Grupo Técnico de Cibersegurança

2° Pesquisa ANBIMA de Cibersegurança | 2018

ANBIMA

ANBIMA

Principais características

- *Pesquisa estruturada e conduzida pelo Grupo Técnico de Cibersegurança da ANBIMA*
- *Objetivo: avaliar o* ***grau de maturidade*** *do mercado local*
  - *Em 2018:* **identificar avanços e recuos** das instituições em relação ao tema entre os dois anos

- *Estrutura do questionário: Benchmark - Guia de Cibersegurança ANBIMA*

- *Alterações em 2018:*
  - *Manutenção da estrutura geral de 2017 – comparabilidade entre os anos*
  - *Aperfeiçoamentos à estrutura e incorporação de pontos trazidos pela regulação*
    - *Governança; Computação em nuvem no exterior; e Compartilhamento de informações sobre incidentes; Relação com terceiros; e Adaptação à regulação*

Principais temas tratados na pesquisa

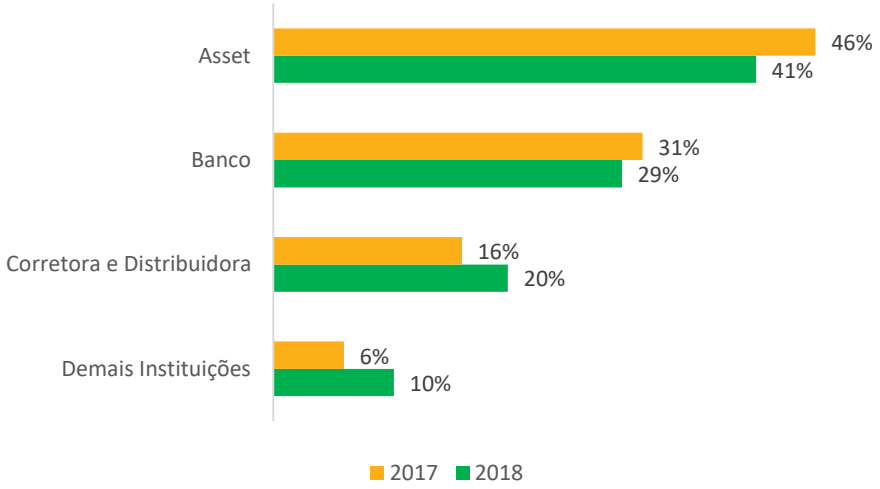
1. **Perfil** das instituições
2. **Programa, política ou formalização** de procedimentos de segurança cibernética – Informações Gerais
3. **Componentes** do programa de segurança cibernética (Guia)
    1. *Avaliação de riscos*
    2. *Ações de prevenção e proteção*
    3. *Monitoramento e testes*
    4. *Criação do plano de resposta a incidentes*
    5. *Reciclagem e revisão*
4. Computação em **nuvem**
5. **Testes**
6. **Regulação**

Aplicação da pesquisa

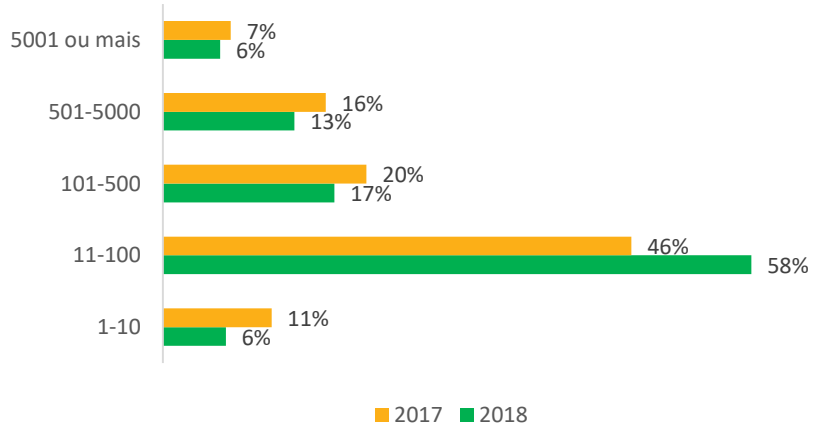
- Envio para todos os associados ANBIMA - **259 instituições**
  - Prazo: *06/11/18 a 07/12/18*
- ***177 respondentes*** - ***68%*** *do total de associados (em 2017: 58%)*
  - *Amostra próxima da população (menor viés de seleção)*

