ANBIMA

3ª Pesquisa ANBIMA de Cibersegurança – 2020

ÍNDICE

APRESENTAÇÃO

As boas práticas em relação à cibersegurança vêm se consolidando nas instituições financeiras. A 3ª Pesquisa ANBIMA de Cibersegurança mostra que 95% das empresas contam com algum programa, política ou formalização de procedimentos de cibersegurança.

Em decorrência do crescimento das ameaças cibernéticas e da importância sistêmica desse tema, a pesquisa buscou mapear o nível de preparo das instituições 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?

Em 2020 vivemos ainda um episódio inédito para todos os setores da economia, que é a pandemia de Covid-19. Por isso, incluímos um capítulo inédito para entender como as mudanças que esse período exigiu afetaram — ou não — as políticas e procedimentos das instituições em relação às possibilidades de ataques cibernéticos.

O estudo também traz, pela primeira vez, não apenas dados dos associados da ANBIMA, também das empresas aderentes aos nossos códigos, que não são nossos associados. Isso permite ter uma compreensão mais ampla do mercado e identificar se existem diferenças entre esses dois públicos quando o assunto é cibersegurança.

As respostas deste relatório medem o grau de maturidade do mercado local em cibersegurança, além de atualizar os dados obtidos em 2017 e 2018. 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.

*Em alguns gráficos e tabelas de respostas únicas os resultados não somam exatamente 100%, variam de 99% a 101%, devido a arredondamentos.

A PESQUISA

Esta é a terceira edição da Pesquisa de Cibersegurança da ANBIMA, que tem como objetivo monitorar a evolução das instituições em relação às práticas de segurança cibernética. O trabalho de campo foi realizado entre os dias 20 de junho e 28 de agosto de 2020.

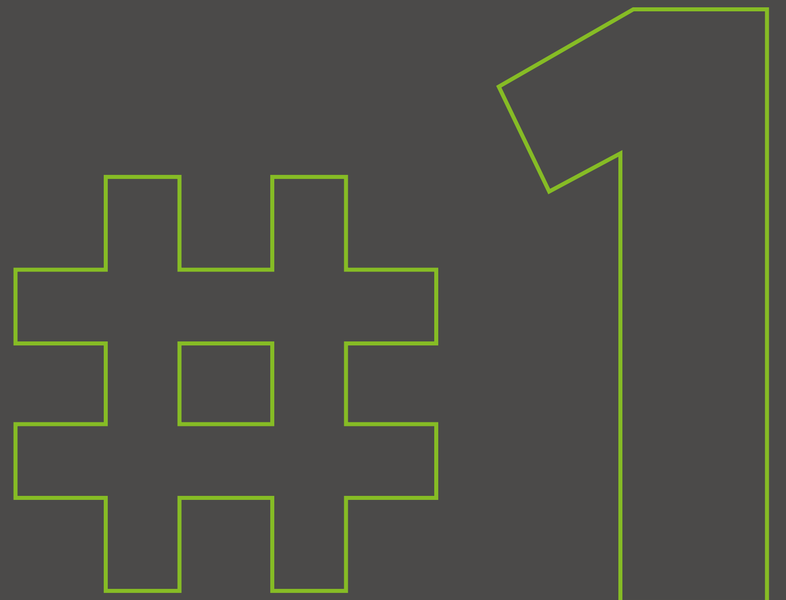
As perguntas da edição anterior, realizada em 2018, foram mantidas e atualizadas, de forma a permitir o acompanhamento do tema. Em razão da pandemia de Covid-19, foi incluído também um bloco sobre o tema com o objetivo de entender como as empresas se organizaram nesse período.

Os resultados da pesquisa mostram o nível de adesão das instituições ao Guia de Cibersegurança da ANBIMA e indicam pontos de atenção que podem ser foco de ações no futuro próximo.

Confira também os relatórios da primeira edição da pesquisa, de 2017, e da segunda edição, de 2018.

Relatório 2017 | Relatório 2018

ANBIMA



PERFIL DAS INSTITUIÇÕES

1.0 – PERFIL DAS INSTITUIÇÕES

Uma das novidades desta edição é que ela traz, pela primeira vez, os resultados não apenas entre nossos associados, como também para os aderentes, que são instituições que aderiram aos códigos da ANBIMA, mas não integram o quadro associativo da instituição.

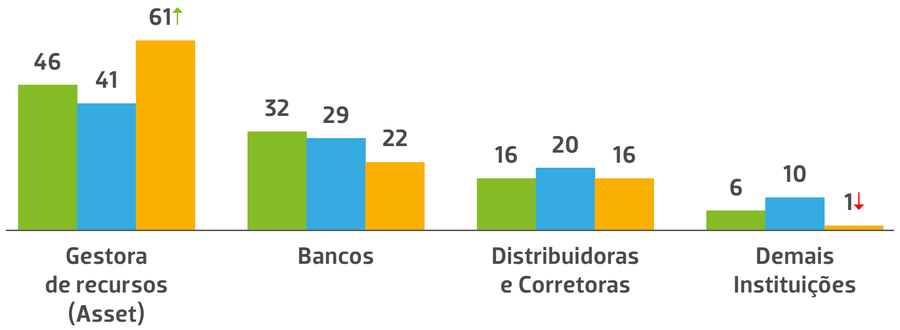
Entre os associados da ANBIMA, 74 responderam à pesquisa, o que corresponde a 27% do total. Houve queda em relação a 2018, quando 177 associados participaram do levantamento. No entanto, entre os aderentes, tivemos 125 participantes. As duas amostras somam, portanto, 199 instituições.

As gestoras de recursos (assets) são o grupo mais numeroso tanto para os associados (61%) quanto para os aderentes (87%). No cômputo geral, elas representam 61% dos respondentes da pesquisa. Em relação às pesquisas anteriores, a participação das assets aumentou.

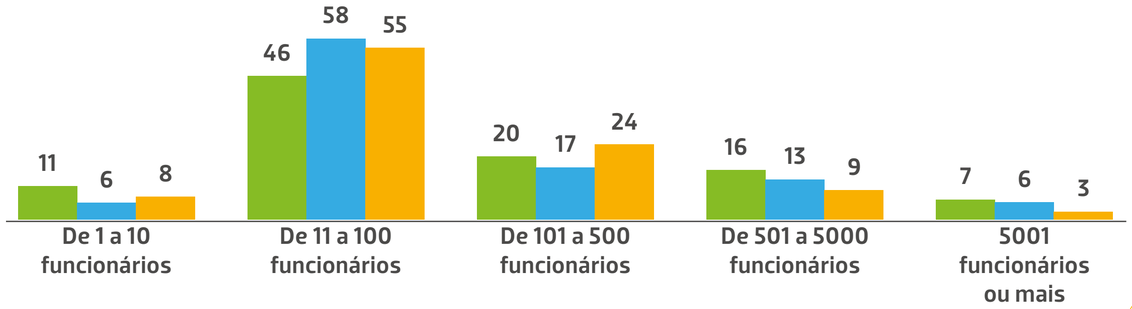
A maior parte dos associados (55%) tem entre 11 e 100 funcionários, enquanto, entre os aderentes, 96% contam com 1 a 100 funcionários.

Perfil das instituições – Evolutivo (em %)

Segmento das instituições



Segmento da instituição – Número de funcionários



*Em alguns gráficos e tabelas de respostas únicas os resultados não somam exatamente 100%, variam de 99% a 101%, devido a arredondamentos.

