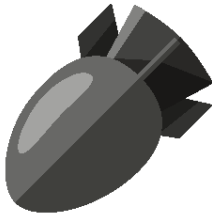
2ª Pesquisa ANBIMA de Cibersegurança

2018

ANBIMA

ÍNDICE

APRESENTAÇÃO



Os cuidados com a segurança cibernética recebem atenção de **85% das instituições** dos mercados financeiro e de capitais – um avanço em relação a 2017, quando essa proporção, referente às empresas que têm um programa formal sobre o tema, era de 71%.

É o que mostra a **2ª Pesquisa ANBIMA de Cibersegurança**. Frente ao crescimento das ameaças cibernéticas e ao entendimento do mercado de que este é um item de importância sistêmica, a pesquisa buscou compreender como as instituições associadas têm se comportado em relação a diferentes aspectos: o mercado está preparado para identificar riscos e se recuperar de possíveis incidentes? Como as instituições reagem frente a um ataque?

As respostas deste relatório **medem o grau de maturidade do mercado local em cibersegurança**, bem como atualizam a fotografia obtida em 2017. Os resultados servirão como base para nortear as próximas ações da ANBIMA no tema, buscando auxiliar os integrantes do mercado na implementação e no fortalecimento dessas práticas.

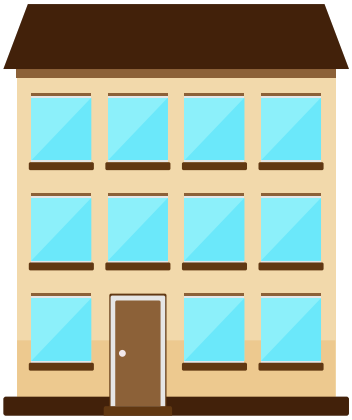
85% das instituições do mercado têm um programa formal de segurança cibernética

A PESQUISA

Realizada entre novembro e dezembro de 2018, a segunda edição da pesquisa mostra a evolução das instituições em relação às práticas de segurança cibernética. As perguntas do ano anterior foram mantidas e atualizadas, de forma a permitir o acompanhamento do tema. Os resultados mostram o nível de adesão das instituições ao **Guia de Cibersegurança da ANBIMA** e indicam pontos de atenção que podem ser foco de ações para 2019.

Confira a **primeira edição da Pesquisa de Cibersegurança** e as demais ações do **Grupo Técnico de Cibersegurança**

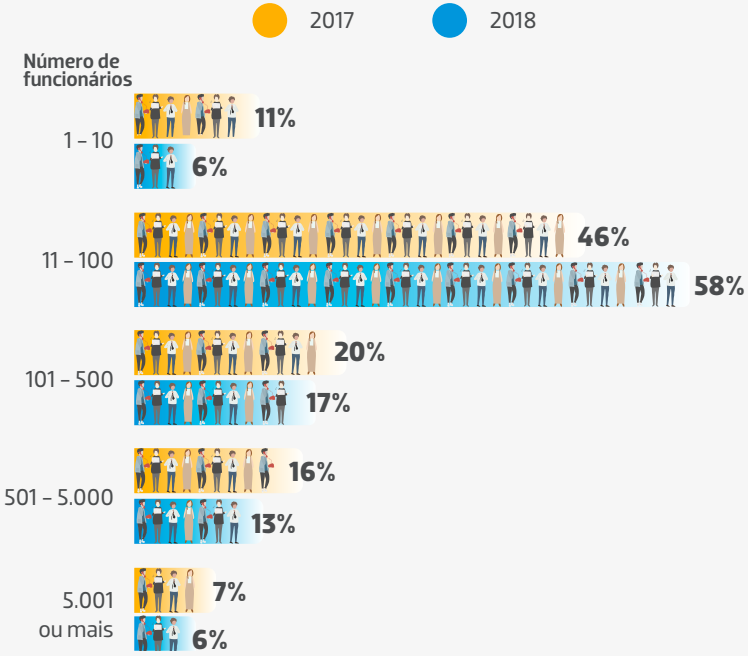
PERFIL DAS INSTITUIÇÕES



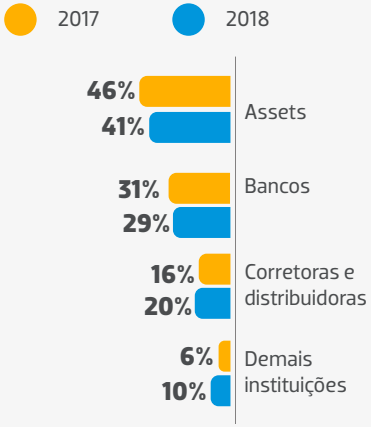
A pesquisa foi respondida por 177 instituições, ou 68% dos 259 associados da ANBIMA – o volume é dez pontos percentuais maior que o obtido em 2017. Mais da metade é representada por instituições que têm entre 11 e 100 funcionários (58%) e em maior parte são assets (41%). O aumento da amostra reduz potencialmente o viés de seleção* da primeira edição da pesquisa, pois inclui outras instituições e pode explicar pequenas variações de valores encontrados ao longo de dois anos da pesquisa.

*Quando a amostra não é aleatória e um grupo de participantes é menos provável de ser incluído nos resultados da pesquisa do que outro.