Perfil das instituições

Segmento da Instituição



Porte da Instituição - nº de funcionários

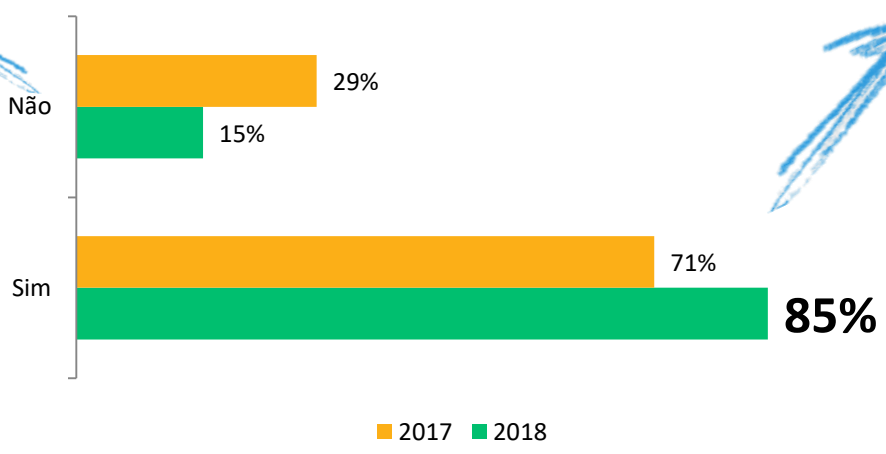


Principais temas tratados na pesquisa

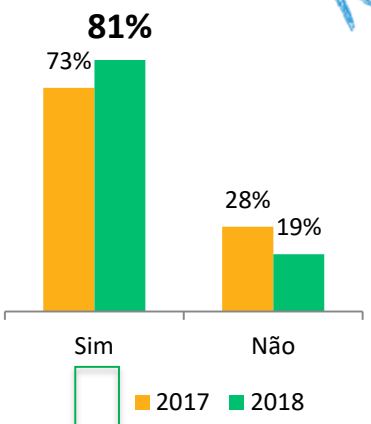
1. Perfil das instituições
2. **Programa, política ou formalização de procedimentos de segurança cibernética – Informações Gerais**
3. Componentes do programa de segurança cibernética
    1. Avaliação de riscos
    2. Ações de prevenção e proteção
    3. Monitoramento e testes
    4. Criação do plano de resposta a incidentes
    5. Reciclagem e revisão
4. Computação em nuvem
5. Testes
6. Regulação

Programa de Segurança Cibernética - Informações Gerais

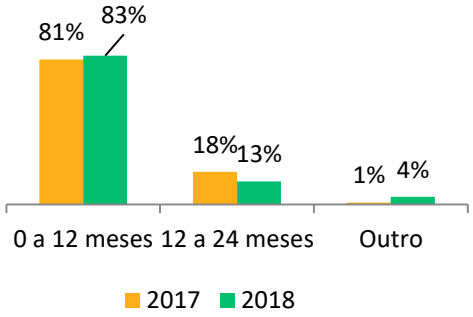
Sua instituição tem um **programa, política ou formalização de procedimentos formal de segurança cibernética?**



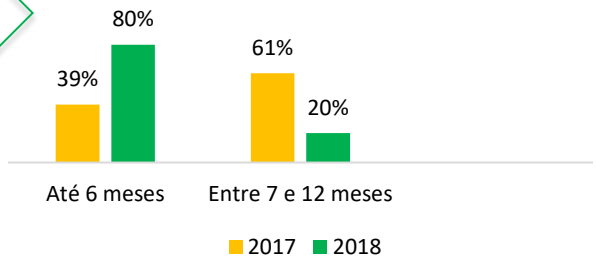
Se NÃO, ele está no planejamento da instituição ou em fase de elaboração?



Se SIM, qual foi a data da última atualização?

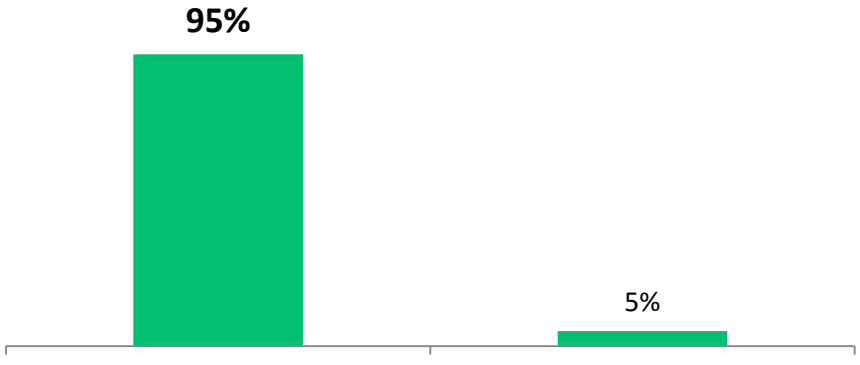


Se sim, em quantos meses será implementado?