1.1 – PROGRAMA DE SEGURANÇA CIBERNÉTICA

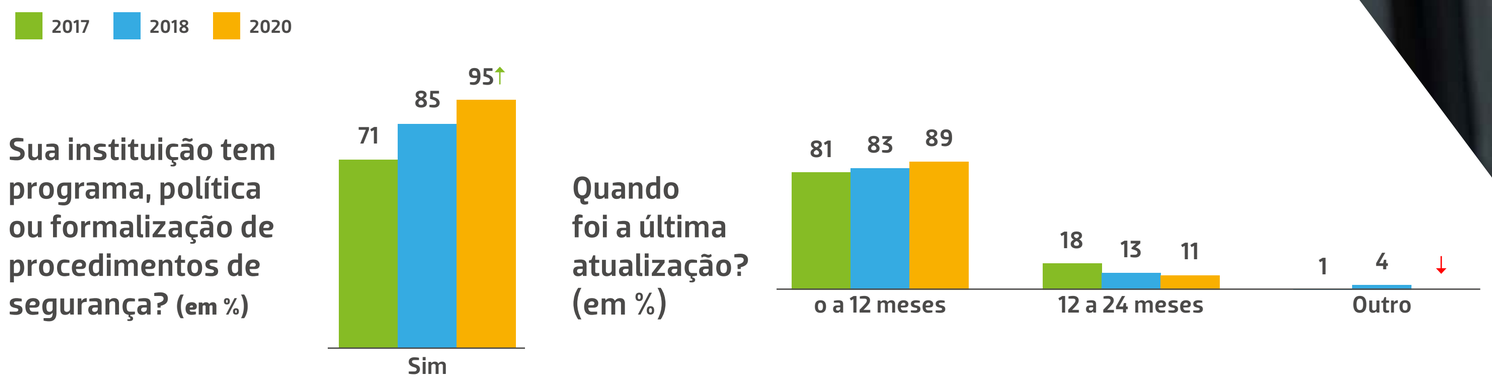
Um dos principais avanços observados nesta edição diz respeito ao percentual das instituições que contam com programas, políticas ou algum tipo de formalização de procedimentos de cibersegurança. Neste ano, 95% das empresas entrevistadas se encontravam nessa condição. Trata-se de um crescimento significativo — 10 pontos percentuais — em relação a 2018. Em 2017, esse número era de apenas 71%.

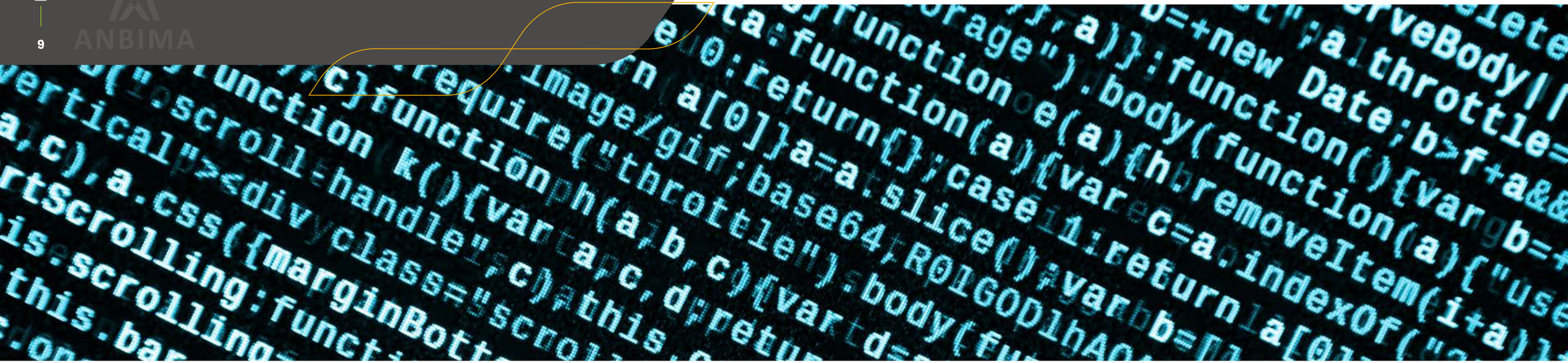
Nesse quesito, não foram constatadas diferenças significativas entre associados e aderentes. Já em relação à atualização do programa, os associados apresentam uma frequência mais elevada do que os aderentes. Entre os associados, 89% afirmaram ter feito alguma atualização nos últimos 12 meses, contra 70% dos aderentes.

Outro ponto relevante é que o tamanho da instituição guarda relação com a presença de programas de cibersegurança. Entre aquelas de porte médio e grande, quase todas apresentam políticas próprias nesse sentido. Já nas de pequeno porte (1 a 10 funcionários), apenas 67% se enquadram nesse quesito.

Assim como na edição de 2018, quase todas as associadas (97%) designam um profissional responsável pelas questões de cibersegurança. Tanto entre os associados quanto entre os aderentes, os cargos mais usuais para essa função são de diretor ou de gerente. Eles costumam estar em áreas de segurança da informação, TI, risco e compliance.

De acordo com o apurado pela pesquisa, houve queda no percentual das associadas que criaram um comitê, fórum ou grupo específico para tratar do tema — de 85% em 2018 para 70% neste ano.





1.2 – AVALIAÇÃO DE RISCOS

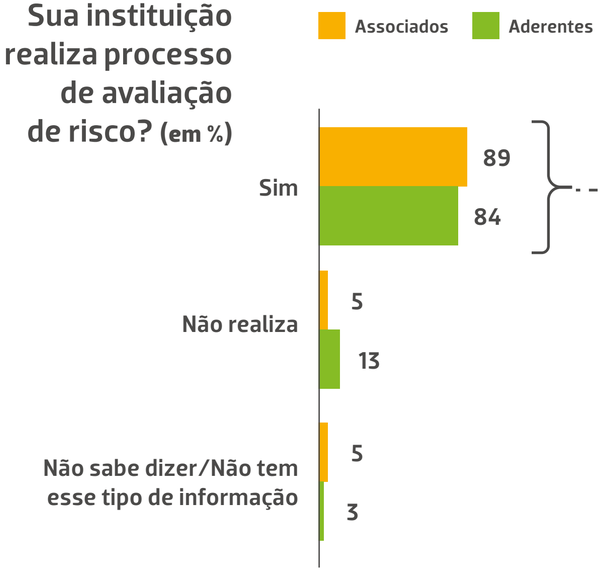
Identificar os riscos a que a instituição está sujeita (risk assessment) é uma prática usual para 89% das associadas — percentual um pouco maior do que o encontrado nas edições anteriores (84% em 2017 e 82% em 2018).

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

Nesse quesito, todos os elementos e ações específicas analisados apresentaram avanços. A maior parte das instituições participantes afirmaram, por exemplo, que identificam todos os seus ativos relevantes e que avaliam as vulnerabilidades desses ativos, reconhecendo as possíveis ameaças e o grau de exposição ao qual estão sujeitos.

Aqui nota-se uma distinção entre associados e aderentes. Entre os aderentes, o percentual dos que realizam processos de avaliação de risco é menor (84%). Dos elementos analisados, as principais diferenças estão na mensuração de possíveis impactos no caso de eventos de segurança e no cálculo da probabilidade desses eventos, além da elaboração de regras para a classificação das informações geradas pela instituição.

Sua instituição realiza processo de avaliação de risco? (em %)



Consultorias especializadas e o Guia de Cibersegurança da ANBIMA estão entre as fontes mais utilizadas para consulta e desenvolvimento de metodologia de avaliação de risco.

Base: Entrevistados que realizam processo de avaliação do risco – Associados: 66 – Aderentes: 105 entrevistados

1.3 – AÇÕES DE PREVENÇÃO E PROTEÇÃO

Uma vez definidos os riscos, 96% das associadas atuam preventivamente para impedir os ataques — resultado em linha com as pesquisas de 2017 e 2018 e sem diferenças significativas entre associados e aderentes (94%).

96%

das instituições adotam ações de prevenção e proteção

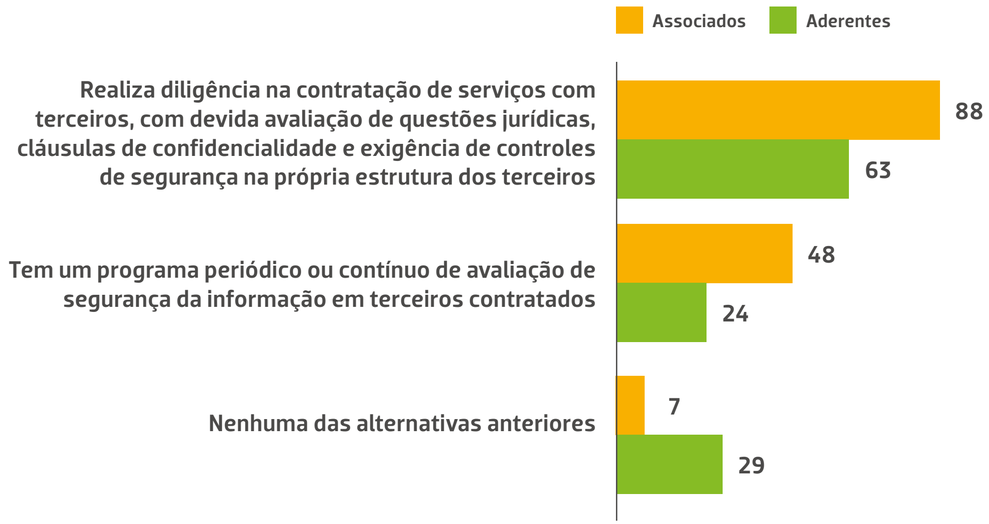
MAIS DE 90% DAS INSTITUIÇÕES AFIRMARAM ADOTAR AS SEGUINTES PRÁTICAS E AÇÕES NESSE SENTIDO:

- controle de acesso adequado aos ativos das instituições
- concessão de acesso limitado apenas a recursos relevantes para o desempenho das atividades
- adoção de política de backup
- implementação de recursos anti-malware nas estações e servidores de rede, como antivírus e firewalls pessoais
- implementação de serviço de backup dos ativos da instituição
- implementação de segurança de borda, nas redes de computadores, por meio de firewalls e outros mecanismos de filtros de pacotes
- configurações seguras de recursos ao incluir novos equipamentos e sistemas em produção

O destaque entre os elementos levados em consideração nas ações de prevenção e proteção fica para o item "configurações seguras de recursos ao incluir novos equipamentos e sistemas em produção". Em 2017, apenas 78% das instituições participantes adotavam essa prática, percentual que subiu para 82% em 2018 e chegou a 93% neste ano.

