Resultados exclusivos
das sondagens de 2014

# Ameaças de segurança de TI e violações de dados

Perceção e Realidade: chegou a hora de as reajustar

O fortalecimento empresarial com base na segurança.
www.kaspersky.pt/business

#securebiz

KASPERSKY lab

# Índice



# Acerca do Relatório global de riscos de TI

No seu 4.º ano, o **Relatório global de riscos de TI da Kaspersky Lab** recolhe informações através de profissionais de TI em todo o mundo. Este relatório, realizado por especialistas de investigação da B2B International e analisado por equipas de investigação e especialistas em informação de ameaças da Kaspersky, proporciona uma perspetiva essencial dos comportamentos e estratégias prevalecentes na indústria relativamente à segurança de TI. Serve também como uma referência para ajudar as empresas a compreender o tipo e o nível de ameaças de segurança de TI que enfrentam.

**Por que deve ler este relatório?**

- **Abrange resultados globais e através de vários setores**
- **Proporciona-lhe uma perspetiva exclusiva das opiniões e estratégias dos profissionais de TI em todo o mundo**
- **Ajuda-o a classificar a sua segurança de TI comparativamente aos seus concorrentes da indústria**

Relatório global de riscos de TI de 2014:

# Resumo executivo

Resumo do inquérito:

- **3900 inquiridos**
- **27 países**
- **Relativo ao período entre abril de 2013 e maio de 2014**
- **Foram inquiridos profissionais de TI com "bons conhecimentos de trabalho" relativamente aos problemas de TI**

## Entre 2013 e 2014, a segurança de TI passou de uma mera "preocupação" para uma "notícia global" onde a espionagem empresarial, as fugas de dados e o cibercrime fizeram as manchetes. Mas o que se passa realmente por trás de todo o burburinho e em que medida isto o afeta?

As considerações estratégicas a longo prazo voltaram a ser importantes nas agendas administrativas graças ao regresso dos mercados globais a uma melhor condição económica. Um novo foco no crescimento e não apenas na sobrevivência no próximo ano fiscal originou uma mudança nas prioridades e, graças a isso, é agora prestada uma maior atenção às estratégias de gestão de riscos. Contudo, estas estratégias apenas são eficazes se estiverem integradas numa compreensão precisa do panorama atual de ameaças.

Um dos fatores mais interessantes destacados no inquérito deste ano é aquilo a que chamamos de **"lacuna de perceção"**, ou seja, a diferença entre a nossa perceção do que está a acontecer e a realidade.

A Kaspersky Lab detetou, entre 2013 e 2014, cerca de 315 000 amostras diárias maliciosas. De entre as empresas inquiridas, apenas **4%** foram capazes de indicar com precisão este valor. Na realidade, **91%** das inquiridas subestimou este facto e **70%** pensou existirem menos de 10 000 ameaças diárias. Trata-se evidentemente de um erro de cálculo grave.

Contudo, esta é apenas uma pequena parte da história. **94%** das empresas passou por alguma forma de ameaça de segurança externa e apenas **68%** das empresas implementou totalmente antimalware nas suas estações de trabalho, enquanto apenas **44%** implementa soluções de segurança nos seus dispositivos móveis.

**94% das empresas passou por alguma forma de ameaça de segurança externa**

Como resolvemos esta situação? É necessário reajustar a nossa perceção da indústria para melhor compreender as ameaças. Para além de ser necessário compreender as falhas de segurança visíveis, também é necessário compreender os riscos de segurança diários e contínuos.

Uma grande preocupação é o controlo e a integração de dispositivos móveis nas práticas de trabalho normais e a segurança relacionada com a virtualização. Porém, apenas **34%** dos responsáveis pelas decisões de TI compreende bem as soluções de segurança virtuais disponíveis, e **46%** das empresas considera que as suas soluções de segurança convencionais proporcionam uma proteção adequada.

O impacto **estimado** das violações de dados nas pequenas e médias empresas (PME) desceu **12%**, de **54 000 USD** para **48 000 USD**, mas o impacto estimado nas grandes empresas aumentou **14%**, de **700 000 USD** para **798 000 USD** . Contudo, isto pode muito bem ser um problema de perceção. As grandes empresas estão melhor equipadas para detetar quebras de segurança, enquanto as pequenas e médias empresas (PME) poderão não saber se estiveram sob ataque.

No entanto, este impacto não é assim tão simples e claro como podemos pensar. **87%** das empresas vítimas de perda de dados requisitou a assistência de serviços profissionais adicionais e quase metade **(47%)** sofreu custos adicionais significativos. No último ano, a média de "danos típicos" (contratação de serviços profissionais, maiores períodos de inatividade e perda de oportunidades de negócio) nas PME provocados por eventos graves equivaleu a 35 000 USD. Nas grandes empresas, este valor equivaleu a 690 000 USD.

O impacto das violações de dados na confiança e na reputação também foi muito aparente. **82%** das empresas consideraria abandonar uma instituição financeira caso esta sofresse uma falha, enquanto **27%** das empresas não considera que os bancos estejam a fazer o suficiente relativamente à proteção das suas informações financeiras.

**82% das empresas consideraria abandonar uma instituição financeira caso esta sofresse uma falha**

Existe, porém, uma divisão de opinião no que diz respeito à perceção de quem é responsável, em última análise, pela proteção das transações financeiras. Apenas **35%** dos clientes considera que as instituições financeiras são as principais responsáveis, enquanto **85%** das instituições financeiras se consideraram responsáveis.

Qual é a razão para isto? As empresas estão a progredir, mas também a indústria do cibercrime. Embora existam ferramentas para as organizações se protegerem, a maioria das empresas ainda toma uma abordagem reativa perante a segurança de TI. As empresas precisam de ser mais proativas e deixar de subestimar a diversidade, o número e a sofisticação das ameaças atuais. Em suma, as soluções antivírus tradicionais já não são suficientes.

As empresas precisam de reconhecer a complexidade do desafio que têm pela frente. A construção de uma defesa multicamada contra as ameaças colocadas por fatores "humanos", o aumento de diversos dispositivos e a emergência de novas tecnologias são agora essenciais, dado que nenhuma empresa dispõe de recursos humanos suficientes para lidar com tudo.

Está na altura de reajustar seriamente o modo como os problemas de segurança são percebidos e resolvidos. As empresas precisam de ser mais proativas e atentas e também devem informar-se. Caso contrário, arriscam-se a tornar-se a próxima grande notícia de segurança de TI.

**Em suma, as soluções antivírus tradicionais já não são suficientes**

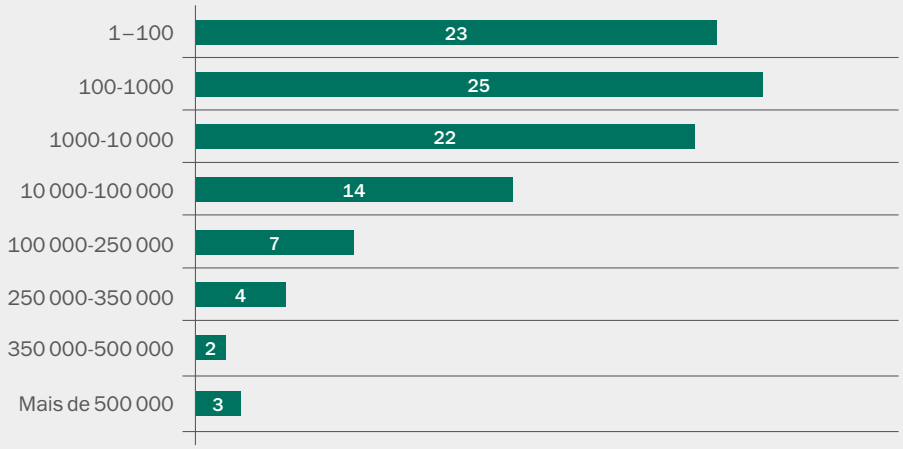
# 1 Relatório global de riscos de TI de 2014: Perceção e realidade – como eliminamos as lacunas?

