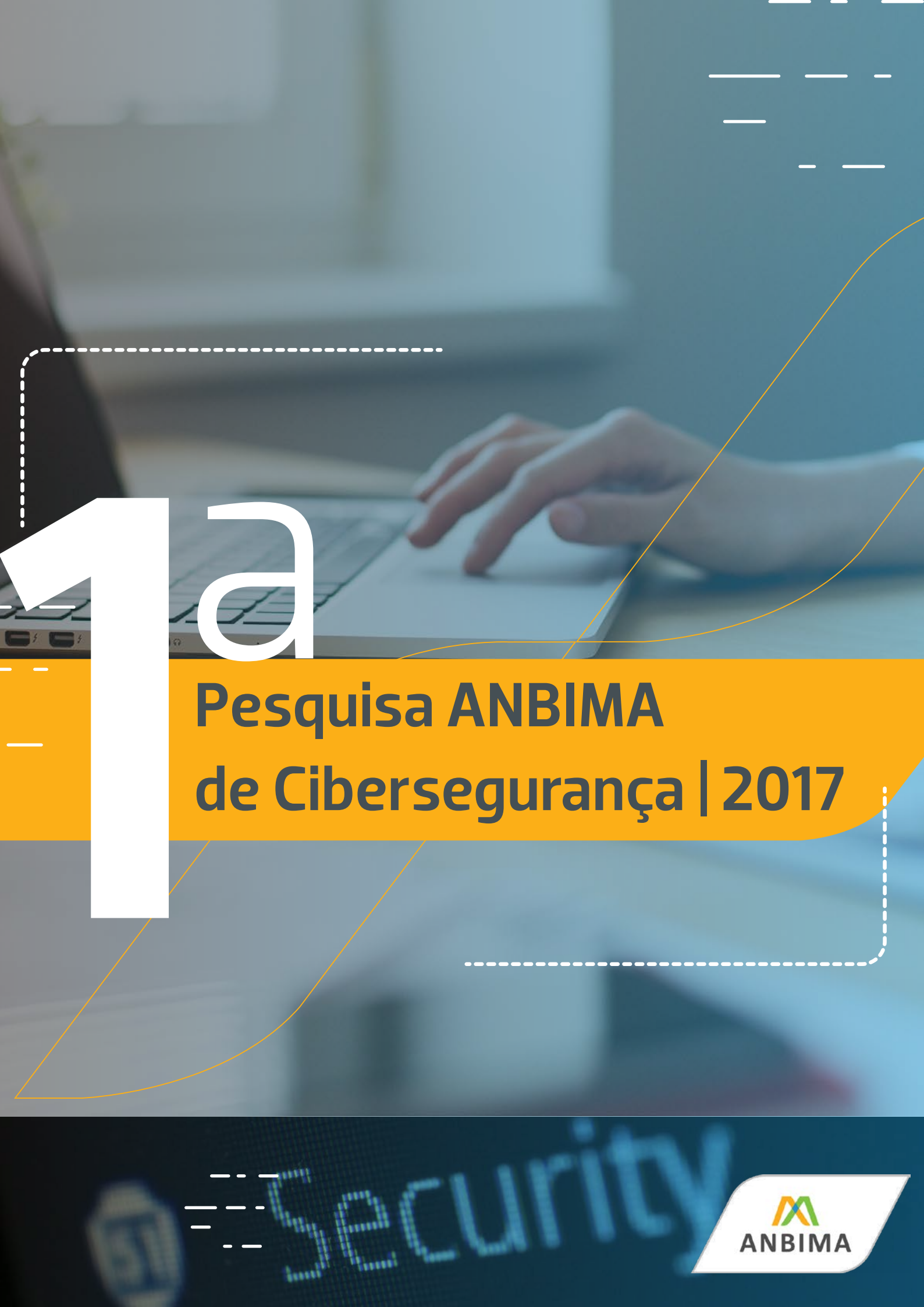


1a Pesquisa ANBIMA de Cibersegurança | 2017

ANBIMA

SUMÁRIO

APRESENTAÇÃO

É notável o aumento das ameaças cibernéticas nos últimos anos: crescem em volume, mas se destacam, principalmente, pela sofisticação. Os diversos integrantes dos mercados financeiros e de capitais têm dado mais atenção para o tema com o objetivo de estabelecer procedimentos que as instituições devem adotar para verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

Qual a nossa intenção?

