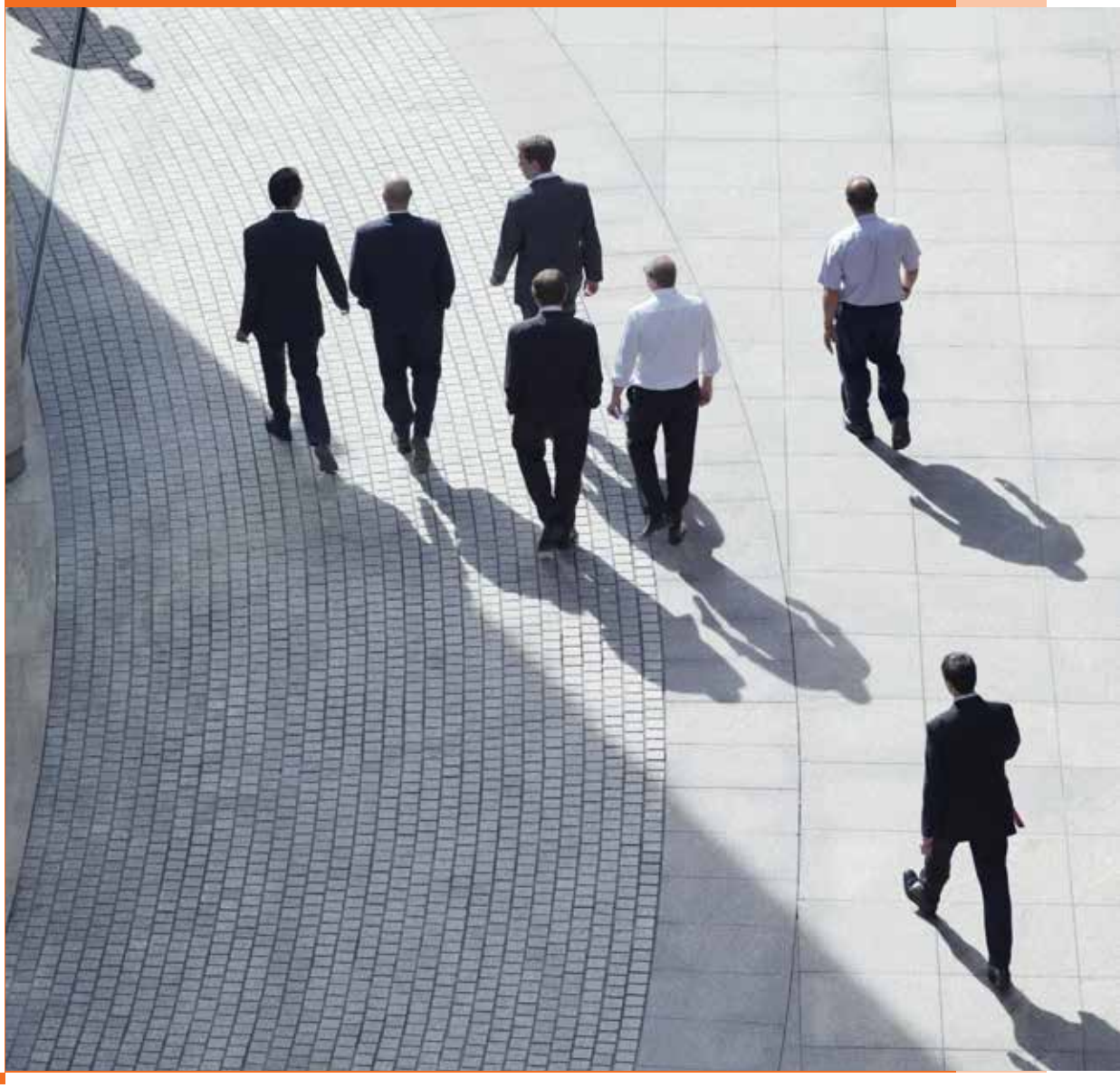
www.pwc.com.br

Uma defesa ultrapassada

Principais resultados da Pesquisa Global de Segurança da Informação 2014 – The Global State of Information Security® Survey 2014

Embora as organizações tenham feito avanços importantes em termos de segurança, elas não estão acompanhando a evolução dos seus adversários atuais. O resultado é que muitas estão confiando nas práticas de segurança de ontem para combater as ameaças de hoje.



pwc

Metodologia

A Pesquisa Global de Segurança da Informação 2014 (The Global State of Information Security® Survey 2014) é um estudo mundial realizado pela PwC em parceria com as revistas CIO e CSO. A pesquisa foi conduzida on-line de 1º de fevereiro a 1º de abril de 2013. Os leitores de ambas as publicações e os clientes da PwC de todo o mundo foram convidados a responder a um questionário via e-mail. Os resultados apresentados neste relatório se baseiam nas respostas de mais de 9.600 executivos, entre eles CEOs, CFOs, CISOs, CIOs, CSOs, vice-presidentes, diretores de TI e de segurança da informação de 115 países. Trinta e seis por cento (36%) dos respondentes são da América do Norte, 26% da Europa, 21% da região Ásia-Pacífico, 16% da América do Sul e 2% do Oriente Médio e da África. A margem de erro é inferior a 1%. Todos os dados e gráficos deste relatório, a menos que se indique o contrário, são relativos aos resultados da pesquisa.

Conteúdo

Apresentação

A Pesquisa Global de Segurança da Informação 2014 da PwC mostra que as empresas vêm fazendo avanços expressivos na área e que os seus executivos, além de estarem dando mais importância à questão, acreditam ter aperfeiçoado substancialmente salvaguardas, processos e estratégias tecnológicas. Os investimentos no setor refletem esse interesse: a média dos orçamentos em segurança da informação cresceu 51% em relação ao ano passado.

Em termos regionais, a América do Sul mostra uma importante evolução no que se refere a gastos, políticas e tecnologias de segurança e apresenta alguns pontos ainda por melhorar, como maior adesão a uma política para treinamento e conscientização de segurança. No Brasil, observamos que a preocupação com o tratamento adequado de novas tecnologias e com a mobilidade tem se acentuado. Na pesquisa deste ano, 12% mais respondentes declararam ter uma estratégia de mobilidade.

Visto assim, tem-se a impressão de que as ameaças estão sendo bem equacionadas e as medidas necessárias à defesa das organizações ganham corpo. Mas uma observação um pouco mais atenta do panorama da segurança da informação permite verificar que nem tudo é o que parece.

A análise das respostas colhidas com 9.600 executivos de 115 países sugere a utilização de antigos modelos para combater novas ameaças cada vez mais sofisticadas, o que resulta numa proteção pouco efetiva. E apesar de o investimento em segurança ter aumentado, nota-se que as empresas ainda se perdem na hora de definir as melhores práticas, têm dificuldade de conduzir analises situacionais e de identificar e priorizar os dados que precisam ser adequadamente resguardados. Poucas estão realmente preparadas para lidar com os riscos crescentes do ciberespaço.

Todas essas questões são aprofundadas neste relatório. Com base nos resultados da pesquisa, sugerimos também uma nova abordagem de prevenção e combate às ameaças futuras. Esperamos, com isso, ajudar as organizações a mapear os pontos que precisam ser trabalhados para que elas aprimorem suas ações de *cyber security* e de segurança da informação. Em um mundo totalmente interconectado por tecnologias digitais, essa é uma medida imperativa.

Fernando Alves
Sócio-presidente
PwC Brasil

Edgar R. Pacheco D'Andrea
Sócio Líder de *Cyber Security* e
Segurança da Informação
PwC Brasil

O cerne da questão

Os riscos de segurança da informação estão evoluindo e se intensificando, mas as estratégias de segurança – historicamente baseadas em conformidade e orientadas por perímetro – não acompanharam essa evolução.

Resultado? Hoje, as organizações costumam se fiar em estratégias de segurança do passado para travar uma batalha em geral ineficaz contra inimigos altamente qualificados que utilizam as ameaças e as tecnologias do futuro.

Esses sofisticados invasores superam as defesas de perímetro ultrapassadas e cometem ataques dinâmicos, extremamente concentrados e difíceis de detectar. Muitos usam avançados ataques de *phishing* cujo alvo é a alta administração. Para piorar a situação, a superfície de ataque – que inclui parceiros, fornecedores, clientes e outros grupos – se expandiu no ciberespaço com o volume sempre crescente de dados fluindo por canais digitais interconectados.

Esses fatores se combinaram para tornar a segurança da informação cada vez mais complexa e desafiante. Ela passou a ser uma disciplina que demanda tecnologias e processos pioneiros, um conjunto de habilidades baseadas em técnicas de contrainteligência e o apoio firme da alta administração. Um princípio fundamental dessa nova abordagem é a compreensão de que um ataque é inevitável e que adotar um alto nível de proteção para todos os dados não é mais viável.

O objetivo da Pesquisa Global de Segurança da Informação 2014 é medir e interpretar como as organizações globais adotam práticas para combater os inimigos altamente qualificados dos dias atuais. A pesquisa deste ano indica que os executivos estão dando mais importância à segurança. Eles estão atentos à necessidade de financiar atividades de segurança avançadas e acreditam ter aperfeiçoado substancialmente salvaguardas, processos e estratégias tecnológicas. Mas embora as organizações tenham melhorado o nível da sua segurança, seus inimigos avançaram ainda mais. A pesquisa deste ano mostra que os incidentes de segurança detectados aumentaram 25% em relação ao ano anterior, enquanto os custos financeiros médios dos incidentes cresceram 18%.

A pesquisa também revela que muitas organizações não empregaram tecnologias capazes de fornecer informações sobre vulnerabilidades e ameaças do ecossistema, identificar e proteger os principais ativos e avaliar ameaças no contexto dos objetivos de negócio. Para muitas empresas, a segurança ainda não é um componente essencial da estratégia de negócios, defendida pelo CEO e pelo conselho e adequadamente subsidiada.

Simplificando, poucas organizações estão se mantendo atualizadas em relação aos riscos crescentes – e menos ainda estão preparadas para administrar as ameaças futuras.

"Não é possível combater as ameaças de hoje com as estratégias de ontem", **diz Viviane Oliveira, diretora da PwC.** *"É necessário um novo modelo de segurança da informação, que leve em consideração o conhecimento das ameaças do ciberespaço, dos ativos de informação e dos motivos e alvos dos potenciais atacantes."*

Nesse novo modelo de segurança da informação, conhecimento é poder. Preserve-o.

Uma análise em profundidade

A universalização das tecnologias digitais transformou o ambiente de negócios.

Hoje, as organizações estão cada vez mais interconectadas, integradas e interdependentes. Elas empregam a tecnologia e a conectividade ubíqua para compartilhar um volume sem precedentes de ativos de informação com clientes, provedores de serviço, fornecedores, parceiros e empregados. Essas sofisticadas tecnologias permitem que as empresas realizem atividades de negócios com uma velocidade e um grau de eficiência sem precedentes.

Mas um ecossistema de negócios em evolução também põe em risco as organizações ao deixá-las à mercê de inimigos que poderiam explorar essas tecnologias e processos para interromper as operações, obter acesso a informações privilegiadas e até destruir a empresa. Como resultado, as ameaças de segurança tornaram-se um risco crítico de negócios para as empresas globais.

A abordagem reativa tradicional quanto à estratégia de segurança da informação – que geralmente relega a segurança a segundo plano para se concentrar nos desafios de TI – ainda é o senso comum. Mas não é mais efetiva, nem defensável.

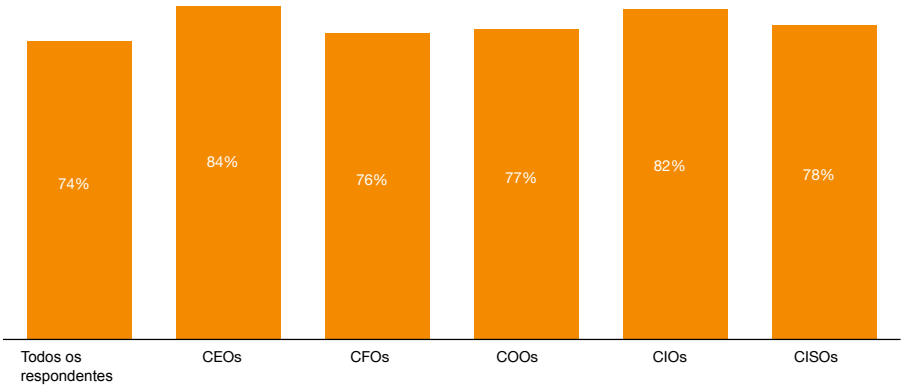
O novo mundo da era cibernética e dos riscos de segurança demanda que as organizações tratem o tema da segurança da informação como uma questão de gestão de riscos corporativos que pode ameaçar seriamente a reputação empresarial e os objetivos do negócio. Proteger todos os dados no nível máximo não é mais realista, nem mesmo possível.

Diante desse cenário, pedimos a executivos de negócios, de segurança e de TI que nos informassem como suas empresas tratam os imperativos de segurança da informação e alinham as salvaguardas de privacidade e segurança da informação com os objetivos do negócio. Os resultados da Pesquisa Global de Segurança da Informação 2014 mostram que a maioria dos executivos em todas as indústrias do mundo estão confiantes nas práticas de segurança da informação de suas organizações.

Forte confiança nas práticas de segurança atuais

É impressionante que, mesmo em um ambiente mais complexo de riscos, os executivos continuem extremamente confiantes nos recursos e nas atividades de segurança de suas organizações. Globalmente, 74% dos respondentes dizem que suas atividades de segurança são eficazes (Figura 1). E esse otimismo é ainda maior no nível hierárquico mais alto das empresas. Por exemplo, 84% dos CEOs dizem que estão confiantes em seu programa de segurança, como também 78% dos CISOs – que têm responsabilidade direta pela área. Entre os executivos, os CFOs são os menos confiantes. Uma visão regional mostra que os participantes da pesquisa na América do Sul (81%) e na Ásia (76%) apresentam os mais altos níveis de confiança em seus programas de segurança.

Figura 1: Confiança nas atividades de segurança (alguma ou muita confiança)



CEOs – diretores executivos;
CFOs – diretores financeiros;
COOs – diretores de operações;
CIOs – diretores de TI;
CISOs – diretores de segurança da informação

Mais de

80%

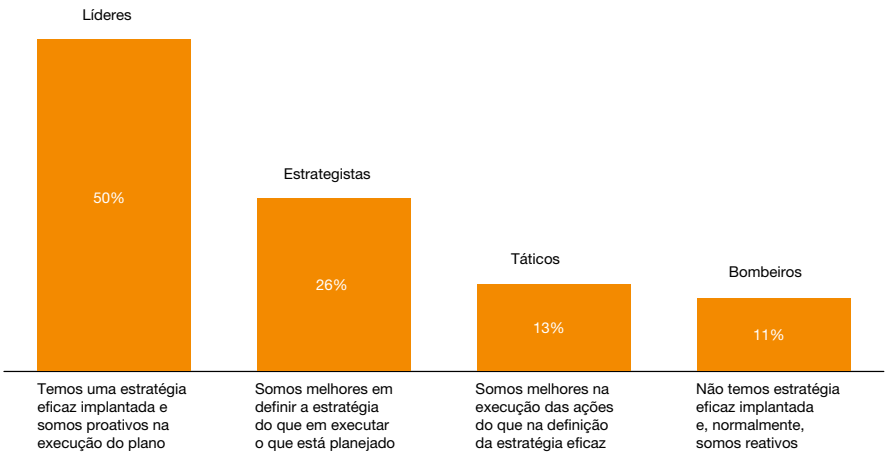
dizem que os gastos e as políticas de segurança estão alinhadas com o negócio.

