Y lo que es peor, el malware evoluciona rápidamente y cambia diariamente. Es como luchar contra un enemigo oculto que está en constante movimiento. A finales de 2013, se detectaron 200 000 muestras únicas de código de malware móvil. Tan solo en el primer semestre de 2014, se crearon 175 000 nuevas muestras más. Las tasas de crecimiento son alarmantes, y se deben tener en cuenta al tratar de definir las estrategias de seguridad para la protección de los datos, la seguridad de las transacciones financieras y el mantenimiento de la continuidad de los servicios a pesar de los ataques DDoS.

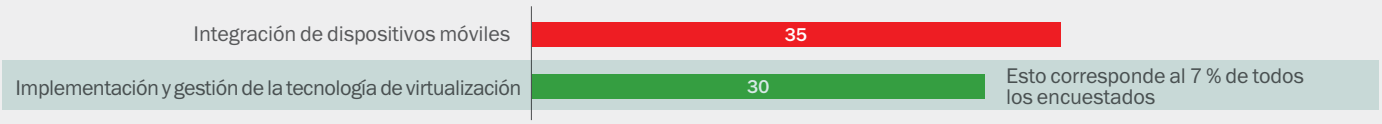
> **Una de las estadísticas más preocupantes de la encuesta es el bajísimo nivel de uso de la aplicación y gestión de parches. Dado que la mayoría de las brechas de seguridad provienen de la vulnerabilidad de una aplicación sin revisar, esto tiene que ser una de las áreas clave para cualquier profesional de IT.**
>
> Sergey Lozhkin, equipo de análisis e investigación global, Kaspersky Lab

Vale la pena tener en cuenta que lo que es mejor para una empresa no lo es necesariamente para otra. Es esencial obtener la solución correcta para su red empresarial, independientemente de si utiliza redes LAN, inalámbricas y de telefonía móvil, redes de área amplia, comunicaciones basadas en IP, o una combinación de estas. Las soluciones de seguridad deben funcionar de forma eficaz en todas estas plataformas sin poner en peligro la seguridad ni el rendimiento. Además, con la virtualización como punto fuerte en el programa de muchas empresas y el papel cada vez más importante que desempeñan los dispositivos móviles en los negocios, ahora es más importante que nunca que las empresas comprendan la necesidad de una protección a varios niveles e integrada contra amenazas que funcione para dispositivos físicos, móviles y virtuales.

En la tabla siguiente, podemos ver que de los encuestados que consideran la "gestión del cambio" una de las principales preocupaciones: el **30 %** afirmaba que la implementación y la gestión de la tecnología de la virtualización es su mayor reto, mientras que el **35 %** sostenía que para ellos, la mayor preocupación era la integración de los dispositivos móviles.

GESTIÓN DEL CAMBIO EN LOS SISTEMAS DE IT

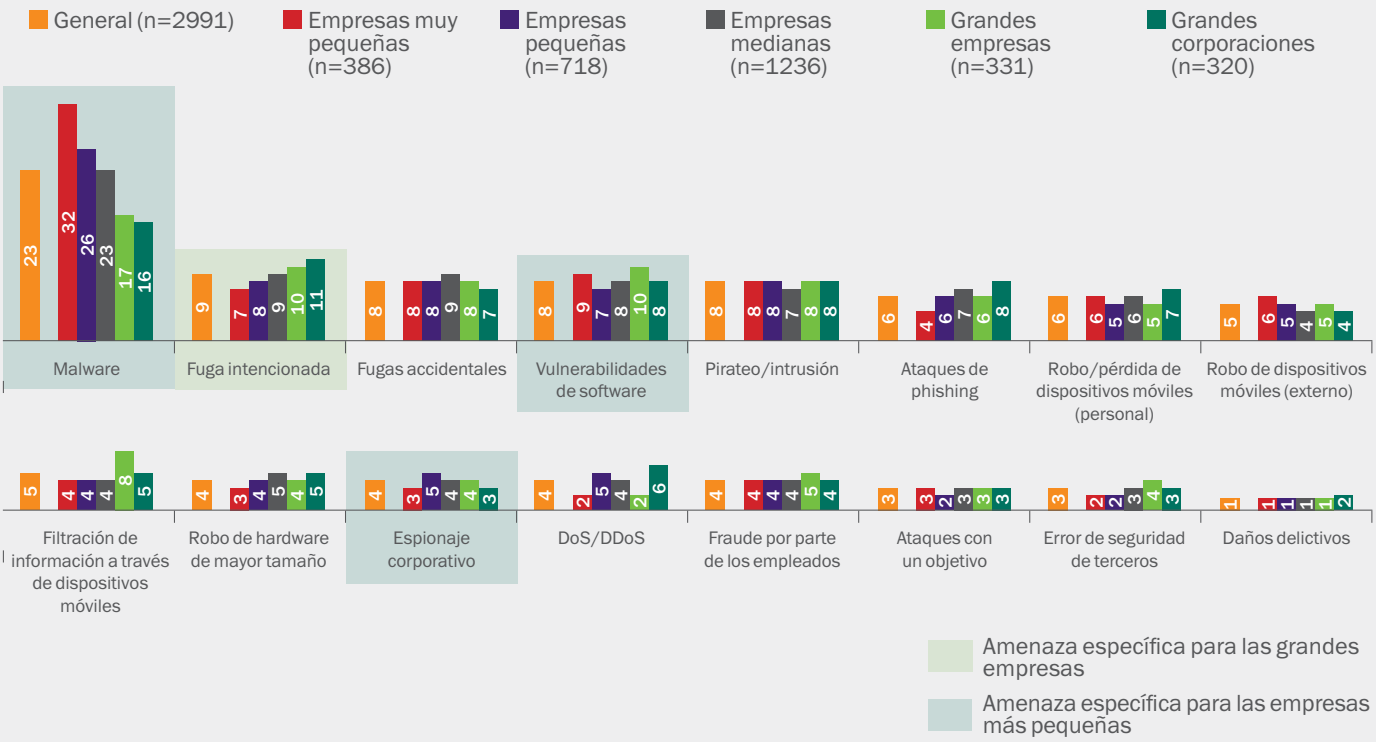
Si estudiamos en detalle el 22 % de los encuestados que considera la gestión del cambio una de las principales preocupaciones, la seguridad móvil y la virtualización son los retos clave



El gráfico siguiente destaca las amenazas tanto para las grandes empresas como para las más pequeñas: desde malware y filtraciones de datos hasta espionaje corporativo y robo de dispositivos móviles.