O assunto está em nosso radar desde 2015. A intenção é contribuir para o aprimoramento da segurança cibernética nos mercados financeiro e de capitais do Brasil. De lá para cá, lançamos o Guia de Cibersegurança que traz as práticas e procedimentos para a elaboração de programas de cibersegurança nas instituições e para a educação das equipes a respeito do tema. Como desdobramento, em abril de 2017, foi criado o Grupo Técnico de Cibersegurança[1]. A pauta do fórum é voltada para a atualização contínua e complementação do guia[2] , além da organização de ações de compartilhamento de informações e atividades voltadas ao aperfeiçoamento das iniciativas de segurança cibernética no mercado local e para a troca e disseminação de informações sobre o tema.

[1] Saiba mais sobre nosso grupo Técnico de Cybersegurança

[2] Confira a segunda edição do Guia de Cibersegurança (2017)

A pesquisa

Para mensurar o grau de maturidade do mercado brasileiro em relação à cibersegurança, realizamos uma pesquisa com nossos associados. Essa avaliação foi importante pois ajudará a direcionar outras atividades: educativas, de suporte a testes e de compartilhamento de informações. A pesquisa foi elaborada pelo nosso Grupo Técnico de Cibersegurança e a primeira edição do guia serviu como benchmark: um ano após seu lançamento, medimos a adesão dos associados às práticas nele recomendadas.

A pesquisa verificou o desenvolvimento dos programas pelas instituições e gestores locais, a observação de elementos considerados usuais e outras características de controle e de monitoramento adotadas pelos participantes.

Perfil das instituições respondentes

Consultamos nossos **262** associados: assets, bancos, distribuidoras, corretoras, entre outros. Obtivemos retorno de 151 instituições, o que representa 58% do total.
A maioria delas que respondeu à pesquisa são assets (46%) e têm entre 11 e 100 funcionários (46%).