> **Existe um fosso crescente entre o que as empresas acreditam ser o panorama de ameaças e o que este realmente é. Chamamos a isto "lacuna de perceção". Mostra que as organizações, independentemente da sua dimensão, subestimam substancialmente a quantidade e a gravidade das ameaças que enfrentam.**
> Costin Raiu, Equipa de Investigação e Análise Global, Kaspersky Lab

Como responsável de decisões de TI, é responsável pelos sistemas críticos para a empresa e respetiva infraestrutura. É responsável pela proteção da sua empresa contra ameaças, pela prevenção contra perda de dados e pela garantia de um bom funcionamento global. Na maioria das vezes consegue cumprir o seu dever. Mas o que deve fazer nas ocasiões em que não consegue? O que deve fazer relativamente às coisas que lhe escapam?

Às vezes, é necessário olhar para a realidade e ajustar a perspetiva para, desta forma, refletir na natureza em constante mudança e evolução das ameaças que enfrenta. **91%** dos decisores empresariais subestima o número de amostras de ameaças descobertas diariamente, e apenas **4%** dos decisores tem uma noção exata do número real existente. Além disso, a maioria de nós subestima dramaticamente este número, em que **70%** considera existirem menos de 10 000 novas amostras descobertas diariamente. O número real detetado pela Kaspersky Lab é de 315 000 novas amostras.

**Número de novas amostras de malware descobertas diariamente (%)**



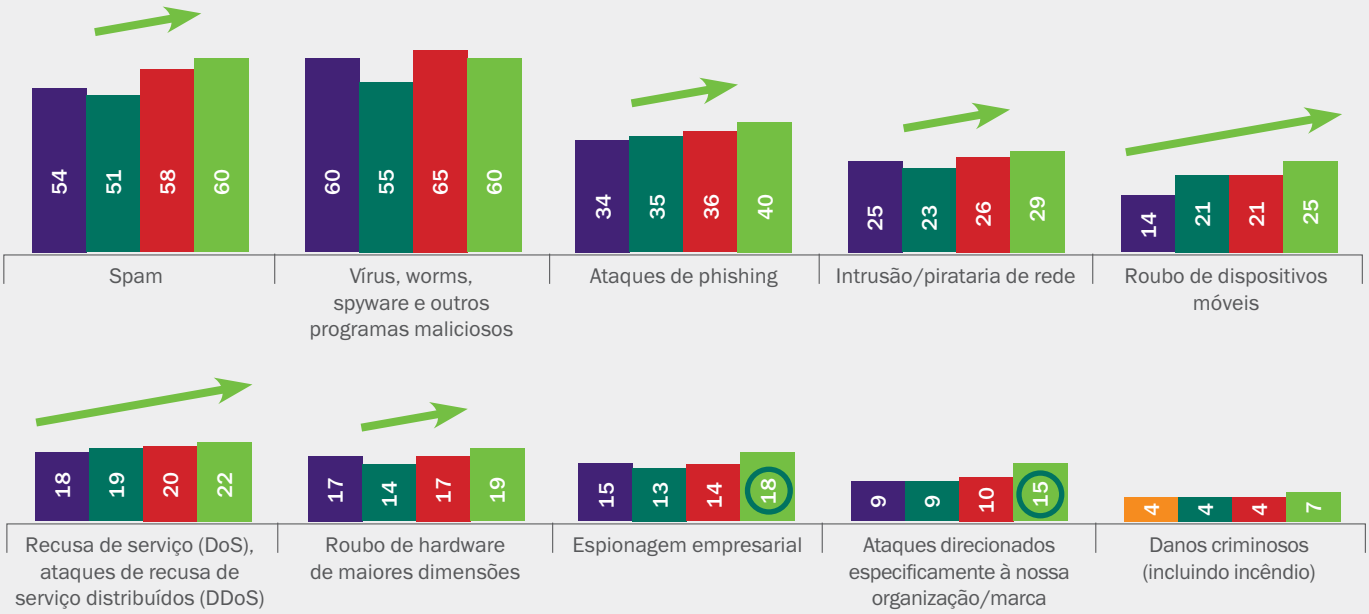

Curiosamente, embora subestimem o número de ameaças, os participantes no inquérito comunicaram um aumento do número de ciberataques todos os anos nos últimos 4 anos. Esta observação pode dever-se ao facto de muitas organizações considerarem ter havido um aumento das ameaças sem terem uma noção clara do quadro global.

As empresas de todas as dimensões indicaram níveis crescentes de spam, phishing e ataques DDoS como áreas de preocupação. A espionagem empresarial e os ataques direcionados estão também a aumentar. O número de organizações que reporta ataques direcionados específicos aumentou **5%** desde 2013, sendo agora de **15%**.

O que está por trás destas ameaças?

## Ameaças externas vividas

94% das empresas assistiu a alguma forma de ameaça de segurança externa. Também se verifica a emergência de algumas tendências evidentes, como o aumento crescente de ataques de recursa de serviço nos últimos quatro anos.




Existe a ideia errada de que o malware é algo específico e discreto em vez de algo que está na realidade integrado nos ciberataques. Embora o número de ataques de malware registados tenha diminuído entre 2013 e 2014, estes continuam a ser as ameaças mais numerosas e perigosas à segurança de TI. Os ataques de phishing, DDoS e direcionados estão todos relacionados com a utilização de malware cada vez mais sofisticado.

Embora existam medidas de segurança que já são empregues, ainda há grandes lacunas nos sistemas de segurança de TI, independentemente da dimensão da empresa.

Independentemente da natureza da ameaça colocada pelo malware, apenas **68%** das empresas tem software antimalware implementado nas estações de trabalho, apenas **42%** das empresas utiliza soluções de segurança em dispositivos móveis e apenas **52%** de todas as empresas inquiridas instala patches ou atualiza o software regularmente, uma tarefa importante na prevenção contra ataques de malware ou violações de dados.

Isto sugere no mínimo que as empresas estão apenas parcialmente protegidas; uma leitura mais crítica sugere que estão lamentavelmente mal preparadas para as ameaças que enfrentam.

Como é que as empresas eliminam estas lacunas? Através de uma melhor compreensão da verdadeira natureza destas ameaças e de uma implementação e manutenção eficazes de soluções de segurança direcionadas.

# 2 Relatório global de riscos de TI de 2014: As ameaças mais sofisticadas exigem uma proteção multicamada

Atualmente as organizações de todo o mundo enfrentam ameaças de segurança cada vez mais complexas. Infelizmente, um único produto ou abordagem não consegue proteger as empresas de todos os tipos de malware, vírus ou programas maliciosos, ao contrário de antigamente. Uma política única para todos os casos não tem a abrangência nem a capacidade de proteção das empresas contra os diversos ataques nas suas infraestruturas de TI.