Outra medida de confiança pode ser captada do modo como os executivos percebem o alinhamento do programa de segurança da empresa com a estratégia de negócios e o investimento geral. Por essa perspectiva, o otimismo também é alto. Mais de 80% dos respondentes dizem que os gastos e as políticas de segurança estão alinhados com os objetivos do negócio, o que representa um aumento em relação ao ano anterior para ambas as categorias. Esses níveis de confiança sugerem que os respondentes entendem que a segurança é parte integrante da agenda de negócios – e pode contribuir para os resultados.

O otimismo também se estende para a forma como os respondentes classificam sua estratégia geral de segurança e sua capacidade de executá-la proativamente. Perguntamos como eles classificam sua abordagem de segurança, e eles se atribuíram uma nota melhor do que nos últimos dois anos.

Chamamos de Líderes aqueles que afirmam ter uma estratégia eficaz em vigor e ser proativos na execução do plano, pois eles exibem dois atributos essenciais a esse perfil. Entre os respondentes deste ano, 50% dizem ter atributos de um líder, uma alta de 17% em relação ao ano anterior (Figura 2). Um em cada quatro (26%) diz que tem a estratégia correta, mas não pode executar com sucesso o que está planejado, uma categoria que chamamos de Estrategistas. Os que se consideram melhores na execução das ações do que na definição de uma estratégia eficaz – os Táticos – representam 13% dos respondentes. E o grupo dos que chamamos de Bombeiros, que não têm uma estratégia implantada e agem normalmente de modo reativo, constituem 11% do total.

Figura 2: Como os respondentes caracterizam sua abordagem à segurança da informação



Os líderes são realmente dignos do nome?

Fizemos uma análise mais cuidadosa das respostas e criamos uma série de requisitos que julgamos definir os "verdadeiros líderes" com base nas capacidades que eles informam e não apenas na autopercepção. Para se qualificar como líderes de fato, os respondentes devem:

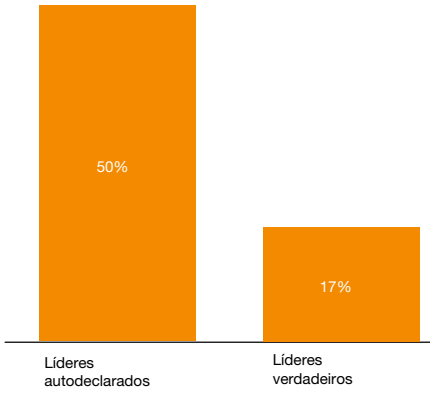
- ter uma estratégia geral de segurança da informação;
- empregar um diretor de segurança da informação (*chief information security officer* ou CISO) ou equivalente, diretamente subordinado à alta liderança – CEO, CFO, COO, CRO ou diretor jurídico;
- ter medido e avaliado a eficácia das medidas de segurança no último ano;
- entender exatamente que tipo de eventos de segurança ocorreram no último ano.

Quando filtramos os respondentes por essas qualidades, vemos que os Líderes não são necessariamente enquadrados como tal. Com base nesses critérios, apenas 17% da amostra total se classificam como líderes verdadeiros (Figura 3). Também descobrimos que os verdadeiros líderes detectam mais incidentes de segurança, têm uma compreensão melhor dos tipos e da origem de incidentes ocorridos, e informam uma média menor de prejuízos financeiros decorrentes de incidentes de segurança.

Verdadeiros líderes detectam mais incidentes de segurança, têm uma compreensão melhor dos tipos e da origem dos incidentes ocorridos, e informam uma média menor de prejuízos financeiros decorrentes de incidentes de segurança.

Regionalmente, os líderes verdadeiros estão mais provavelmente na Ásia-Pacífico (28%) e na América do Norte (26%), seguidos de Europa (24%), América do Sul (21%), Oriente Médio e África (1%). As indústrias mais representadas são as de tecnologia (16%), serviços financeiros (11%) e produtos de varejo e bens de consumo (9%).

Figura 3: Líderes autodeclarados x verdadeiros



Outro motivo de otimismo: os orçamentos estão crescendo

Se a maioria dos respondentes se considera altamente competente em suas práticas de segurança da informação, aqueles que detêm o poder de decisão na empresa também parecem estar otimistas sobre a função de segurança – ou talvez entendam que o ambiente atual de ameaças elevadas demande um impulso nos investimentos de segurança. De ambas as formas, aumentos substanciais nos investimentos de segurança são um bom indicador dos esforços nessa área. Embora os orçamentos variem muito entre indústrias e portes de empresas, os participantes dizem que os gastos giram, em média, em torno de US$ 4,3 milhões em 2013, um aumento de 51% em relação ao ano anterior. Apesar do aumento, porém, os orçamentos de segurança da informação representam apenas 3,8% do gasto total de TI no ano, um investimento relativamente pequeno.

A média dos orçamentos de segurança da informação cresceu

51%

em relação ao ano passado.

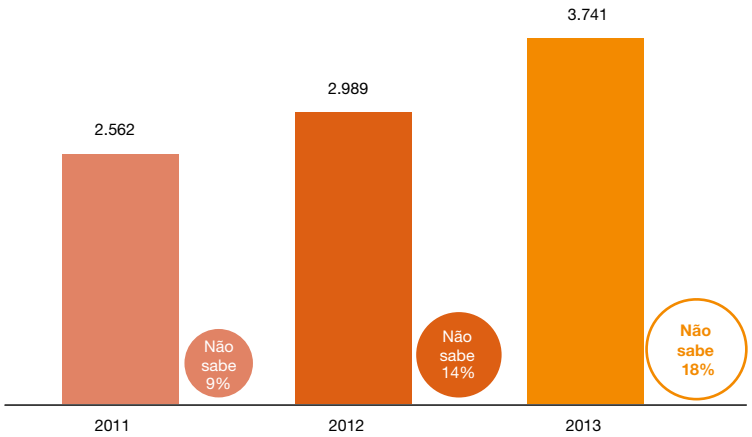
Mas e o futuro? Também há otimismo em relação a ele. Quase metade (49%) dos respondentes afirma que os gastos de segurança nos próximos 12 meses aumentarão, em comparação com 45% no ano passado. Regionalmente, os respondentes da América do Sul (66%) e da Ásia-Pacífico (60%) esperam que os investimentos em segurança cresçam. Mas apenas 38% dos respondentes da América do Norte preveem uma alta nas despesas relacionadas a essa área, o que os torna os menos propensos a gastar.

Incidentes de hoje, estratégias de ontem

Foi quase impossível ignorar a enxurrada de notícias sobre violações de segurança cada vez mais sofisticadas, e geralmente bem-sucedidas, ao longo do último ano. Mas, devido à natureza às vezes sensacionalista da cobertura desses eventos, é compreensível que se questione a precisão das reportagens sobre ataques cibernéticos. Os resultados da pesquisa deste ano confirmam algumas, mas não todas, as notícias divulgadas sobre incidentes de segurança.

Um fato é incontestável: esses incidentes* estão aumentando. Os participantes da pesquisa relatam um aumento de 25% nos episódios detectados ao longo do último ano (Figura 4). Isso parece confirmar as perigosas ameaças de segurança no ciberespaço alardeadas pelas manchetes. Por outro lado, uma quantidade maior de incidentes detectados também pode significar que as organizações estão melhorando na identificação dessas ocorrências.

Figura 4: Número médio de incidentes de segurança nos últimos 12 meses



* Definimos um incidente de segurança como qualquer ocorrência negativa que ameace algum aspecto da segurança dos ativos de informação.

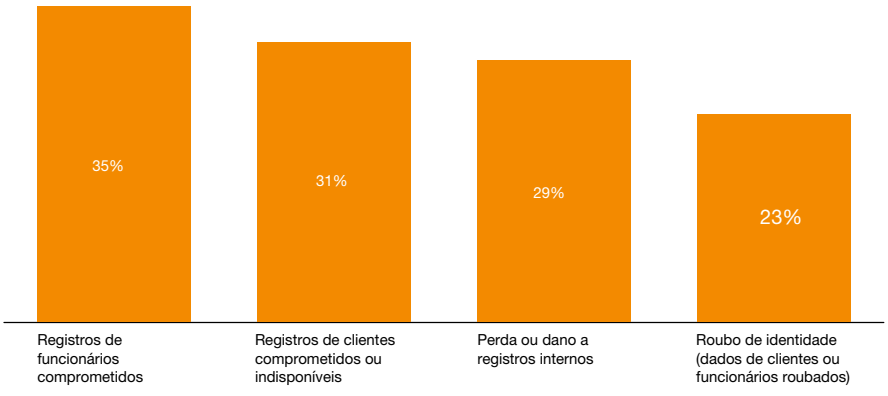
"Os incidentes estão crescendo não só porque existem mais ameaças, mas também porque algumas empresas investiram em novas tecnologias para detectá-los melhor", **diz Edgar D'Andrea, sócio da PwC.** *"Nesse sentido, a maior detecção de incidentes de segurança deve ser vista como um acontecimento positivo."*

Mas o número de participantes que desconhecem a frequência dos incidentes continua a crescer ano a ano – agora está em 18% – e isso parece contradizer a ideia de que as organizações estão se tornando mais competentes na detecção de invasões. Essa descoberta, na verdade, sugere mais provavelmente que os antigos modelos de segurança em uso podem ter sido violados ou ser ineficazes.

O número maior de incidentes, combinado a um aumento paralelo no volume de dados de negócios compartilhados digitalmente, leva a uma conclusão pouco surpreendente: a proliferação da perda de dados. Este ano, 24% dos respondentes relataram ter perdido dados em consequência de incidentes de segurança, uma elevação de 16% em relação a 2012.

Investigar os tipos de dados explorados revela alguns fatos interessantes. Os registros de funcionários (35%) e de clientes (31%) comprometidos lideram a lista de categorias de dados afetados (Figura 5). Ano após ano, os participantes da pesquisa nos informam que esses dados são as informações mais valiosas que eles detêm – portanto, é de se presumir que os esforços de segurança estejam concentrados em protegê-los. Mas a realidade sugere que os esforços atuais de proteção de dados não são efetivos ou não estão direcionados para os riscos corretos.

Figura 5: Impacto dos incidentes de segurança



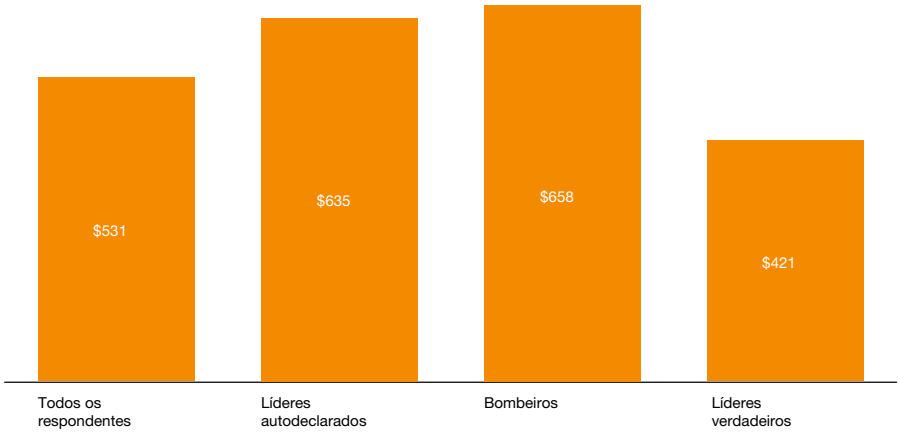
Observação: Nem todos os fatores são mostrados. A soma não equivale a 100%.
Os respondentes puderam indicar vários fatores.

A combinação de custo do prejuízo

Parece lógico que, com o aumento do número de incidentes de segurança, aumentam também os custos financeiros. E, de fato, é assim que tem ocorrido: descobrimos que a perda financeira média associada a incidentes de segurança cresceu 18% em relação ao ano passado.

"De modo geral, os custos e a complexidade para responder aos incidentes estão aumentando", **diz Fernando Carbone, diretor da PwC.** *"Isso inclui o custo de investigar; de entender os riscos de negócios e conter os incidentes; de gerenciar a notificação aos órgãos reguladores, clientes e consumidores; e de litígio. Além disso, o custo de remediação está crescendo porque mais registros em mais jurisdições estão sendo afetados, e os controles de segurança não estão acompanhando o ambiente de ameaças em constante mudança."*

Figura 6: Custo médio por incidente de segurança



Analisando os dados um pouco mais, descobrimos que as perdas financeiras estão se acelerando de forma acentuada entre os participantes da pesquisa, que relatam um impacto de valor elevado em dólar. Um bom exemplo: o número de respondentes que relataram perdas acima de US$ 10 milhões cresceu 51% desde 2011. Esperávamos que algumas indústrias que historicamente têm sido proativas em investir em iniciativas de segurança informariam perdas menores, mas, para nossa surpresa, não foi o que aconteceu. Entre as indústrias que informaram perdas de US$ 10 milhões ou mais estão a farmacêutica (20%), a de serviços financeiros (9%) e a de tecnologia (9%).

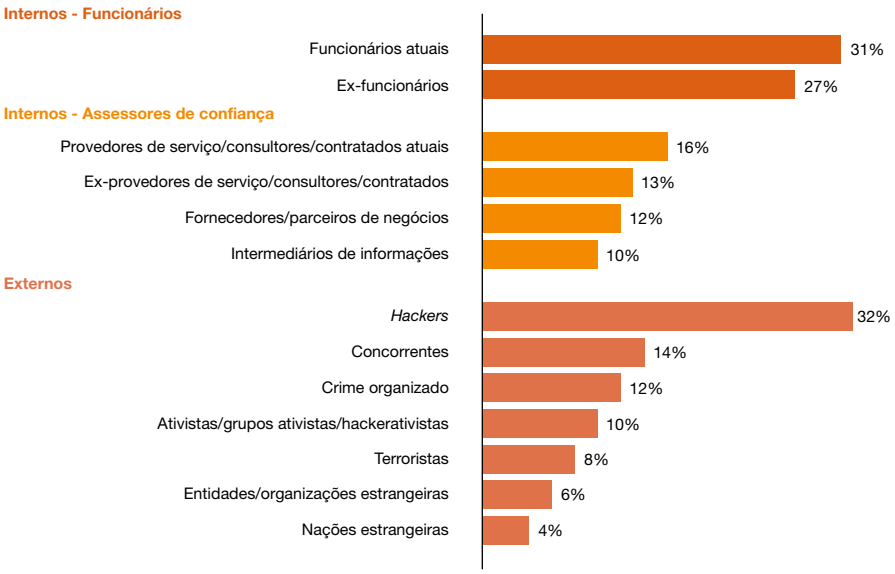
Em geral, o custo médio das invasões por incidente é de US$ 531 (Figura 6). Os respondentes que identificamos como líderes verdadeiros informam o menor custo por incidente, uma média de US$ 421, o que não é surpresa. O que não esperávamos é que os que se autodeclararam líderes tivessem gasto US$ 635 por incidente – quase tanto quanto os bombeiros, que se autoavaliaram como menos preparados para executar um programa de segurança efetivo. Isso coloca em questão a real eficácia dos líderes autodeclarados.

Inimigos internos, externos e *hackers*

Como já observamos, as manchetes nem sempre refletem a realidade das equipes que combatem as ameaças. Incidentes bastante divulgados, como invasões sofisticadas atribuídas a ameaças persistentes avançadas (APTs, na sigla em inglês), têm uma grande repercussão, mas são muito raros.