Tipos de instituições

- 46% Asset
- 32% Banco
- 16% Corretora e Distribuidora
- 6% Demais instituições

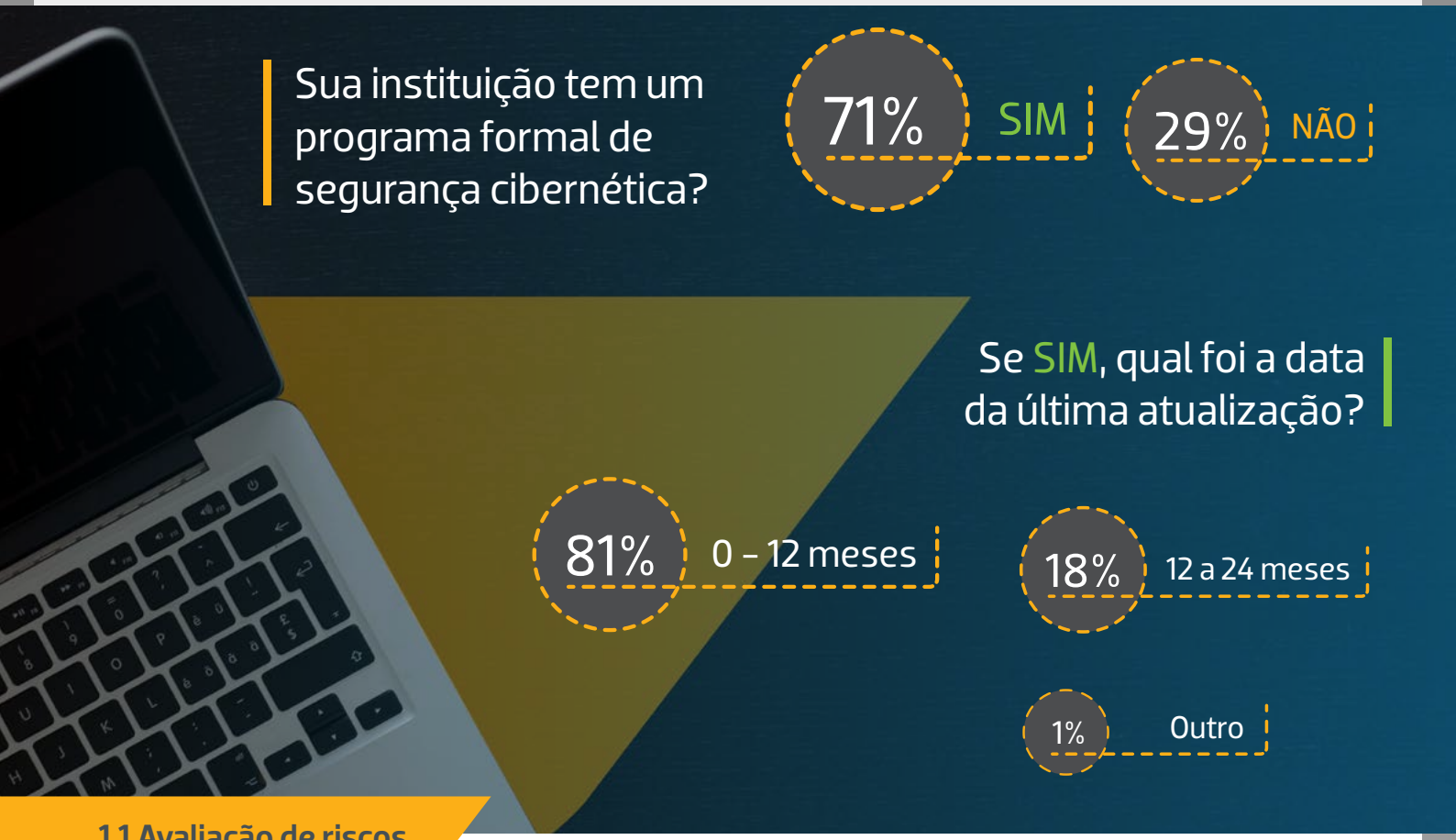
Nº de funcionários

- 46% 11 – 100
- 20% 101 – 500
- 16% 501 a 5000
- 11% 1 – 10
- 7% 5001 ou mais

1. Programa de segurança cibernética

Um programa eficiente de segurança cibernética deveria conter pelo menos cinco funções bem definidas, de acordo com o nosso Guia de Cibersegurança: identificação e avaliação de riscos (risk assessment); ações de prevenção e proteção; monitoramento e testes; criação do plano de resposta; e reciclagem e revisão.

Esse é um aspecto que recebe atenção dos associados: **71%** afirmaram possuir um programa formal e, destes, **81%** o atualizaram no último ano. Entre os que não possuem o programa, **73%** pretendem elaborá-lo em 2018.



Sua instituição tem um programa formal de segurança cibernética?

71% SIM

29% NÃO

Se SIM, qual foi a data da última atualização?

81% 0 - 12 meses

18% 12 a 24 meses

1% Outro

1.1 Avaliação de riscos

A identificação de riscos cibernéticos internos e externos e dos ativos de hardware, software e de processos que precisam de proteção, chamada de avaliação de riscos (risk assessment), é feita por 84% das instituições. Entre elas, 59% mensuram os possíveis impactos financeiros, operacionais e reputacionais, e 48% determinam e utilizam metodologia para avaliações de risco cibernético.

Com relação à governança, apenas 42% das instituições que realizam a avaliação de riscos alegaram ter criado um comitê, fórum ou grupo específico para tratar dos aspectos da segurança cibernética dentro da instituição, com representação e governança apropriados. No caso das assets, essa proporção foi de 27%.

1.2 Ações de prevenção e proteção

O tópico que recebe atenção de quase a totalidade das instituições (99%) é atuar preventivamente para impedir a ocorrência de um ataque cibernético.

Entre essas empresas, a grande maioria respondeu que adota medidas como serviços de backup, controles de acessos, segurança de borda (inclusive firewalls) e regras mínimas para definição de senhas, entre outros. Já 74% declararam ter controles para impedir a instalação e execução de softwares e aplicações não autorizadas.