Programa de Segurança Cibernética - Governança

Há um **responsável** dentro da instituição para tratar e responder questões de segurança cibernética? (nova em 2018)

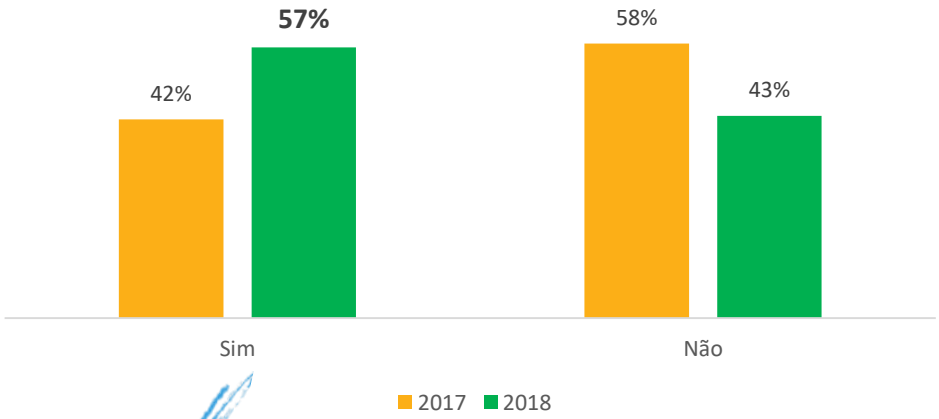


*Corretoras – Não: **11%***

Cargos, como:

- Sócio; VP
- Diretor de Compliance; Risco; Operações
- Gerencia de Seg. Informação; TI; Tecnologia; Riscos
- Coordenador ou analista

Sua instituição desenvolveu ou indicou um **comitê, fórum ou grupo** para tratar de segurança cibernética internamente, com representação e governança apropriados?

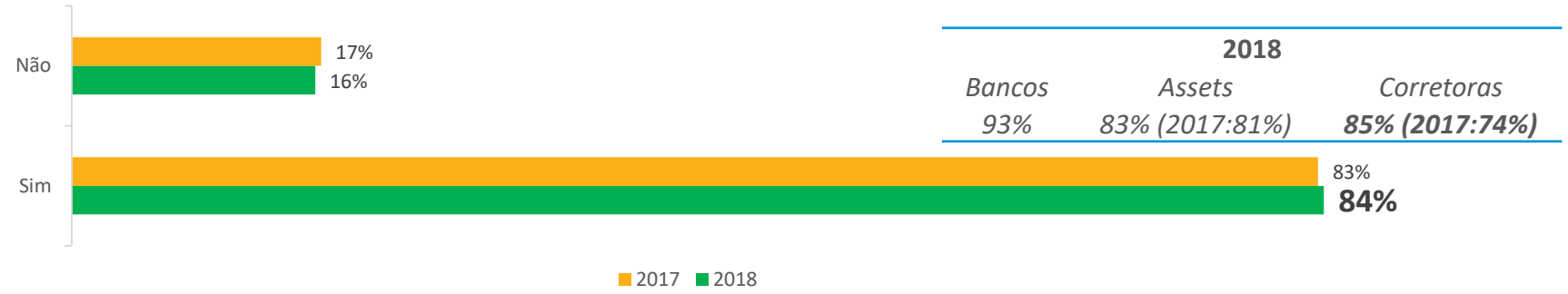


26 p. p. Corretoras (2017: 41%; 2018: 67%)

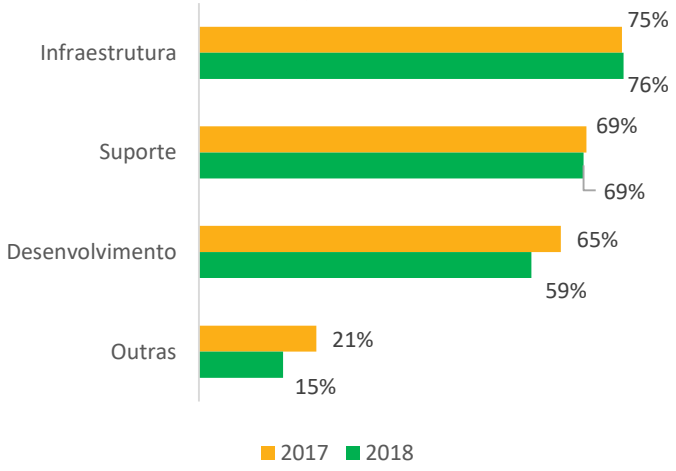
18 p. p. Assets (2017: 27%; 2018: 45%)