Tamanho das instituições em número de funcionários



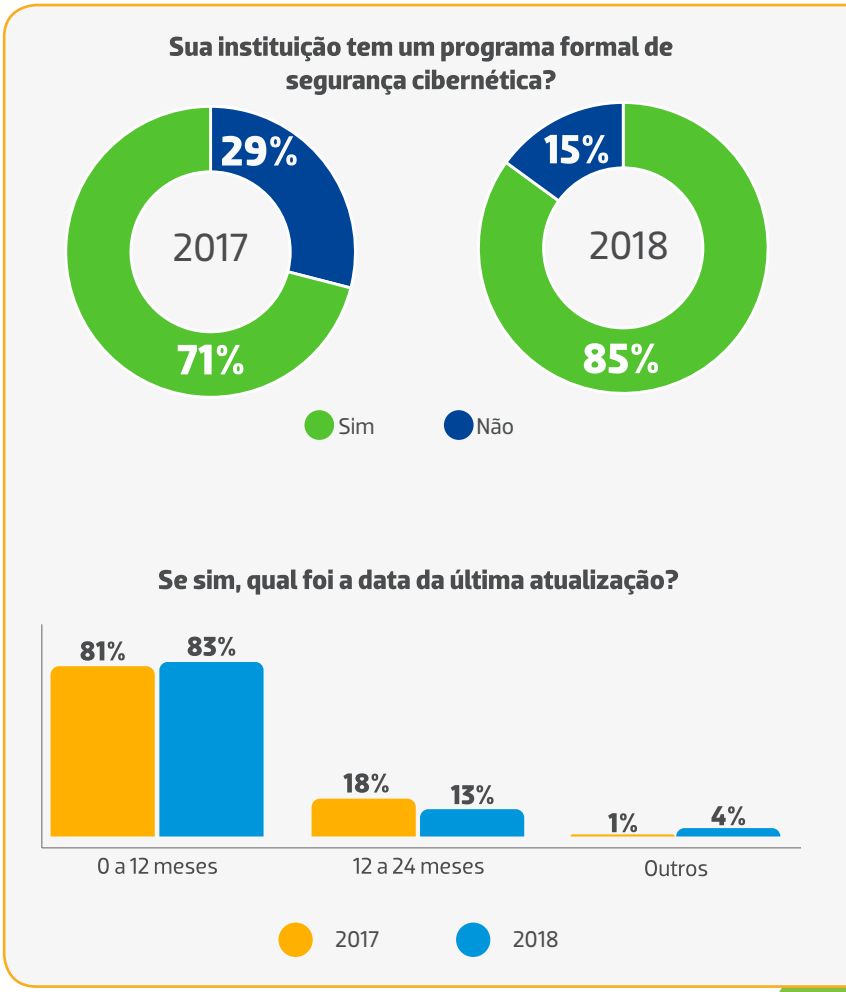
Tipos de instituição por atividade



1. PROGRAMA DE SEGURANÇA CIBERNÉTICA

Um programa formal sobre o tema já é realidade para 85% das instituições – significativo avanço em relação a 2017, de 14 pontos percentuais. Dentre elas, 83% promoveram atualizações no último ano. A frequência de revisão do documento também se mostrou como prioridade para as empresas. Entre aquelas que ainda não possuem o programa, mais de 76% pretendem implantá-lo no próximo ano.

De acordo com o **Guia de Cibersegurança da ANBIMA**, esse programa deve conter pelo menos cinco funções bem definidas: identificação e avaliação de riscos (risk assessment); ações de prevenção e proteção; ações de monitoramento e testes; medidas relacionadas ao plano de resposta; e ações de reciclagem e revisão.



Em quase todas as instituições (95%), há um **profissional responsável** pelas questões de cibersegurança. Esse percentual é de 90% entre as corretoras e de 93% no caso das assets. De modo geral, essa pessoa está na área de TI ou de segurança da informação, mas há também aquelas em compliance e, mais raramente, em riscos.

Pouco mais da metade (57%) das empresas criou um **comitê, fórum ou grupo específico** para tratar o tema, com representação e governança apropriados – um avanço de 15 pontos percentuais em comparação a 2017. No caso das assets, o crescimento é ainda maior: 45% diante de 27% no ano anterior.

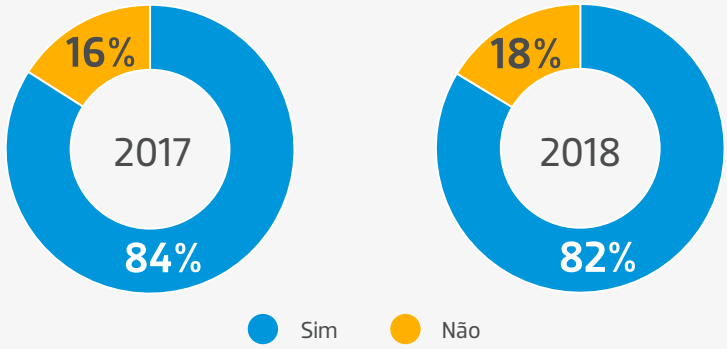
1.1 Avaliação de riscos

Identificar os riscos a que a instituição está sujeita (risk assessment) é uma prática para 82% das instituições – volume um pouco menor que o encontrado no ano anterior (84%). O recuo também foi observado nas assets.

Essa avaliação inclui **identificar ameaças internas e externas**, além de mapear processos, hardwares e softwares que precisam de proteção.

Entre aquelas que avaliam riscos, 54% elaboram regras para a classificação das informações geradas pela instituição, permitindo a implementação de processos para o devido manuseio, armazenamento, transporte e descarte dessas informações. Além disso, 59% mensuram os possíveis impactos financeiros, operacionais e reputacionais de um ataque cibernético, e 51% estabelecem uma metodologia para as avaliações – resultados superiores aos de 2017.

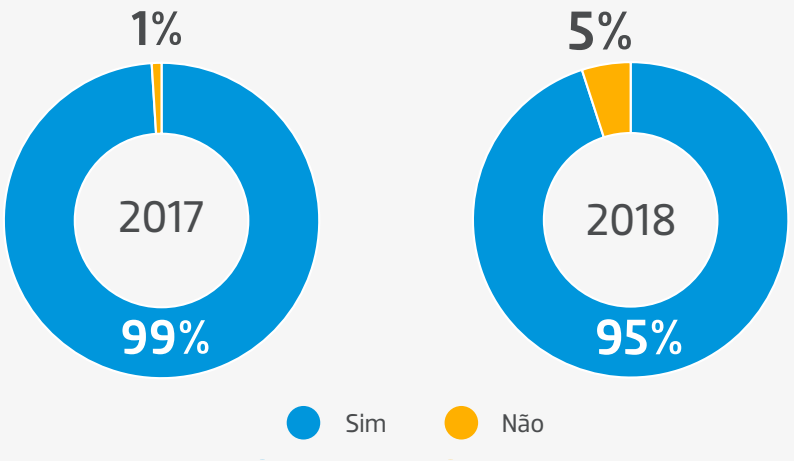
Sua empresa realiza avaliação de riscos?



1.2 Ações de prevenção e proteção

Uma vez definidos os riscos, 95% das instituições atuam preventivamente para impedir os ataques – redução de quase quatro pontos percentuais em relação a 2017.

Definidos os riscos, sua instituição adota ações de prevenção e proteção?