De fato, a realidade é muito mais banal. A maioria dos participantes atribui incidentes de segurança a inimigos internos conhecidos, como funcionários ativos (31%) ou ex-funcionários (27%) (Figura 7). Muitos veem as ameaças internas como algo bem mais significativo do que as ameaças que saem na mídia, e são pouco frequentes.

Figura 7: Origem provável estimada dos incidentes



Observação: Nem todos os fatores são mostrados. A soma não equivale a 100%. Os respondentes puderam indicar vários fatores.

"Eu percebo o aumento da importância da ameaça interna com mais intensidade do que no passado", **diz Michael A. Mason, diretor de Segurança da Verizon Communications. Segundo ele, a Verizon define inimigos internos como qualquer pessoa que tenha acesso aos dados da empresa.** *"E é importante observar que as ameaças internas não necessariamente são causadas por uma 'pessoa mal-intencionada'; pode ser um bom funcionário fazendo o seu trabalho honesto de um modo inseguro. Nossos problemas são mais humanos do que tecnológicos."*

Dada a prevalência de riscos provocados pelos funcionários, é surpreendente que muitas organizações não estejam preparadas para lidar com ameaças internas comuns. Outra pesquisa copatrocinada pela PwC, a 2013 US State of Cybercrime Survey, revelou que um terço dos respondentes americanos não tem um plano de resposta para lidar com incidentes de segurança internos[1]. E entre aqueles que têm um plano de resposta, apenas 18% descrevem o esforço como extremamente efetivo.

"Uma razão para as organizações não terem adotado planos eficazes para ameaças internas é que muitos inimigos internos, como parceiros e fornecedores, são convidados a entrar nos perímetros da rede, e elas presumem um determinado nível de confiança", **diz João Castilho, gerente da PwC.** *"As empresas precisam entender que a confiança nos parceiros não deve ser implícita."*

Entre os fatores de risco externos, é importante observar que alguns inimigos muito conhecidos – *hackers*, em especial – realmente cumprem o seu potencial de risco. Basta considerar que 32% dos respondentes da pesquisa atribuem incidentes de segurança a *hackers*, um aumento de 27% em relação ao ano anterior.

E o que dizer de incidentes que alcançam grande publicidade, como ataques promovidos por nações estrangeiras que empregam APTs para obter informações? Os participantes da pesquisa dizem que invasões apoiadas por nações estrangeiras representam apenas 4% dos incidentes detectados.

Não se trata de uma grande preocupação para muitas empresas, entre elas a Verizon. "Preocupar-se com ameaças persistentes avançadas é, de certa maneira, como ter medo de pegar um resfriado em uma fábrica de antraz", diz Mason.

Embora as APTs possam representar um risco potencial remoto, estar consciente das ameaças cibernéticas de rápida evolução é uma prioridade para muitas grandes organizações, inclusive a Cablevision Systems Corporation, uma operadora multisserviços (MSO) cujas atividades incluem o fornecimento de TV a cabo, de Internet e a edição de um jornal diário de alta circulação.

"Como a maioria das MSOs, estamos atentos às reportagens publicadas sobre a detecção crescente de atividades patrocinadas por nações ou ciberterroristas, especificamente quando elas têm como alvo empresas de comunicação e serviços públicos", diz Jennifer Love, vice-presidente sênior de operações de segurança. "Usamos informações de várias fontes, inclusive da indústria e do governo, para identificar riscos e orientar as decisões."

Uma defesa fraca contra os adversários

Para combater os riscos atuais, as organizações devem ser capazes de obter discernimento e inteligência permanentes sobre vulnerabilidades do ecossistema e ameaças dinâmicas. Atividades e investimentos devem ser orientados pelo melhor conhecimento disponível sobre ativos de informação, ameaças ao ecossistema e vulnerabilidades – e avaliados no contexto da atividade de negócios.

Para muitos, isso representa uma mudança importante em termos de conceitos e planejamento. Dessa forma, não surpreende que muitos participantes da pesquisa afirmem não ter implementado tecnologias e processos que ofereçam uma visão dos riscos atuais. Por exemplo, 52% dos respondentes não implantaram ferramentas de monitoramento e definição de perfis de comportamento, e 46% não implantaram tecnologias de gestão de eventos e informações de segurança. Ferramentas de gestão de ativos são fundamentais para proteger dados dos ativos, embora não tenham sido implantadas por 39% dos participantes da nossa pesquisa. Mesmo tecnologias bem estabelecidas que podem ser essenciais para proteger informações confidenciais estão subutilizadas. Em especial, descobrimos que 42% dos respondentes não utilizam ferramentas de prevenção de perda de dados (DLP).

[1] 2013 US State of Cybercrime Survey, copatrocinada pela revista CSO, pelo CERT Coordination Center da Carnegie Mellon University, pelo FBI (Federal Bureau of Investigation), pela PwC e pelo Serviço Secreto dos EUA, março-abril 2013.

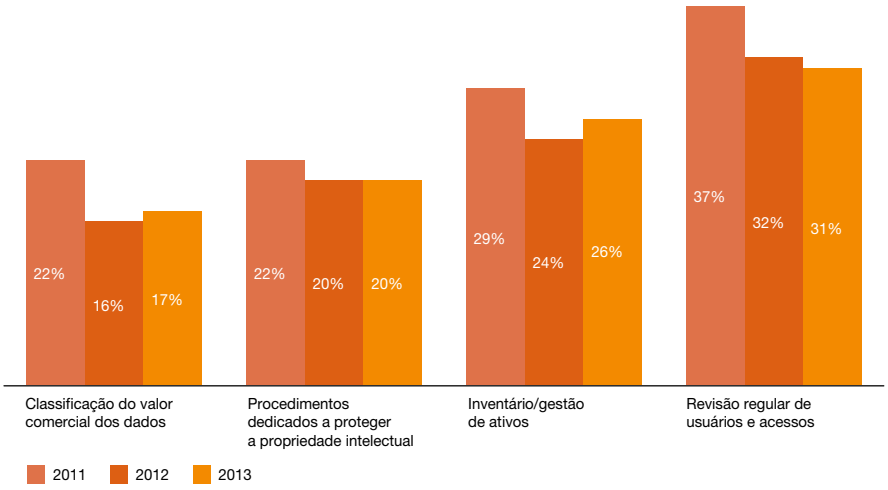
À medida que os dados se proliferam e são compartilhados com mais parceiros, fornecedores e clientes, torna-se mais crítico que as empresas entendam os riscos associados a compartilhar dados com terceiros. E mais: as organizações devem ter certeza de que terceiros cumprem ou superam seus requisitos de segurança de dados.

Por isso, é preocupante constatar que, nos EUA, muitos respondentes não têm políticas nem ferramentas para avaliar riscos de segurança de terceiros, segundo outra pesquisa copatrocinada pela PwC[2]. Por exemplo, apenas 20% dizem que avaliam mais de uma vez por ano a segurança de terceiros com os quais compartilham dados ou acesso à rede. Além disso, 22% afirmam que nunca avaliam seus terceiros, enquanto 35% informam que essa avaliação ocorre no máximo uma vez por ano.

Da mesma forma, apenas 22% dos respondentes dizem conduzir um planejamento de resposta a incidentes com parceiros de *supply chain*, e 52% nunca realizam esse planejamento.

Conforme observado, o ambiente atual de ameaças elevadas e crescentes requer que as organizações entendam que não é mais viável – ou, na verdade, possível – proteger todas as informações com a mesma prioridade. Em um novo modelo de segurança, as empresas precisam identificar e priorizar as informações que realmente importam.

Figura 8: Políticas adotadas para proteger a propriedade intelectual e os segredos comerciais



Observação: Nem todos os fatores são mostrados. A soma não equivale a 100%. Os respondentes puderam indicar vários fatores.

Obviamente, essas informações variam entre as organizações e as indústrias e podem incluir propriedade intelectual, como *design* de produtos, planos de *marketing*, comunicações executivas e estratégias de negócios. Para dar uma definição mais geral, trata-se de qualquer informação que possa causar sérias dificuldades para a empresa se perdida, roubada ou comprometida.

Ativos não tangíveis, como a propriedade intelectual, hoje representam 80% do valor associado às firmas listadas na S&P 500, segundo a Ocean Tomo, firma do Intellectual Capital Merchant Banc™ [3]. E com o aumento do valor da propriedade intelectual, cresce também seu apelo para os criminosos cibernéticos.

Apesar disso e dos potenciais prejuízos que a perda desse ativo de informação pode causar, a pesquisa deste ano revela que muitos participantes não identificam nem protegem adequadamente suas informações de alto valor. Por exemplo, apenas 17% dos respondentes classificam o valor comercial dos dados e somente 20% implementaram procedimentos dedicados a proteger a propriedade intelectual (Figura 8). Um percentual ligeiramente maior (26%) mantém inventário e gestão de ativos. Os resultados da pesquisa mostram que, em algumas indústrias, a inclusão de políticas para proteger a propriedade intelectual está, na verdade, diminuindo.

[2] 2013 US State of Cybercrime Survey, copatrocinada pela revista CSO, pelo CERT Coordination Center da Carnegie Mellon University, pelo FBI (Federal Bureau of Investigation), pela PwC e pelo Serviço Secreto dos EUA, março-abril 2013.

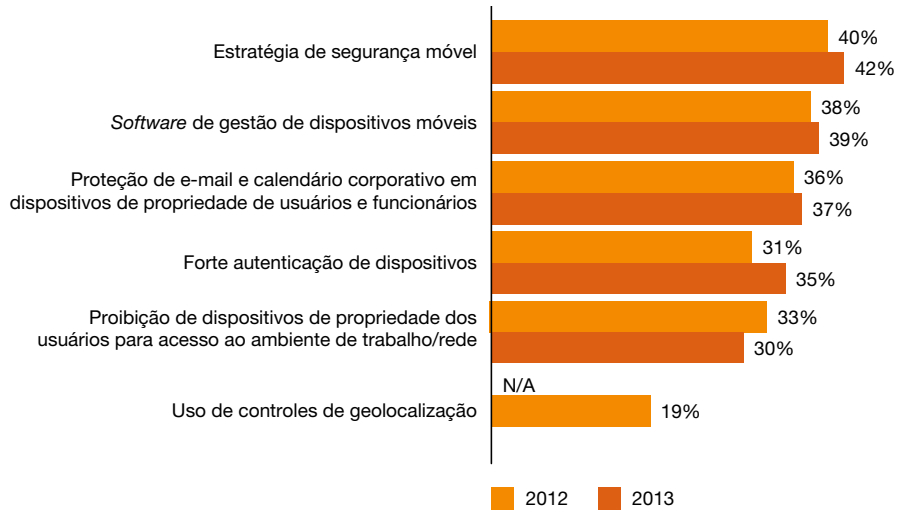
[3] Ocean Tomo, Ocean Tomo's Annual Study of Intangible Asset Market Value, abril/2011.

Outro risco importante para a segurança de dados é a expansão do uso de dispositivos móveis, como *smartphones* e *tablets*, além da tendência de que os funcionários utilizem seus próprios dispositivos no ambiente da empresa (BYOD – *Bring your own device* em inglês). Embora o uso de dispositivos móveis para compartilhar e transmitir dados continue a crescer, a implantação de políticas de segurança móvel não acompanha a proliferação desses aparelhos. De fato, os respondentes da pesquisa indicam que os esforços para implementar programas de segurança móvel não mostram ganhos significativos em relação ao ano passado e, em alguns casos, até declinam (Figura 9). Por exemplo, apenas 42% dizem ter uma estratégia de segurança móvel em vigor, e menos (39%) afirmam que suas organizações implantaram *softwares* de gestão de dispositivos móveis (MDM, na sigla em inglês), uma ferramenta essencial para a gestão automatizada de um elevado volume de *smartphones*.

Apenas ***18%*** ***dos participantes dizem ter políticas para a gestão de serviços na nuvem.***

A computação em nuvem é uma realidade há mais de uma década e tornou-se lugar-comum no ecossistema das corporações. Quase metade (47%) dos respondentes utiliza alguma forma de computação em nuvem, um ganho importante de 24% em relação ao ano anterior. Entre aqueles que usam serviços na nuvem, 59% informam que sua postura de segurança melhorou. Assim sendo, causa certa surpresa saber que muitas organizações não têm abordado seriamente as implicações dos serviços em nuvem.

Figura 9: Iniciativas adotadas para lidar com os riscos de segurança móvel



Observação: Nem todos os fatores são mostrados. A soma não equivale a 100%.
Os respondentes puderam indicar vários fatores.

Por exemplo, entre os participantes da pesquisa que usam serviços na nuvem, apenas 18% dizem ter políticas para governança desse ambiente.

"A falta de políticas de computação em nuvem representa uma séria lacuna de segurança para as empresas", diz Edgar D'Andrea, sócio da PwC. "A proliferação de dados compartilhados, em conjunto com o uso crescente de dispositivos móveis, cria um ambiente no qual os serviços em nuvem são utilizados de modo mais amplo pelos funcionários – com risco de abusos. Ao mesmo tempo, é essencial que as empresas garantam que terceiros que atuam como provedores de serviços em nuvem concordem em seguir práticas de segurança previamente definidas (APTs)."

As ameaças persistentes avançadas, conforme já observamos, estão sendo alvo constante da atenção da mídia, e isso pode explicar por que mais organizações parecem estar dando maior atenção ao tema. Por exemplo, 54% de todos os respondentes da pesquisa dizem ter implantado tecnologias de gestão de proteção/detecção. Em uma análise das indústrias, vemos um alto percentual de respondentes que afirmam ter implantado uma solução para APTs nos setores aeroespacial e de defesa (61%), público (58%) e farmacêutico (58%).

De acordo com a pesquisa US State of Cybercrime Survey 2013, as ferramentas de APT mais comuns são análise de malware, inspeção de tráfego de saída, verificação de dispositivos não autorizados e análise e geolocalização de tráfego IP.[4]

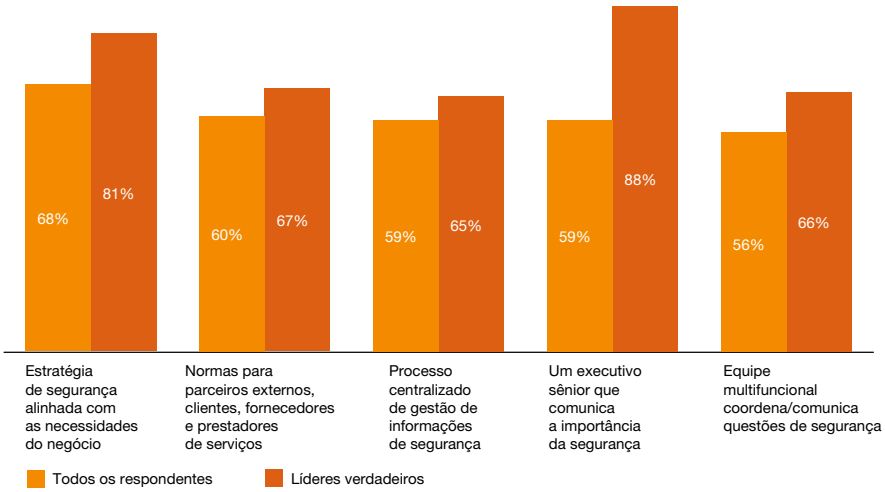
[4] 2013 US State of Cybercrime Survey, copatrocinada pela revista CSO, pelo CERT Coordination Center da Carnegie Mellon University, pelo FBI (Federal Bureau of Investigation), pela PwC e pelo Serviço Secreto dos EUA, março-abril 2013.