4 Contratação de serviços terceirizados de TI

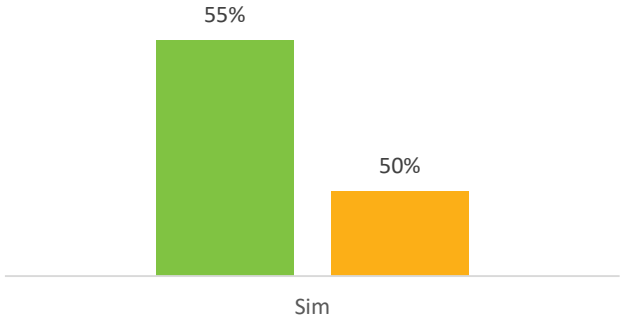
Instituições que contratam serviços terceirizados de TI



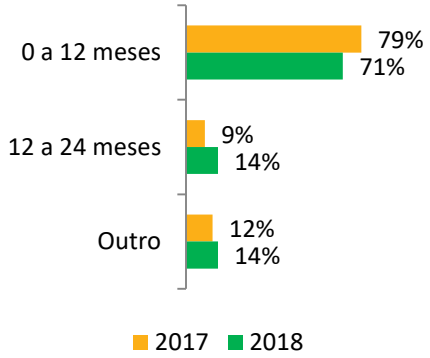
Se sim, em quais áreas?



Se sim, exige **relatório periódico para acompanhamento** de qualidade?



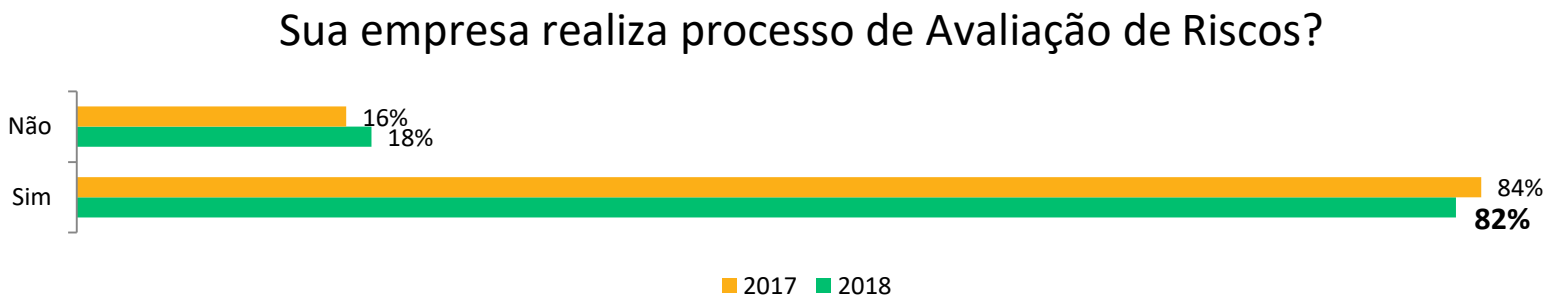
Se exige, qual periodicidade?



Principais temas tratados na pesquisa

1. Perfil das instituições
2. Programa, política ou formalização de procedimentos de segurança cibernética – Informações Gerais
3. **Componentes do programa de segurança cibernética**
    1. **Avaliação de riscos**
    2. Ações de prevenção e proteção
    3. Monitoramento e testes
    4. Criação do plano de resposta a incidentes
    5. Reciclagem e revisão
4. Computação em nuvem
5. Testes
6. Regulação

3.1 Avaliação de riscos (Risk assessment)



Elementos e ações específicas

	2017	2018	Δ2018/2017 em p .p
Identifica todos os **ativos relevantes** (equipamentos, sistemas, dados ou processos).	80%	78%	↓ -2
Avalia as **vulnerabilidades dos ativos** em questão (possíveis ameaças e o grau de exposição)	80%	86%	↑ 6
Mensura os possíveis **impactos financeiros, operacionais e reputacionais**, e expectativa	59%	59%	-
Determina e utiliza **metodologia** para avaliações de risco cibernético.	48%	51%	↑ 3
Elabora **regras para a classificação das informações** geradas, permitindo a implementação de processos para manuseio, armazenamento, transporte e descarte dessas informações.	48%	54%	↑ 6