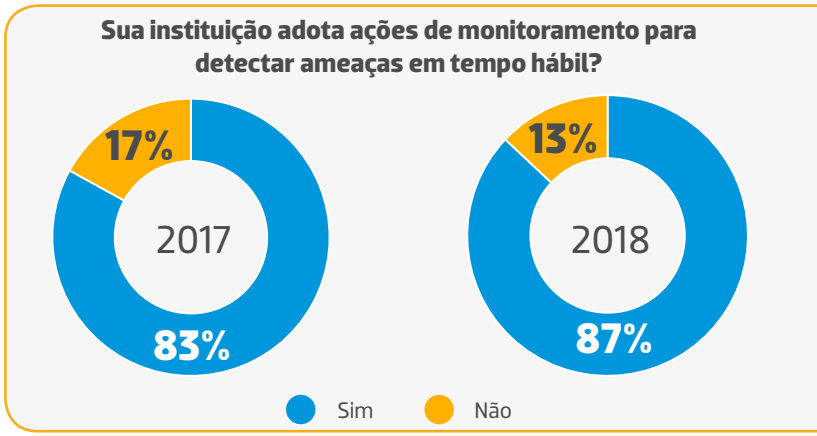


Dentre elas, mais de **90%** declaram adotar medidas e ações nos seguintes pontos:

Na hora de contratar serviços de terceiros, 76% realizam diligência e avaliam questões jurídicas, cláusulas de confidencialidade e exigem controles de segurança na estrutura dos fornecedores – um incremento de quatro pontos percentuais em relação a 2017. Os bancos alcançam 81% e as assets, 68%. Por outro lado, apenas 32% das instituições têm um programa periódico para essa avaliação.

1.3 Monitoramento e testes

Ações de monitoramento para detectar ameaças são adotadas por 87% das empresas, que reforçam os controles, caso necessário, e identificam possíveis irregularidades no ambiente tecnológico, como a presença de usuários, componentes ou dispositivos não autorizados. O mesmo engajamento é encontrado entre as assets, que evoluíram seis pontos percentuais de 2017 para 2018.



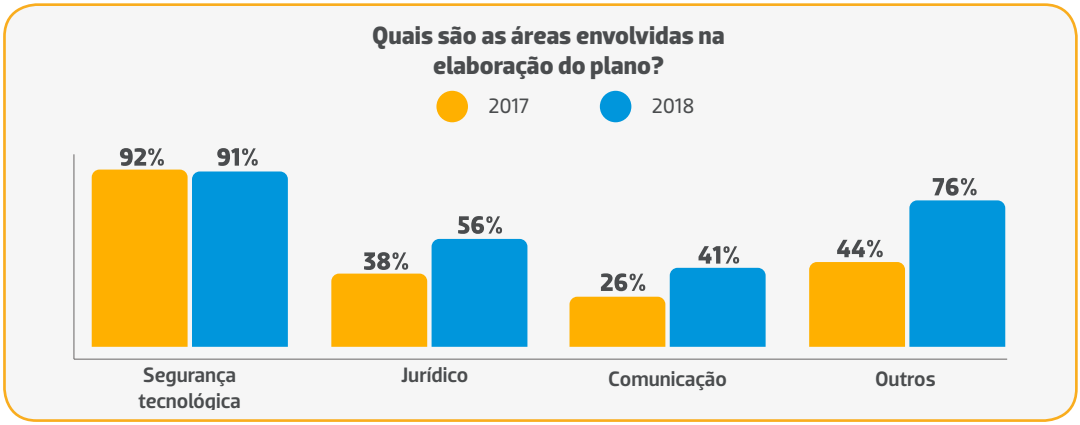
A maioria das instituições (92%) mantém os sistemas operacionais e softwares atualizados. Na comparação com 2017, houve aumento de sete pontos percentuais nas empresas que mantêm inventários atualizados de hardware e software e os verifica com frequência.

Com relação ao monitoramento de logs e trilhas de auditoria, 84% os criam sempre que os sistemas permitem. A análise desses materiais é prática constante para 70%, o que auxilia na rápida identificação de ataques, e 50% utilizam ferramentas de centralização e análise de logs.

1.4 Criação do plano de resposta a incidentes

Na hora de reagir aos ataques, 76% das instituições têm um plano de resposta, tratamento e recuperação de incidentes, incluindo ações de comunicação interna e externa. Dentre elas, apenas metade (53%) testa o plano e todas o fazem com intervalos menores que um ano (51% e 100%, respectivamente, em 2017).

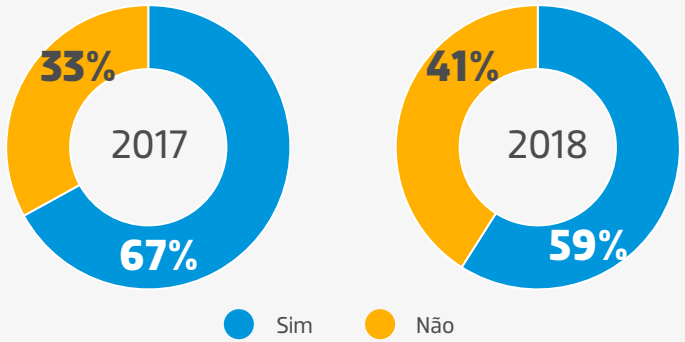
De modo geral, os planos são elaborados por equipes interdisciplinares – integração que aumentou de 2017 para 2018 –, envolvendo as áreas de segurança tecnológica, jurídico, comunicação, compliance e riscos.



As ameaças previstas na avaliação de riscos estão nos planos de resposta de 75% das instituições, porcentagem próxima à observada em 2017. Um ponto de destaque foi a redução daquelas que apresentam critérios para classificação dos incidentes por severidade.

Os papéis e as responsabilidades de cada profissional dentro do plano estão definidos em 73% das empresas, prevendo o acionamento de funcionários-chaves e de contatos externos – um recuo em relação a 2017. Nesses casos, aproximadamente um terço delas não faz testes com essas pessoas para validar a eficácia do processo.

Há critérios para classificação dos incidentes por severidade?



Todas as empresas afirmaram ter um **plano de continuidade dos negócios e processos de recuperação**, incluindo restauração, reconstrução ou substituição dos sistemas e bases de dados impactados (96% em 2017). Questões de segurança e controles de acesso são consideradas também nas instalações de contingência para 95% das instituições (indicador próximo ao 2017). O percentual é o mesmo das que arquivam documentações sobre o gerenciamento de incidentes e o plano para servir como evidência em eventuais questionamentos (dez pontos percentuais acima do observado em 2017).

Quanto às iniciativas voltadas para o compartilhamento de informações sobre incidentes cibernéticos, é possível observar que essa ainda é uma questão em evolução para os participantes do mercado local. Embora o percentual de instituições que afirmaram já participar de alguma iniciativa nesse sentido tenha aumentado – de 11% para 26% – entre 2017 e 2018, a comparação dos números absolutos aponta para uma estabilidade nesse grupo de instituições entre os dois períodos – dez companhias.