Como se preparar para as ameaças futuras

Atualmente, o inimigo está aperfeiçoando constantemente sua capacidade de explorar novas vulnerabilidades. Combater essas ameaças exige que as organizações definam suas ações e direcionem seus investimentos em segurança com base no mais apurado conhecimento disponível sobre os ativos de informação, os riscos para o ecossistema e as vulnerabilidades associadas. Essas ações devem ser avaliadas no contexto da atividade empresarial correspondente, saindo do lugar-comum de segurança como proteção para segurança como criação de valor para a organização.

A pesquisa deste ano indica que aqueles respondentes que definimos como líderes verdadeiros estão aperfeiçoando sua capacidade nesse sentido, implementando políticas que elevam a segurança ao topo das decisões de negócios e não apenas a um desafio de TI. Como assim?

Figura 10: Políticas e salvaguardas de segurança atualmente em vigor – Todos os respondentes x líderes verdadeiros



Observação: Nem todos os fatores são mostrados. A soma não equivale a 100%. Os respondentes puderam indicar vários fatores.

Os líderes verdadeiros estão alinhando a segurança às necessidades do negócio, definindo padrões para parceiros externos e, em geral, reavaliando os fundamentos da segurança (Figura 10). Por exemplo, 88% dos líderes verdadeiros têm um executivo sênior que comunica a importância da segurança da informação para toda a empresa. Outra política com visão de futuro é designar uma equipe multifuncional que coordene e comunique questões de segurança. Essa prática é adotada por 66% dos líderes verdadeiros.

"Esses tipos de políticas demonstram um novo compromisso com a segurança, que destaca o envolvimento da alta liderança e do conselho para garantir que a empresa crie e implemente um programa de segurança eficaz", **diz Eliane Kihara, sócia da PwC.** *"Eles também enfatizam a necessidade de ampliar a consciência sobre questões de segurança entre funcionários e terceiros que lidam com dados confidenciais."*

"Na Cablevision, a diretoria e o conselho apoiam prontamente as iniciativas de segurança", **diz Jennifer Love, vice-presidente sênior de operações de segurança.** *"Nossos executivos e o conselho entendem a importância da segurança da informação e expressam um forte interesse em compreender quais ameaças enfrentamos e o que estamos fazendo para reduzir nossas vulnerabilidades."*

Entretanto, políticas e apoio dos executivos representam apenas o início. Uma medida da real intenção da organização pode ser obtida quando se verifica se as empresas também implantaram tecnologias para executar essas políticas.

Os líderes verdadeiros tendem a implantar ferramentas que fornecem uma análise em tempo real de atividades suspeitas registradas em *hardware* e aplicativos de rede. Por exemplo, 66% desses líderes dizem ter implementado tecnologias de gestão de eventos e informações de segurança (SIEM, na sigla em inglês). Da mesma forma, 66% dos líderes verdadeiros afirmam ter implantado ferramentas de correlação de eventos, que agregam e correlacionam informações de ferramentas diversas, como sistemas de monitoramento de vulnerabilidades e intrusão. Soluções de verificação de vulnerabilidade, utilizadas por 71% dos líderes verdadeiros, avaliam as fragilidades de redes e aplicativos.

Embora nosso foco sejam os líderes verdadeiros que implementaram as tecnologias acima, é igualmente importante enfatizar que, em virtude do cenário atual de ameaças elevadas, todas as organizações devem considerar fortemente a implementação dessas salvaguardas, quando aplicável.

Outro exemplo pode ser encontrado em programas de treinamento e conscientização sobre segurança para os funcionários. Essa é uma iniciativa essencial para o sucesso de qualquer programa de segurança, e 60% dos respondentes dizem que têm programas desse tipo em vigor para os funcionários. Como os inimigos geralmente procuram abordar os funcionários usando técnicas de engenharia social, 100% dos participantes devem implementar um programa de treinamento eficaz para os funcionários.

"Muitos ataques têm como alvo o que está na mão dos funcionários", **diz Susan Mauldin, diretora de segurança da Equifax, agência global de informações sobre crédito ao consumidor.** *"Por isso, nosso programa de treinamento e conscientização dos funcionários se baseia em funções e é voltado para grupos de alto risco, como empregados de call-center, usuários com privilégios diferenciados e executivos, sendo que os exercícios atuais se concentram em ataques de phishing específicos."*

Para avaliar as prioridades dos participantes na preparação para as ameaças futuras, investigamos as prioridades de implementação de salvaguardas de processos e tecnologia para os próximos 12 meses. Estávamos interessados em cinco categorias específicas: proteção de ativos críticos, segurança da infraestrutura, ameaças à segurança, análise e segurança de dispositivos móveis.

Uma segurança eficaz atualmente requer que as organizações identifiquem e priorizem a proteção das "joias da coroa". Vinte e cinco por cento (25%) dos respondentes afirmam que vão priorizar a implantação de um programa para identificar ativos confidenciais nos próximos 12 meses, e 17% dizem que a prioridade serão as ferramentas de gestão de ativos (Figura 11). Esses tipos de soluções fornecem uma maneira importante de entender, avaliar e gerenciar os dados confidenciais de uma organização.

Para aprimorar a segurança da infraestrutura, 24% dos participantes dizem que implementarão normas de segurança para parceiros, fornecedores, prestadores de serviços externos e consumidores. É uma iniciativa crítica no momento em que mais organizações abrem redes, aplicativos e dados para terceiros. Além disso, tecnologias como a virtualização e os serviços na nuvem amplificaram o potencial de comprometimento de dados pela ação de um usuário interno com privilégios. Como resultado, monitorar e administrar os usuários com privilégios é hoje um desafio importante; descobrimos que 17% dos respondentes planejam implantar ferramentas de gestão de acesso de usuários privilegiados ao longo dos próximos 12 meses.

Figura 11: Salvaguardas não implantadas, mas que são uma prioridade para os próximos 12 meses

Observação: Nem todos os fatores são mostrados. A soma não equivale a 100%. Os respondentes puderam indicar vários fatores.

Outras prioridades são tecnologias que podem ajudar a entender melhor as ameaças, além de aperfeiçoar a segurança para dispositivos móveis. Pela primeira vez, perguntamos se há planos de adotar serviços de assinatura de inteligência contra ameaças como forma de obter ajuda de terceiros e alertas rápidos sobre novos riscos e falhas de segurança do tipo "dia zero". E muitas empresas têm planos: 49% dos participantes disseram usar esses serviços e, entre os que não usam, 25% afirmam que a sua implementação será uma prioridade nos próximos 12 meses.

Na Equifax, a prioridade é proteger os dispositivos dos funcionários de forma que a empresa possa entender melhor quem são os agentes das ameaças. "Estamos analisando o *hardware* usado por funcionários e basicamente estamos simulando o ambiente para proteger os computadores de vírus e malware", diz Mauldin. "Isso protege contra riscos, mas também ajuda a identificar que tipos de ameaças estão surgindo e quem está considerando a Equifax como um alvo."

Dado o interesse crescente no *Big Data*, quisemos saber também se as organizações planejam usar a análise como um meio de melhorar a segurança. É uma estratégia que está ganhando aprovação: 20% dos respondentes dizem que pretendem priorizar ferramentas de gestão de informações de segurança e gestão de eventos, e um número igual afirma que tecnologias de correlação de eventos de segurança são uma das maiores prioridades.

"Esses tipos de tecnologias podem ajudar as organizações a detectar padrões e anomalias em atividade capazes de fornecer visões e inteligência sobre as ameaças cibernéticas que a empresa enfrenta", afirma Rodrigo Milo, diretor da PwC. "Com essas informações, os líderes de negócios podem antecipar alterações no perfil de ameaças cibernéticas de suas empresas e reagir de forma dinâmica."

Outro aspecto relevante é a segurança de dispositivos móveis. Quase um em cada quatro respondentes diz que planeja priorizar a criptografia de *smartphones*, implantar soluções de gestão de dispositivos móveis (MDM) e adotar uma estratégia para o uso de dispositivos pessoais na rede corporativa.

No ano passado, compartilhar informações sobre ameaças de segurança – mesmo entre concorrentes – tornou-se uma poderosa ferramenta ofensiva.

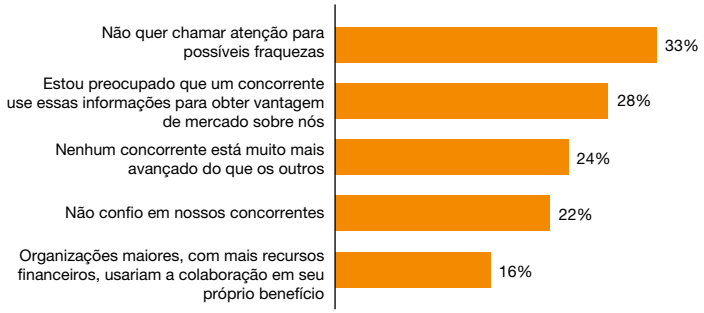
Acreditamos que a colaboração pode levar as empresas a se adaptarem mais rapidamente a mudanças no mercado. Na 5th Annual Digital IQ Survey[5], da PwC, descobrimos que as empresas que têm uma diretoria colaborativa interligam TI e a estratégia de negócios, o que geralmente melhora o desempenho de uma organização.

Dessa forma, estávamos curiosos para saber como os participantes globais da pesquisa, muitos dos quais operam em um ambiente cada vez mais competitivo, encaravam a colaboração com outras empresas para melhorar a segurança e compartilhar conhecimentos sobre ameaças. Muitas organizações percebem as vantagens da colaboração: 50% dos respondentes disseram que colaboram com terceiros e, entre os líderes, esse percentual sobe para 82%.

A Equifax fornece um exemplo. "Participamos do FS ISAC (Financial Services Information Sharing and Analysis Center)", diz o CSO Mauldin. "Isso é bastante importante para nós porque muitas agências do governo também participam do FS ISAC, e esse centro fornece uma maneira proativa de se aprender sobre a evolução das ameaças." A Equifax participa de vários outros grupos da indústria, e também colabora com seus pares no mesmo segmento.

Entre os 28% de participantes que não compartilham informações, as principais razões são o temor de que isso acentue fraquezas ou de que um concorrente possa usar informações em seu benefício, além da clara desconfiança dos concorrentes (Figura 12). Por fim, 22% dos respondentes não sabem se a sua organização colabora com outras.

Figura 12: Motivos para não colaborar sobre segurança da informação



Observação: Nem todos os fatores são mostrados. A soma não equivale a 100%. Os respondentes puderam indicar vários fatores.

[5] PwC, PwC's 5th Annual Digital IQ Survey, 2013.

Obstáculos ao avanço da segurança

Embora a maioria dos *stakeholders* de segurança concorde que ações devem ser tomadas para melhorar a segurança da informação, parece haver pouco consenso sobre os desafios em fazê-lo.

Pedimos aos participantes que identificassem os maiores obstáculos para melhorar a segurança. As respostas revelaram uma ampla gama de opiniões divergentes e, em alguns casos, com trocas de acusações. De modo geral, os participantes da pesquisa dizem que os obstáculos mais importantes são insuficiência de investimentos, entendimento inadequado de como futuras necessidades de negócios afetarão a segurança das informações, liderança comprometida e falta de uma estratégia de segurança eficaz (Figura 13).

Quando se leva em conta a expansão dos orçamentos de segurança este ano, parece que o problema de capital já está resolvido. Mas é perturbador saber que questões fundamentais, como o entendimento e o alinhamento da segurança com futuras necessidades de negócios e a eficácia das estratégias de segurança, estão entre as maiores preocupações. Os respondentes também tendem a apontar a liderança executiva, o CEO em especial, como um dos principais impedimentos ao aperfeiçoamento da segurança.

Figura 13: Maiores obstáculos para melhorar a segurança da informação

Observação: A soma não equivale a 100%. Os respondentes puderam indicar vários fatores.

E quem ou o que os CEOs culpam? Curiosamente, os CEOs, por esmagadora maioria, apontaram a si mesmos como o obstáculo nº 1. Os CFOs, por sua vez, apontam o CEO como principal impedimento, seguido do CIO, do CISO e do CSO. Quando a pergunta é feita aos CISOs, os executivos diretamente responsáveis pela segurança da informação, eles colocam o financiamento insuficiente (tanto de capital como operacional) no topo da lista, seguido da falta de conhecimentos técnicos internos. Os CIOs apontam a falta de estratégia, visão e liderança dos CEOs e executivos de segurança.

"Essa falta de clareza sobre os obstáculos à segurança eficaz mostra, em parte, que as empresas estabeleceram diálogo suficiente sobre a questão. Nessa conversa, funcionários, executivos e terceiros, todos entendem seu papel na segurança da informação, as grandes prioridades e os principais riscos", **diz Edgar D'Andrea, sócio da PwC**. *"Criar e apoiar uma cultura de consciência sobre segurança também exigirá o apoio total dos principais executivos, inclusive do CEO e do conselho. Essa deve ser uma discussão permanente."*

A corrida global de defesa cibernética

Por vários anos, a região da Ásia-Pacífico esteve na liderança do investimento em tecnologias, processos e gastos de segurança. Como resultado, a região saltou à frente das outras no desenvolvimento e na implementação de programas de segurança efetivos (Figura 14). E ela ainda mantém o primeiro lugar.

De fato, 28% do que identificamos como líderes verdadeiros são da Ásia-Pacifico, o que representa apenas 21% do total geral de respondentes.

Mas a elevada classificação da Ásia-Pacífico nas práticas de segurança está sendo seriamente desafiada pela América do Sul. Pela primeira vez, os sul-americanos parecem prontos para assumir a liderança em termos de investimentos, políticas e salvaguardas de segurança da informação. O continente lidera em fatores-chave, como gastos de segurança e emprego de um CISO para supervisionar a segurança, e está no mesmo patamar que a região Ásia-Pacífico em muitas outras questões.

No entanto, a Ásia-Pacífico permanece muito forte em gastos de segurança e adoção das melhores práticas. A Europa e a América do Norte, por sua vez, estão atrasadas em muitos aspectos, inclusive no emprego de um CISO, na inclusão de políticas importantes, como *backup* e recuperação/continuidade de negócios, e colaboração com outras empresas. A América do Norte exibe algumas forças importantes, como a exigência de que terceiros cumpram políticas de privacidade e também a conscientização e o treinamento de funcionários, mas está defasada em relação a muitas outras medidas.

Figura 14: Práticas de segurança por região

	América do Sul	Ásia-Pacífico	Europa	América do Norte
Os gastos de segurança aumentarão nos próximos 12 meses	66%	60%	46%	38%
Tem uma estratégia geral de segurança	75%	79%	77%	81%
Emprega um diretor de segurança da informação	75%	74%	68%	65%
Tem um executivo sênior que comunica a importância da segurança	68%	69%	51%	55%
Mediu/avaliou a eficácia de políticas e procedimentos de segurança no ano passado	70%	69%	53%	49%
Tem uma política de *backup* e recuperação/continuidade de negócios	58%	55%	45%	47%
Exige que terceiros cumpram políticas de privacidade	55%	58%	55%	62%
Emprega um programa de conscientização e treinamento de segurança	54%	63%	55%	64%
Tem procedimentos dedicados para proteger a propriedade intelectual	20%	24%	17%	21%
Tem tecnologias de detecção de intrusão em vigor	64%	67%	63%	67%
Inventário sobre onde os dados pessoais são coletados, transmitidos e armazenados	53%	60%	52%	64%
Colabora com terceiros para melhorar a segurança e reduzir riscos	66%	59%	45%	42%

Observação: Nem todos os fatores são mostrados. A soma não equivale a 100%. Os respondentes puderam indicar vários fatores.