Além disso, para piorar ainda mais a situação, o malware evolui depressa e muda diariamente. É como lutar contra um inimigo em constante movimento. No final de 2013, observaram-se 200 000 amostras únicas de códigos de malware móvel. Só na primeira metade de 2014, foram criadas mais 175 000 novas amostras. Estas taxas de crescimento preocupantes devem ser tidas em conta na definição das suas estratégias de segurança para a proteção de dados, segurança das transações financeiras e manutenção da continuidade do serviço contra ataques DDoS.

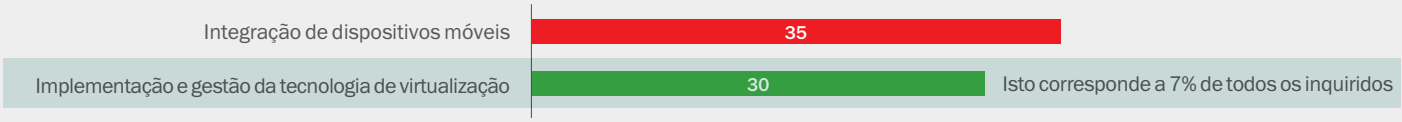
> **Uma das estatísticas do inquérito mais preocupantes foi a utilização muito reduzida da gestão de aplicações e patches. Dado que a maioria das falhas de segurança se deve à vulnerabilidade de uma aplicação insegura, esta deve ser uma área de foco importante para qualquer profissional de TI.**
>
> Sergey Lozhkin, Equipa de Investigação e Análise Global, Kaspersky Lab

É importante denotar que o que é melhor para uma empresa não é necessariamente o melhor para outra. É essencial obter a solução adequada para a rede da sua empresa, quer opere redes LAN, sem fios e móveis, redes de longa distância ou comunicações baseadas em IP, ou uma combinação destas. As soluções de segurança precisam de funcionar eficazmente nestas plataformas sem comprometerem a segurança ou o desempenho. Uma vez que a virtualização é um objetivo prioritário para muitas das empresas e devido à crescente importância dos dispositivos móveis, agora é mais importante do que nunca que as organizações compreendam a necessidade de uma proteção contra ameaças multicamada integrada que funcione nos dispositivos físicos, móveis e virtuais.

De acordo com o gráfico abaixo, podemos verificar que dos inquiridos que consideram a "gestão da mudança" a principal preocupação, **30%** afirmou que a implementação e a gestão da tecnologia de virtualização era o seu maior desafio, enquanto **35%** afirmou que era a integração de dispositivos móveis.

## GESTÃO DA MUDANÇA NOS SISTEMAS DE TI

Se observarmos mais detalhadamente os 22% de inquiridos que consideram a gestão da mudança a principal preocupação, a plataforma móvel e a virtualização são desafios principais



O próximo gráfico destaca as ameaças colocadas às empresas de grande e pequena dimensão, desde malware e fugas de dados a espionagem empresarial e roubo de dispositivos móveis.

## EVENTO MAIS GRAVE DE PERDA DE DADOS

O malware é atualmente a principal causa dos eventos de perda de dados mais graves. É um problema menor para as empresas maiores, onde a fuga intencional de informações é uma preocupação muito maior.


Base: varia para todos os inquiridos de cada dimensão que perderam dados

De acordo com o gráfico acima, é evidente que o malware é a principal causa de perda de dados. Então, por que razão, entre 2013 e 2014, as empresas observaram uma queda de **5%** nos ataques de malware? Em termos simples, **91%** das empresas subestima o número de novas amostras descobertas diariamente e, além disso, ainda não foi amplamente compreendido que muitos dos ataques direcionados têm malware no seu núcleo, como phishing e DDoS. Tudo isto não significa que as infiltrações de malware diminuíram; os ataques não são simplesmente observados como ataques de malware.

**O que podemos aprender com estas conclusões?**

1. As soluções antivírus tradicionais já não são eficazes nem proporcionam a profundidade e escala de proteção de que as empresas necessitam.
2. A complexidade crescente das infraestruturas de TI proporciona uma maior oportunidade para ataques maliciosos.
3. O erro humano e a avaliação errónea não podem ser ignorados e o aumento da iniciativa Bring Your Own Device (BYOD) facilitou a exploração das práticas de trabalho.

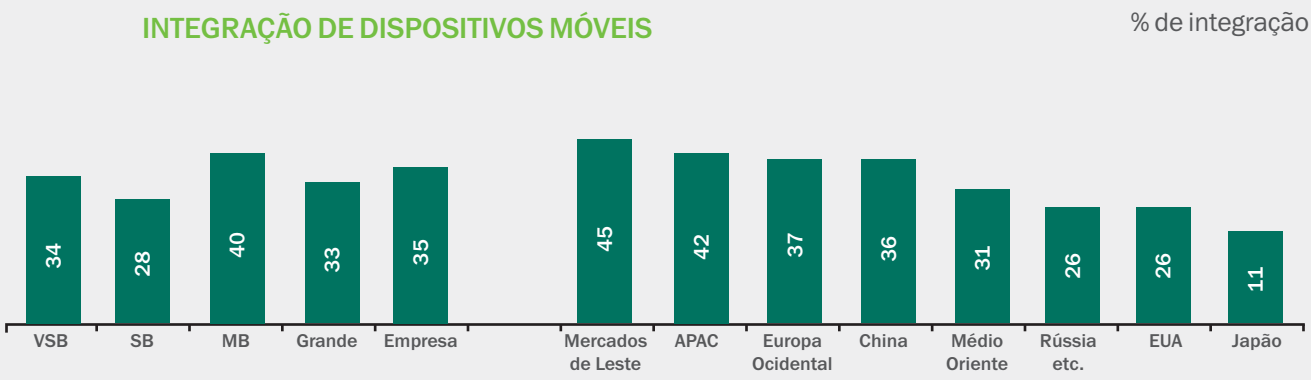
# 3 Relatório global de riscos de TI de 2014: Plataformas móveis: a ameaça emergente

O trabalho móvel está a ser rapidamente adotado pelas empresas de todo o mundo. Mas o seu ponto forte, nomeadamente a prestação de ajuda aos colaboradores para serem mais flexíveis, não vale de nada se não forem implementadas medidas de segurança adequadas. Um dispositivo móvel desprotegido proporciona acesso a dados sensíveis e oferece aos cibercriminosos um ponto de entrada fácil para um sistema protegido.

É por esse motivo que **35%** das empresas reconheceu que a integração de dispositivos móveis era um dos seus maiores desafios para o próximo ano. Este não é apenas um tópico relevante para as empresas de maior dimensão. A integração de dispositivos móveis é essencial para as empresas de todas as dimensões, como podemos ver no gráfico abaixo. Apenas as pequenas empresas, **28%**, apresentam menos de um terço de inquiridos que indica a integração móvel como uma preocupação principal. Contudo, tal poderá dever-se ao facto das pequenas empresas subestimarem as potenciais ameaças provenientes de e destinadas aos dispositivos móveis.

**24%** das empresas indicou a iniciativa BYOD como uma das suas principais prioridades de segurança de TI nos próximos 12 meses, e este valor aumentou para 32% nas empresas muito pequenas. Isto não deve constituir uma surpresa, uma vez que **42%** das empresas realiza atualmente transações delicadas nos seus dispositivos móveis.