CASOS MÁS GRAVES DE PÉRDIDA DE DATOS

El malware es actualmente la principal causa de graves pérdidas de datos. Es un problema menor para las empresas más grandes, donde la fuga intencionada de información es una preocupación mucho mayor.



Base: varía en función de todos los encuestados de cada tamaño de empresa que perdieron datos

De acuerdo con el gráfico anterior, es evidente que el malware es la principal causa de pérdida de datos. Entonces, ¿por qué, de 2013 a 2014, las empresas percibieron la reducción en un **5 %** de los ataques de malware? En otras palabras, el **91 %** de las empresas infravaloran el número de muestras nuevas descubiertas diariamente, y no se comprende correctamente que muchos ataques con un objetivo, como el phishing y los ataques DDoS, en realidad están basados en malware. Por lo tanto, no es que las infiltraciones de malware hayan disminuido, sino que los ataques no se pueden percibir como ataques de malware.

Por lo tanto, ¿qué podemos deducir de estos resultados?

1. Las soluciones antivirus tradicionales ya no son eficaces y no ofrecen la profundidad y magnitud de la protección que requieren las empresas.
2. La creciente complejidad de la infraestructura de IT ofrece más oportunidades para los ataques maliciosos.
3. Los errores humanos y de percepción no se pueden ignorar, y el aumento de la utilización de los programas "Traiga su propio dispositivo" (BYOD) ha facilitado la explotación de las prácticas de trabajo.

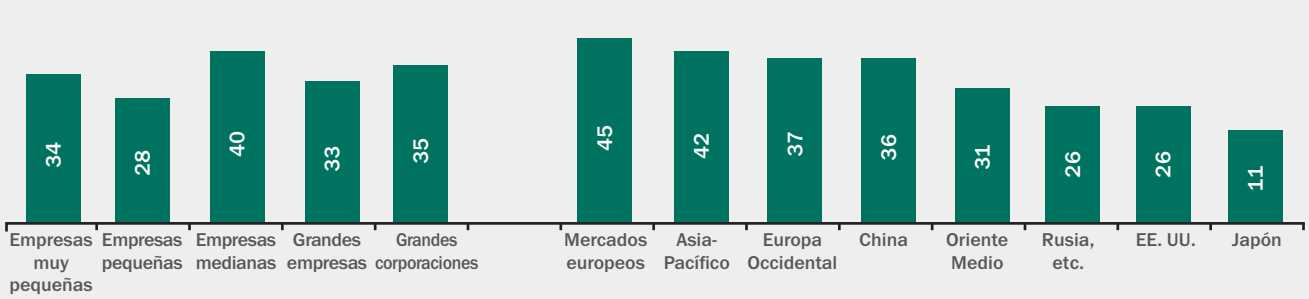
3 Informe Global de Riesgos de IT 2014
Móvil: la amenaza actual

Las empresas de todo el mundo están adoptando rápidamente el trabajo desde dispositivos móviles. Pero su fuerza, es decir, la ayuda que ofrecen a los trabajadores para ser más flexibles, no vale nada si no se adoptan las medidas de seguridad correctas. Un dispositivo móvil no protegido proporciona acceso a datos confidenciales y supone para los cibercriminales un punto de entrada fácil a un sistema que sería seguro si estuviera protegido correctamente.

Por este motivo, el **35 %** de las empresas reconoció que la integración de los dispositivos móviles era uno de los mayores retos para el año que se presenta. Y no es un tema destacado solamente para las grandes empresas. La integración de los dispositivos móviles es esencial para las empresas de todos los tamaños, como muestra el gráfico siguiente. Solo las pequeñas empresas, en un **28 %**, tienen menos de un tercio de los encuestados que consideran la integración móvil una de las principales preocupaciones. No obstante, esto podría deberse a que las pequeñas empresas infravaloran las amenazas potenciales a dispositivos móviles y desde estos.

El **24 %** de las empresas nombraron el programa BYOD como una de sus mayores prioridades en materia de seguridad de IT en los próximos 12 meses, cifra que aumentó a un 32 % entre las empresas muy pequeñas. Esto no debería considerarse realmente una sorpresa, dado que el **42 %** de las empresas realizan actualmente transacciones confidenciales a través de sus dispositivos móviles.