Na hora de contratar serviços de terceiros, 72% realizam diligência e avaliam questões jurídicas, cláusulas de confidencialidade e exigem controles de segurança na estrutura dos fornecedores.

1.3 Monitoramento e testes

Sua instituição adota ações de monitoramento e teste para detectar ameaças em tempo hábil?

As ameaças são detectadas por 83% das instituições e 94% das corretoras, que reforçam os controles, caso necessário, e identificam possíveis irregularidades no ambiente tecnológico, como a presença de usuários, componentes ou dispositivos não autorizados.

Dentre essas instituições, apenas metade (51%) testa o plano de resposta a incidentes, 42% destas o fazem com intervalos de um ano e 58% em menos de 6 meses.

1.4 Criação do plano de resposta

Quanto à reação aos ataques, 75% das instituições afirmaram ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.

As áreas responsáveis por esse plano nas empresas são segurança tecnológica (92%), jurídico (38%) e comunicação (26%). Outras áreas mencionadas com destaque foram compliance, risco e negócios.

As ameaças previstas na avaliação de risco estão nos planos de resposta de 75% das instituições e 78% determinam os papéis e responsabilidades dentro do plano de ação.

1.5 Reciclagem e revisão

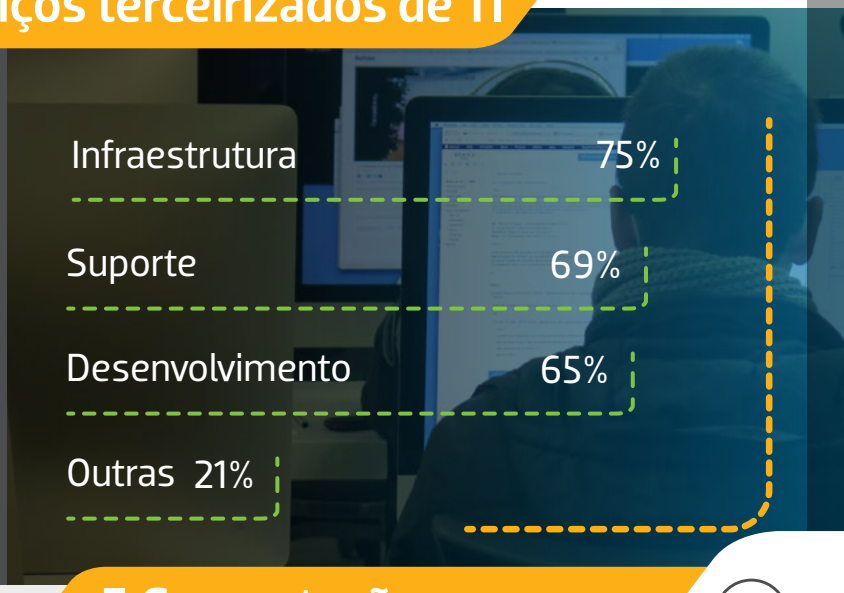
Identificar novos riscos, ativos e processos e reavaliar os riscos residuais do programa de segurança cibernética, mantendo-o sempre atualizado, é uma das ações tomada por 77% das instituições.

Os grupos de profissionais envolvidos com o programa também se mantêm atualizados sobre vulnerabilidades e ameaças em 86% dos associados. Para estas instituições, as informações são obtidas por meio de esforço interno (85%); por fornecedores especializados (75%); e pela participação em grupos de compartilhamento de informações (56%).

Do total de respondentes, 75% promovem e disseminam uma cultura de segurança, contando com a criação de canais de comunicação internos para divulgar o programa de segurança cibernética e realização de treinamentos. Os indicadores de desempenho (key performance indicators), que auxiliam na conscientização e no envolvimento da alta administração e dos demais órgãos da instituição, são definidos e mantidos por apenas 30% dos associados.

2. Contratação de serviços terceirizados de TI

Os serviços terceirizados de TI são contratados por 83% das instituições, principalmente nas áreas de infraestrutura e suporte. Os relatórios periódicos para acompanhamento de qualidade são exigidos por apenas 55% das instituições que aderem a esses serviços.