Ásia-Pacífico: Ainda na liderança

A região da Ásia-Pacífico continua na liderança em termos de gastos e práticas de segurança. O investimento é forte: a média dos orçamentos de segurança aumentou 85% em relação ao ano passado. A região informa ter o mais alto orçamento de segurança da informação como percentual do gasto de TI: 4,3%. Os respondentes estão otimistas sobre o futuro dos gastos com segurança da informação: 60% dizem que seu orçamento de segurança aumentará nos próximos 12 meses. No entanto, a média das perdas financeiras devido a incidentes de segurança cresceu 28% em relação ao ano passado.

Os orçamentos de segurança cresceram em média

85%

na Ásia-Pacífico.

A Ásia-Pacífico se equipara à América do Sul em relação a práticas importantes, como empregar um CISO para supervisionar o programa de segurança. A região também tem um percentual maior de adoção de novas medidas de segurança progressistas, como ter um executivo sênior para comunicar a importância da segurança (69%) e colaborar com outras empresas para melhorar a segurança (59%). Também tende mais a implantar tecnologias de detecção de intrusão (67%) e a ter

um inventário dos locais onde dados pessoais são coletados, transmitidos e armazenados (60%) em comparação com a América do Sul.

No entanto, uma comparação ano a ano revela que a Ásia-Pacífico está começando a paralisar a implementação de algumas políticas e tecnologias de segurança. Por exemplo, o número de respondentes que informam ter uma política de *backup* e um plano de recuperação/continuidade de negócios é menor do que no ano anterior, e outras políticas importantes, como treinamento de funcionários e procedimentos dedicados a proteger a propriedade intelectual, estão essencialmente paradas.

A China representa 33% dos respondentes da Ásia-Pacífico na pesquisa, seguida de Índia (31%) e Japão (17%). Em vários aspectos, os chineses ofuscam outros países em práticas e políticas de segurança. Por exemplo, 60% dos respondentes da China utilizam monitoramento e perfil comportamental, 73% têm armazenamento centralizado de dados de usuários, e 72% empregam ferramentas de verificação de vulnerabilidades, todos acima das taxas de adoção de outros países. Além disso, 62% dos participantes chineses têm soluções de gestão de proteção/detecção para APTs e 66% implementaram tecnologias SIEM, resultados que superam em muito os de outras nações. E mais: nenhum país adotou políticas de segurança para dispositivos móveis, BYOD (sigla em inglês para a utilização do próprio dispositivo dos funcionários na rede corporativa) e mídias sociais em percentuais maiores do que a China.

Por exemplo, 71% dos respondentes da China têm uma política em vigor para o uso de dispositivos pessoais na rede da empresa, contra 64% nos EUA e 54% na Índia. Em comparação com a China, a Índia vem obtendo ganhos expressivos com programas e políticas de segurança, mas está defasada em praticamente todos os outros aspectos.

América do Sul: A nova potência

A América do Sul mostra fortes avanços em termos de gastos, políticas e tecnologias de segurança. Em vários aspectos, a região se equipara – e às vezes supera – a Ásia-Pacífico.

Por exemplo, os orçamentos de segurança da informação saltaram 69% em relação ao ano anterior, e 66% dos respondentes da região dizem que os gastos de segurança aumentarão ao longo dos próximos 12 meses. O orçamento de segurança representa 4,1% do gasto geral de TI, menor apenas que o da Ásia-Pacífico. Os respondentes da América do Sul tendem a empregar um CISO (75%) e a ter uma política de *backup* e planos de recuperação/continuidade de negócios (58%). O continente lidera em colaboração com terceiros (66%) e está empatado com a Ásia-Pacífico em políticas progressistas, como ter um executivo sênior que comunique a importância da segurança (68%). A média de perdas financeiras totais devido a incidentes de segurança está crescendo modestamente (4%) em comparação com o ano passado.

75% ***dos respondentes da América do Sul dizem que suas organizações empregam um CISO.***

Os participantes do Brasil representam o maior percentual da América do Sul (48% do total), seguidos de México (30%) e Argentina (21%). O Brasil lidera em muitos aspectos – monitoramento e definição de perfis (57%) e uso de ferramentas de verificação de vulnerabilidades (63%), por exemplo – mas, em geral, está atrás da China e dos EUA.

A América do Sul também tem suas fraquezas. Por exemplo, a porcentagem de respondentes cujas organizações têm uma política para treinamento e conscientização de segurança é comparativamente baixa (54%), como também a das empresas que têm um inventário dos locais onde os dados pessoais são coletados, transmitidos e armazenados (53%).

Os orçamentos de segurança na Europa caíram

3%

em relação ao ano passado.

Europa: Ficando para trás em investimento e salvaguardas

Ao contrário do que acontece em outras regiões, o investimento em segurança da informação está caindo ligeiramente (3%) na Europa em relação ao ano passado, e o continente continua atrasado na adoção de importantes salvaguardas de segurança.

Além da pequena degradação dos investimentos em segurança, somente 46% dos participantes europeus acreditam que os gastos com a área aumentarão ao longo dos próximos 12 meses. Enquanto o número de incidentes de segurança detectados caiu 22% em um ano, a média das perdas financeiras devido a esses incidentes subiu 28%.

A implementação de políticas importantes, inclusive de *backup* e recuperação/continuidade de negócios (45%) e comunicação e treinamento para conscientização sobre segurança (21%), é comparativamente baixa na Europa.

Também é baixo o percentual dos respondentes que informam colaborar com terceiros (45%) e daqueles que têm uma política de segurança móvel (38%).

América do Norte: resultados opostos

O investimento em segurança está crescendo na América do Norte, como também o número de incidentes detectados. E, embora a adoção de políticas-chave de segurança permaneça baixa, a América do Norte lidera em algumas áreas importantes.

A média dos orçamentos de segurança cresceu 80% em relação ao ano anterior, mas o panorama para gastos no próximo ano é o mais baixo de todas as regiões: apenas 38% dos respondentes da América do Norte dizem que os gastos de segurança aumentarão nos próximos 12 meses. O número de incidentes de segurança detectados saltou 117% em relação a 2012, enquanto as perdas financeiras médias causadas por incidentes de segurança aumentaram 48%.

A América do Norte lidera outras regiões em algumas práticas importantes, incluindo ter uma estratégia geral de segurança (81%), exigir que terceiros cumpram políticas de privacidade (62%), e oferecer treinamento para conscientização de segurança dos funcionários (64%). A região também tem como prática manter um inventário dos locais onde coleta, transmite e armazena dados pessoais (64%) e ter tecnologias de detecção de intrusão (67%). Em contrapartida, a América do Norte está atrás de outras regiões na colaboração com outras empresas (42%) e no emprego de um CISO (65%). Os respondentes norte-americanos apresentam também menos probabilidade de ter analisado a eficácia de suas práticas de segurança no último ano.

Na América do Norte, os incidentes detectados aumentaram

117%

em relação ao ano passado.

Os EUA, que representam 84% dos participantes da nossa pesquisa na América do Norte, estão bem classificados em estratégias de computação em nuvem (52%), segurança de dispositivos móveis (60%), mídias sociais (58%) e BYOD (64%), atrás apenas da China na maioria dos aspectos analisados.

Mercado brasileiro

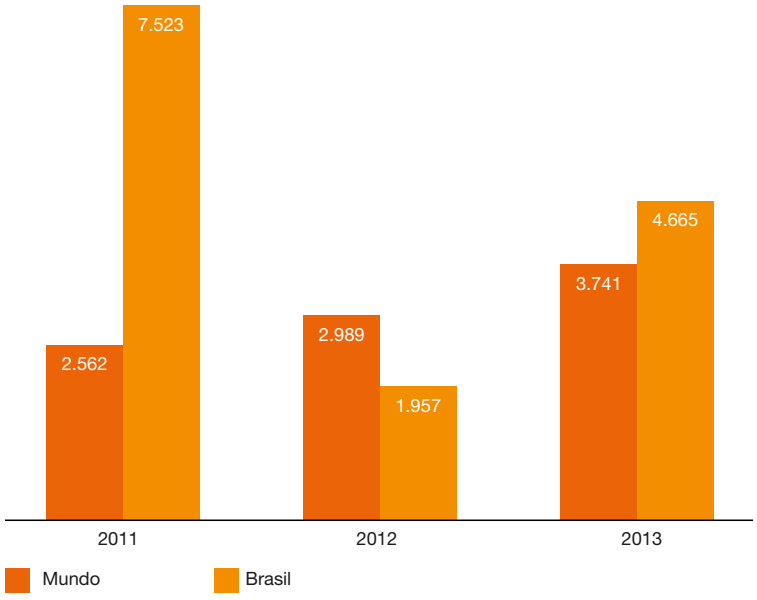
Incidentes de hoje, estratégias de ontem

No Brasil, o volume de incidentes segue a mesma tendência do resto do mundo: continua a crescer. Em 2012, houve uma redução em relação ao ano anterior, porém, em 2013, foi registrada uma elevação superior a 200%.

De forma semelhante, a interpretação desses dados nos leva a duas conclusões: (1) o volume de incidentes de fato tem aumentado e (2), concomitantemente, as empresas estão adotando novas tecnologias que possibilitam a identificação de tais incidentes.

O fato de as organizações estarem se tornando alvo de ataques cada vez mais frequentes faz com que elas aprimorem seus controles detectivos, e isso pode explicar a suposta elevação no volume de incidentes. A Figura 17 confirma essa suposição. Ao analisarmos as principais tecnologias empregadas para detecção de ameaças, para todas, sem exceção, houve elevação no número de respondentes que afirmam empregar o componente tecnológico.

Figura 15: Número de incidentes nos últimos 12 meses



O volume de respondentes que desconhecem se foram alvo de incidentes permaneceu praticamente estável desde 2011, como demonstra o gráfico, mas vale destacar um aumento considerável na quantidade de incidentes relatados em relação ao ano anterior.

Os resultados indicam que as ferramentas de detecção de códigos maliciosos continuam sendo predominantes dentro das organizações. Todavia, foi possível observar um avanço na utilização de soluções de ferramentas de *Data Loss Prevention*, Correlação de Eventos de Segurança e Monitoramento de Internet.

Figura 16: Número de incidentes ocorridos

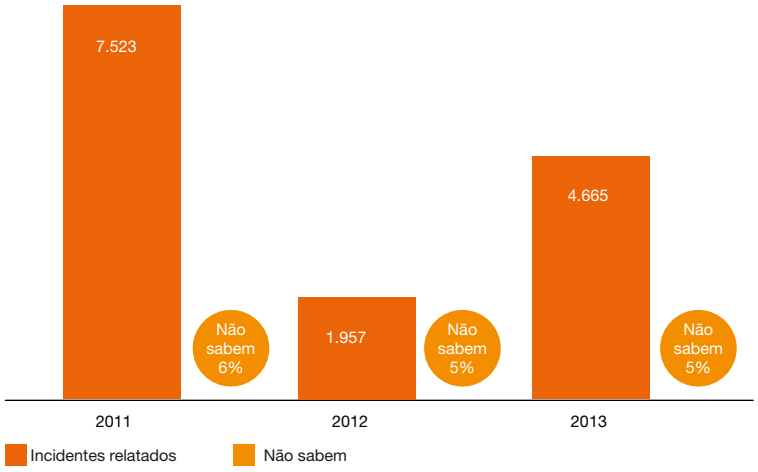


Figura 17: Principais tecnologias empregadas para detecção

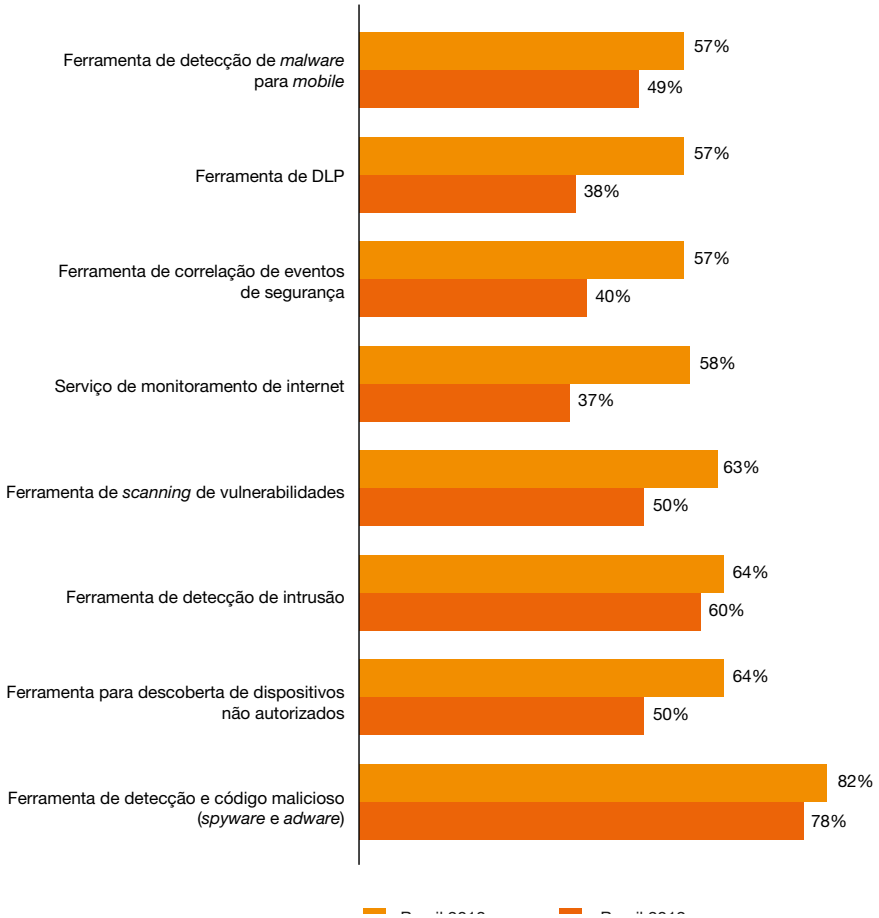
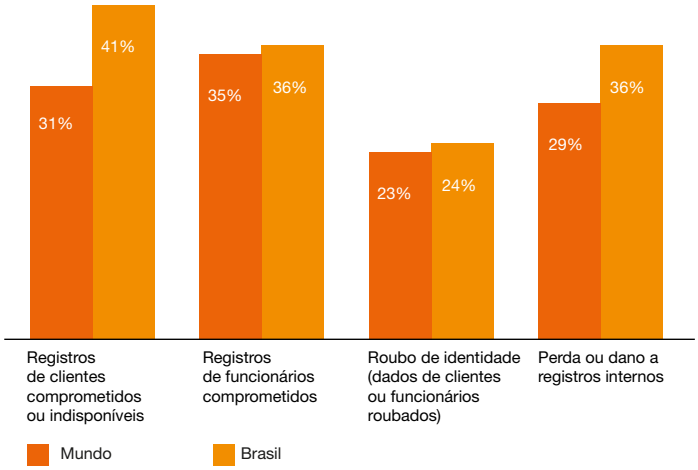


Figura 18: Impacto dos incidentes de segurança



No Brasil, o principal impacto dos incidentes, em termos de privacidade, está relacionado ao comprometimento dos registros de clientes. No resto do mundo, o principal aspecto comprometido são os registros de empregados. Outro aspecto cuja tendência segue a do resto do mundo é a origem dos incidentes. No Brasil, 41% dos respondentes afirmam que os *hackers* são ainda a principal origem dos incidentes, enquanto nos demais países esse percentual ficou em 32%.