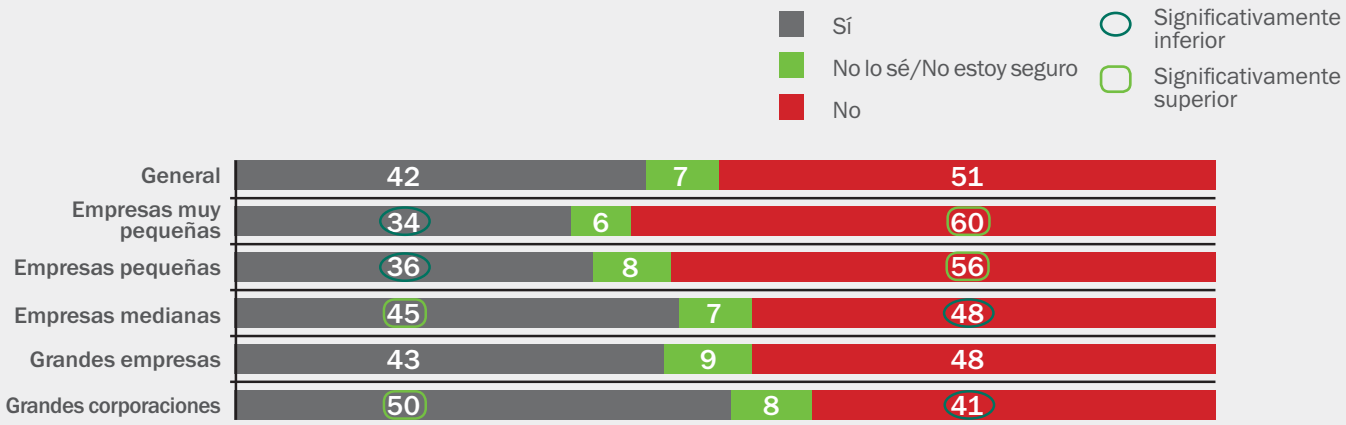
INTEGRACIÓN DE DISPOSITIVOS MÓVILES



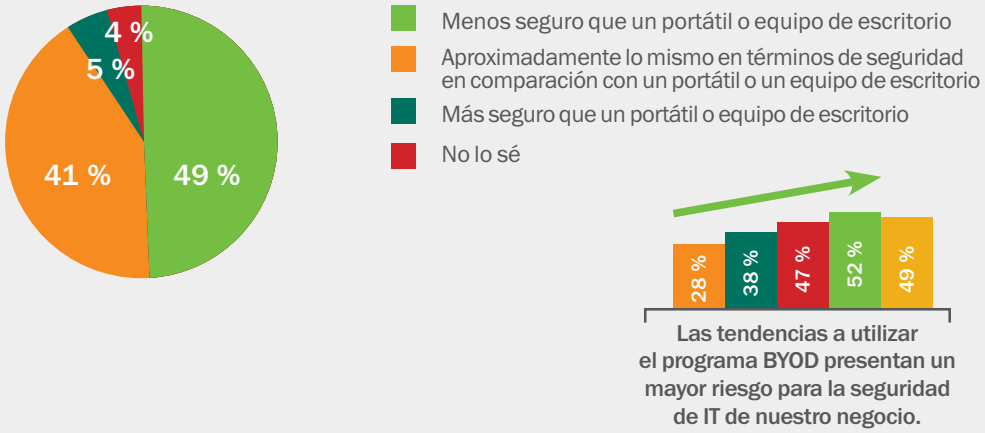
> **Todos sabemos que las empresas son más móviles, pero el perfil de uso está cambiando: ahora vemos que la mayoría de las empresas utilizan dispositivos móviles para compartir información confidencial e incluso realizar transacciones financieras.**
>
> David Emm, Kaspersky Lab, equipo de análisis e investigación global

USO Y ACTITUDES HACIA LAS TRANSACCIONES MÓVILES

¿Su empresa realiza transacciones confidenciales a través de dispositivos móviles?



¿Hasta qué punto son seguras las transacciones a través de dispositivos móviles?



Las tendencias a utilizar el programa BYOD presentan un mayor riesgo para la seguridad de IT de nuestro negocio.

Lo que sí podría considerarse una sorpresa es que poco menos de la mitad de los encuestados (**49 %**) considera que los dispositivos móviles son menos seguros que un portátil o un equipo de escritorio. El **41 %** piensa que su dispositivo móvil es tan seguro como su portátil o equipo de escritorio, el **5 %** afirmó que su dispositivo móvil es más seguro y el **4 %** no lo sabía.

Es interesante ver que todas las empresas ven el programa BYOD como una amenaza a su seguridad. Pero la percepción de esta amenaza cambia con el tamaño de la empresa. Básicamente, a medida que aumenta el tamaño de la empresa, también lo hace su preocupación por los riesgos de seguridad del programa BYOD. El **28 %** de las empresas muy pequeñas cree que presenta una amenaza cada vez más importante, una cifra que aumenta al **47 %** y el **49 %** para las medianas y grandes empresas, respectivamente.

Y llevan razón. En los últimos cuatro años, el **30 %** de las empresas ha experimentado la pérdida o el robo de un dispositivo móvil. Y aunque la pérdida de datos resultante por este problema ha disminuido en los dos últimos años, del **26 %** en 2012 al **21 %** en 2014, sigue siendo la segunda manera más habitual de que una empresa pierda sus datos, solo superado por los casos en los que su personal comparte de forma accidental los datos.

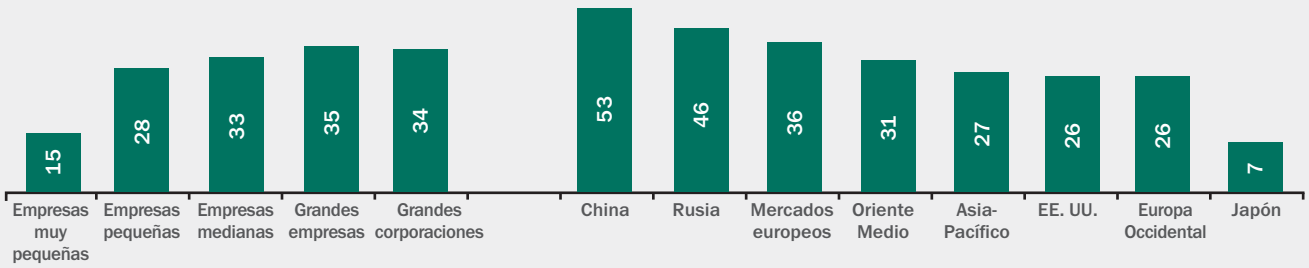
En los últimos cuatro años, el 30 % de las empresas ha experimentado la pérdida o el robo de un dispositivo móvil.

4 Virtualización: protección de nuevos entornos de trabajo

Para muchas empresas, la virtualización ha sido parte de su estrategia de IT durante algún tiempo, pero la implementación real de medidas de seguridad específicas de virtualización es baja. Se trata de un problema que muchas personas tienen presente, y un **14 %** de las empresas encuestadas lo ha mencionado como una prioridad de seguridad de IT clave para los próximos 12 meses (una cifra que aumenta a un **21 %** de las grandes empresas tipo corporaciones).

IMPLEMENTACIÓN Y GESTIÓN DE LA TECNOLOGÍA DE VIRTUALIZACIÓN

% que indica cada uno de ellos como un reto de gestión al que se enfrenta actualmente.



> **La virtualización es una parte cada vez más importante de la estrategia de IT de la mayoría de las empresas. Pero cuando se trata de adoptar soluciones de seguridad especializadas, son muy pocas las que cuentan con una comprensión clara de las soluciones disponibles o los requisitos de seguridad que crea un entorno virtualizado.**
> Sergey Lozhkin, equipo de análisis e investigación global, Kaspersky Lab

La virtualización es más una preocupación de las grandes empresas o corporaciones que de las empresas de menor tamaño. Más de una tercera parte de las medianas y grandes empresas la consideran un reto clave, frente al **28 %** de las pequeñas empresas y el **15 %** de las empresas muy pequeñas.