Ao avaliar a contratação de serviços de terceiros, os comportamentos de associados e de aderentes mostram diferenças significativas. No primeiro grupo, 88% realizam diligência e avaliam questões jurídicas, cláusulas de confidencialidade e exigem controles de segurança na estrutura dos fornecedores. Já entre os aderentes, esse percentual é de apenas 63%.

Elementos levados em consideração nas ações de prevenção e proteção relacionados aos prestadores de serviços e terceiros (em %)



1.4 – MONITORAMENTO E TESTES

Ações de monitoramento para detectar ameaças são adotadas por 93% das associadas, que reforçam os controles, caso necessário, e identificam possíveis irregularidades no ambiente tecnológico, como a presença de usuários, componentes ou dispositivos não autorizados. O percentual mostra um avanço nessas práticas tanto em relação a 2018 (87%) quanto na comparação com 2017 (83%).

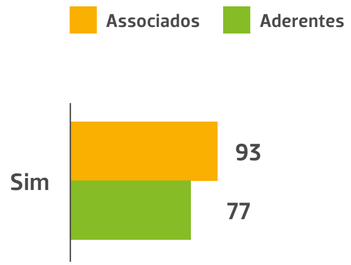
93%

das associadas adotam ações de monitoramento e teste para detectar ameaças em tempo real

Entre os elementos levados em consideração na etapa de monitoramento e testes, o mais utilizado pelas associadas (95%) é a manutenção de sistemas operacionais e softwares de aplicação atualizados. Por outro lado, apenas 52% utilizam ferramentas de centralização e análise de logs.

De forma geral, os associados (93%) têm mais costume de realizar monitoramentos e testes, quando comparados aos aderentes (77%), o que se traduz em percentuais mais altos em todos os elementos analisados.

Sua instituição adota ações de monitoramento e testes para detectar ameaças em tempo hábil? (em %)



Associados	Aderentes	
95%	92%	Mantém os sistemas operacionais e softwares de aplicação sempre atualizados
85%	74%	Monitora diariamente as rotinas de backup, executando testes regulares de restauração dos dados
85%	65%	Monitora vulnerabilidades e a bem-sucedida aplicação de patches de segurança em seus sistemas operacionais e softwares de aplicação
83%	69%	Mantém inventários atualizados de hardware e software, e os verifica com frequência para identificar elementos estranhos à instituição
78%	55%	Cria mecanismos de monitoramento de todas as ações de proteção implementadas
69%	46%	Analisa os logs e trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos ou externos
52%	40%	Utiliza ferramentas de centralização e análise de logs
–	1%	Nenhum dos itens anteriores

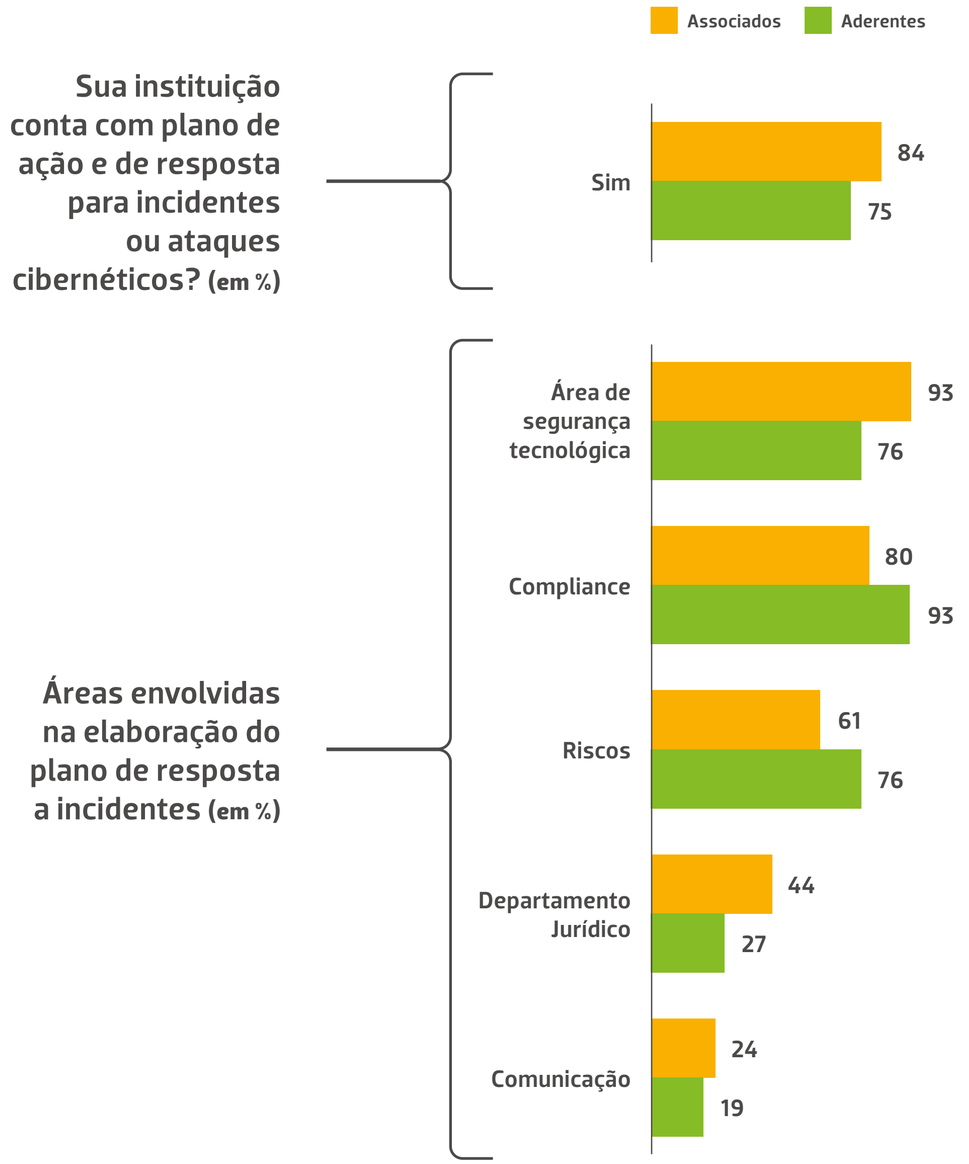
1.5 – CRIAÇÃO DO PLANO DE RESPOSTA A INCIDENTES

Na hora de reagir aos ataques, 84% dos associados têm um plano de resposta, percentual superior ao verificado em 2018 (76%) e 2017 (75%). Mais uma vez, essa fatia se mostrou menor entre os aderentes (75%).

Entre os associados, 47% testam o plano de ação e 86% o fazem com intervalos com intervalos menores do que um ano, um recuo quando comparado com os 100% de 2018. No caso das aderentes, o percentual das que testam o plano é um pouco menor (43%), assim como o das que o fazem com intervalo inferior a um ano (82%).

Verifica-se também uma diferença em relação às áreas envolvidas na elaboração desses planos. Embora eles sejam feitos por equipes multidisciplinares, entre os associados a área de maior peso é a de segurança tecnológica, enquanto entre os aderentes essa posição é ocupada pelo compliance.

Outro ponto que merece ser observado é que a área de comunicação perdeu força e foi citada por apenas 24% dos associados, um decréscimo em relação a 2018 (41%) e em linha com os resultados de 2017 (26%).