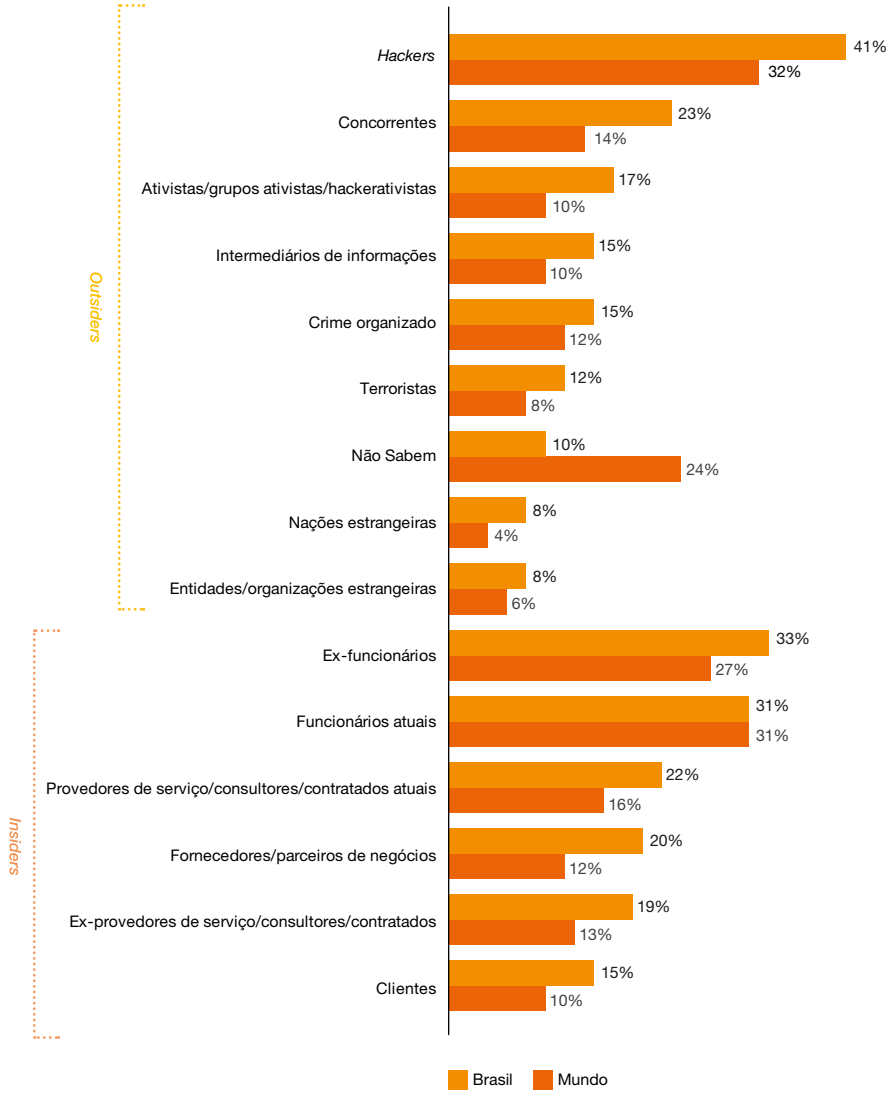
De acordo com a Pesquisa de Segurança da Informação 2014, 61,5% dos respondentes disseram conduzir voluntariamente testes regulares de penetração de dados a fim de avaliar suas vulnerabilidades e seu nível de exposição.

De modo complementar, apenas 10% dos respondentes no Brasil afirmam desconhecer a origem dos incidentes, enquanto nos demais países esse percentual é de 24%.

No Brasil, a identificação precisa da origem provável dos incidentes identificados é superior em todos os casos, com exceção apenas dos que responderam “Funcionários atuais” e “Não sabe” (Figura 19).

De acordo com os dados da pesquisa, é possível observar que, no Brasil, a ação de *hackers* e concorrentes é quase 10% maior do que no restante do mundo.

Figura 19: Origem provável dos incidentes



Uma defesa fraca contra os adversários

No Brasil, as empresas também estão buscando se reinventar para conseguir lidar com o aumento significativo no volume de incidentes.

De fato, além de conhecer as origens desses problemas, é muito importante que as empresas conheçam quais são os principais alvos dos ataques, a fim de orientar corretamente os investimentos.

Com relação às práticas adotadas para proteger a propriedade intelectual de suas informações, o Brasil continua fortemente alinhado às tendências globais. Aproximadamente 32% dos respondentes afirmam que empregam práticas regulares de revisão dos privilégios de acesso. No resto do mundo, o percentual é de 31%.

É importante destacar que a correta gestão dos privilégios de acesso de colaboradores e/ou terceiros contribui para conter o potencial impacto dos incidentes, independentemente de sua origem.

O segundo aspecto mencionado no Brasil e no resto do mundo como medida preventiva é a execução do inventário como parte da gestão de ativos, o que foi informado por 26% dos respondentes (local e globalmente).

Figura 20: Políticas para proteger a propriedade intelectual e os segredos comerciais

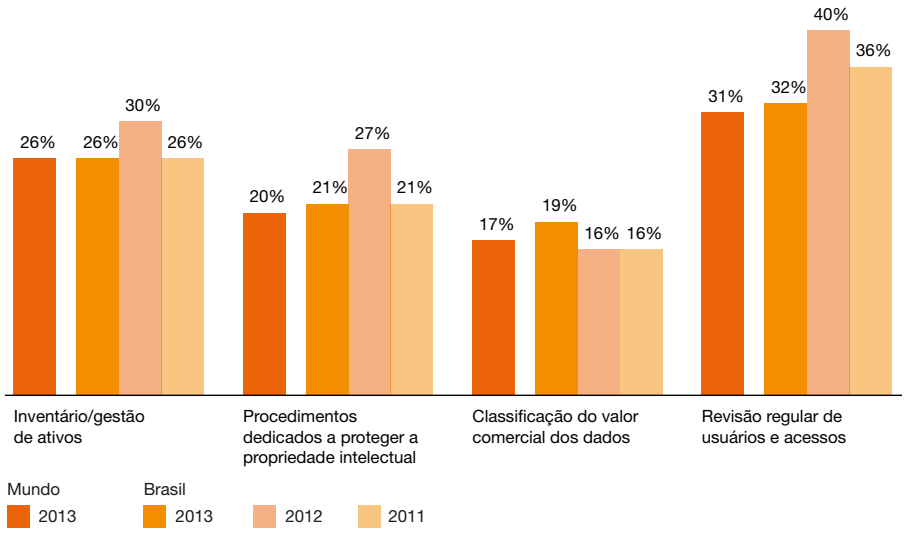
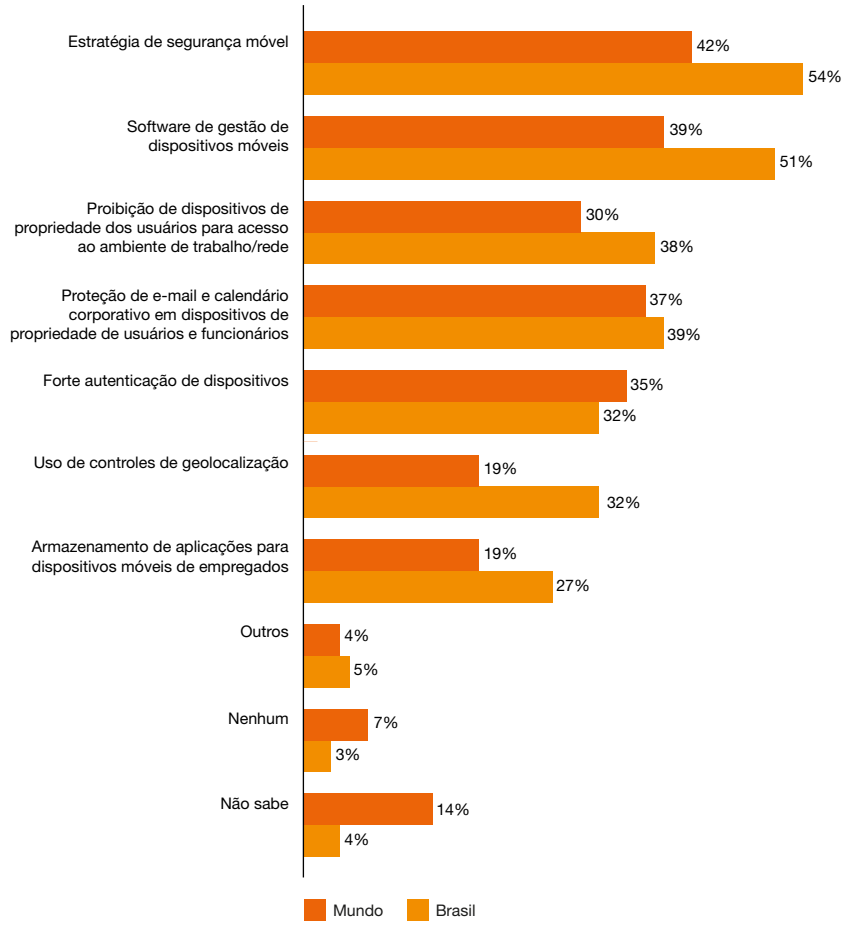


Figura 21: Iniciativas adotadas para lidar com os riscos de segurança móvel



O uso de dispositivos móveis é uma questão amplamente discutida tanto no âmbito local quanto global. De fato, essa é uma realidade que forçou as empresas a se posicionar rapidamente, dado o crescimento exponencial no volume de dispositivos utilizados por colaboradores e terceiros.

As principais ações apontadas pelos respondentes brasileiros a fim de mitigar os riscos provenientes das tecnologias móveis são: (1) estabelecer uma estratégia para segurança móvel; e (2) adoção de software para gestão de dispositivos móveis. Apenas 3% dos respondentes no Brasil informaram que não executam nenhuma ação específica para controlar os riscos de tecnologias móveis.

No Brasil, podemos observar que há uma forte preocupação com o tratamento dado aos dispositivos móveis, pois o percentual de respondentes que afirmou ter uma estratégia de segurança móvel foi 12 pontos maior que a do restante do mundo. A mesma diferença entre os resultados globais e do Brasil foi observada em relação aos que afirmam ter um software para gestão de dispositivos móveis (MDM - Mobile Device Management).

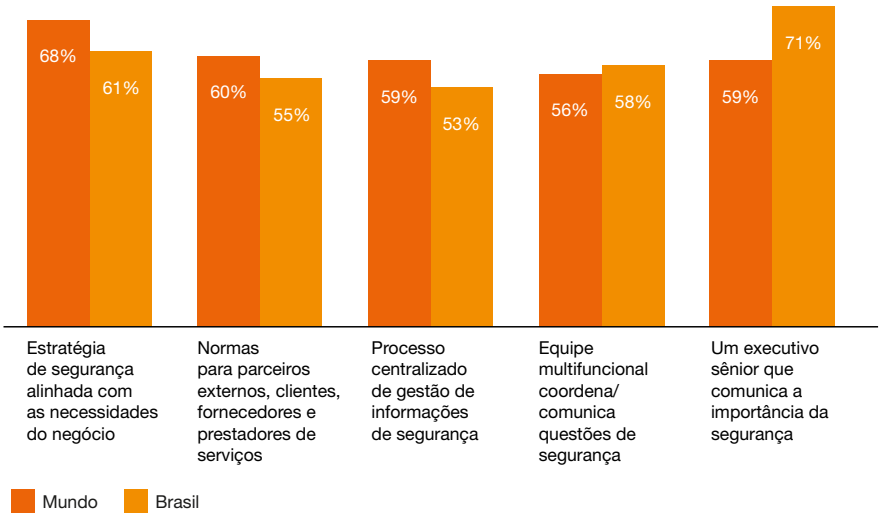
Em contrapartida, no restante do mundo nota-se uma postura mais restritiva do que no Brasil em relação ao uso de dispositivos de propriedade dos usuários para acesso ao ambiente de trabalho ou rede corporativa: 38% disseram proibir o uso desses dispositivos em comparação com 30% no Brasil.

Como se preparar para as ameaças futuras

Para combater ativamente as ameaças às quais estão sujeitas, as empresas têm buscado reinventar a forma de fazer segurança da informação. Nesse contexto, obter o patrocínio adequado da alta administração é essencial para implantação das ações. No Brasil, 71% dos respondentes afirmam contar com um executivo sênior que comunica a importância da segurança para a corporação. Esse aspecto é essencial para o sucesso das demais iniciativas.

Em paralelo, 61% dos respondentes afirmam que sua estratégia de segurança está alinhada com as necessidades de negócio. De fato, esse alinhamento permite que haja uma real percepção de valor pelas áreas usuárias.

Figura 22: Políticas e salvaguardas de segurança atualmente em vigor



No resto do mundo, o alinhamento da estratégia de segurança com as necessidades do negócio foi informado por 68% dos respondentes como uma das principais salvaguardas.

Obstáculos no avanço da segurança

Existe um entendimento comum de que ações de segurança da informação devem ser implementadas para deter as ameaças cada vez mais diversificadas.

No Brasil, a pesquisa mostrou que 39% dos respondentes não atuam de forma colaborativa com as demais empresas do mesmo setor, pois "não querem chamar a atenção para possíveis fraquezas". Esse é um aspecto que merece reflexão cuidadosa. Por um lado, ao compartilhar as dificuldades, as empresas conseguem aprender com a experiência de outras do mesmo setor e se antecipar na adoção de contramedidas. Na contramão desse benefício direto, existe a insegurança quanto à exposição excessiva.

Os demais indicadores mapeados pela pesquisa corroboram com esse quadro. Do total de respondentes, 31% "estão preocupados que um concorrente use essas informações para obter vantagem de mercado", enquanto 30% afirmam que "não confiam nos concorrentes".