Principais temas tratados na pesquisa

1. Perfil das instituições
2. Programa, política ou formalização de procedimentos de segurança cibernética – Informações Gerais
3. **Componentes do programa de segurança cibernética**
    1. Avaliação de riscos
    2. **Ações de prevenção e proteção**
    3. Monitoramento e testes
    4. Criação do plano de resposta a incidentes
    5. Reciclagem e revisão
4. Computação em nuvem
5. Testes
6. Regulação

3.2 Ações de Prevenção e Proteção

Sua instituição adota ações de prevenção e proteção, uma vez definidos os riscos?

Elementos e ações específicas

	2017	2018	Δ2018/2017 em p .p
• Tem **política de backup**.	-	99%	-
• Implementa **serviço de backup** dos diversos ativos da instituição	99%	96%	↓ - 3
• **Controle de acesso** aos ativos e sistemas das instituições	96%	96%	-
• Implementa recursos anti-malware nas estações e servidores de rede, como antivírus e firewalls pessoais	95%	94%	↓ -1
• **Regras mínimas na definição de senhas** de acesso a sistemas e rede	89%	91%	↑ 3
• Segurança de borda, nas redes de computadores, através de firewalls e outros mecanismos de filtros de pacotes	95%	90%	↓ -5
• Concessão de **acesso limitado a apenas recursos relevantes** para o desempenho das atividades	89%	86%	↓ -3
• **Restrição de acesso físico** nas áreas com informações críticas/sensíveis	92%	84%	-
• Cria **logs e trilhas** de auditoria sempre que os sistemas permitem.	90% *(Asset – 88%)*	84% *(Asset – 71%)*	↓ -6 (-17)
• Ao incluir novos equipamentos e sistemas em produção, garante que sejam feitas configurações seguras de seus recursos	78%	82%	↑ 4

3.2 Ações de Prevenção e Proteção (continuação)

Elementos e ações específicas

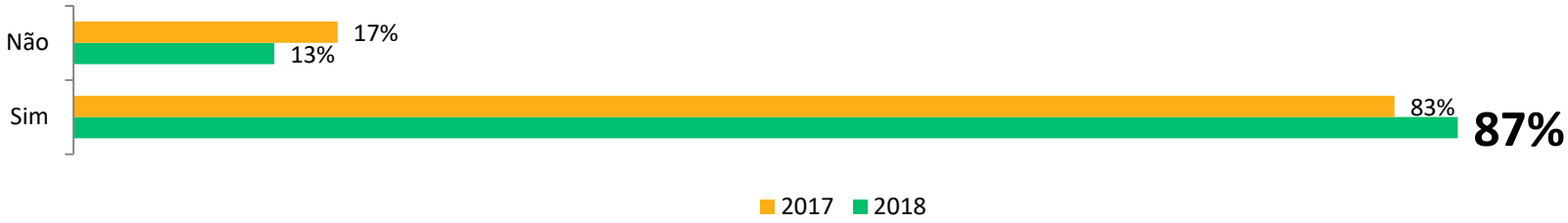
	2017	2018	Δ2018/2017 em p .p
• Controles **impedindo a instalação** e execução de software e aplicações não autorizadas	74%	80%	↑ 6
• Os eventos de logins e alteração de senhas são **auditáveis e rastreáveis**	81%	78%	↓ -3
• Implementa **segregação de serviços** sempre que possível, restringindo-se o tráfego de dados apenas entre relevantes	80% *(Corretora – 76%)*	78% *(Corretora – 100%)*	↓ -2 ↑ (14)
• Concessão de acesso implementada de forma a ser **revogada rapidamente** quando necessário	85%	76%	↓ -9
• Realiza **diligência na contratação de serviços** com terceiros, com devida avaliação de questões jurídicas, cláusulas de confidencialidade e exigência de controles de segurança na própria estrutura dos terceiros	72%	76%	↑ 4
• Realiza **teste em ambientes de homologação e de prova de conceito**, antes do envio à produção	81% *(Asset – 68%)*	73% *(Asset – 51%)*	↓ -8 (-17)
• Considera **questões de segurança já durante as fases, pré-projeto e o desenvolvimento** de novos sistemas, softwares ou aplicações	73%	65%	↓ -8
• Utiliza **gerenciador de senhas** para evitar o uso da mesma senha para facilitar a memorização em vários serviços	44%	34%	↓ -10
• Tem um **programa periódico de avaliação de segurança da informação em terceiros contratados**	-	32%	-