Entre as ações específicas no plano de resposta a incidentes, quase todas as instituições contam com um plano de continuidade dos negócios e processos de recuperação e remediação, levam em consideração questões de segurança e controles de acesso também nas instalações de contingência e arquivam documentos relacionados ao gerenciamento dos incidentes e ao plano de continuidade de negócios para servir como evidência.

Outros itens pesquisados já apresentaram adesão menor por parte das instituições, com destaque para os critérios para classificação dos incidentes por severidade, adotado por apenas 67% dos associados, percentual superior a 2018 (59%), mas apenas em linha com 2017.

Nesse quesito, os aderentes tiveram, em geral, números inferiores aos associados em quase todos os elementos analisados. Houve duas exceções. Em relação ao plano de continuidade dos negócios e processos de recuperação e remediação, associados e aderentes estão no mesmo patamar. Já quanto à definição de papéis e responsabilidades dentro do plano de ação e respostas, os aderentes (83%) tiveram desempenho melhor do que os associados (75%).

Sua instituição conta com plano de ação e de resposta para incidentes ou ataques cibernéticos?

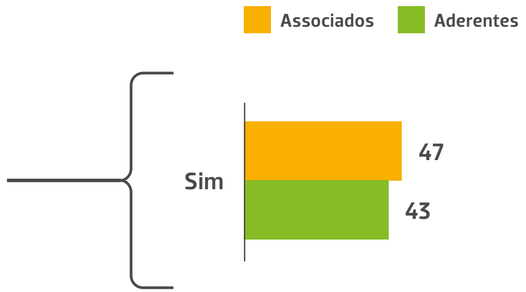
2017
75%

2018
76%

2020
84%

Um ponto de atenção é que houve queda no percentual de associados que testam o plano de resposta para incidentes, de 53% em 2018 para 47% neste ano. Quando realizam o teste, a maioria (54%) adota uma periodicidade anual para isso. Entre os aderentes, apenas 43% aderem à prática.

Sua instituição realiza teste do plano de ação e de resposta para incidentes? (em %).



Cerca de metade dos associados (49%) adota algum protocolo de comunicação com outras entidades quando o plano de resposta é ativado. Já entre os aderentes, esse percentual é de apenas 33%.

Banco Central, CVM (Comissão de Valores Mobiliários) e instituições pares são as mais acionadas pelos associados. Os aderentes, por sua vez, além de utilizarem menos os protocolos de comunicação, quando usam, acionam principalmente CVM e instituições pares.

Quanto às iniciativas voltadas para o compartilhamento de informações sobre incidentes cibernéticos, essa ainda é uma questão que precisa ser trabalhada entre os participantes do mercado local. Entre as 59 instituições associadas que disseram, na pesquisa, terem algum plano de ação e respostas para incidentes, apenas 13 participam de iniciativas de compartilhamento.

Entre os que compartilham as informações, os respondentes citaram iniciativas que incluem fóruns da ANBIMA e do FS-ISAC (Centro de Compartilhamento e Análise de Informações Financeiras). Devido ao número reduzido de respondentes, não é possível fazer comparações estatísticas nesse critério, para evitar informações distorcidas.

1.6 – RECICLAGEM E REVISÃO

Manter os programas de segurança revisados e atualizados é uma prática que quase todas as instituições associadas (93%) adotam. O número aponta para um crescimento significativo tanto em relação à última edição (82%) quanto na comparação com 2017 (77%).

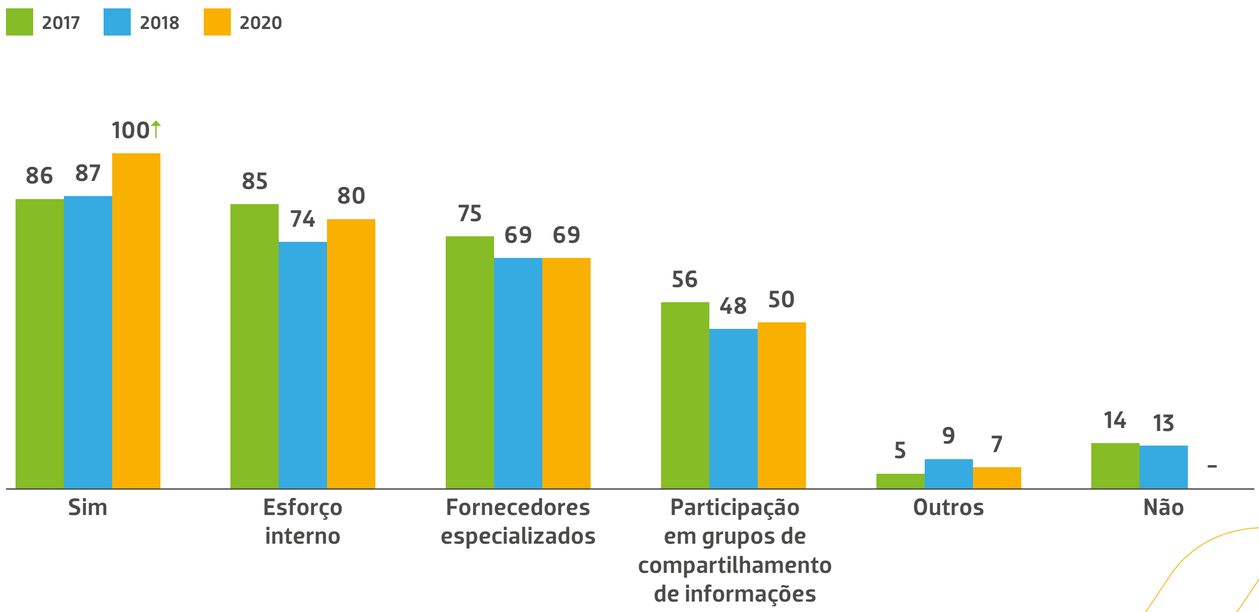
A grande maioria (89%) revisa o programa com periodicidade de até um ano, praticamente o mesmo patamar observado em 2018 (88%).

Em linha com as demais frentes da pesquisa, o percentual de aderentes que adotam essa prática é um pouco menor (89%).

Em todas empresas associadas que participaram do estudo, os grupos envolvidos com o programa se mantêm atualizados sobre novas vulnerabilidades e ameaças. Trata-se de um grande avanço em relação a 2018, quando 87% dos respondentes se encontravam nessa situação.

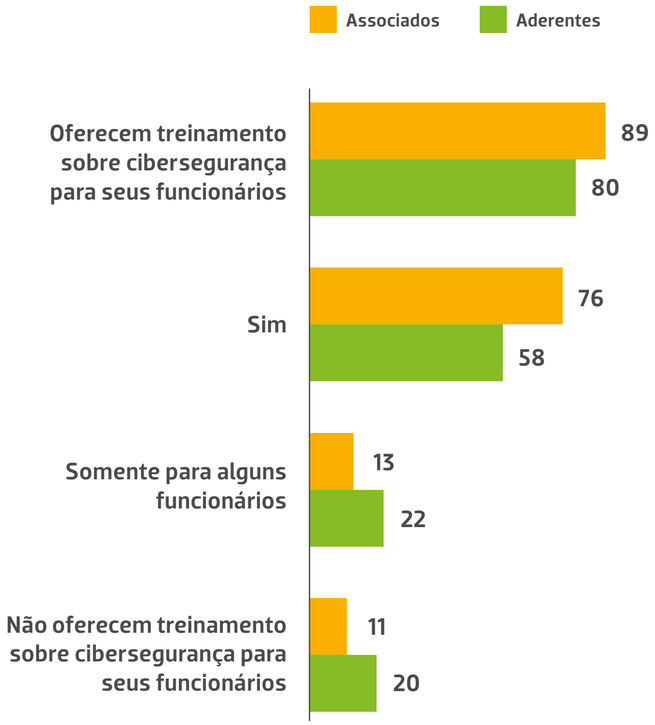
Na maioria das vezes, os associados obtêm as informações por esforço interno (80%), seguida por fornecedores especializados (69%) e por meio da participação em grupos de compartilhamento de informações (50%). A ordem é a mesma para os aderentes, mas com percentuais sistematicamente mais baixos.