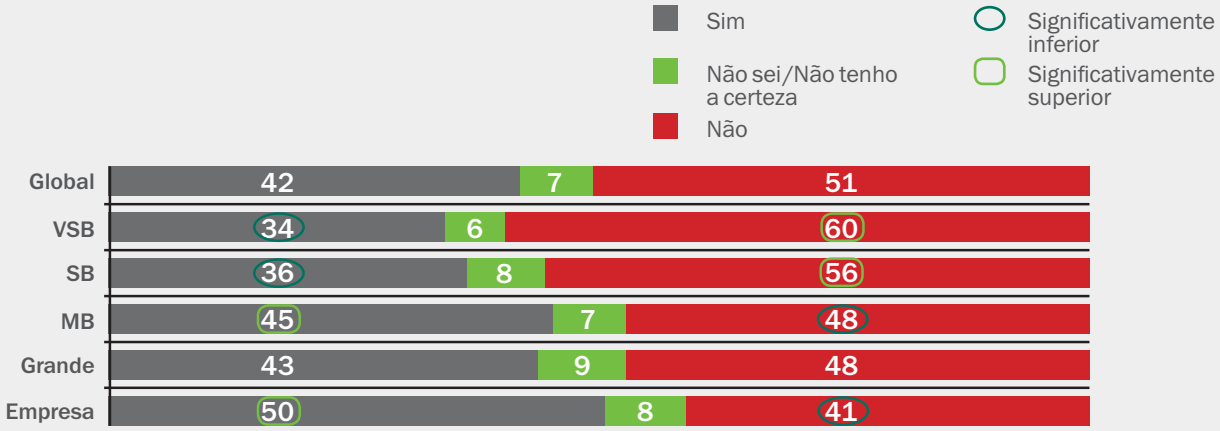
## INTEGRAÇÃO DE DISPOSITIVOS MÓVEIS



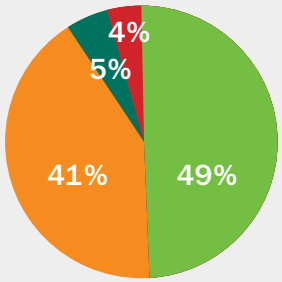

> **Todos sabemos que as empresas estão mais móveis, mas o perfil de utilização está a mudar: agora pode ver como a maioria das empresas utiliza dispositivos móveis para a partilha de informações sensíveis e até para a realização de transações financeiras.**
>
> David Emm, Kaspersky Lab, Equipa de Investigação e Análise Global

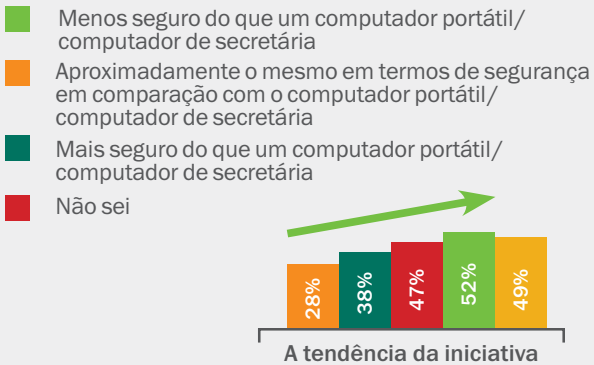
## UTILIZAÇÃO E COMPORTAMENTOS RELATIVAMENTE ÀS TRANSAÇÕES MÓVEIS

A sua empresa realiza transações delicadas em dispositivos móveis?




Qual o nível de segurança das transações realizadas em dispositivos móveis?




**A tendência da iniciativa BYOD apresenta um maior risco para a segurança de TI da nossa empresa.**

Contudo, o que poderá ser uma surpresa, é que quase metade **(49%)** considera os dispositivos móveis menos seguros do que os computadores portáteis ou de secretária. **41%** considera que o seu dispositivo móvel é tão seguro como o seu computador portátil ou de secretária, **5%** afirma que o seu dispositivo móvel é mais seguro e **4%** não sabe.

É interessante verificar que todas as empresas consideram a iniciativa BYOD uma ameaça para a sua segurança. Contudo, esta ameaça muda consoante a dimensão da empresa. Basicamente, à medida que a dimensão da empresa aumenta, aumenta igualmente a preocupação relativamente aos riscos de segurança da iniciativa BYOD. **28%** das empresas muito pequenas considera que a iniciativa BYOD representa uma ameaça crescente e, nas médias e grandes empresas, este valor aumenta para **47%** e **49%** respetivamente.

Estas empresas têm razão em pensar assim. Nos últimos quatro anos, **30%** das empresas assistiu ao roubo ou perda de um dispositivo móvel. Apesar da resultante perda de dados ter diminuído nos últimos dois anos, de **26%** em 2012 para **21%** em 2014, esta continua a ser a segunda maior razão para a perda de dados de uma empresa, sendo a primeira a partilha acidental de dados pela equipa.

**Nos últimos quatro anos, 30% das empresas assistiu ao roubo ou perda de um dispositivo móvel.**

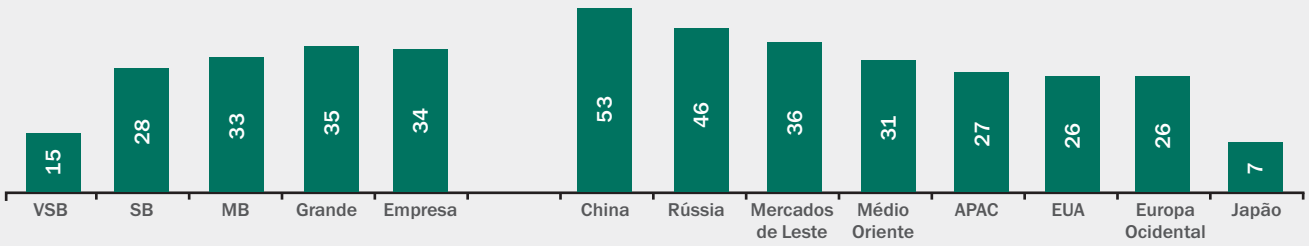
Relatório global de riscos de TI de 2014:

# 4 Virtualização – proteção de novos ambientes de trabalho

Desde há algum tempo que a virtualização tem feito parte da estratégia de TI de algumas empresas, contudo a implementação real de medidas específicas de segurança de virtualização ainda é reduzida. Trata-se de um problema que preocupa muitas pessoas e que foi mencionado como sendo a principal prioridade de segurança de TI nos próximos 12 meses em **14%** das empresas inquiridas (o valor aumenta para **21%** nas médias empresas).

## IMPLEMENTAÇÃO E GESTÃO DA TECNOLOGIA DE VIRTUALIZAÇÃO

A % de cada um indica um desafio de gestão da mudança com o qual está atualmente a lidar.




> **A virtualização é uma parte cada vez mais importante da estratégia de TI da maioria das empresas. Contudo, no que diz respeito à adoção de soluções de segurança especializadas, muito poucas empresas compreendem claramente as soluções disponíveis ou os requisitos de segurança que são originados por um ambiente virtual.**
>
> Sergey Lozhkin, Equipa de Investigação e Análise Global, Kaspersky Lab

A virtualização suscita maior preocupação nas grandes empresas do que nas empresas mais pequenas. Mais de um terço das médias e grandes empresas indicou como o principal desafio esta preocupação, em comparação com **28%** das pequenas empresas e **15%** das empresas muito pequenas.