Figura 23: Motivos para não colaborar sobre segurança da informação

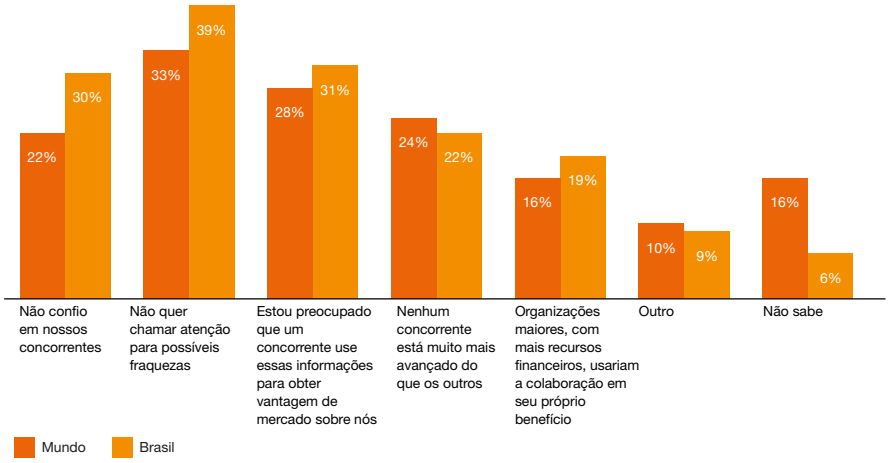
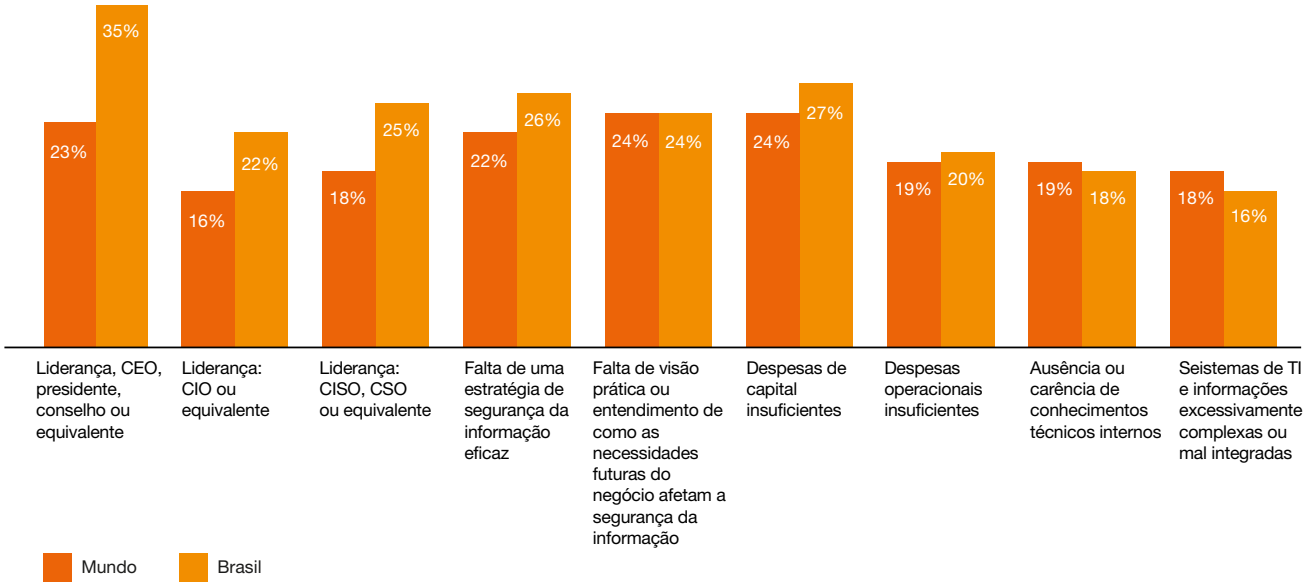


Figura 24: Maiores obstáculos para melhorar a segurança da informação



A implantação de um programa robusto de segurança da informação envolve diversos aspectos, que compreendem desde investimentos adequados e entendimento das necessidades de negócio, até a obtenção do patrocínio da alta administração para suportar tais iniciativas. Quando um desses componentes não é adequadamente abordado pela empresa, o sucesso das ações de segurança pode ficar comprometido.

No Brasil, 35% dos respondentes acreditam que a maior dificuldade para melhorar a segurança da informação em sua empresa está relacionada à liderança da organização. O orçamento inadequado foi mencionado por 27% dos participantes como a segunda grande preocupação.

Aspectos relevantes no contexto brasileiro

Investimentos em segurança da informação

No Brasil, o orçamento destinado à segurança da informação ainda é fortemente condicionado pela situação econômica do país, conforme indicado por 47,8% dos respondentes.

Quando perguntados sobre o investimento dedicado a segurança da informação, 28% dos respondentes estimam que seus orçamentos atinjam o teto de um milhão de dólares, o que pode ser considerado razoavelmente baixo quando comparado à perda financeira que uma ameaça pode causar à empresa, ao explorar uma vulnerabilidade.

Principais desafios de segurança da informação

Ao analisarmos os cinco principais desafios de segurança mencionados pelos respondentes, observamos que existe uma certa coerência entre as questões indicadas em 2012 e 2013, como demonstra a figura a seguir. Um ponto de destaque, ao compararmos os desafios indicados em cada ano, é que o tema da computação em nuvem deixou de ser uma preocupação, e o da prevenção contra vazamento de informações ganhou visibilidade. O volume acentuado de incidentes apresentados na mídia ao longo de 2013 pode ter contribuído para que a perda de dados tenha ganhado destaque.

Figura 25: Magnitude dos investimentos

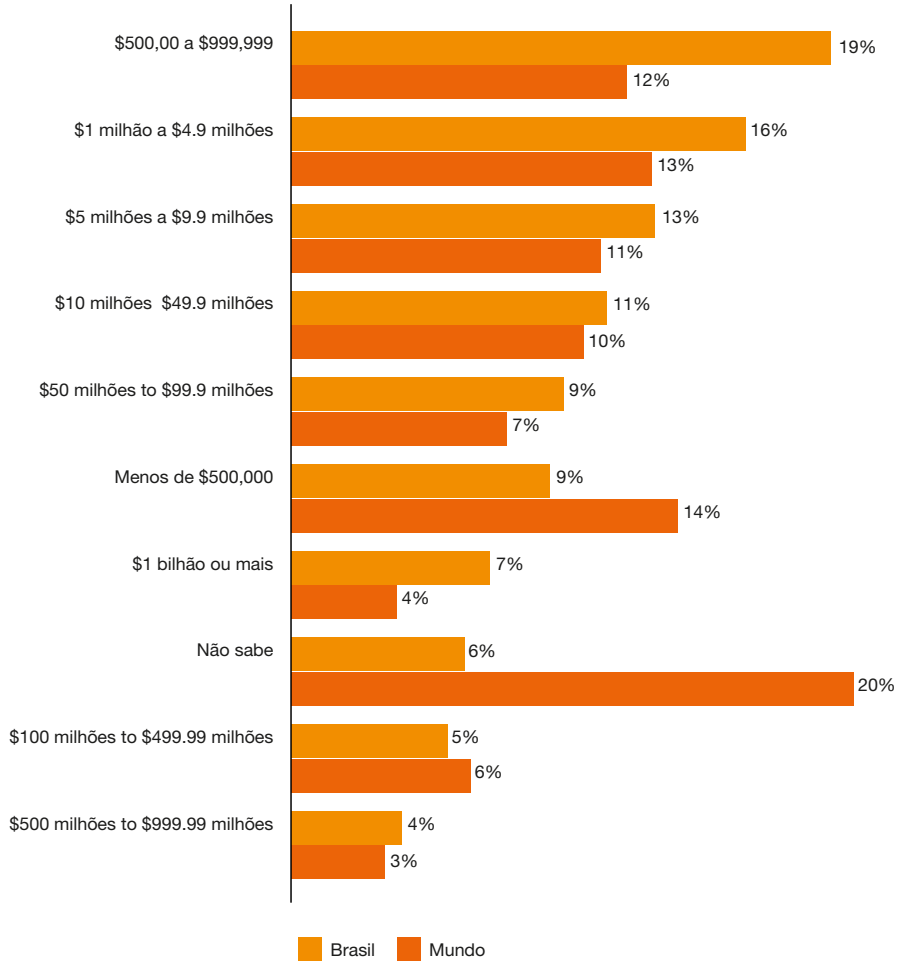
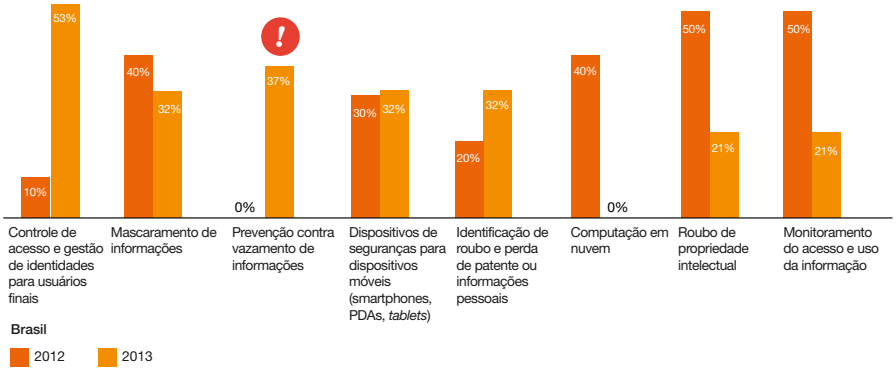


Figura 26: Principais desafios de segurança

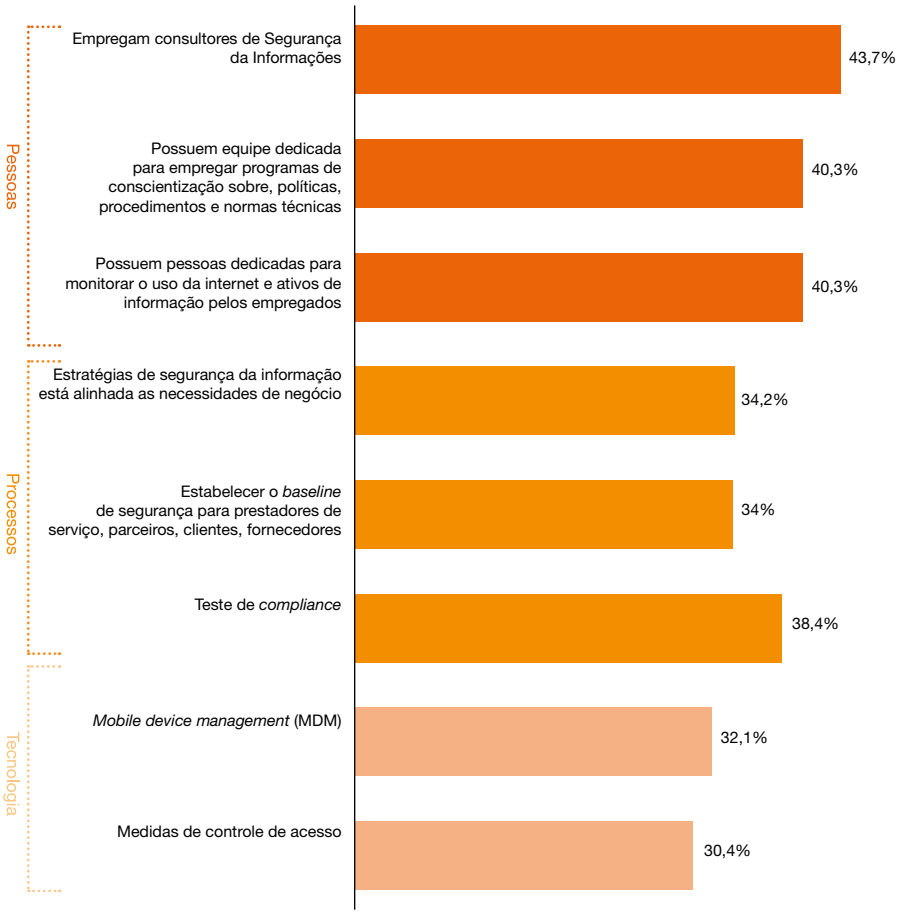


O que as empresas terceirizam em termos de segurança da informação

Há tempos os profissionais da área vêm discutindo com muita cautela o tema da terceirização no contexto de segurança da informação. Por um lado, existe forte pressão por redução de custos, e isso se traduz na busca de alternativas que viabilizem a execução de uma determinada atividade, conduzindo a solução para um cenário de terceirização. Por outro lado, será que a organização não se expõe demais ao transferir a um terceiro a atribuição de executar determinados procedimentos de segurança? De fato, esse hiato não será de fácil solução. A experiência tem demonstrado que, embora determinadas funções de segurança sejam terceirizadas, as atividades de controle e medição do serviço prestado têm relevância acentuada.

A figura abaixo mostra quais são as principais áreas em que as empresas têm terceirizado suas atribuições, do ponto de vista de processos, pessoas e tecnologia.

Figura 27: Principais atividades de segurança terceirizadas pelas organizações



Como as organizações têm lidado com as novas tecnologias

Computação em nuvem

A *cloud computing* já é uma realidade para muitas empresas no Brasil. Nos últimos anos, houve grande discussão a respeito da garantia da privacidade de dados no ambiente da nuvem. Isso exigiu dos fornecedores desse tipo de serviço discursos comerciais embasados tecnicamente e contratos consistentes em relação a suas práticas de segurança e privacidade. O objetivo é demonstrar o conjunto de controles empregados para proteger as informações das organizações clientes.

No Brasil, entre os diferentes tipos de serviços em nuvem oferecidos, o principal é o *Software as Service,* conforme mostra a Figura 28. A adoção de serviços em nuvem no Brasil também tem se mostrado maior do que no restante do universo da pesquisa, principalmente no que tange a Infraestrutura (IaaS) e Plataforma (PaaS).

Os respondentes do Brasil têm uma percepção positiva sobre a segurança que o ambiente de nuvem pode fornecer. Entre os participantes, 73% afirmam que a segurança do ambiente está melhor do que no passado, enquanto nos demais países esse percentual é de 59%. Para 16% dos respondentes da pesquisa global a situação piorou, enquanto para 20% não houve mudança significativa. No Brasil, esses percentuais são de 10% e 14%, respectivamente.

Figura 28: Tipo de serviço em nuvem utilizado pelas empresas

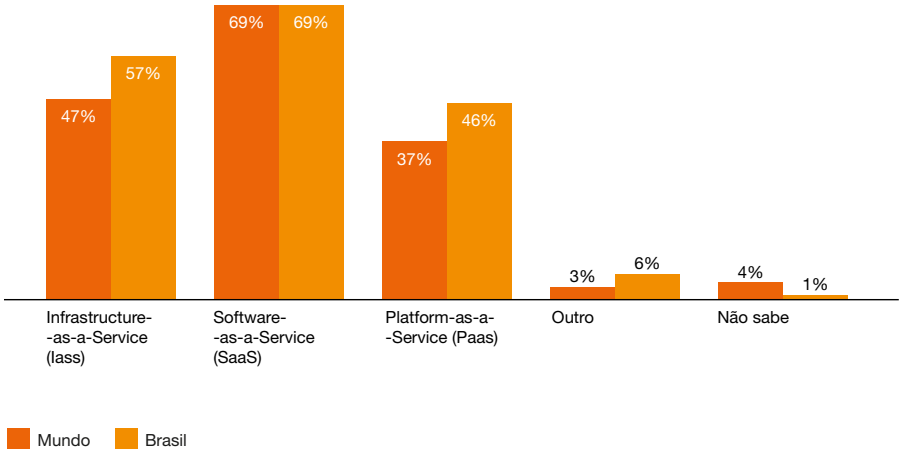
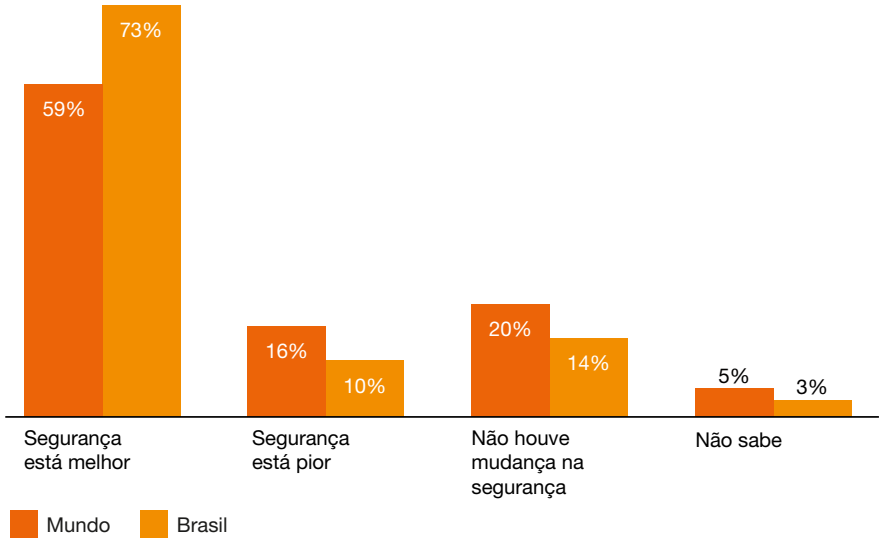


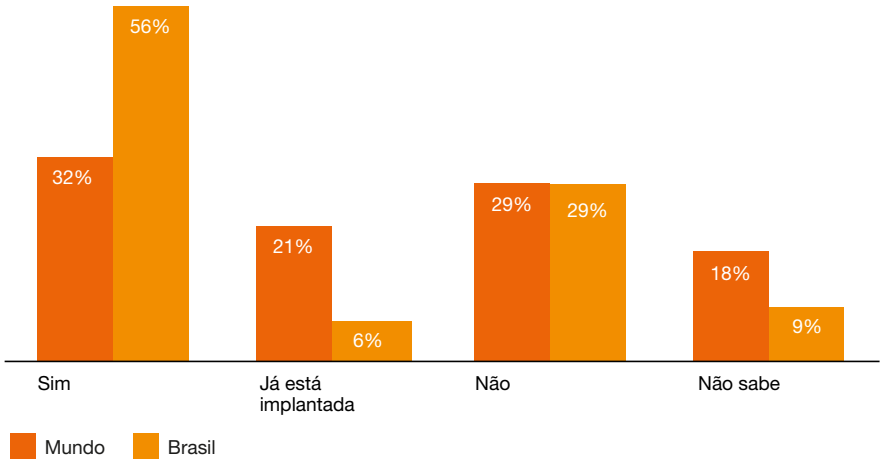
Figura 29: Como a computação em nuvem afeta a sua organização?