Os grupos envolvidos com o programa se mantêm atualizados sobre novas vulnerabilidades e ameaças? (em %)



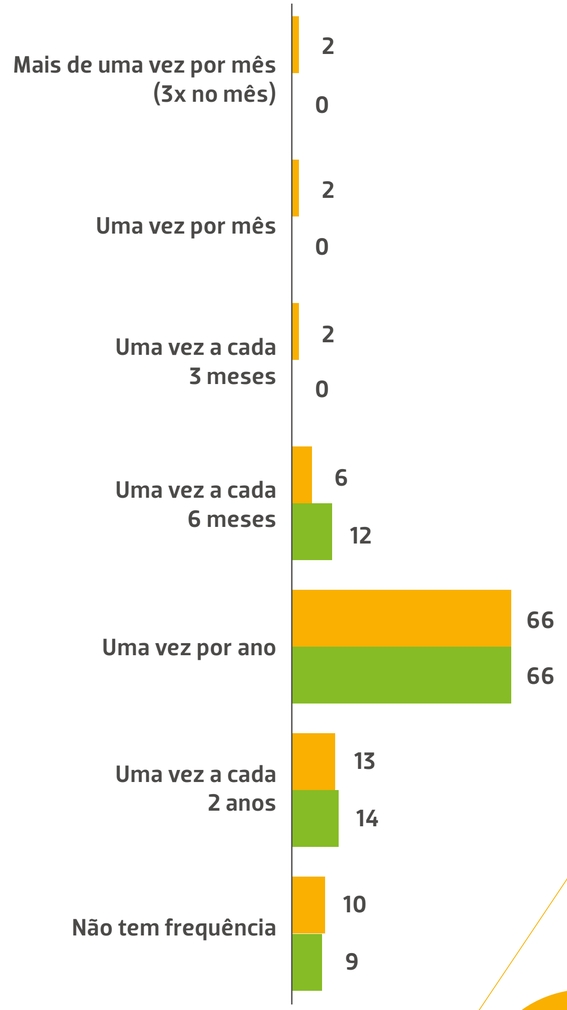
Para garantir que as práticas de cibersegurança da empresa estejam atualizadas com o mercado, a maioria das instituições oferece treinamento sobre o tema para seus funcionários — 89% das associadas e 80% das aderentes. Em geral, isso ocorre cerca de uma vez por ano.

A instituição promove treinamentos sobre cibersegurança e política de segurança cibernética para todos os funcionários? (em %)



Identificar ou avaliar riscos em fornecedores ou prestadores de serviço está na pauta de 91% das empresas associadas. Entre as ações adotadas com essa finalidade, estão cláusulas contratuais, avaliação remota e avaliação presencial. Já entre os aderentes, esse percentual cai para 77%.

Com que frequência os treinamentos acontecem? (em %)



ANBIMA

#2

CONTRATAÇÃO DE SERVIÇOS TERCEIRIZADOS DE TI

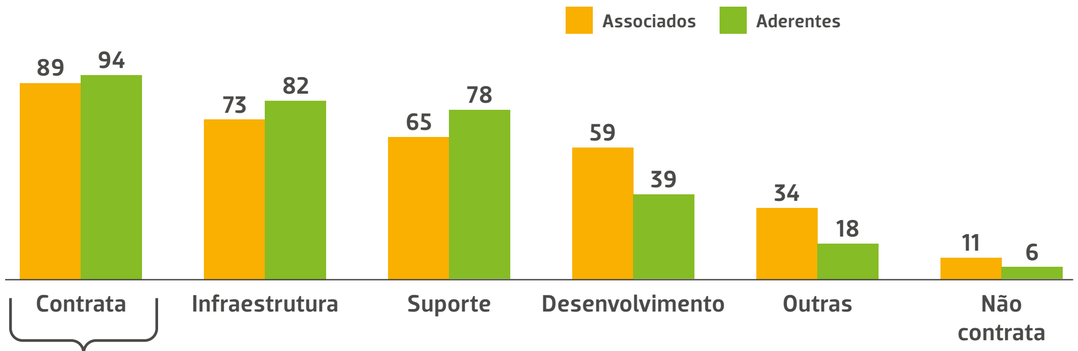
CONTRATAÇÃO DE SERVIÇOS TERCEIRIZADOS DE TI

A terceirização dos serviços de TI se mantém como uma prática usual para 89% das empresas associadas, um aumento tanto em relação a 2018 (84%) quanto ante 2017 (83%). As principais áreas em que isso ocorre são infraestrutura, suporte e desenvolvimento, nessa ordem.

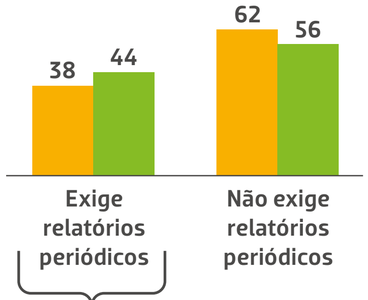
Por outro lado, entre as que terceirizam os serviços de TI, apenas 38% exigem relatórios periódicos do prestador de serviço, contra 50% em 2018 e 55% em 2017. Embora a terceirização seja uma prática normal e corriqueira, esse número pode sugerir menos controle sobre a atuação do fornecedor, o que é um dado preocupante.

É interessante notar que o percentual de aderentes que contratam serviços terceirizados de TI é ainda maior (94%), mas eles também têm um percentual maior de exigência de relatórios (44%). Na quase totalidade dos casos — tanto para associados quanto para aderentes —, esse relatório tem periodicidade de até um ano.

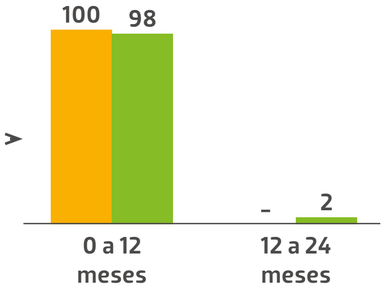
Sua instituição contrata serviços terceirizados de TI? Em caso afirmativo, para quais áreas? (em %)



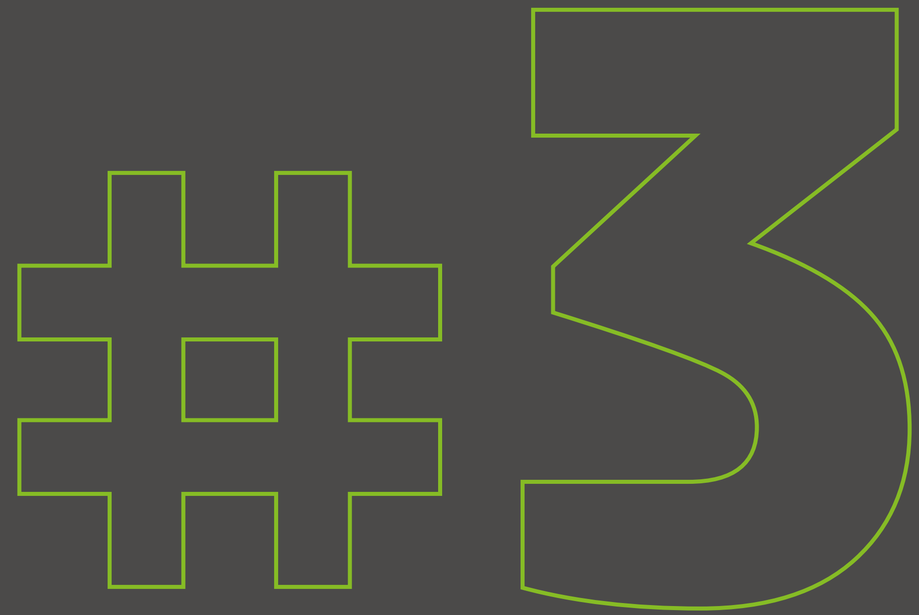
Sua instituição exige relatórios periódicos ao prestador de serviços de TI?



Qual é a periodicidade desses relatórios?