A compreensão das opções de segurança de virtualizações é diversificada, mesmo entre os profissionais de TI. Apenas um terço das organizações inquiridas compreende claramente as soluções disponíveis e cerca de um quarto compreende-as mal ou nem sequer as compreende.

## GLOSSÁRIO:

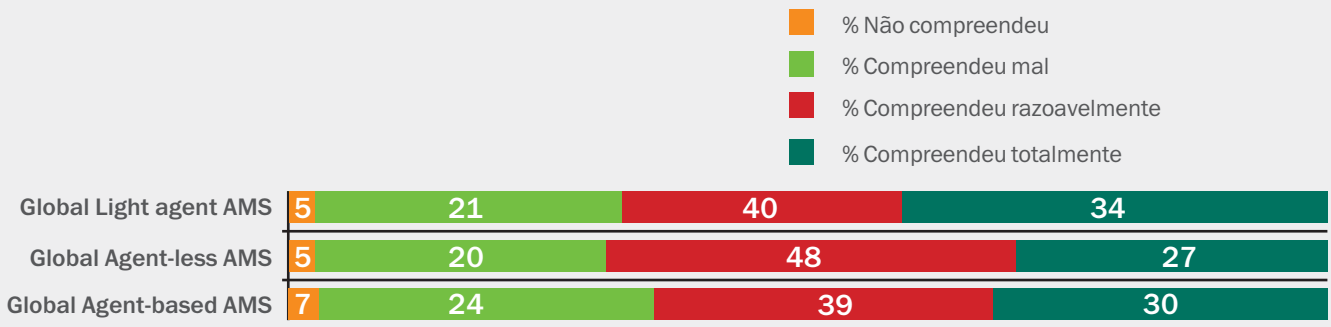
Os três tipos de software antimalware disponíveis para as redes virtuais oferecem diferentes opções de segurança que são melhor implementadas de formas diferentes.

Agent-less: baseado na tecnologia push e design centralizado. Controlado por uma consola central que não requer agentes para a sua instalação em máquinas individuais ou virtuais. Pode reduzir custos, reduzir a gestão e é de fácil implementação nas grandes empresas.

Agent-based: baseado na tecnologia pull, que requer um software do lado do cliente antes de fornecer atualizações num servidor. As soluções agent-based são indicadas para os utilizadores em roaming ou para as máquinas desligadas e podem ser um complemento útil para as soluções agent-less.

Light Agent: reencaminha cargas de trabalho pesadas para um equipamento virtual, ao mesmo tempo que protege os terminais contra as ameaças. O Light Agent é uma combinação de agent-less e agent-based.

## COMPREENSÃO DA SOLUÇÃO DE SEGURANÇA DO AMBIENTE VIRTUAL ENTRE ESPECIALISTAS EM SEGURANÇA




**24%** das empresas considera que o seu software antimalware existente proporciona uma melhor proteção e, ainda mais importante, um melhor desempenho do que as soluções especializadas. **20%** afirmou que não teve quaisquer problemas com as suas soluções tradicionais e **13%** sentiu que a ameaça aos seus ambientes virtuais não foi suficiente para justificar o custo adicional de implementação de uma solução especializada.

Independentemente da compreensão muito diversificada das opções de segurança disponíveis, **52%** das empresas inquiridas concordou com a declaração **"Os ambientes virtuais formam cada vez mais uma parte essencial da nossa infraestrutura de TI crítica".** Logo, à medida que se tornam uma parte essencial das práticas de trabalho de uma empresa, estes devem ser eficientes e seguros. Porém é evidente que um processo de educação é necessário para que estes ambientes sejam implementados eficazmente.

O quadro global demonstra que as empresas parecem não estar preparadas para mudar os seus requisitos de segurança quando implementam ambientes virtuais. Estes requisitos incluem a melhoria da sua compreensão da segurança de virtualização e a adoção de plataformas de segurança especializadas. Estes dois requisitos são cruciais para a segurança nesta área.

# 5 Relatório global de riscos de TI de 2014: Antifraude – avaliação de custos

A prevenção contra a fraude está quase no topo nos objetivos de muitas empresas. **63%** dos inquiridos concordou com a declaração **"Fazemos todos os esforços por assegurar a atualização das nossas medidas antifraude"**. Este valor foi pelo menos **10%** superior em relação aos preocupados com a integração móvel, a virtualização, os ataques DDoS e outras questões principais relacionadas com a estratégia de TI.

Contudo, **43%** das organizações continua a sentir que precisa de melhorar o modo como protege as suas transações financeiras com o seu banco.

Estes receios têm um bom fundamento. Em 2013, o número de ciberataques que envolvem malware financeiro aumentou para 28,4 milhões: 27,6% mais do que em 2012.[1] No mesmo período, a Kaspersky Lab protegeu 3,8 milhões de utilizadores contra ataques financeiros e bloqueou mais de 330 milhões de ataques de phishing.[2]

**Em 2013, o número de ciberataques que envolvem malware financeiro aumentou para 28,4 milhões: 27,6% mais do que em 2012.[1]**

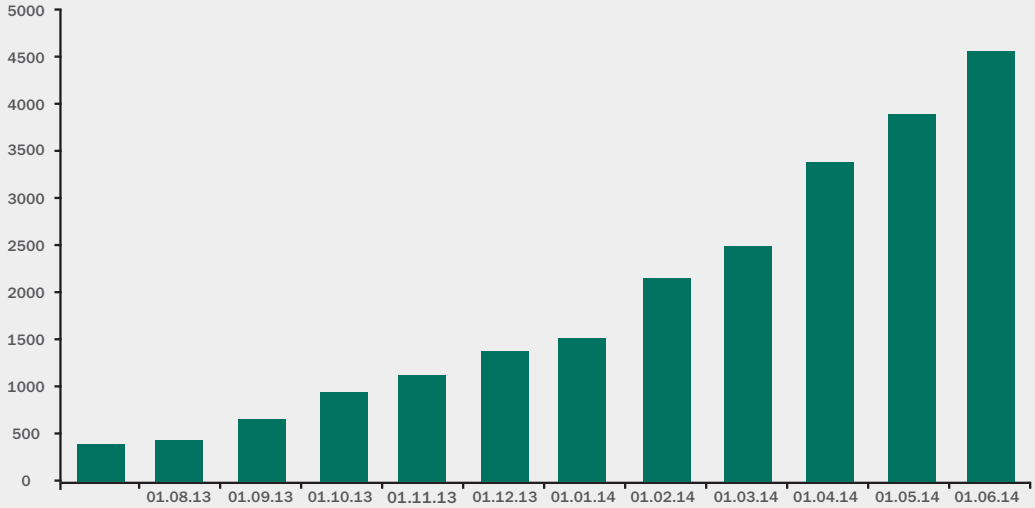
## TROJANS BANCÁRIOS MÓVEIS

O malware móvel foi concebido para gerar dinheiro para os cibercriminosos. Funcionam com Trojans baseados em Windows e contornam as técnicas tradicionais de autenticação, atacando e roubando números de transações móveis (mTAN) emitidos pelos bancos, possibilitando desta forma transferências ilegais de fundos.