Em 2017, um número elevado de instituições respondeu negativamente a essa pergunta, enquanto em 2018, foi mantido o número de respostas positivas entre os participantes – mas o universo de entrevistados caiu significativamente. Esse resultado pode estar refletindo um maior número de instituições que estão considerando a adoção dessas soluções, ainda que sem

efetivá-las, ou que estão em vias de aderirem a uma delas. De fato, as discussões na ANBIMA a esse respeito vêm revelando que, por um lado, as alternativas de compartilhamento já existentes ainda são acessíveis a um grupo limitado de instituições por questões de porte e atuação global ou ainda não estão representadas por ferramentas robustas de troca de informações em nível local. Nos diversos países, a participação em plataformas ou outras soluções semelhantes também é discutida, verificando-se, inclusive, a adesão de instituições a câmaras já consolidadas – como a FS-ISAC. Outras alternativas e soluções locais estão sendo analisadas em outros países e no Brasil.

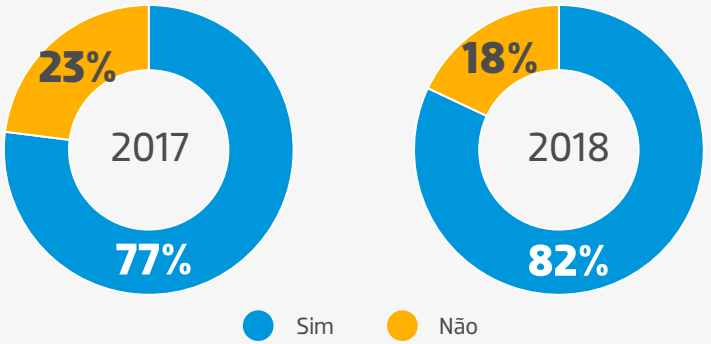
As iniciativas de compartilhamento citadas incluem fóruns da Febraban, ABBC (Associação Brasileira de Bancos) e da FS-ISAC (Centro de Compartilhamento e Análise de Informações Financeiras)

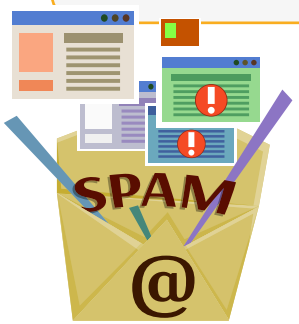
1.5 Reciclagem e revisão

Identificar novos riscos, ativos e processos, bem como os riscos residuais do programa de segurança cibernética, mantendo-o sempre atualizado, são ações realizadas por 82% das empresas. Entre elas, a revisão do programa é feita com frequência de até um ano em 88% dos casos e de um a dois anos para 12% delas (valores de 79% e 19%, respectivamente, em 2017).

Os grupos de profissionais envolvidos com o programa se mantêm atualizados sobre vulnerabilidades e ameaças em 87% dos respondentes. Para essas instituições, as informações são obtidas pelos próprios funcionários, ou seja, por meio de esforço interno (75%); por fornecedores especializados (70%); e pela participação em grupos de compartilhamento de informações (9%).

O programa de segurança cibernética é revisado periodicamente, mantendo seus tópicos sempre atualizados?





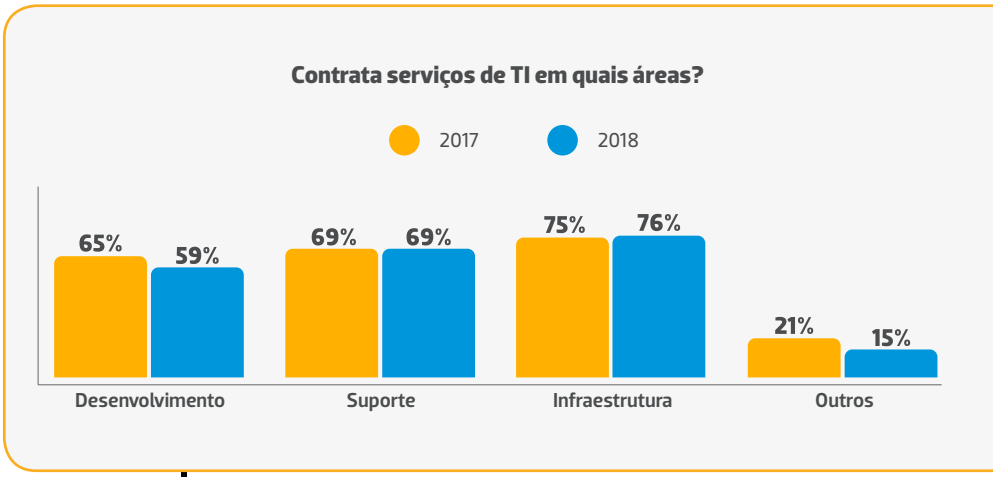
Aproximadamente 75% promovem e disseminam uma **cultura** sobre o tema, utilizando a comunicação interna para divulgar o programa de segurança cibernética, conscientizar sobre riscos, boas práticas, treinamentos e repasse de novas orientações (76% em 2017). Relativamente a ações de conscientização, 80% declararam ter alguma política de uso adequado da estrutura tecnológica, de forma independente ou como parte de um documento mais abrangente (86% em 2017).

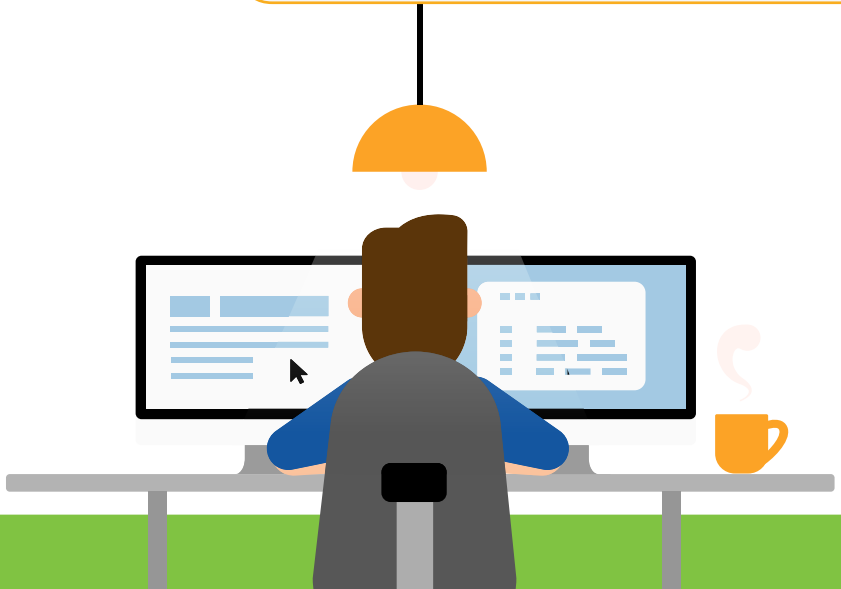
No entanto, esse programa é divulgado aos prestadores de serviços de menos da metade das instituições (47%). Os mecanismos de acompanhamento de controles e indicadores de desempenho (key performance indicators) são definidos e mantidos por apenas 37% dos associados. Esses programas auxiliam no envolvimento da alta administração da empresa e na implementação da política, do plano de ação e de resposta a incidentes. Ainda que pequeno, o valor representa aumento em relação aos 30% de 2017.