ANBIMA



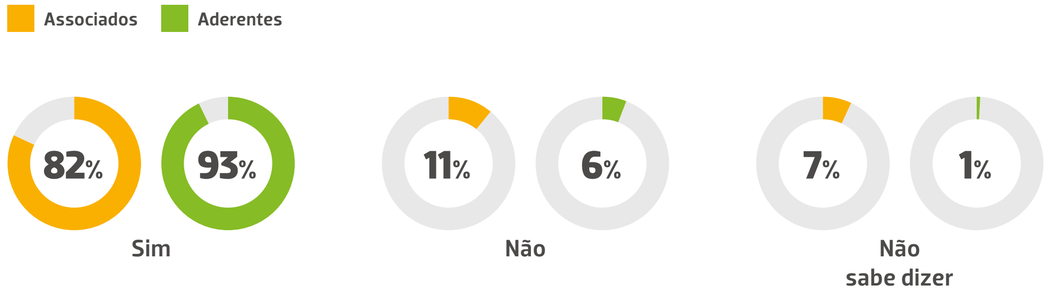
COMPUTAÇÃO EM NUVEM

COMPUTAÇÃO EM NUVEM

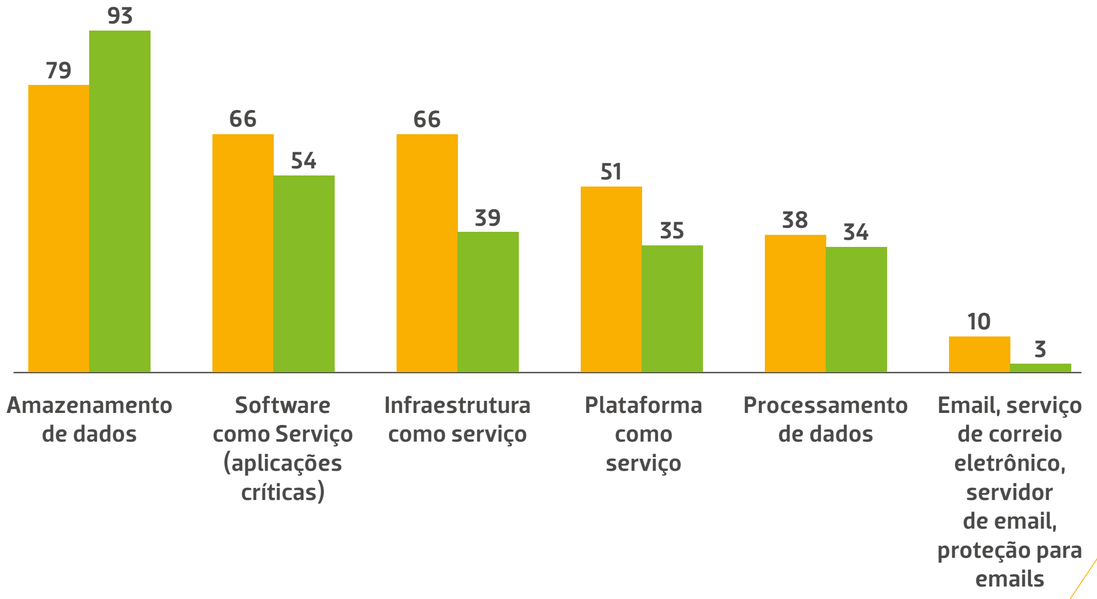
O uso da computação em nuvem segue crescendo de forma consistente. Entre as empresas associadas, 82% afirmaram ter ativos localizados na nuvem, três pontos percentuais a mais do que em 2018 e sete pontos percentuais acima de 2017.

Os aderentes se destacam nesse quesito, com 93% fazendo uso da computação em nuvem. Entre os serviços contratados, o armazenamento de dados é o mais utilizado, principalmente pelos aderentes, seguido por software como serviço, infraestrutura como serviço, plataforma como serviço e servidor de e-mail.

Sua instituição contrata serviço ou possui ativo localizado em computação em nuvem? (em %)



Serviços contratados



Vale lembrar que 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 situações, além de requisitos adicionais no caso de contratação do serviço no exterior.

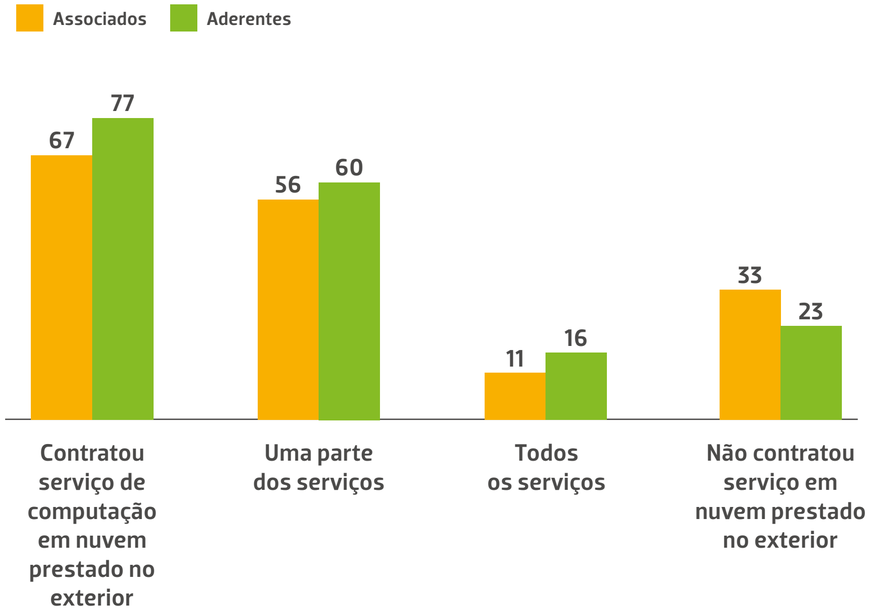
Em linha com as edições anteriores, três quartos dos associados que contratam computação em nuvem realizam diligência na contratação do serviço. Entre os aderentes, esse percentual cai para 63%.

No corte por segmento, as gestoras de recursos são o grupo que mais contrata serviço ou possui ativo localizado em computação em nuvem — 89% das assets associadas e 93% das aderentes. Faz sentido que seja assim uma vez que as assets estão fora do perímetro regulatório da resolução citada.

A maioria dos recursos em nuvem está alocada em rede privada, tanto entre associados (61%) quanto entre os aderentes (72%). Outro ponto de atenção é que aproximadamente 70% dos serviços em nuvem estão localizados no exterior, principalmente nos EUA, uma vez que as principais prestadoras desse tipo de serviço – como Amazon, Microsoft e Google –, estão lá. Apesar disso, apenas uma pequena parcela das empresas deixa todos os serviços alocados fora do país (11%).

De modo geral, infraestrutura e plataforma como serviço são os mais utilizados por empresas de grande porte fora do país.

Sua instituição contrata serviço de computação em nuvem prestado no exterior? (em %)



Sua instituição realiza diligência na contratação do serviço em nuvem?

ANBIMA

TESTES

4.1 – TESTES EXTERNOS DE PENETRAÇÃO

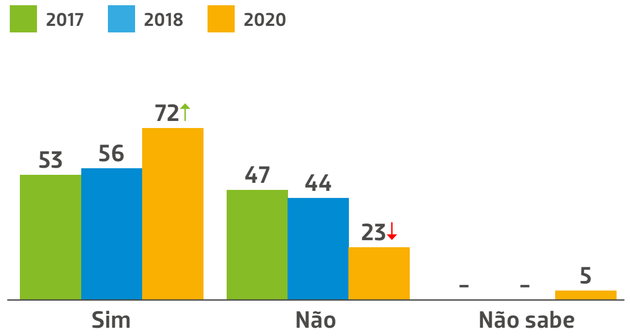
A realização de testes externos de penetração foi um dos destaques desta edição da pesquisa. Nas edições anteriores da Pesquisa de Cibersegurança da ANBIMA, percebeu-se uma incidência reduzida de testes de penetração em geral em gestoras.

Para mitigar essa situação, a associação promoveu uma iniciativa piloto, incluída no Plano de Ação 2019 da Associação, que realizou testes de penetração compartilhados em 15 gestoras. O objetivo da iniciativa foi fomentar a cultura de realização de testes de penetração, além de disseminar os resultados como boas práticas a todos os associados.

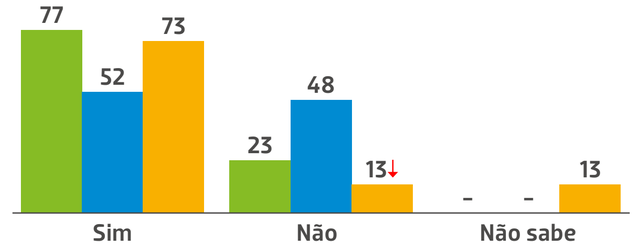
Seja decorrente dessa iniciativa, seja em razão de uma maior conscientização sobre o tema, o fato é que, nesta pesquisa, cerca de 70% dos associados afirmaram ter feito esse tipo de teste no último ano, contra apenas 56% em 2018 e 53% em 2017. Em 89% dos casos, a periodicidade do teste é de até um ano. Entre os aderentes, 44% disseram ter realizado testes desse tipo.

Na maioria dos casos (85%), o teste foi feito por terceiros. Entre aqueles que não realizaram testes, 77% têm planos para fazê-los, o que representa um crescimento de 21 pontos percentuais ante 2018.