La comprensión de las opciones de seguridad de virtualización es contradictoria, incluso entre los profesionales de IT. Solo alrededor de un tercio de las empresas encuestadas posee una comprensión clara de las soluciones disponibles y aproximadamente un cuarto de ellas tiene una comprensión escasa o ninguna en absoluto.

GLOSARIO:

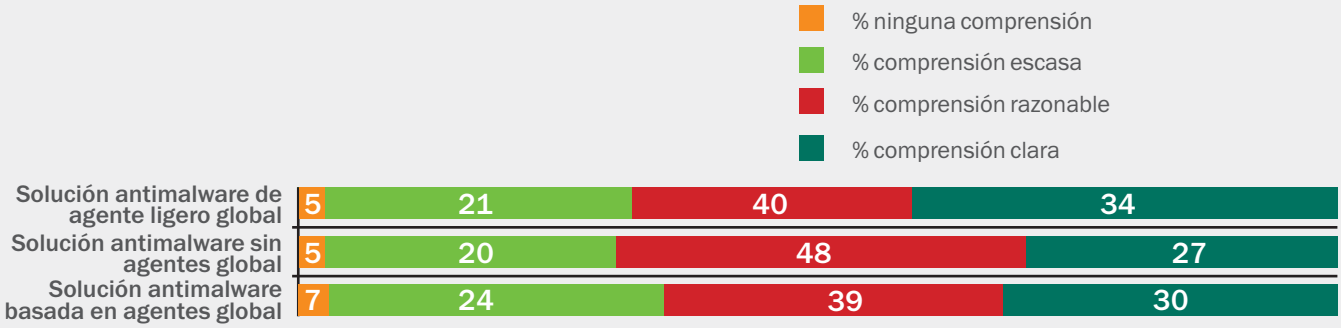
Los tres tipos de software antimalware disponibles para redes virtuales ofrecen diferentes opciones de seguridad y se implementan mejor en diferentes formas.

Sin agentes: está basado en tecnología de inserción y en un diseño centralizado. Está controlado por una consola central y no requiere la instalación de agentes en máquinas individuales o virtuales. Puede reducir los costes y la gestión, y se implementa fácilmente en grandes empresas.

Basado en agentes: se basa en tecnología de extracción y requiere software del cliente antes de proporcionar actualizaciones a un servidor. Las soluciones basadas en agentes son buenas para los usuarios itinerantes o las máquinas desconectadas, y pueden ser un complemento útil para las soluciones sin agentes.

Agente ligero: funciona desviando fuertes cargas de trabajo a un aparato virtual al tiempo que protege los endpoints contra las amenazas. La solución de agente ligero es una mezcla de la solución sin agente y la solución basada en agentes.

COMPRENSIÓN DE LA SOLUCIÓN DE SEGURIDAD DEL ENTORNO VIRTUAL ENTRE LOS EXPERTOS EN SEGURIDAD



El **24 %** de las empresas piensa que su software antimalware actual proporciona una mejor protección y, lo que es más importante, un mejor rendimiento que las soluciones especializadas. El **20 %** afirmó que no tenían problemas con sus soluciones tradicionales y el **13 %** indicó que consideraba que la amenaza para sus entornos virtualizados no era suficiente para justificar el coste adicional de la implementación de una solución especializada.

A pesar de la comprensión tan variada de las opciones de seguridad disponibles para estas, el **52 %** de las empresas encuestadas coincide con la afirmación de que **"Los entornos virtualizados constituyen cada vez más una parte central de nuestra infraestructura de IT crítica".** Por lo tanto, a medida que se convierten en la parte central de las prácticas de trabajo de una empresa, tienen que ser eficientes y seguros, pero está claro que se requiere un proceso de formación para que se puedan proteger eficazmente.

El panorama general es que las empresas parecen no estar preparadas para cambiar sus requisitos de seguridad a la hora de implementar entornos virtuales. Entre estos se incluye el aumento de su comprensión de la seguridad de la virtualización y la adopción de plataformas de seguridad especializadas. Ambas son fundamentales para la seguridad en este aspecto.

5 Informe Global de Riesgos de IT 2014
Antifraude: cálculo de costes

La prevención del fraude es uno de los temas candentes en los programas de muchas empresas. El **63 %** de los encuestados estuvieron de acuerdo con la afirmación **"Hacemos todo lo posible para asegurar que nuestras medidas antifraude estén actualizadas"**. Esta cifra fue aproximadamente un **10 %** más alta que la de los encuestados preocupados por la integración móvil, la virtualización, los ataques DDoS y otros problemas clave de estrategia de IT.

No obstante, el **43 %** de las empresas aún sienten la necesidad de mejorar la forma de garantizar la seguridad de sus transacciones financieras con el banco.

Y estos temores están bien fundados. En el año 2013, el número de ciberataques de malware financiero aumentó a 28,4 millones, un 27,6 % más que en 2012.[1] En el mismo periodo, Kaspersky Lab protegió a 3,8 millones de usuarios contra los ataques financieros y bloqueó más de 330 millones de ataques de phishing.[2]

En el año 2013, el número de ciberataques de malware financiero aumentó a 28,4 millones, un 27,6 % más que en 2012.[1]