Principais temas tratados na pesquisa

1. Perfil das instituições
2. Programa, política ou formalização de procedimentos de segurança cibernética – Informações Gerais
3. **Componentes do programa de segurança cibernética**
    1. Avaliação de riscos
    2. Ações de prevenção e proteção
    3. **Monitoramento e testes**
    4. Criação do plano de resposta a incidentes
    5. Reciclagem e revisão
4. Computação em nuvem
5. Testes
6. Regulação

3.3 Monitoramento e Testes

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



Elementos e ações específicas

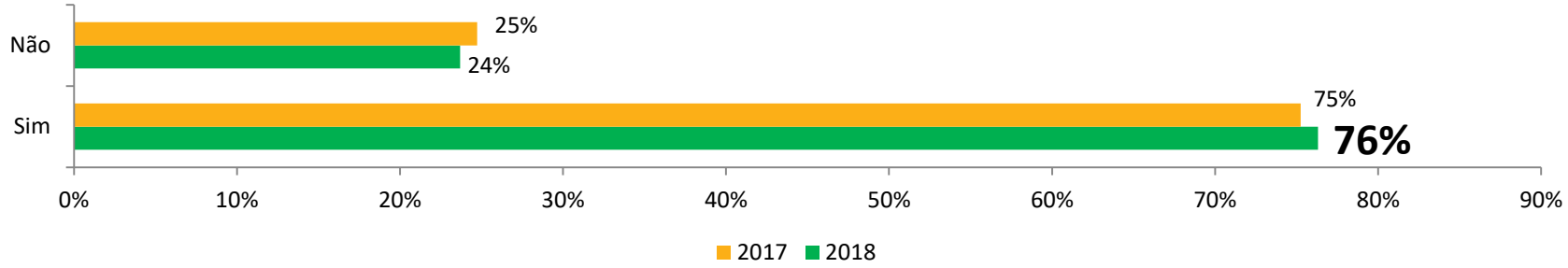
	2017	2018	Δ2018/2017 em p .p
▪ Mantém os sistemas operacionais e softwares de aplicação sempre **atualizados**.	92%	92%	-
▪ Monitora diariamente as **rotinas de backup**, executando testes regulares de restauração dos dados.	90%	89%	↓ -1
▪ Mantém **inventários atualizados de hardware e software**, e os verifica com frequência	81%	92%	↑ 11
▪ Cria mecanismos de **monitoramento de todas as ações de proteção** implementadas.	75%	69%	↓ -6
▪ **Analisa logs e trilhas de auditoria** criados	69%	70%	↑ 1
▪ Utiliza ferramentas de **centralização e análise de logs**.	46%	50%	↑ 4

Principais temas tratados na pesquisa

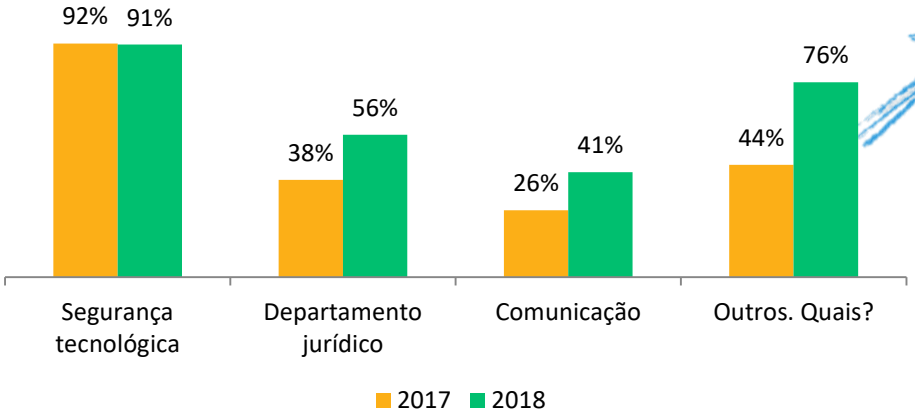
1. Perfil das instituições
2. Programa, política ou formalização de procedimentos de segurança cibernética – Informações Gerais
3. **Componentes do programa de segurança cibernética**
    1. Avaliação de riscos
    2. Ações de prevenção e proteção
    3. Monitoramento e testes
    4. **Criação do plano de resposta a incidentes**
    5. Reciclagem e revisão
4. Computação em nuvem
5. Testes
6. Regulação

3.4 Criação do Plano de Resposta

A sua instituição conta com **plano de ação e resposta** para incidentes ou ataques cibernéticos visando implementação do Programa de Cibersegurança?