3.Computação na nuvem

Os ativos das instituições podem estar localizados interna ou externamente, muitas vezes em nuvem. A última opção é a escolha de 75% das instituições, que afirmaram ter algum serviço ou ativo localizado em nuvem. Esse percentual alcança 90% no caso das assets. A maioria das instituições utiliza nuvem para armazenamento de dados e sistemas críticos, mas também em outros serviços, como backup de arquivos, e-mail, serviços executados com sistemas de terceiros, servidores, sistemas não críticos, websites e controles financeiros.

- 60% Dados
- 36% Sistemas críticos
- 35% Outros
- 21% Ativos

A computação em nuvem pode ser considerada uma contratação de serviço de terceiros, de acordo com organismos internacionais, como NIST[3] e FFIEC[4], e desse modo envolve determinados riscos que devem ser avaliados pelas instituições. Nesse sentido, constatou-se que grande parte dos entrevistados garante que sejam feitas configurações seguras de seus recursos e a maioria também realiza diligência com terceiros em nuvem.

Ao contratar serviço em nuvem,

garante que sejam feitas configurações seguras de seus recursos?

- SIM 86%
- NÃO 14%

realiza diligência com terceiros na nuvem?

- SIM 68%
- NÃO 32%

Saiba mais

[3]Nactional Institute of Standards and Tecnology. Ver NIST Cloud Computing Program – NCCP

[4]Federal Financial Institutions Examination Council. Ver "Outsourced Cloud Computing" (FFIEC, 10/7/12).

4. Testes

4.1 Testes externos de penetração

No último ano, 53% das empresas realizaram testes externos de penetração, o que é feito por 80% delas anualmente e, em 84% dos casos, pela contratação de terceiros. Dentre os 47% que não realizaram testes de penetração externo no último ano, 77% têm planos para fazê-lo. No caso das corretoras, 56% não realizam tais testes e, destas, 56% têm planos para realizá-los.

Se sim,

qual é a peridiocidade dos testes de penetração?

80% 0 – 12 meses

20% 12 – 24 meses

o teste foi realizado por:

84% terceiros

16% internos

Se não,

há algum plano prevendo a realização desse teste?