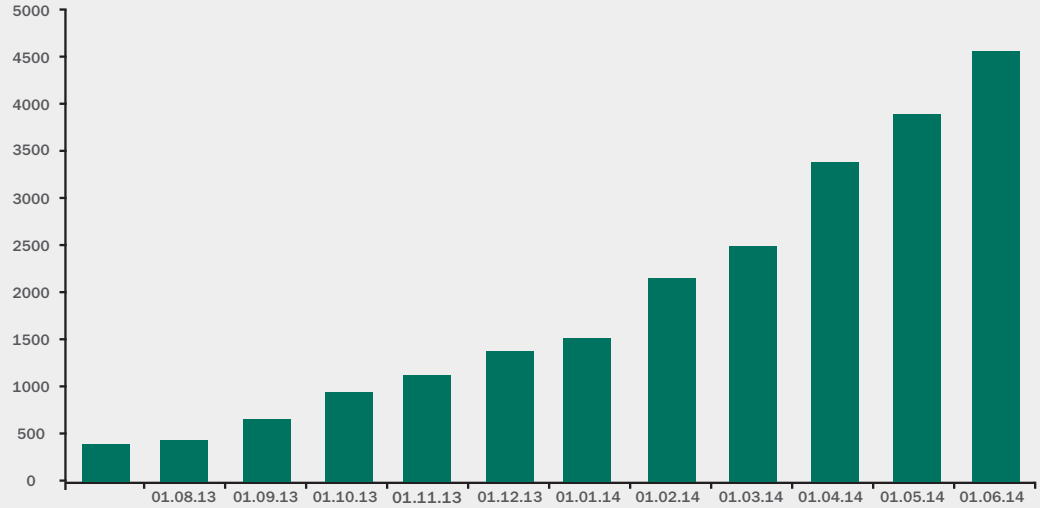
TROYANOS BANCARIOS MÓVILES

El malware móvil está diseñado para que los cibercriminales consigan dinero. Operan con troyanos basados en Windows y burlan las técnicas tradicionales de autenticación, atacando y robando números para transacciones móviles (mTAN, del inglés mobile Transaction Authentication Numbers) emitidos por los bancos, permitiendo a su vez las transferencias ilegales de fondos.

Se ha producido un repentino y considerable crecimiento de troyanos bancarios Android autónomos en los últimos 18 meses, de solo 67 troyanos bancarios a comienzos de 2013 a 1321 a finales de año, y otros 3215 adicionales registrados a mediados de 2014.3 Aunque estos ataques, hasta ahora, se han dirigido principalmente a los usuarios de Rusia y la Comunidad de Estados Independientes, es probable que los cibercriminales sigan desarrollando sus técnicas, amplíen su alcance y entren en nuevos mercados.

1. http://www.kaspersky.com/about/news/virus/2014/Kaspersky-Lab-statistics-attacks-involving-financial-malware-rise-to-28-million-in-2013
2. http://securelist.com/analysis/kaspersky-security-bulletin/59414/financial-cyber-threats-in-2013-part-2-malware/
3. http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/.

NÚMERO DE TROYANOS BANCARIOS DETECTADOS, 2.º TRIMESTRE DE 2014



Fuente: http://securelist.com/analysis/quarterly-malware-reports/65340/it-threat-evolution-q2-2014/

Algunos ejemplos bien conocidos son ZeuS-in-the-Mobile (ZitMo), SpyEye-in-the-Mobile (SpitMo), Carberp-in-the-Mobile (CitMo) y Svpeng. Svpeng es un troyano Android que roba los datos de inicio de sesión y contraseñas de la aplicación bancaria móvil de un usuario. También puede robar información de la tarjeta bancaria del usuario al solicitarle que introduzca sus datos bancarios cuando Google Play está abierto. En los tres meses de la existencia del troyano, Kaspersky Lab descubrió 50 de sus modificaciones y bloqueó más de 900 instalaciones [4].

Los mercados financieros se basan en la confianza, la confianza en que se cumplan las obligaciones, se efectúen los pagos y se protejan los datos. Por lo tanto, no es de extrañar que la protección de su reputación y trayectoria sean las preocupaciones clave para las empresas involucradas en la seguridad de los datos financieros.

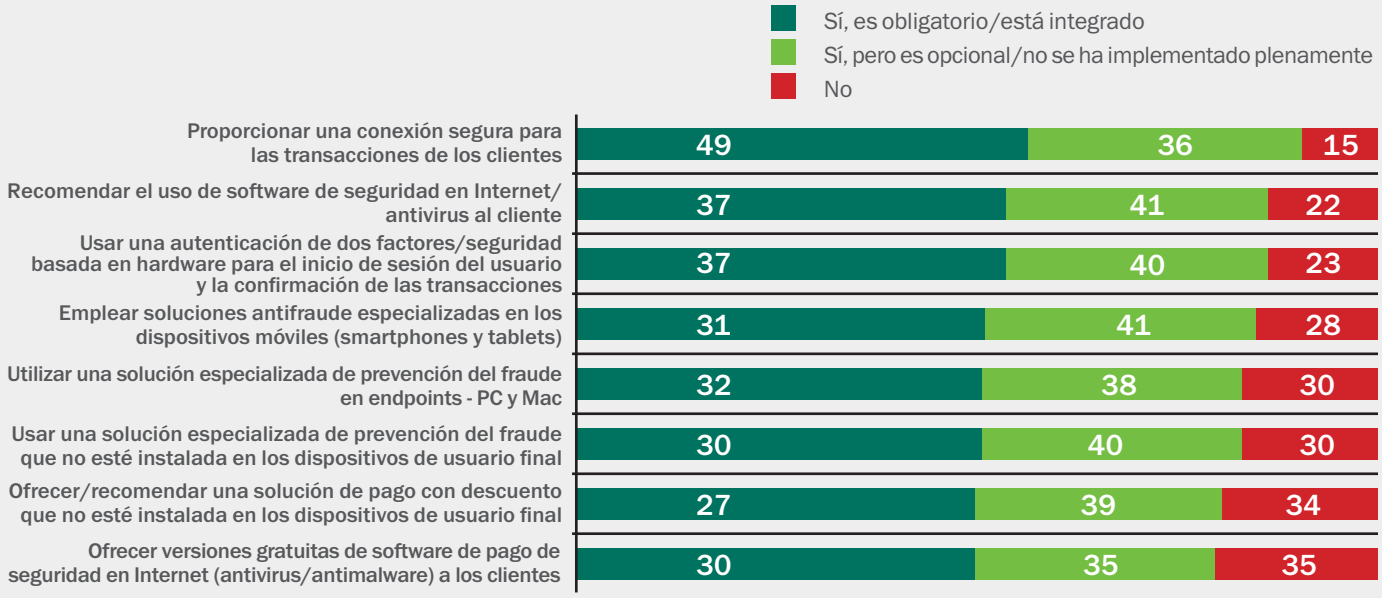
El **73 %** de las empresas se vio influenciada por la reputación de la seguridad de un banco a la hora de decidir con quién trabajar, y el **82 %** afirmó que consideraría abandonar sus relaciones con un banco si este ha sufrido una filtración de datos. Esto no debería ser una sorpresa: tener en cuenta la reputación de una empresa es una buena gestión de riesgos. Tampoco debería ser una sorpresa que proteger los datos de los clientes sea una de las prioridades del programa de las empresas encuestadas. Tal vez lo más interesante sea que el **18 %** habría de tolerar una brecha en la seguridad relativa a su seguridad financiera.