Observou-se um crescimento repentino e substancial de Trojans bancários para Android autónomos nos últimos 18 meses – de apenas 67 Trojans bancários no início de 2013 para 1321 no final do ano, e mais 3215 registados nos meados de 2014.[3] Embora estes ataques tenham sido até agora principalmente direcionados aos utilizadores da Rússia e da Comunidade de Estados Independentes, é provável que os cibercriminosos continuem a desenvolver as suas técnicas, a expandir o seu alcance e a deslocar-se para novos 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 TROJANS BANCÁRIOS DETETADOS NO SEGUNDO TRIMESTRE DE 2014




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

Exemplos conhecidos incluem o ZeuS-in-the-Mobile (ZitMo), o SpyEye-in-the-Mobile (SpitMo), o Carberp-in-the-Mobile (CitMo) e o Svpeng. Svpeng é um Trojan para Android que rouba os dados de início de sessão e de palavra-passe através da aplicação bancária móvel de um utilizador. Também consegue roubar informações do cartão bancário do utilizador solicitando ao utilizador a introdução dos seus dados bancários quando o Google Play é aberto. Nos três meses de existência do Trojan, a Kaspersky Lab descobriu 50 das suas modificações e bloqueou mais de 900 instalações[4].

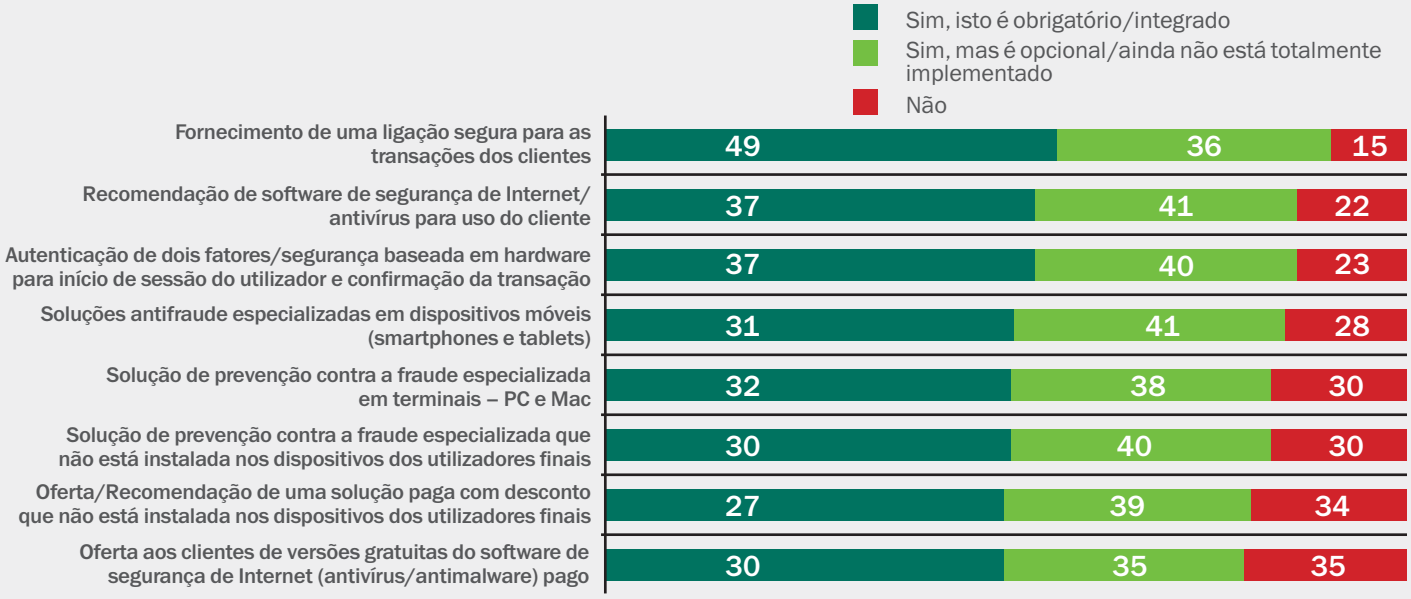
Os mercados financeiros têm como base a confiança de que as obrigações serão cumpridas, de que os pagamentos serão feitos e de que os dados serão protegidos. É por esta razão que não constitui surpresa o facto de a proteção da reputação e o registo de dados serem as principais preocupações das empresas envolvidas na segurança de dados financeiros.

**73%** das empresas afirmou que a reputação de segurança de um banco influenciou a sua decisão de adesão ao dito banco e **82%** afirmou que consideraria abandonar um banco caso este tivesse sofrido uma violação de dados. Isto não deve ser surpreendente – ter em conta a reputação de uma organização é uma boa gestão de riscos. Também não deveria constituir uma surpresa o facto da proteção dos dados do cliente ser um dos principais objetivos das empresas inquiridas. O que é ainda mais interessante, é que **18%** das empresas toleraria uma falha de segurança relacionada com a sua segurança financeira e, ainda mais alarmante, é que apenas pouco mais de metade **(51%)** de todas as empresas inquiridas considera que as organizações financeiras fazem um trabalho satisfatório relativamente à proteção das suas informações financeiras. O que fazem os fornecedores de serviços financeiros ou os operadores de comércio eletrónico para proteger os seus clientes e impedir a fraude?

O inquérito foi dirigido a mais de 2500 empresas que trabalham neste campo e os resultados demonstram na maioria uma indústria em transição. Enquanto perto de metade dos inquiridos ofereceu uma ligação segura, cerca de um terço dos inquiridos estava ainda a implementar um serviço seguro ou não o executava e **15%** dos inquiridos não oferecia nenhum serviço seguro. Relativamente aos métodos restantes de proteção das transações, a maioria das organizações estava ainda no processo de desenvolvimento de fornecimento de capacidades, oferecendo medidas antifraude opcionais, ou não as tinha implementado de todo.

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

## MEDIDAS ANTIFRAUDE IMPLEMENTADAS PELOS FORNECEDORES DE SERVIÇOS FINANCEIROS E OPERADORES DE COMÉRCIO ELETRÓNICO




BASE: 2680. Todos os inquiridos em serviços financeiros ou que operam na plataforma online, pública

Os bancos e os clientes têm diferentes opiniões sobre quem é responsável pela segurança financeira. Apenas **35%** dos clientes considerou as instituições financeiras as principais responsáveis pela segurança financeira, em comparação com **85%** das próprias instituições. As pequenas empresas e as muito pequenas foram as que tiveram mais inclinação para considerar a instituição financeira responsável – **48%** e **41%** respetivamente – em comparação com apenas **27%** das organizações empresariais.

Devido à falta de equipas de segurança dedicadas nas pequenas empresas, a equipa de TI tem de ser totalmente responsável pelas suas falhas e pela proteção do processo. **28%** dos clientes considera o seu departamento de TI o principal responsável. Este facto realça ainda mais a necessidade de uma proteção multicamada integrada capaz de abranger todas as necessidades das PME.