2. CONTRATAÇÃO DE SERVIÇOS TERCEIRIZADOS DE TI

Os serviços de TI são terceirizados por 84% das instituições, principalmente nas áreas de infraestrutura e suporte (valor próximo ao de 2017). Metade delas exige relatórios periódicos para acompanhar a qualidade das atividades prestadas – cinco pontos percentuais abaixo do que o encontrado em 2017.

Os bancos são os que mais recorrem a esses serviços (93%), optando, em sua maioria (89%), por contratos de desenvolvimento de TI. As corretoras e assets terceirizam em 85% e 83% dos casos, respectivamente.



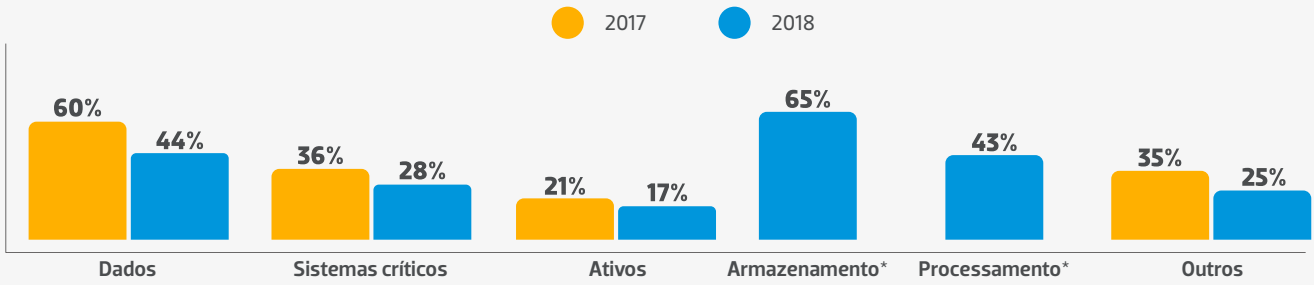


3. COMPUTAÇÃO EM NUVEM

Os ativos das empresas são mantidos interna ou externamente, muitas vezes em nuvem. Esse armazenamento cresceu quatro pontos percentuais em 2018, alcançando 79% das instituições. No caso das assets, chega a 85%, uma redução de cinco pontos percentuais em relação a 2017.

A maioria utiliza nuvem para armazenamento, processamento e sistemas críticos, mas também para outros serviços, como backup de arquivos, e-mail, contingência, serviços executados com sistemas não críticos e sites. No caso das assets, a utilização para armazenamento ocorre na maioria: 75%.

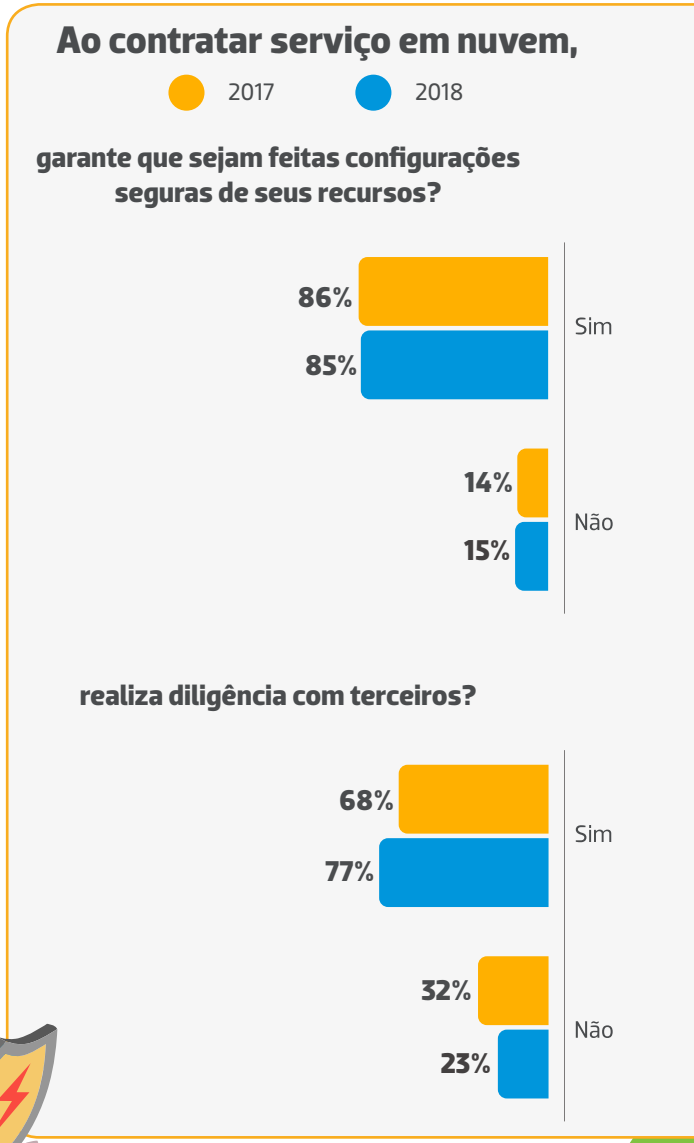
Quais serviços sua instituição contrata por computação em nuvem?

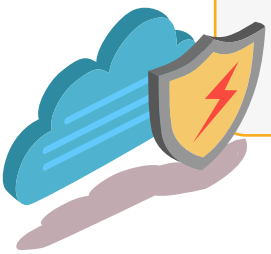


*Opções incluídas na pesquisa de 2018.