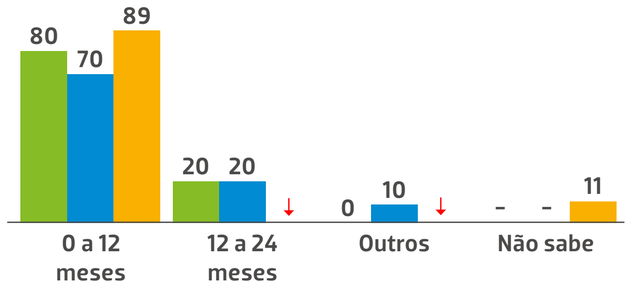
Sua instituição realizou testes externos de penetração no último ano? (em %)



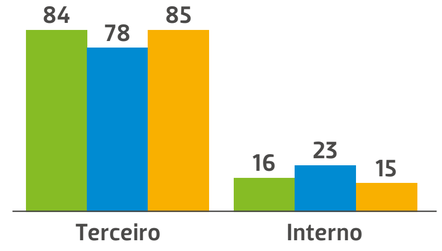
Há algum plano prevendo este teste? (em %)



Qual é a periodicidade do teste? (em %)



Quem realizou o teste? (em %)



4.2 – TESTES INTERNOS DE PENETRAÇÃO

A realização de testes internos de penetração é uma prática adotada por 65% das instituições associadas, percentual superior ao observado em 2018 (58%) e em linha com o de 2017 (63%). Chama a atenção, nesta edição, o fato de que 73% dos associados têm planos de fazer esse tipo de teste, um crescimento significativo em relação às pesquisas anteriores.

Entre os aderentes, a prática é menos comum. Em geral, a periodicidade desses testes é de até 12 meses.

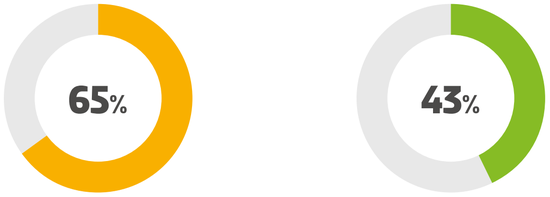
Sua instituição já realizou teste internos de penetração?

2017	2018	2020
63%	58%	65%

Há algum plano para a realização de teste?

2017	2018	2020
42%	43%	73% ↑

Já realizou testes internos de penetração?



4.3 – PHISHING

A realização de exercício de phishing foi outro ponto de destaque desta edição, alcançando 59% das associadas, o que representa um aumento significativo ante 2018 (46%) e 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.

Além disso, quase todas as instituições (96%) orientam os usuários para ter atenção especial antes de clicar em links, mesmo vindos de pessoas conhecidas.

Instituição realizou exercício de phishing no último ano

2017	2018	2020
44%	46%	59% ↑

ANBIMA

#5

REGULAÇÃO

REGULAÇÃO

O mundo digital impõe enormes desafios aos reguladores, que precisam acompanhar as rápidas mudanças desse universo. Ao mesmo tempo, tudo deve ser analisado e amadurecido, para que as regras cumpram seu papel de garantir a segurança de todos, e não de ser simplesmente um obstáculo para os negócios.

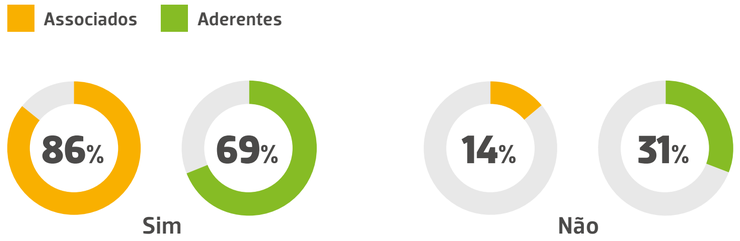
Entre as empresas associadas, 86% afirmam que suas políticas de cibersegurança contemplam a regulação sobre o tema. O número mostra um aprimoramento do mercado, levando em consideração o avanço significativo em relação a 2018, quando esse percentual era de 52%.

Nota-se, ainda, uma diferença considerável nesse sentido entre os associados da ANBIMA e os aderentes, entre os quais apenas 69% afirmaram contemplar a regulação em suas políticas.

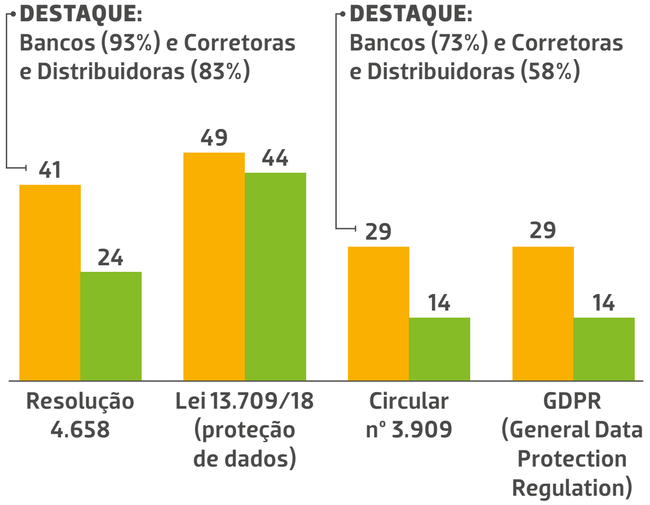
Neste quesito, é importante olhar também os dados por segmento — gestoras, bancos e corretoras —, uma vez que as diferentes legislações e regulamentações nem sempre têm abrangência sobre todos eles. A Resolução 4.658 da CVM contempla bancos e corretoras, mas não incide sobre gestoras, enquanto a ICVM 505 e a ICVM 612 incidem sobre corretoras, mas não sobre bancos e gestoras, e a LGPD, que entrou em vigor em 2020, contempla todos os segmentos. Isso ajuda explicar as diferenças no gráfico ao lado, que mostram percentuais diferentes de adesão dependendo da legislação.

Entre os associados, 100% das corretoras e distribuidoras e dos bancos associados afirmaram que suas políticas de cibersegurança levam em consideração a regulação sobre o tema. Para as assets, esse percentual cai 76%. Não temos bancos entre os aderentes, mas, nesse recorte, o percentual de corretoras e distribuidoras que dizem o mesmo é de 90% e o das assets, para 66%.

A implementação das políticas de cibersegurança da instituição contempla a regulação sobre o tema? (em%).



Quais regulações estão sendo contempladas?



ANBIMA

#6

COVID-19

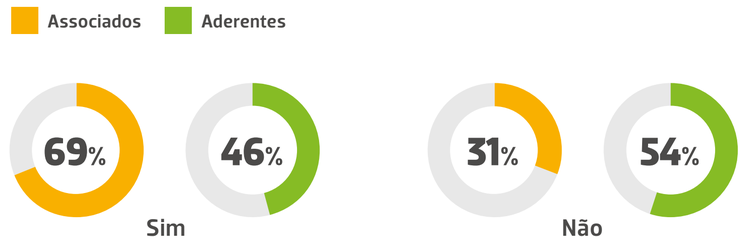
COVID-19

A pandemia de Covid-19 afetou os negócios em todas as frentes. Para entender os efeitos disso sobre a segurança cibernética incluímos um capítulo a mais nesta edição.

A maioria dos associados revisou o plano de continuidade de negócio (69%). Já entre os aderentes, menos da metade das empresas (46%) adotou essa política.

As áreas mais envolvidas no plano de continuidade foram as de Segurança Tecnológica e de Negócios. Cerca de 20% das instituições utilizaram interlocução de terceiros para a revisão do plano de continuidade.

Sua instituição revisou o plano de continuidade de negócio em virtude da Covid-19?



Quantas áreas, em média, foram envolvidas?

Quais áreas foram envolvidas no plano de continuidade? (em %).

Apesar de a maioria das instituições associadas ter site de contingência (86%), grande parte (78%) não o acionou durante a pandemia. Isso decorre da própria natureza da situação, que demandava distanciamento social, sendo mais adequada a política de home office. Entre os aderentes, 66% contam com site de contingência e 37% o acionaram nesse período. Ainda assim, apenas uma pequena parcela buscará alternativas para o site de contingência — 20% para os associados e 15% para os aderentes.

Sobre o home office, cerca de 40% das associadas já contavam com programa para esse regime de trabalho. A adoção dessa modalidade para todos os funcionários é maior entre os aderentes e tende a ser maior em empresas de menor porte, uma vez que é mais fácil acompanhar o programa.

Devido à necessidade de isolamento e distanciamento social, a política de home office foi estendida ou implantada para grande parcela dos funcionários. Na maioria dos casos, foram despendidas até duas semanas para isso, com um pouco mais de rapidez entre aderentes e empresas de pequeno porte.