> **Há uma verdadeira falta de clareza sobre quem é responsável pela proteção das transações. A resposta a esta questão é que a empresa e as instituições financeiras precisam de se esforçar muito mais. Trata-se da gestão de riscos e a situação atual sugere que as pessoas estão demasiado expostas.**
>
> David Emm, Equipa de Investigação e Análise Global, Kaspersky Lab

# 6 Relatório global de riscos de TI de 2014: O verdadeiro custo das violações de dados

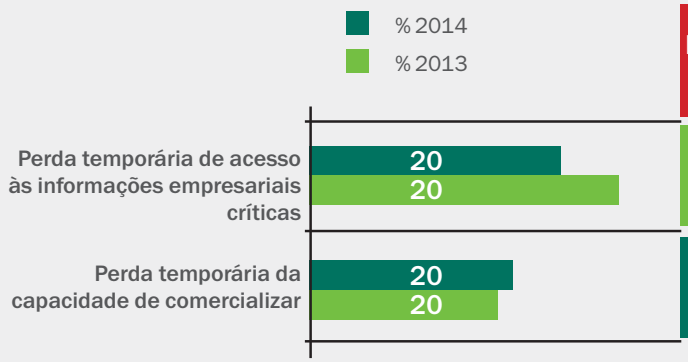
O que pode custar à sua empresa uma violação de dados? Esta pergunta é difícil de responder se ainda não viveu este problema. Caso já o tenha vivido, saberá muito bem o preço que terá de ser pago pela sua empresa. As consequências de uma violação de dados são sempre superiores à perda inicial de informações sensíveis e confidenciais e os danos provocados são ainda mais profundos.

As falhas de segurança resultam muitas vezes num número de despesas adicionais, incluindo medidas corretivas e preventivas. Sim, existe o receio imediato de que as informações confidenciais da empresa estejam agora nas mãos de cibercriminosos, mas as repercussões a longo prazo podem incluir custos de perda de dados, danos à reputação, eficiência organizacional reduzida, custos de terceiros, despesas reativas e oportunidades perdidas.

Estas podem ser catastróficas para qualquer empresa. De entre as empresas inquiridas que sofreram uma violação de dados, **55%** afirmou ser muito difícil funcionar como anteriormente. E isto não acontece apenas a curto prazo. **54%** das empresas revelou que a perda de dados teve um impacto negativo na sua reputação, reduzindo a sua fiabilidade aos olhos dos clientes, das partes interessadas e do mundo empresarial global.

Os valores abaixo apresentam mais dados sobre a longevidade da perturbação que pode ser provocada por uma violação de dados, bem como o elevado número de empresas que ficou incapacitada de trocar e fazer dinheiro.

## IMPACTO ENTRE OS QUE REPORTAM CADA EVENTO




| | Prazo muito curto | Curto prazo | Significa-tivo | Alargado |
|---|---|---|---|---|
| Perda temporária de acesso às informações empresariais críticas | 20 | 39 | 31 | 10 |
| Perda temporária da capacidade de comercializar | 17 | 42 | 30 | 10 |

A grande maioria das empresas – **87%** na realidade – não foi capaz de resolver sozinha o problema, pelo que tiveram que procurar a ajuda de serviços profissionais. Estes serviços incluem consultores de segurança de TI e advogados, até auditores e consultorias de gestão de riscos. Quase metade destas empresas (**47%**) afirmou que estes serviços resultaram em custos adicionais significativos.

Contudo, a despesa reativa não se limita apenas à utilização de serviços de terceiros. Se as PME sofrerem uma violação de dados, tal poderá resultar numa despesa adicional de 7000 USD em pessoal, 6000 USD em formação e 9000 USD em sistemas. As empresas de maior dimensão, que têm sem sombra de dúvida mais a perder, podem estar sujeitas a uma despesa adicional de 59 000 USD em pessoal, 35 000 USD em formação e 75 000 USD em sistemas.

> **Após uma falha de segurança, a perda de dados é apenas a ponta do iceberg financeiro: o verdadeiro custo é muito superior. Há custos elevados óbvios como medidas de segurança adicionais e aconselhamento legal, porém os danos à reputação e à marca são sem sombra de dúvida maiores.**
>
> Costin Raiu, Equipa de Investigação e Análise Global, Kaspersky Lab

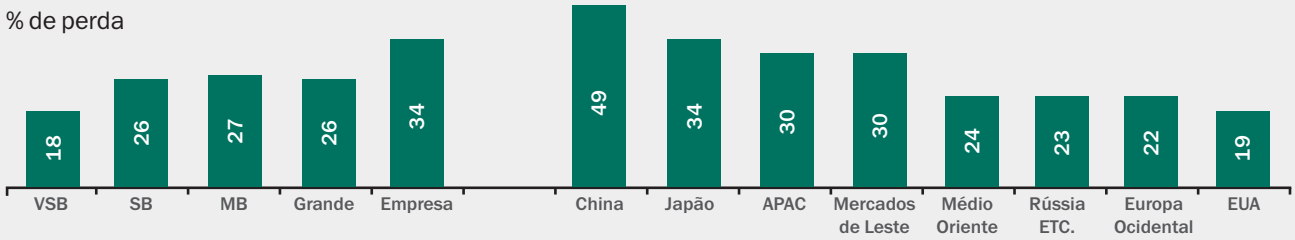
A perda da capacidade de funcionar é outra principal causa que suscita preocupação após uma violação de dados ou ataque de segurança. Das empresas que sofreram perdas de dados, perto de um terço perderam a capacidade de comercializar. Contudo, há boas notícias: entre 2013 e 2014, as pequenas e grandes empresas tornaram-se melhores na sua proteção neste caso, observando-se uma redução do custo médio de períodos de inatividade nas pequenas, médias e grandes empresas conforme ilustrado abaixo.

| Dimensão da empresa | Custo de períodos de inatividade | |
|---|---|---|
| | 2013 | 2014 |
| PME | 64 000 USD | 57 000 USD |
| Empresas | 1,7 milhões USD | 1,6 milhões USD |

O que as empresas podem aprender com estas conclusões? Basicamente que a despesa reativa é sempre mais dispendiosa do que a despesa proativa. Logo, as empresas não precisam de colocar a questão "Podemos custear não nos proteger?"

Temos uma resposta inteligente para esta questão. Em média, pouco mais de um quarto das empresas (**26%**) está disposto a aceitar uma perda de dados ou falha de segurança. Porquê? Porque consideram ser menos dispendioso do que atualizar os seus sistemas de TI para impedir estes mesmos acontecimentos como podemos verificar abaixo.

**"Estamos dispostos a suportar algumas perdas financeiras provocadas pelo cibercrime, uma vez que tal implica menos custos do que os envolvidos na atualização dos nossos sistemas de TI para nos protegermos contra esses mesmos crimes".**




Embora pudéssemos estar interessados em ver os cálculos que foram feitos para se chegar a esta conclusão, não concordamos. Os potenciais danos resultantes das violações de dados vão muito além dos custos imediatos. A continuidade da empresa, o valor da marca, a reputação e os potenciais custos de serviços de terceiros ultrapassam de longe o custo financeiro de uma proteção multicamada eficaz contra as ameaças.

# 7 Relatório global de riscos de TI de 2014: O desafio de gestão – a necessidade de simplificar as coisas num mundo complexo

O inquérito deste ano trouxe ao de cima a complexidade que as organizações de todas as dimensões enfrentam.

As empresas enfrentam a complexidade em duas frentes:

## 1. Complexidade crescente das ameaças

O malware tornou-se rapidamente bastante mais sofisticado. Para continuarem protegidas, todas as organizações necessitam de uma proteção mais profunda do que o que uma simples solução "antivírus" pode oferecer. Isto deu origem à perceção de um conjunto de ferramentas mais oneroso e complexo de gerir. Esta perceção justifica-se em alguns casos. O mercado da segurança apresenta milhares de ofertas de produtos de nicho que as equipas de TI com recursos humanos limitados procuram dominar, integrar e gerir.