A computação em nuvem pode ser considerada uma contratação de serviço de terceiros, de acordo com organismos internacionais, como **Nist** (Instituto Nacional de Padrões e Tecnologia) e **FFIEC** (Conselho Federal de Análise das Instituições Financeiras), o que envolve alguns riscos. No Brasil, o tema tem sido bastante discutido nos últimos anos e foi regulamentado pela Resolução CMN 4.658, que trouxe uma série de salvaguardas e cuidados contratuais para essas contratações e requisitos adicionais no caso de contratação do serviço no exterior.

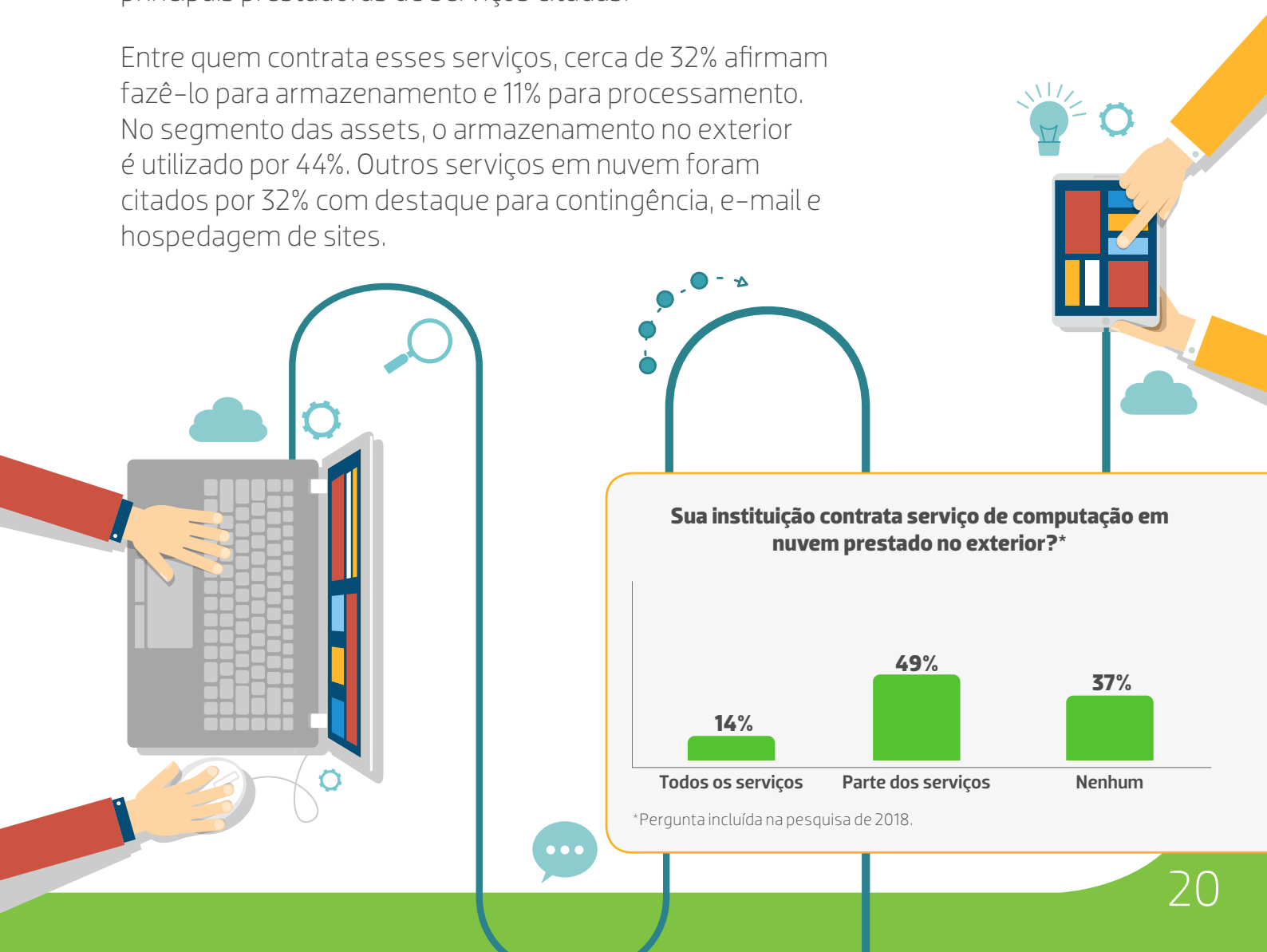
Assim como em 2017, grande parte dos entrevistados (85%) e a totalidade das corretoras respondentes garantem que são feitas configurações seguras de seus recursos. A maioria também realiza diligência na contratação de serviços em nuvem, com aumento de nove pontos percentuais em 2018.





Mais da metade das instituições contrata esses serviços de computação em nuvem no exterior. Estados Unidos é o país que mais recebe dados e informações de empresas brasileiras, com Amazon, Microsoft e Google sendo as principais prestadoras de serviços citadas.

Entre quem contrata esses serviços, cerca de 32% afirmam fazê-lo para armazenamento e 11% para processamento. No segmento das assets, o armazenamento no exterior é utilizado por 44%. Outros serviços em nuvem foram citados por 32% com destaque para contingência, e-mail e hospedagem de sites.



Sua instituição contrata serviço de computação em nuvem prestado no exterior?*

*Pergunta incluída na pesquisa de 2018.