Lo realmente alarmante es que poco más de la mitad (**51 %**) de las empresas encuestadas considera que las entidades financieras están haciendo lo suficiente para proteger su información financiera. Entonces, ¿qué hacen los proveedores de servicios financieros y comercio electrónico para proteger a sus clientes y evitar el fraude?

La encuesta habla de más de 2500 empresas que trabajan en esta área y los resultados en su mayoría muestran un sector en transición. Mientras que casi la mitad de los encuestados ofrecía una conexión segura, aproximadamente un tercio aún estaba implementando un servicio seguro o no lo cumplía, y otro **15 %** no ofrecía ningún servicio seguro. Para las formas restantes de garantizar la seguridad de las transacciones, la mayoría de las empresas estaba en pleno proceso de entrega de capacidades, ofreciendo medidas antifraude opcionales, o no las había implementado en absoluto.

4. http://securelist.com/blog/research/57301/the-android-trojan-svpeng-now-capable-of-mobile-phishing/

MEDIDAS ANTIFRAUDE EMPLEADAS POR PROVEEDORES DE SERVICIOS FINANCIEROS Y OPERADORES DE COMERCIO ELECTRÓNICO



BASE: 2680. Todos los encuestados trabajan en el área de servicios financieros u operan online, pública

Los bancos y los clientes tienen diferentes opiniones acerca de quién es el responsable de seguridad financiera. Solo el **35 %** de los clientes considera que las instituciones financieras son las que tienen la responsabilidad final en materia de seguridad financiera, en comparación con el **85 %** de las instituciones mismas. Las empresas muy pequeñas y pequeñas eran las más inclinadas a creer que la responsabilidad recaía en la institución financiera (el **48 %** y **41 %** respectivamente), en comparación con solo el **27 %** de las grandes empresas.

Debido a la falta de equipos de seguridad especializados en las pequeñas empresas, el personal de IT tiene que asumir plenamente las tareas para asegurar el proceso y la responsabilidad de sus errores. El **28 %** de los clientes afirmaba que la responsabilidad final recaía sobre su departamento de IT. Esto subraya aún más la necesidad de una protección a varios niveles y totalmente integrada que sea capaz de cubrir toda la gama de necesidades de las pymes.

> **Hay una absoluta falta de claridad sobre quién es el responsable de la seguridad en las transacciones. La respuesta es que tanto las empresas como las instituciones financieras deben hacer mucho más. Se trata de la gestión de riesgos, y el estado actual del sector sugiere que la gente está demasiado expuesta.**
>
> David Emm, equipo de análisis e investigación global, Kaspersky Lab

Informe de riesgos de IT globales 2014:

6 El verdadero coste de las filtraciones de datos

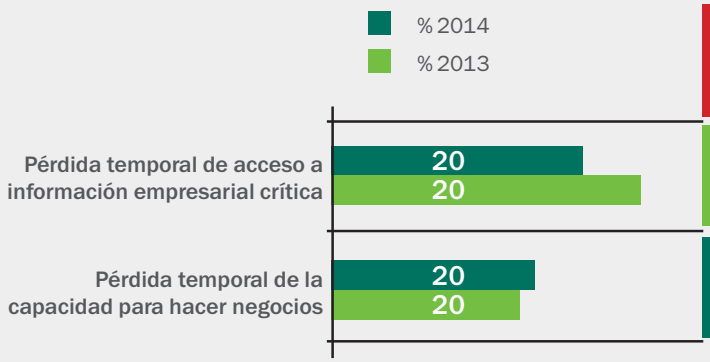
¿Cuánto podría costarle una filtración de datos a su empresa? Si no ha sufrido esta dura experiencia, puede que sea una pregunta difícil de responder. De lo contrario, sabe demasiado bien el precio que su empresa tuvo que pagar. Las consecuencias de una filtración de datos siempre van más allá de la pérdida inicial de información delicada y confidencial, y el daño que causa es mucho más grave.

Las brechas en la seguridad suelen tener como resultado una serie de gastos adicionales, incluidas las acciones correctivas y preventivas. Sí, existe el temor inmediato de que la información confidencial de la empresa esté ahora en manos de los cibercriminales, pero las repercusiones a largo plazo pueden incluir el coste de la pérdida de datos, el daño a la reputación, la reducción de la eficiencia organizativa, los costes de terceros, los gastos reactivos y las oportunidades perdidas.

Estas consecuencias pueden ser catastróficas para cualquier empresa. De las empresas encuestadas que habían sufrido una filtración de datos, el **55 %** afirmaba que fue muy difícil funcionar como lo habían hecho antes. Y no solo a corto plazo. El **54 %** de las empresas indicó que la pérdida de datos había tenido un impacto negativo en su reputación, reduciendo la percepción de fiabilidad a los ojos de los clientes, los accionistas y el resto del mundo de los negocios.

Las cifras indicadas a continuación muestran más información sobre la amplia duración de las consecuencias negativas que puede tener una filtración de datos, así como la gran cantidad de empresas que se quedan sin la posibilidad de hacer negocios y, por tanto, hacer dinero.

IMPACTO ENTRE LOS INFORMES DE CADA CASO



	Muy corto plazo	Corto plazo	Importante	Prolongado
Pérdida temporal de acceso a información empresarial crítica	20	39	31	10
Pérdida temporal de la capacidad para hacer negocios	17	42	30	10

La gran mayoría de las empresas (el **87 %**) no pudo resolver el problema por sí mismas y tuvo que buscar ayuda de servicios profesionales. Estos incluyeron desde servicios de consultores de seguridad de IT y abogados hasta auditores y asesorías de gestión de riesgos. Casi la mitad de estas empresas (**47 %**) afirmó que estos servicios se tradujeron en importantes costes adicionales.