## 2. Maior complexidade da infraestrutura de TI

Até mesmo as organizações de pequena dimensão estão alicerçadas num conjunto de ferramentas tecnológicas surpreendentemente complexo. Além de uma LAN básica, as organizações executam normalmente vários tipos de software globais; para além disso, algumas pessoas instalam aplicações de forma autónoma nos seus sistemas. Acrescente-se a este quadro o aumento da virtualização e temos uma imensidão de elementos que é preciso monitorizar e gerir. Contudo, é a mobilidade que constitui o maior desafio para os profissionais de TI.

Neste contexto, o que devem os profissionais de TI fazer quando a tarefa é tão desafiante? Esta é a nossa lista de recomendações:

### Faça a gestão de um sistema de segurança unificado

O desafio com que nos deparamos mais frequentemente é que, quando surge uma nova tarefa (por exemplo, corrigir aplicações), dá-se um impulso para adquirir uma solução específica. Apesar de, isoladamente, parecer ser uma boa resolução, com o passar do tempo vai sendo criado um conjunto complexo de sistemas desgarrados. Na prática, significa mais soluções para gerir e cria mais trabalho, dando azo a novas vulnerabilidades (uma vez que há demasiados elementos a ter em conta).

### Inclua as plataformas móveis no plano geral

Parta do princípio que a grande maioria da sua força de trabalho deverá ter alguma percentagem de mobilidade no decorrer das suas tarefas e estará no caminho certo. Mais uma vez, uma ferramenta de segurança para plataformas móveis acabará por ser outro elemento a gerir, o que, no final de contas, cria novas vulnerabilidades na segurança global de TI.

### Reajuste a sua abordagem: invista numa proteção de vários níveis

Com o crescente aumento do número e da sofisticação das ameaças, torna-se evidente que estamos a subestimar a escala e a gravidade dos desafios que enfrentamos em termos de segurança. As invasões da rede, os ataques de phishing e DDoS são ameaças significativas, e podem conduzir a fugas de dados extremamente dispendiosas. Mas qual é a verdadeira ameaça? Continua a ser o malware.

Perante este quadro, é fundamental que as empresas invistam numa proteção de vários níveis. Os antivírus por si só não chegam. As empresas precisam de ter uma abordagem mais proativa na gestão do comportamento do malware sofisticado que existe em websites aparentemente seguros, em ficheiros aparentemente inocentes, que aproveita as vulnerabilidades da aplicação e tira partido de dispositivos não protegidos ou até mesmo de WiFi não protegida. O volume de malware novo, a juntar à sua sofisticação, torna fundamental a existência de uma proteção proativa e não de uma apenas reativa.

## Não pense que nunca vai ser vítima de fraude

Não é surpresa que a reputação de uma empresa seja importante para os seus clientes. O que é surpreendente é que mais de um quarto das empresas inquiridas considera que os bancos não fazem o suficiente para proteger as suas informações financeiras. Talvez mais surpreendente ainda é que 4% das empresas que operam algum tipo de serviço online não toma qualquer medida específica na proteção dos seus clientes.

## Nunca desista da educação dos utilizadores

Enquanto profissional de TI, é sua responsabilidade garantir que tem implementados as ferramentas e os sistemas adequados, e que os seus funcionários têm formação. Os funcionários podem inadvertidamente permitir uma falha de segurança e a tecnologia pode, em grande medida, evitá-la. Mas aliar tecnologia com formação e com regras e políticas estritas vai melhorar consideravelmente os seus níveis de segurança em TI.

**Há muito a fazer, mas a tarefa não é tão impossível como algumas pessoas a consideram.**

# Conheça os nossos especialistas

A perspetiva profissional neste relatório é oferecida pela Equipa de Investigação e Análise Global da Kaspersky Lab.

**Costin Raiu**
Costin é o Diretor da Equipa de Investigação e Análise Global. Anterior Perito de Segurança Responsável, Costin trabalha na Kaspersky desde 2000 e é especialista em páginas de Internet maliciosas, segurança e vulnerabilidades de browsers, malware de e-banking, segurança a nível empresarial e ameaças de Web 2.0. Leia o seu blogue em http://securelist.com/author/costin/ ou siga @craiu no Twitter.

**David Emm**
David começou a trabalhar na indústria antivírus em 1990 e ingressou na Kaspersky Lab em 2004, onde concebeu e desenvolveu o workshop da empresa sobre a defesa contra malware. Atualmente, é Investigador Regional Sénior no Reino Unido, e faz regularmente comentários na comunicação social. Os seus principais ramos de pesquisa são o ecossistema de malware, o roubo de identidade, os aspetos humanos da segurança e as tecnologias KL. Pode encontrar o blogue do David em http://securelist.com/author/davidemm/ ou seguir @emm_david no Twitter

**Sergey Lozhkin**
Sergey, Investigador de Segurança Sénior na Equipa de Investigação e Análise Global, juntou-se à Kaspersky Lab em 2012. Na sua função atual, investiga a ciberespionagem, a análise estática e dinâmica de malware, redes Undernet como TOR, engenharia social, transferências de dados seguras, análise de exploração, redes anónimas e cibercrime no geral.

Antes de se juntar à Kaspersky Lab, Sergey trabalhou em várias empresas como especialista em testes de penetração e analista de vírus. Investigou igualmente cibercrimes para o Ministério do Interior russo depois de se ter graduado da Academia Omsk do Ministério da Administração Interna.
Leia este blogue em http://securelist.com/author/sergeyl/ ou siga @61ack1ynx no Twitter

# COMECE AGORA:
# AVALIAÇÃO DE 30 DIAS GRÁTIS

Descubra como a nossa segurança premium consegue proteger a sua empresa contra o malware e o cibercrime com uma avaliação sem compromissos.

Registe-se hoje para transferir versões completas de produtos e avalie como protegem com sucesso a sua infraestrutura de TI, terminais e dados empresariais confidenciais.

RECEBA JÁ A SUA AVALIAÇÃO GRÁTIS

## JUNTE-SE À CONVERSA

#securebiz

Veja-nos no YouTube

Veja-nos no Slideshare

Goste no Facebook

Visite o nosso blogue

Siga-nos no Twitter

Junte-se a nós no LinkedIn

**Saiba mais em www.kaspersky.pt/business**

### ACERCA DA KASPERSKY LAB

A Kaspersky Lab é o maior fornecedor privado do mundo de soluções de proteção de terminais. A empresa encontra-se classificada entre os quatro principais fornecedores de soluções de segurança para utilizadores de terminais a nível mundial*. Ao longo dos seus mais de 17 anos de história, a Kaspersky Lab foi sempre uma inovadora na segurança de TI e fornece soluções de segurança digital eficientes para grandes empresas, PME e consumidores. A Kaspersky Lab, cuja sociedade gestora de participações sociais está registada no Reino Unido, opera atualmente em quase 200 países e territórios por todo o mundo, oferecendo proteção a mais de 300 milhões de utilizadores. Saiba mais em www.kaspersky.pt.

* A empresa ocupava o quarto lugar na classificação IDC de Worldwide Endpoint Security Revenue by Vendor, de 2012. A classificação foi publicada no relatório IDC "Worldwide Endpoint Security 2013–2017 Forecast and 2012 Vendor Shares" (IDC #242618, agosto de 2013). O relatório classificava os fornecedores de software consoante as suas receitas em vendas de soluções de segurança de terminais em 2012.