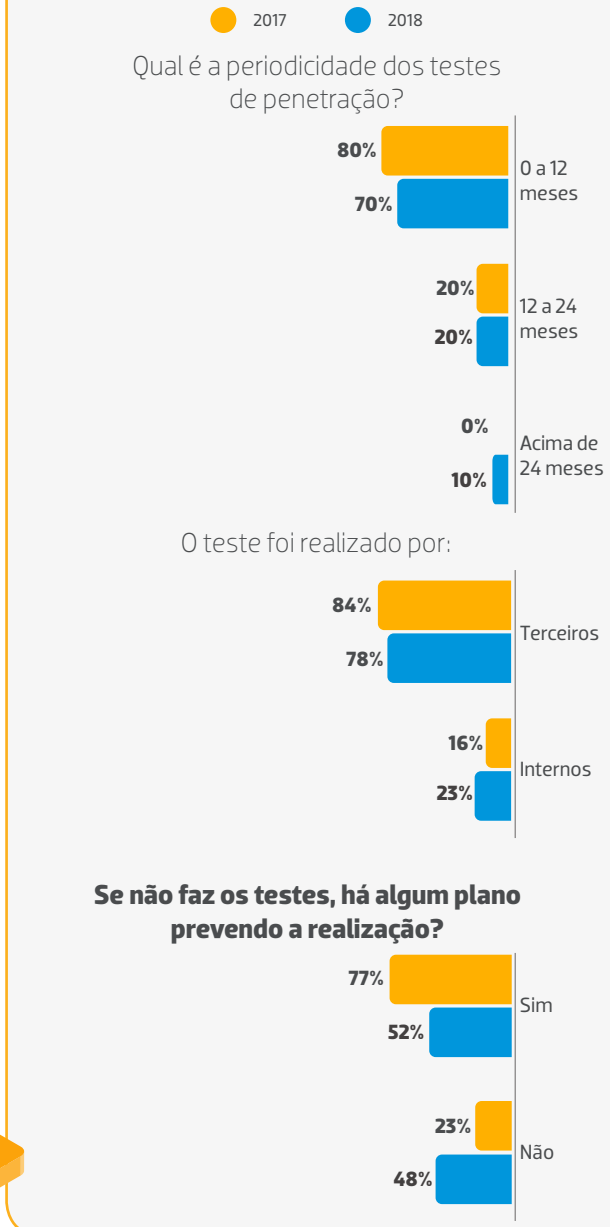
4. TESTES

4.1 Testes externos de penetração

Testar a capacidade de proteção da empresa em caso de invasão externa é uma atividade realizada por 56% das instituições (53% em 2017). Os testes são feitos anualmente por 70% e por meio de terceiros em 78% dos casos.

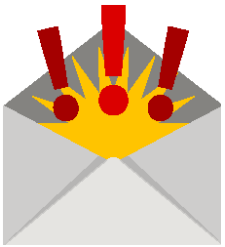
Dentre os 44% que não realizaram esses testes no último ano, 52% têm planos para fazê-lo, valor mais baixo do que o obtido em 2017. No caso das corretoras, 65% não fizeram testes no ano anterior e, destas, 55% têm planos para colocá-los em prática. Em relação às assets, 60% não realizaram teste externo de penetração (três pontos percentuais abaixo do que constatado em 2017) – desse conjunto, 67% preveem algum plano para fazê-lo. O aumento da realização entre 2017 e 2018 mostra maior preocupação com a segurança cibernética.

Entre aquelas que realizam os testes...

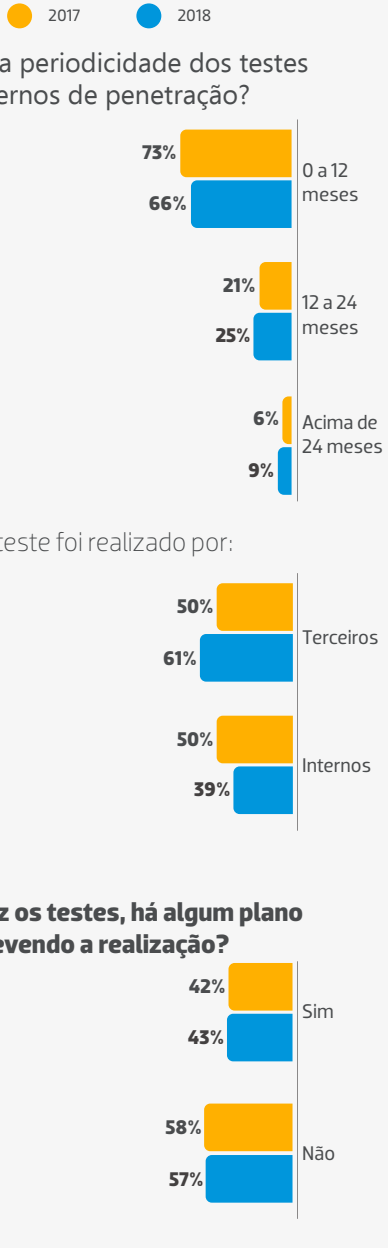


4.2 Testes internos de penetração

Os testes internos são feitos por 58% das instituições: 66% delas o realizam anualmente e 61% utilizam serviços de terceiros para essa atividade. O número caiu em relação a 2017 (63%), e, quando realizados, tiveram maior participação de terceiros. A periodicidade de até um ano diminuiu, enquanto cresceu a realização entre um e dois anos e outros períodos. Entre aquelas que não fizeram testes internos de penetração, apenas 43% têm planos de realizá-lo.



Entre aquelas que realizam os testes...



Se não faz os testes, há algum plano prevendo a realização?

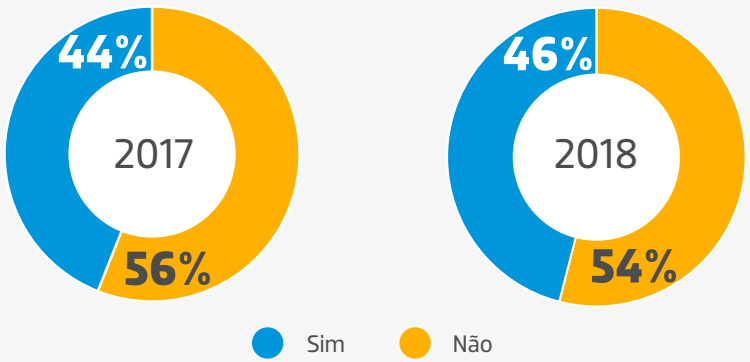
4.3 Phishing

Menos da metade das empresas (46%) fez testes de phishing, proporção semelhante a 2017 (44%). Eles compreendem o envio de links por e-mail para os funcionários, simulando uma pessoa ou empresa confiável passando um comunicado oficial, com o objetivo de obter informações confidenciais. A ideia é ver se os profissionais acreditam e clicam no material ou o descartam por suspeita.

O aumento nas assets é notável, já que em 2017 esse percentual era de apenas 29% e chegou a 40% em 2018. Já entre as corretoras, houve uma redução de 28 pontos percentuais (47% em 2017 e 19% em 2018).

De modo geral, 93% das instituições participantes afirmam a existência de alguma orientação aos usuários quanto a ter atenção especial antes de clicar em links recebidos, mesmo vindos de pessoas conhecidas – esse percentual foi de 91% em 2017.

Sua instituição realizou exercício de phishing no último ano?