Carteiras virtuais

As carteiras virtuais têm se mostrado uma tendência e já há movimentos empresariais no sentido de adotá-las. Cerca de 56% dos respondentes declaram estar preparados para a implementação de sistemas que suportem as carteiras virtuais, porém apenas 6% disseram já tê-los implementado.

Figura 30: Sua organização está se preparando para implementar sistemas para suportar o conceito de carteiras digitais?

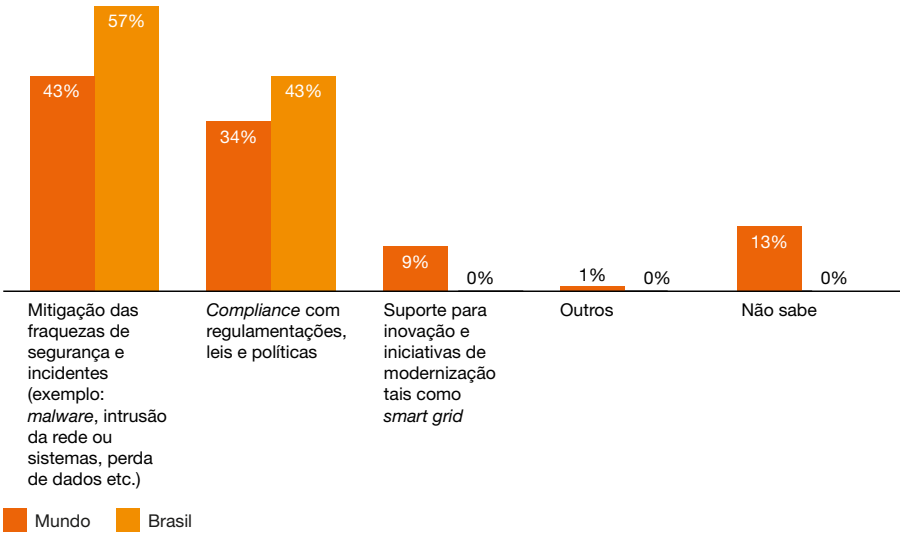


Cyber security

A atenção ao tema de *cyber security* tem se consolidado, em reação aos inúmeros casos de ataques digitais a governos, organizações e indivíduos no país. A veiculação desses casos pela mídia tem contribuído para que o tema esteja na pauta de discussões dos profissionais da área, bem como na agenda dos executivos.

As organizações já estão cientes de que as ameaças se sofisticaram, os motivadores das invasões são outros e que os controles atualmente empregados não são mais suficientes para conter tais ações.
Os resultados da pesquisa deste ano mostram que a mitigação das fraquezas de segurança e a contenção dos incidentes continuam sendo o maior direcionador dos gastos em *cyber security* no Brasil, assim como no restante do mundo. Esse aspecto nos leva a uma reflexão interessante sobre o nível de consciência das organizações a respeito da relevância dos temas de *cyber security* e *cyber investigation*.

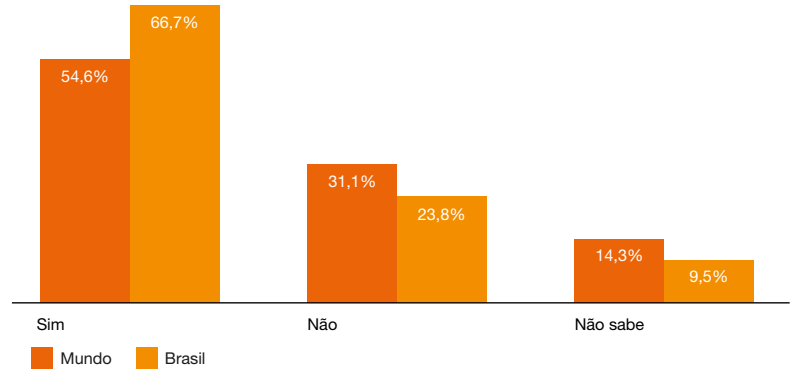
Figura 31: Principais direcionadores para os gastos de *cyber security* em sua organização



Outro aspecto que demonstra o nível de interesse e preparo das organizações sobre o tema de *cyber security* é o fato de que, no Brasil, 66,7% dos respondentes afirmaram possuir um *framework* integrado de competências para abordar os riscos de *cyber security*.

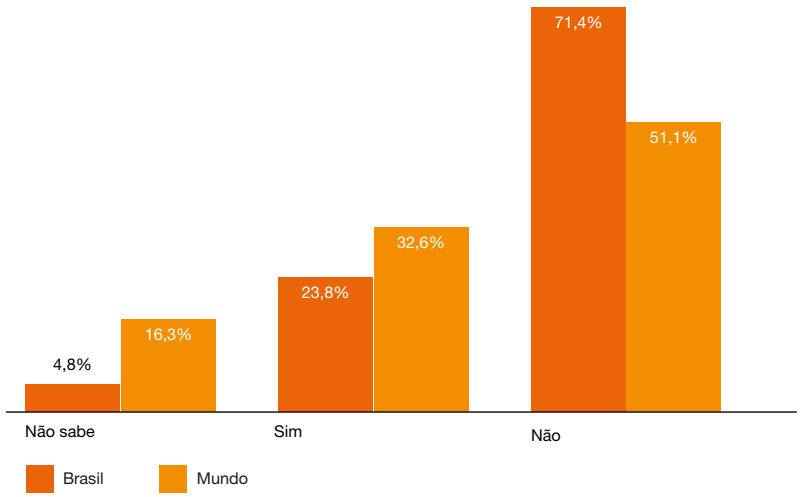
De fato, a contenção desses riscos demanda que as organizações façam investimentos coordenados em tecnologia, processos e pessoas. A antiga ideia de que um arsenal isolado de ferramentas tecnológicas seria suficiente para minimizar os riscos parece não ser mais uma realidade no presente.

Figura 32: A empresa adota um *framework* integrado para abordar os riscos de *cyber security*



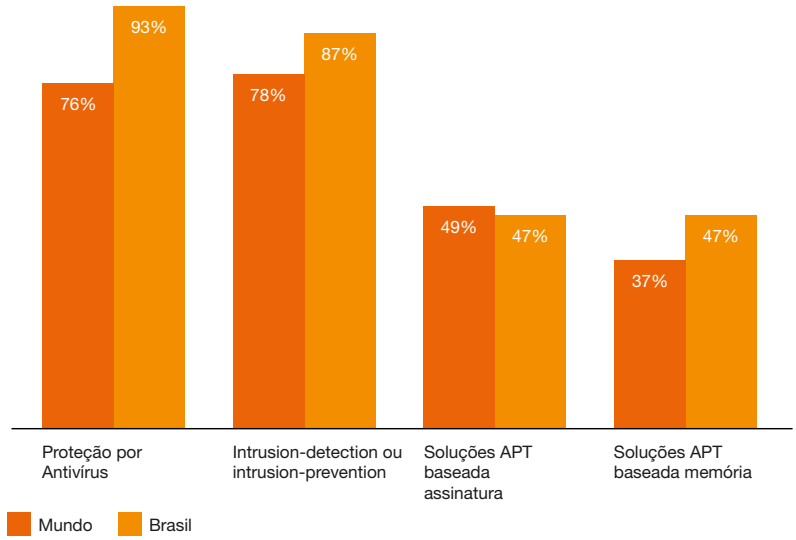
As ameaças persistentes avançadas foram responsáveis por boa parte dos incidentes de segurança da informação de grande impacto recentemente. As estratégias adotadas até então não cuidavam totalmente dessas ameaças, mas, após acontecimentos marcantes em alguns países, as organizações passaram a se preocupar mais com essas questões. A pesquisa mostra que, no Brasil, essa preocupação ainda é 20% maior do que no restante do mundo e que 71% dos respondentes declararam possuir um programa para monitorar e responder aos ataques de APT.

Figura 33: Quantidade de empresas que possuem um programa para monitorar e responder a APTs – *Advanced Persistent Threats*



Para combater as APTs, as empresas têm se baseado principalmente em soluções de segurança tradicionalmente empregadas, como antivírus, IDS e IPS. As soluções específicas para tratamento de APTs, sejam baseadas em memória ou assinatura, não são tão frequentes. Os respondentes no Brasil declaram que as soluções baseadas em memória fazem parte de suas realidades com mais frequência que os do restante do mundo. O mesmo não acontece com as baseadas em assinatura.

Figura 34: Tecnologias empregadas para se proteger contra APTs



O que isso significa para a sua empresa

Os resultados da Pesquisa Global de Segurança da Informação 2014 revelam que a área vive um momento incerto: encontra-se ao mesmo tempo no limiar da mudança e paralisada na inércia. Os participantes da pesquisa demonstram avanços na implantação de importantes iniciativas de segurança de um lado, mas parecem desatentos em relação a estratégias-chave, como proteção da propriedade intelectual, de outro. Há um compromisso renovado com o investimento em segurança, que convive com um direcionamento incerto sobre como melhorar as práticas.

Dadas as enormes mudanças e os desafios provocados pela evolução do ecossistema de ameaças, não surpreende por completo que o caminho a seguir seja ambíguo. Uma coisa é certa: as defesas do passado não são eficazes contra as ameaças atuais em rápida evolução. E os riscos futuros demandarão um modelo completamente novo de segurança da informação.

Sugerimos uma abordagem mais sofisticada do que pode ser a segurança, baseada no conhecimento das ameaças, dos ativos relevantes e dos inimigos. Uma abordagem na qual os incidentes de segurança sejam tratados como um risco crítico para o negócio que nem sempre pode ser prevenido, mas que pode ser gerenciado em níveis aceitáveis.

Identificamos esse modelo como "Da Consciência à Ação". No que tem de mais básico, essa abordagem abrange quatro preceitos importantes:

- **A segurança é um imperativo de negócios.** A segurança eficaz requer que se entenda a exposição e o impacto potencial de negócio associado a operar no ciberespaço, em um ecossistema global e interconectado de empresas. Uma estratégia de segurança integrada deve ser uma parte essencial do seu modelo de negócios; a segurança não é mais simplesmente um desafio de TI e nem apenas um conjunto de ações para proteger o negócio. A segurança deve ser definida com base em riscos e ter um direcionamento de criação de valor.

- **Ameaças de segurança são riscos de negócios.** Você deve ver os riscos de segurança como ameaças organizacionais. É essencial antecipar essas ameaças, conhecer as vulnerabilidades da organização e ser capaz de identificar e gerenciar os riscos associados. Assegure-se de que fornecedores, parceiros e outras organizações com quem se relaciona conheçam – e concordem em aderir a – suas políticas e práticas de segurança.

- **Proteja as informações que realmente importam.** Uma segurança eficaz requer que você entenda as mudanças no ambiente de ameaças e se adapte a elas, identificando suas informações mais valiosas. Saiba onde estão localizadas essas "joias da coroa" e quem tem acesso a elas o tempo todo. Aloque e priorize, de modo competente, os recursos da organização para proteger suas informações mais valiosas.

- **Ganhe vantagem com o modelo "Da Consciência à Ação".** Nesse novo modelo de segurança da informação, todas as atividades e todos os investimentos devem estar baseados no melhor conhecimento disponível sobre ativos de informação, ameaças e vulnerabilidades do ecossistema e monitoramento de atividades de negócios. Você deve criar uma cultura de segurança que comece com o compromisso dos principais executivos e se desdobre para todos os funcionários e terceiros. Participe de projetos de colaboração público-privada com outras organizações para melhorar os conhecimentos sobre ameaças.

Podemos ajudá-lo a entender as implicações dessa nova abordagem de segurança da informação e a aplicar seus conceitos às necessidades exclusivas da sua empresa, do seu setor e do seu ambiente de ameaças. Podemos mostrar a você como combater de forma eficaz os riscos de segurança atuais e como planejar sua proteção contra os riscos futuros.

Para obter mais informações, entre em contato com:

São Paulo e Barueri
Av. Francisco Matarazzo, 1400
05001-903 – São Paulo/SP
Torre Torino – Água Branca
Telefone: (11) 3674-2000

Edgar R. P. D'Andrea
edgar.dandrea@br.pwc.com

Eliane Kihara
eliane.kihara@br.pwc.com

Sergio Alexandre
sergio.alexandre@br.pwc.com

Ana Rosa
ana.rosa@br.pwc.com

Claudinei Vieira
claudinei.vieira@br.pwc.com

Viviane Oliveira
viviane.oliveira@br.pwc.com

Camilla Gemelli
camila.gemelli@br.pwc.com

Claudia Fukasawa
claudia.fukasawa@br.pwc.com

João Castilho
joao.castilho@br.pwc.com

Maria Román
maria.roman@br.pwc.com

Mauricio Baldin
mauricio.baldin@br.pwc.com

Rio de Janeiro
Av. José Silva de Azevedo Neto,
200 – 1º e 2º Torre Evolution IV,
Barra da Tijuca
22775-056 – Rio de Janeiro/RJ
Telefone: (21) 3232-6112

Rodrigo Milo
rodrigo.milo@br.pwc.com

Eduardo Luczinski
eduardo.luczinski@br.pwc.com

Região Centro Oeste
SHS Quadra 6, Conj. A –
Bloco C – Edifício Business
Center Tower – Salas 801 a 811
CEP: 70322-915 – Brasília –
Distrito Federal
Telefone: (61) 2196-1800

Fernando Bravo
fernando.bravo@br.pwc.com

Região Nordeste e Norte
Av. Tancredo Neves, 620 - 30º e 34º
Ed. Empresarial Mundo Plaza
41820-020 – Salvador/BA
Telefone: (71) 3319-1900

Ricardo Santana
ricardo.santana@br.pwc.com

Bruno Barros
bruno.barros@br.pwc.com

Interior de São Paulo
Rua José Pires Neto, 314 - 10º
13025-170 – Campinas/SP
Telefone: (19) 3794-5400

Edmilson Monutti
edmilson.monutti@br.pwc.com

Região Sul
Rua Mostardeiro, 800 – 8º e 9º
Edifício Madison Center
90430-000 – Porto Alegre/RS
Telefone: (51) 3378-1700

Jerri Ribeiro
jerri.ribeiro@br.pwc.com

Renato Lara
renato.lara@br.pwc.com

Ou visite www.pwc.com/gsiss2014 para conhecer os dados detalhados do seu setor de atuação ou fazer um *benchmarking* da sua empresa.

Siga-nos Twitter@PwCBrasil

facebook.com/PwCBrasil