Quais são as áreas envolvidas na elaboração do plano?



Outros, como:

- Compliance;
- Riscos;
- Infraestrutura;
- Áreas de negócio;
- Deptos. Operacional e Financeiro;
- Operações e Back Office;

Aumento da interdisciplinaridade

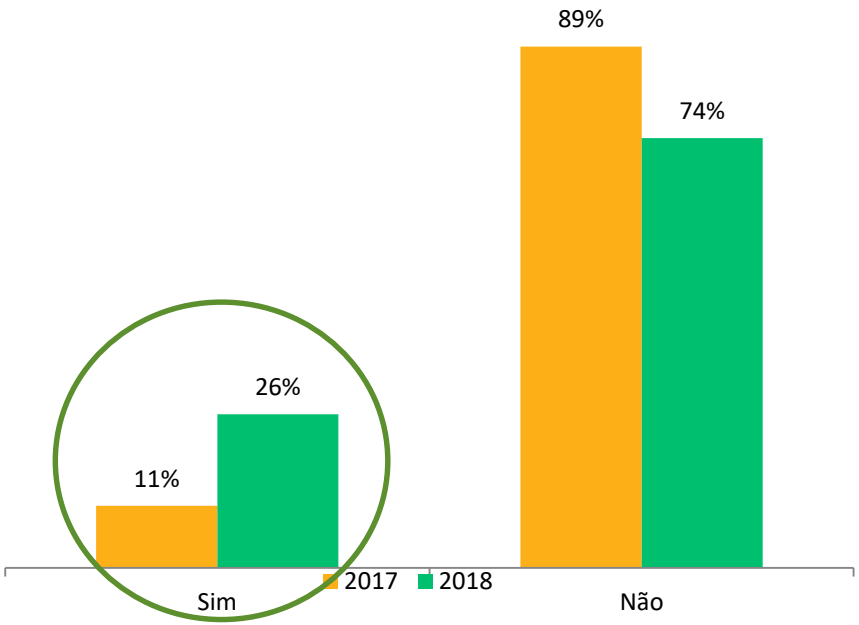
3.4 Criação do Plano de Resposta (continuação)

Elementos e ações específicas

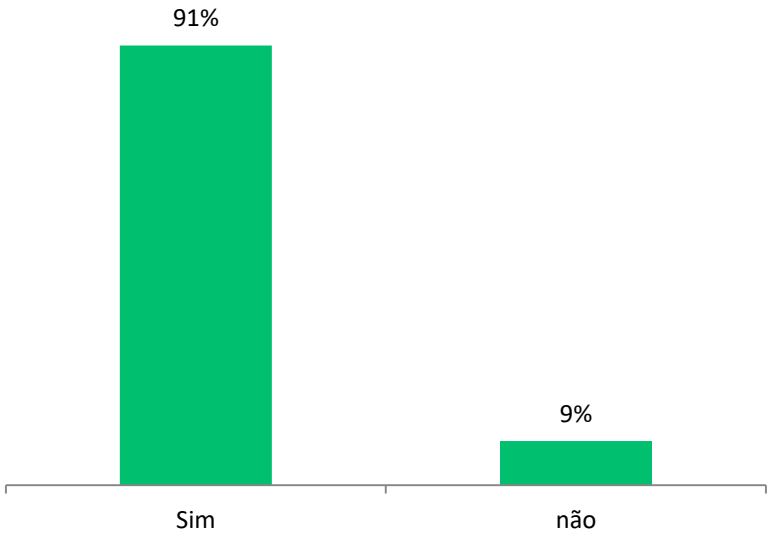
	2017	2018	Δ2018/2017 em p .p
Apresenta **plano de continuidade dos negócios** e processos de recuperação e remediação	96%	100%	↑ 4
Realiza o **arquivamento de documentações** relacionadas ao gerenciamento dos incidentes e ao plano de continuidade de negócios para servir como evidência	85%	95%	↑ 10
Leva em consideração questões de Segurança e **controles de acesso também nas instalações de contingência**	96%	95%	↓ -1
O plano leva em consideração os cenários de ameaças previstos na avaliação de risco	74%	75%	↑ 1
Há a **definição de papéis e responsabilidades dentro do plano de ação e respostas**, prevendo acionamento dos colaboradores e contatos externos?	78%	73%	↓ -5
Sua instituição **testa o acionamento** destas pessoas com o intuito de validar a eficácia do processo?	-	68%	-
Há **critérios para classificação dos incidentes**, por severidade	67%	59%	↓ -8

3.4 Criação do Plano de Resposta (continuação)

Sua instituição participa de alguma iniciativa para o **compartilhamento de informações** sobre os incidentes sofridos?