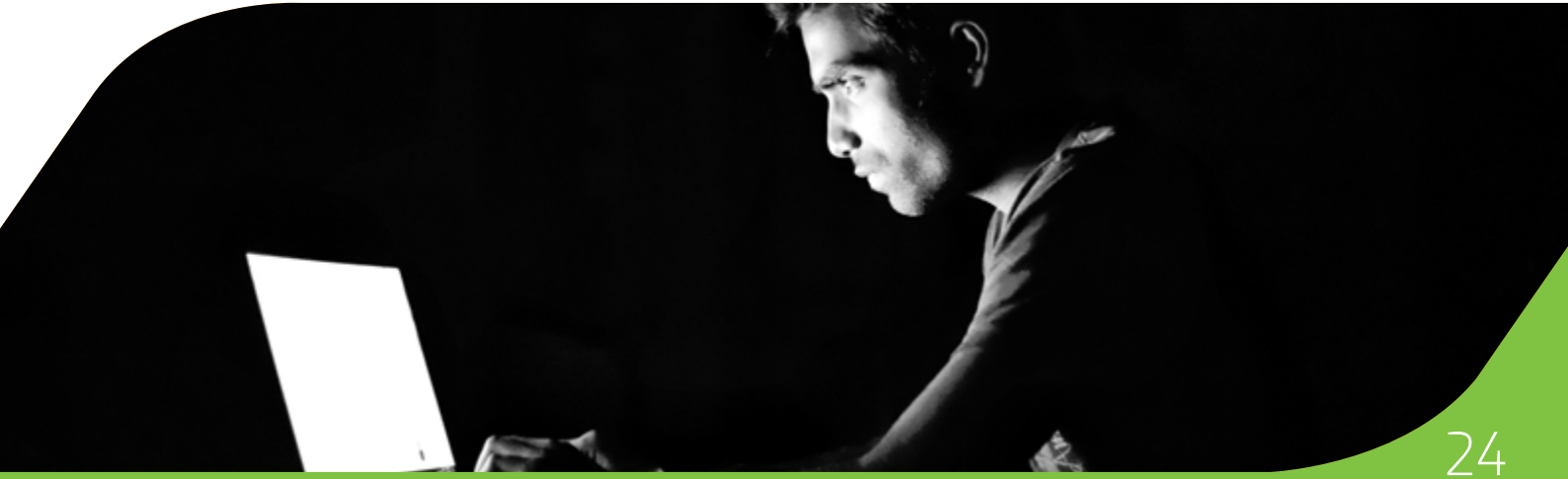


5. REGULAÇÃO

Com o aumento das ameaças virtuais, cresce também a cautela dos reguladores sobre o tema. Novas normas foram editadas em 2018 e outras já foram aprovadas para entrar em vigor em breve – por isso, o tema entrou para a segunda edição da pesquisa. As respostas mostraram que cerca de 52% já contemplam essas normas em suas políticas de segurança cibernética.

O atendimento à **Resolução 4.658** do CMN é mencionado por 55% das empresas. Na sequência, a categoria "outros", marcada por 19%, inclui o **Código ANBIMA de Administração de Recursos de Terceiros**, o próprio **Guia de Cibersegurança** e a **Circular 3.909** (que traz normas de segurança virtual para as instituições de pagamento). A **GDPR** (Lei Geral Europeia de Proteção de Dados) é citada por 14% das instituições e a Lei de Proteção de Dados no Brasil (13.709/18), por 11%.

No quesito regulação, houve muitas citações de instituições afirmando que estão se adaptando às normas vigentes. Em relação aos bancos – múltiplos, de investimento e comerciais –, cerca de 74% dos participantes já estão com programas em acordo com a Resolução 4.658. Em relação à lei de proteção de dados, 20% das assets já estão com seus programas adequados à regulação.



CONCLUSÃO

A segunda edição da Pesquisa ANBIMA de Cibersegurança mostrou uma evolução no grau de maturidade dos associados em relação às principais questões sobre o tema. A maioria mantém um programa formal nessa área e segue diversos procedimentos do Guia de Cibersegurança da Associação. Os aspectos principais de um programa eficiente incluem identificação e avaliação de riscos; ações de prevenção e proteção; monitoramento e testes; criação do plano de resposta; e reciclagem e revisão.

Um outro aspecto observado é que em alguns grupos de requisitos da pesquisa, enquanto os resultados gerais refletiram avanços sensíveis entre 2017 e 2018 – risk assessment, por exemplo – ações ou elementos específicos desses componentes registraram resultado oposto, em alguns poucos casos com recuos também significativos. Parte desse comportamento pode ser explicado pelo aumento do universo de participantes da pesquisa, o que sempre pode afetar de forma diferenciada a comparabilidade de resultados. Um outro fator a ser considerado é a característica de maior interdisciplinaridade que vem sendo demonstrada pelo desenvolvimento e acompanhamento das políticas de cibersegurança, o que pode estar levando a mudanças na distribuição das tarefas que integram os respectivos componentes nas áreas. Houve um aumento percentual das instituições que afirmaram participar de iniciativas de compartilhamento

de informações, mas representando em mesmo número de instituições em termos absolutos nesses anos. Um menor número de empresas respondeu esta questão em 2018, o que explica o aumento do indicador em termos relativos.

Os testes externos de penetração tiveram valores maiores que em 2017, especialmente para alguns segmentos, como gestoras de recursos – com alerta para a redução do número de empresas que pretendem realizar o teste, dentre aquelas que não o fizeram no último ano. Também se destacam os serviços em nuvem: além do alto índice de utilização, houve maior preocupação em relação à diligência com esses contratados.

Esses dados servirão para basear a agenda de atividades do Grupo Técnico de Cibersegurança da ANBIMA em 2019. O tema integra o plano de ação de 2019 da Associação, com destaque para a continuidade das ações de compartilhamento de testes e de informações sobre incidentes voltadas para o fortalecimento do mercado de forma sistêmica. As informações são relevantes, ainda, para fomentar o debate entre associados, reguladores e demais players.

2ª Pesquisa ANBIMA de Cibersegurança

Realização da Pesquisa
Grupo Técnico de Cibersegurança
Superintendência de Representação Institucional
(Estudos Regulatórios)

Edição
Flávia Nosralla

Diagramação
José Carlos Oliveira

Rio de Janeiro
Praia de Botafogo, 501 – 704, Bloco II – Botafogo,
Rio de Janeiro – RJ – CEP: 22250-042
Tel.: (21) 3814-3800

São Paulo
Av. das Nações Unidas, 8501, 21° andar, Pinheiros,
São Paulo – SP – CEP: 05425-070
Tel.: (11) 3471-4200

www.anbima.com.br