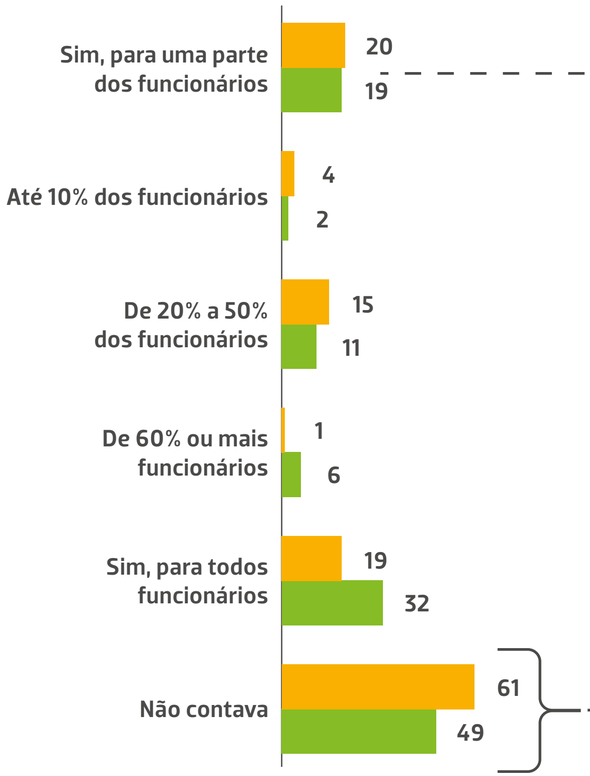
A pandemia também causou mudanças de paradigmas de gestão de continuidade de negócios para 42% dos associados. Entre os aderentes, esse percentual é menor (13%). De modo geral, essa percepção de mudança foi sentida em empresas de grande porte, como bancos e corretoras e distribuidoras.

Ainda que no cômputo geral a maioria das instituições não tenha identificado aumento de ataques cibernéticos ou engenharia social em decorrência da implementação do trabalho remoto, esse é um dado que precisa ser segmentado. No caso dos bancos, 63% observaram elevação nesse tipo de ataque.

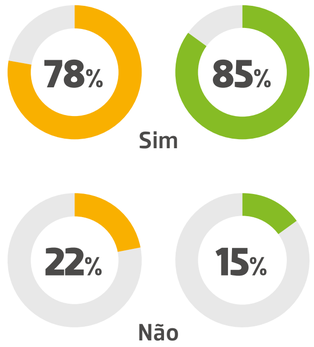
Vale destacar que os bancos costumam ser instituições maiores e que controlam mais de perto os ataques, identificando de forma mais adequada e prematura quaisquer incidentes dessa natureza. Nesse sentido, a combinação de computação em nuvem e home office em maior escala pode trazer riscos adicionais que devem ser avaliados e monitorados com cautela e frequência especiais.

Associados Aderentes

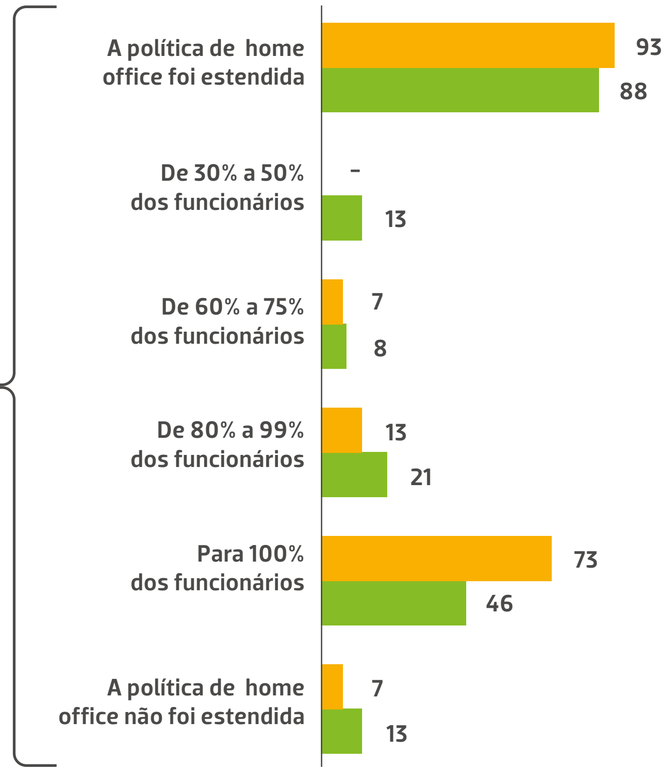
Sua instituição contava com sistema de home office? (em %)



Foi implantado o home office com a pandemia? (em %)



Com a pandemia o home office foi estendido para maior número de funcionários? (em %)



ANBIMA

#7

CONCLUSÃO

CONCLUSÃO

A despeito dos efeitos da pandemia de coronavírus, a terceira edição da Pesquisa ANBIMA de Cibersegurança mostra uma consolidação das práticas relacionadas a cibersegurança. A existência de programa, política e formalização vem crescendo ao longo dos anos do estudo e chegou a praticamente 95% das instituições entrevistadas, sem diferenças significativas entre associados e aderentes nesse aspecto.

A pesquisa também permite entender as especificidades dos comportamentos de associados e aderentes em relação ao tema, trazendo resultados para esse grupo pela primeira vez. Em geral, os números mostram que os associados exibem um leque maior de tipos de metodologias desenvolvidas por outras fontes para a avaliação de risco cibernético.

Chamam a atenção a baixa adesão dos aderentes aos monitoramentos e testes. O aumento de instituições com programa, política e formalização é motivo de celebração, mas, para que eles produzam o efeito desejado, as empresas precisam se manter atualizadas sobre novas vulnerabilidades e ameaças. A importância do assunto justifica a priorização da pauta. Não é à toa que, entre as empresas associadas, todas declararam que os grupos envolvidos com o programa se mantêm atualizados sobre novas ameaças.

Outra constatação importante é que os aderentes trabalham mais com computação em nuvem e contam com programas de home office mais ampliados que os associados. É bastante provável que isso se deva ao fato de haver mais empresas de pequeno porte entre os aderentes. Isso torna mais fácil

tanto a implantação e o acompanhamento das equipes em trabalho remoto. Como mencionado acima, a combinação de computação em nuvem e home office em maior escala pode trazer riscos adicionais.

Os números mostraram também que a entrada em vigor, neste ano, da LGPD (Lei Geral de Proteção de Dados) contribuiu para que uma grande parcela das políticas de cibersegurança também contemplassem a regulação sobre o tema.

De forma geral, as instituições associadas apresentam um programa de cibersegurança mais robusto em comparação com as aderentes. Essa constatação não chega a causar surpresa, principalmente porque muitos associados são empresas de médio ou grande porte, enquanto, entre os aderentes, é mais comum encontrarmos empresas de menor porte. As próximas edições da pesquisa devem ajudar a compreender qual é o melhor caminho para que essas empresas também avancem nas políticas e práticas de cibersegurança.

Esses dados servirão para basear a agenda de atividades do Grupo Técnico de Cibersegurança da ANBIMA em 2021. O tema está na pauta de discussão da Associação, com destaque para o aprimoramento de boas práticas de cibersegurança, com a revisão do guia e das seções de cibersegurança dos códigos de autorregulação, levando em conta os impactos da pandemia e as novas formas de trabalho. Ações compartilhadas, como fomento ao compartilhamento de incidentes cibernéticos, também estão incluídas na pauta a ser discutida. As informações são relevantes, ainda, para fomentar o debate entre associados, reguladores e demais players.

3ª PESQUISA ANBIMA DE CIBERSEGURANÇA

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

Presidente
Carlos Ambrósio

Vice-presidentes
Carlos Constantini, Gilberto Duarte, José Eduardo Laloni, Luiz Sorge, Roberto Paolino, Roberto Paris e Sergio Cutolo

Diretores
Adriano Koelle, Carlos Takahashi, Eduardo Azevedo, Fernando Rabello, Gabriel Cardozo, Gabriel Leal, Jan Karsten, Luciane Ribeiro, Luiz Chrysostomo, Luiz Fernando Figueiredo, Lywal Salles Filho, Pedro Juliano, Pedro Rudge e Teodoro Lima

Comitê Executivo
Zeca Doherty, Francisco Vidinha, Guilherme Benaderet, Patrícia Herculano, Eliana Marino, Lina Yajima, Marcelo Billi, Soraya Alves e Thiago Baptista

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

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

ANBIMA

WWW.ANBIMA.COM.BR