Pero los gastos reactivos no solo se limitan a recurrir a terceros. Si las pymes experimentan filtraciones de datos, podrían incurrir en unos gastos adicionales de hasta 6.000€ estadounidenses en personal, 7.500€ en formación y 5.000€ en sistemas. Y las grandes empresas (mayores, pero con mucho más en juego) podrían incurrir en unos gastos adicionales de hasta 50.000€ estadounidenses en personal, 30.000€ en formación y 64.000€ en sistemas.

> **Tras una brecha en la seguridad, la pérdida de datos es solo la punta del iceberg del problema financiero: el coste real es mucho mayor. Hay costes graves evidentes, tales como las medidas adicionales de seguridad y el asesoramiento jurídico, pero el daño a la marca y la reputación son probablemente mucho mayores.**
> Costin Raiu, equipo de análisis e investigación global, Kaspersky Lab

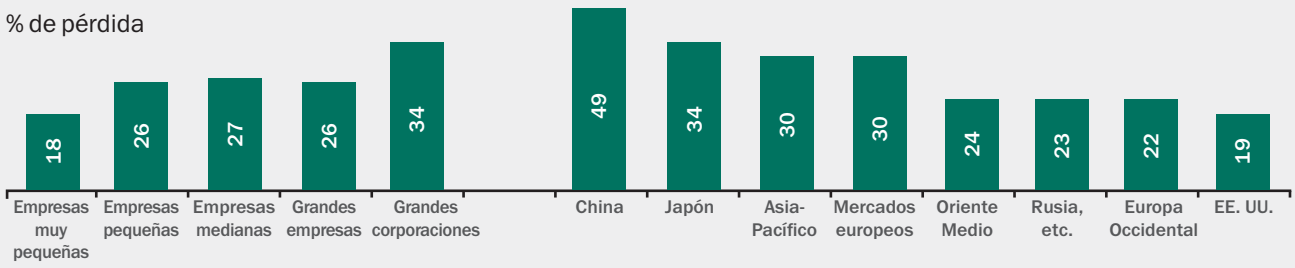
La pérdida de capacidad para operar es otra de las principales causas de preocupación después de una filtración de datos o un ataque a la seguridad. De las empresas que habían experimentado pérdidas de datos, aproximadamente una tercera parte se quedó sin la capacidad para hacer negocios. No obstante, también hay buenas noticias en este sentido: tanto en 2013 como en 2014, tanto las empresas pequeñas como las grandes se ha protegido mejor en estos casos, y el coste medio del tiempo de inactividad ha disminuido para pymes y grandes empresas, como se muestra a continuación.

Tamaño de la empresa	Coste del tiempo de inactividad	
	2013	2014
Pymes	64 millones de dólares	57 millones de dólares
Grandes corporaciones	1,7 millones de dólares	1,6 millones de dólares

¿Qué pueden aprender las empresas de estas conclusiones? Básicamente, que el gasto reactivo siempre es más caro que el gasto proactivo. Por lo tanto, las empresas deben hacerse ahora la siguiente pregunta: "¿Podemos permitirnos el lujo de no protegernos a nosotros mismos?"

Hay una interesante respuesta a esta pregunta. De media, un poco más de la cuarta parte de las empresas (**26 %**) está dispuesta a aceptar una pérdida de datos o una brecha en la seguridad. ¿Por qué? Porque creen que es menos costoso que actualizar sus sistemas de IT para evitar que se produzca el problema, como podemos ver a continuación.

"Estamos dispuestos a aceptar algunas pérdidas financieras por el cibercrimen, ya que siempre serán menores que los costes que implica actualizar nuestros sistemas de IT para impedirlo".



Aunque sin duda estamos interesados en ver los cálculos efectuados para llegar a esta conclusión, no estamos de acuerdo. Los daños potenciales resultantes de las filtraciones de datos se extienden mucho más allá de los costes inmediatos. Los costes atribuidos a la continuidad del negocio, el valor de marca, la reputación y los costes potenciales de terceros superan con creces los costes financieros de una protección eficaz a varios niveles.

Informe Global de Riesgos de IT 2014

7 El verdadero reto de la gestión es que, en un mundo complicado, tenemos que hacer que las cosas sean más sencillas

La encuesta de este año puso de manifiesto la complejidad a la que se enfrentan las empresas de todos los tamaños.

Y la complejidad a la que deben enfrentarse tiene dos frentes:

1. La complejidad creciente de las amenazas

El malware se ha convertido de forma muy rápida en algo mucho más sofisticado. Para mantener la seguridad, todas las empresas necesitan una protección más profunda de la que puede ofrecer una simple solución "antivirus". Esto ha creado la percepción de tener que gestionar un conjunto de herramientas complejas mucho más molestas. Y en algunos casos esta percepción está justificada. El mercado de seguridad está repleto de miles de ofertas de productos nicho que obligan a los equipos de IT con escasos recursos a esforzarse por aprender, integrar y gestionar.

2. El aumento de la complejidad de la infraestructura de IT

Incluso las empresas pequeñas se alimentan de una sorprendente y compleja gama de tecnología. Además de la red LAN básica, suelen tener varios tipos de software para toda la empresa, así como personas que instalan aplicaciones "maliciosas" en sus sistemas. Si añade esto al crecimiento de la virtualización, el resultado es una gran cantidad de elementos que deben controlarse y gestionarse. Pero es la movilidad lo que realmente plantea el mayor reto para los profesionales de IT.

Por lo tanto, ¿qué deberían hacer los profesionales de IT cuando la tarea parece algo tan complicado? A continuación le presentamos nuestra lista de recomendaciones:

Administre un sistema de seguridad unificado

El reto que detectamos con mayor frecuencia es que la aparición de una nueva tarea (por ejemplo, la actualización de aplicaciones) provoca el impulso de comprar una solución específica. Aunque en un entorno de aislamiento está bien, después de un tiempo, el resultado es una compleja gama de sistemas desconectados. En la práctica, esto se traduce en más gestión y la creación de más trabajo, y abre las puertas a nuevas vulnerabilidades (ya que hay muchas cosas que vigilar).