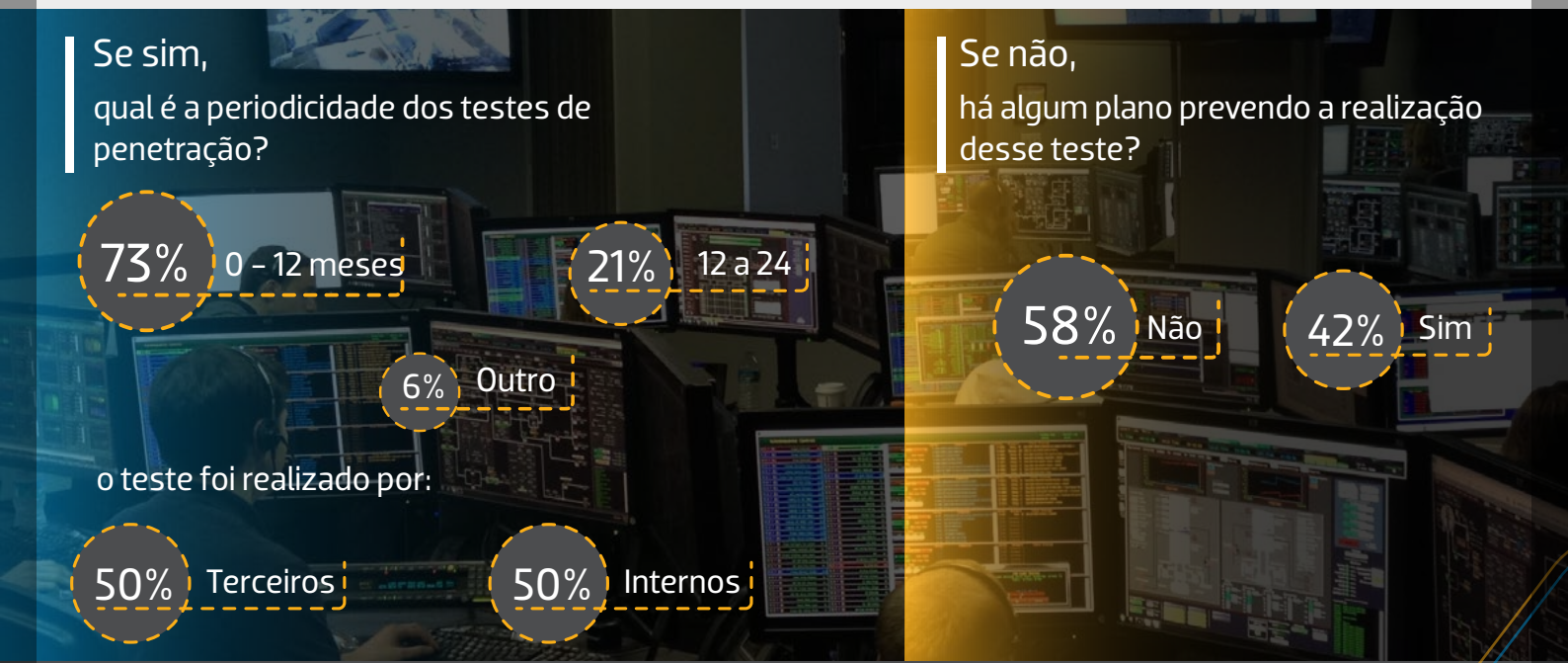
77% Sim

23% Não

4.2 Testes internos de penetração

Já os testes internos são feitos por 63% das instituições: 73% delas o realizam anualmente e 50% utilizam serviços de terceiros para essa atividade.

Entre aquelas que não realizaram testes internos de penetração, apenas 42% têm planos para sua realização.



Se sim,

qual é a periodicidade dos testes de penetração?

73% 0 – 12 meses

21% 12 a 24

6% Outro

o teste foi realizado por:

50% Terceiros

50% Internos

Se não,

há algum plano prevendo a realização desse teste?

58% Não

42% Sim

4.3 Phishing

Os testes de phishing foram realizados por 44% das empresas e por 29% das assets no último ano. Esses testes compreendem o envio de links por e-mail que simulam uma pessoa ou empresa confiável enviando um comunicado oficial, com o objetivo de obter informações confidenciais.

Conclusões

A primeira edição da nossa pesquisa sobre cibersegurança no mercado local buscou contribuir para o aperfeiçoamento das práticas de segurança cibernética nas instituições dos mercados financeiro e de capitais. Os resultados mostraram um satisfatório grau de maturidade das instituições participantes com relação às principais questões de cibersegurança. A maioria das instituições mantém um programa formal de segurança cibernética e informou que já observou diversos procedimentos orientados pelo nosso Guia de Cibersegurança, como a realização de processo de avaliação de riscos, ações de prevenção e proteção e de monitoramento e testes. Um número expressivo de empresas revelou contratar serviços terceirizados de TI.

Serviços localizados em nuvem também receberam atenção: além do alto índice de utilização verificado entre as instituições, com destaque para o armazenamento de dados, foi verificado um elevado percentual de realização de diligência com estas empresas. Por outro lado, um ponto para maior atenção foi a realização de testes externos de penetração e phishing.

Dessa forma, além de estimular o debate entre os associados e demais representantes do mercado para construir uma governança adequada ao tema, essas respostas basearão a agenda de atividades do nosso Grupo Técnico de Cibersegurança em 2018. As ações serão focadas, principalmente, no compartilhamento de testes junto às instituições, tanto de informações como de atividades voltadas para o aumento da resiliência do mercado local e seus participantes.

Expediente

Rio de Janeiro
Avenida República do Chile, 230, 13° andar
CEP 20031-170
+ 21 3814 3800

São Paulo
Av. das Nações Unidas, 8501, 21° andar
CEP 05425-070
+ 11 3471 4200

ANBIMA
www.anbima.com.br