Incluya los dispositivos móviles como parte del plan más amplio

Asuma que la inmensa mayoría de la fuerza de trabajo tendrá siempre algún tipo de aspecto de movilidad en su trabajo, pues estará pensando de la manera correcta. Una vez más, una herramienta de seguridad móvil independiente acabará siendo otra cosa que hay que gestionar, y en realidad, creará nuevas vulnerabilidades en la seguridad general de IT.

Vuelva a calibrar su enfoque: invierta en protección a varios niveles

Con el continuo aumento en el número y la sofisticación de las amenazas, es evidente que estamos infravalorando la magnitud y la gravedad de los retos a los que nos enfrentamos en materia de seguridad. Las intrusiones en la red, los ataques de phishing y los ataques DDoS son amenazas importantes que pueden conducir a filtraciones de datos muy costosas. Pero, ¿sabe cuál es la amenaza real? Sigue siendo el malware.

Por eso, ahora es crucial que las empresas inviertan en protección a varios niveles. El software antivirus por sí mismo ya no es suficiente. Las empresas deben adoptar un enfoque mucho más proactivo en la gestión del comportamiento del malware sofisticado que se esconde en sitios web aparentemente seguros, que aparece en los archivos aparentemente inocentes, que se beneficia de las vulnerabilidades de las aplicaciones y que se aprovecha de los dispositivos no seguros o incluso de las redes Wi-Fi no seguras. El volumen de los nuevos programas de malware, junto con su sofisticación, hacen que la protección proactiva sea fundamental y no una simple "protección adicional".

No piense que el fraude no puede ocurrirle a usted

No es de extrañar que la reputación de una empresa sea importante para sus clientes. Lo que resulta sorprendente es que más de una cuarta parte de las empresas encuestadas no cree que los bancos estén haciendo lo suficiente para proteger su información financiera. Quizá lo más sorprendente aún es que el 4 % de las empresas que realizan algún tipo de servicio online no tomó medidas específicas para proteger a sus clientes.

Nunca se dé por vencido con la educación de los usuarios

Como profesional de IT, su trabajo es asegurarse de que las herramientas y los sistemas adecuados están implementados, y garantizar que su personal tiene la formación necesaria. Los empleados pueden, de forma accidental, permitir una brecha en la seguridad y la tecnología puede ayudar a prevenir en gran medida este problema. Pero la combinación de este enfoque con formación y reglas y políticas verdaderamente sólidas y rápidas mejorará notablemente la seguridad de IT.

Hay mucho por hacer, pero la tarea no es tan imposible como algunas personas creen.

Conozca a nuestros expertos

El equipo de análisis e investigación global de Kaspersky Lab ha proporcionado el análisis experto incluido en este informe.

Costin Raiu
Costin es el director del equipo de análisis e investigación global. Costin fue anteriormente el experto en seguridad jefe, ha trabajado para Kaspersky desde el año 2000 y se especializa en sitios web maliciosos, seguridad y exploits de navegadores, malware de banca electrónica, seguridad a nivel de empresa y amenazas de la web 2.0. Lea su blog en http://securelist.com/author/costin/ o siga a @craiu en Twitter.

David Emm
David se unió por primera vez al sector antivirus en 1990 y comenzó a trabajar para Kaspersky Lab en 2004, donde ideó y desarrolló nuestro taller Malware Defence Workshop. Actualmente es investigador regional sénior en el Reino Unido y es comentarista habitual en la prensa. Sus principales intereses en investigación giran en torno al ecosistema del malware, el robo de identidad, los aspectos humanos de la seguridad y las tecnologías KL. El blog de David se puede encontrar en http://securelist.com/author/davidemm/, y también puede seguirle en @emm_david en Twitter.

Sergey Lozhkin
Investigador sénior en seguridad del equipo de análisis e investigación global, Sergey se unió a Kaspersky Lab en 2012. En su puesto actual, lleva a cabo investigaciones sobre ciberespionaje, el análisis estático y dinámico del malware, redes Undernet como TOR, ingeniería social, transferencias de datos seguras, análisis de exploits, redes anónimas y el cibercrimen en general.

Antes de unirse a Kaspersky Lab, Sergey trabajó en varias empresas como especialista en pruebas de introducción y analista de virus. También investigó cibercrímenes para el Ministerio del Interior de Rusia después de graduarse de la Academia de Omsk del Ministerio de Asuntos Internos. Lea su blog en http://securelist.com/author/sergeyl/ o siga a @61ack1ynx en Twitter.

COMIENCE HOY MISMO: PRUEBA GRATUITA DE 30 DÍAS

Descubra cómo nuestra seguridad premium puede proteger su empresa contra el malware y el cibercrimen con una prueba sin compromiso.

Regístrese hoy mismo para descargar las versiones completas de los productos y evaluar la gran protección que ofrecen para su infraestructura de IT, endpoints y datos confidenciales de su empresa.

OBTENGA SU PRUEBA GRATUITA AHORA

UNIRSE A LA CONVERSACIÓN

#securebiz

Véanos en YouTube

Véanos en Slideshare

Síganos en Facebook

Revise nuestro blog

Síganos en Twitter

Únase a nosotros en LinkedIn

Más información en www.kaspersky.com/sp/business

ACERCA DE KASPERSKY LAB

Kaspersky Lab es el mayor proveedor privado de soluciones de protección de endpoints del mundo. La empresa figura entre los cuatro proveedores principales de soluciones de seguridad para usuarios de endpoints.* A lo largo de sus más de 17 años de historia, Kaspersky Lab se ha mantenido como una empresa innovadora en seguridad de IT y suministra eficaces soluciones de seguridad digitales para grandes empresas, pymes y particulares. Kaspersky Lab, cuya sociedad de cartera está registrada en el Reino Unido, opera actualmente en casi 200 países y territorios del globo, y brinda protección a más de 300 usuarios en todo el mundo. Más información en www.kaspersky.es.

* La empresa logró el cuarto puesto en el índice de IDC de ingresos de seguridad para endpoints en todo el mundo por proveedor de 2012. Este índice se publicó en el informe de IDC "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares" (IDC núm. 242618, agosto de 2013). En el informe se clasifican los proveedores de software según los ingresos de ventas de soluciones de seguridad para endpoints en 2012.