Se SIM, o compartilhamento de informações envolve **informações sobre incidentes recebidas de empresas prestadoras de serviços a terceiros**?



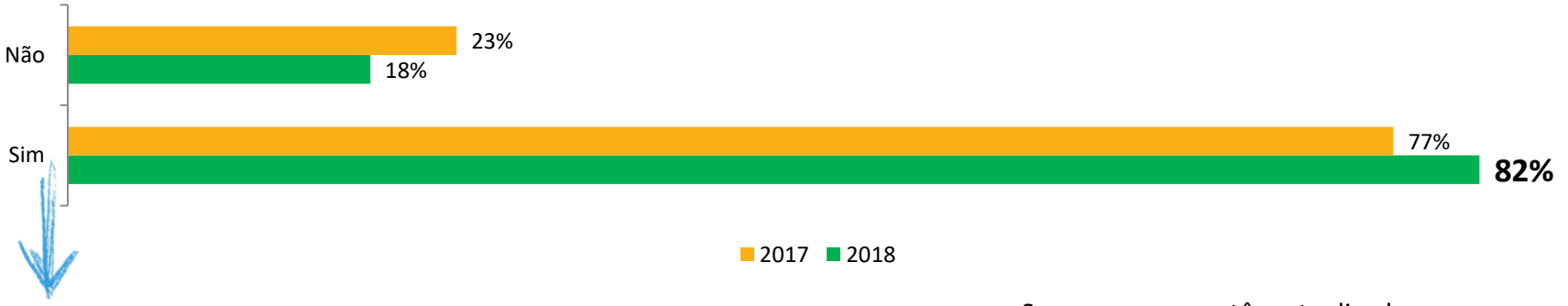
Mesmo número absoluto (10) de instituições!

Principais temas tratados na pesquisa

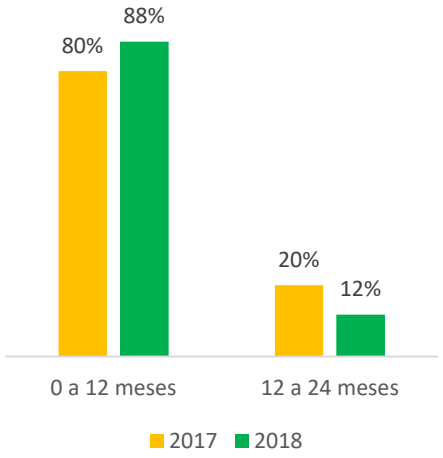
1. Perfil das instituições
2. Programa, política ou formalização de procedimentos de segurança cibernética – Informações Gerais
3. **Componentes do programa de segurança cibernética**
    1. Avaliação de riscos
    2. Ações de prevenção e proteção
    3. Monitoramento e testes
    4. Criação do plano de resposta a incidentes
    5. **Reciclagem e revisão**
4. Computação em nuvem
5. Testes
6. Regulação

3.5 Reciclagem e Revisão

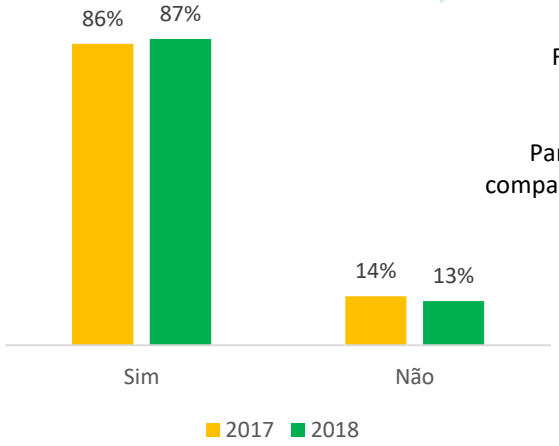
O Programa de Segurança Cibernética é **revisado periodicamente**, mantendo atualizados as avaliações de risco, as implementações de proteção, os planos de resposta a incidentes e o monitoramento dos ambientes?



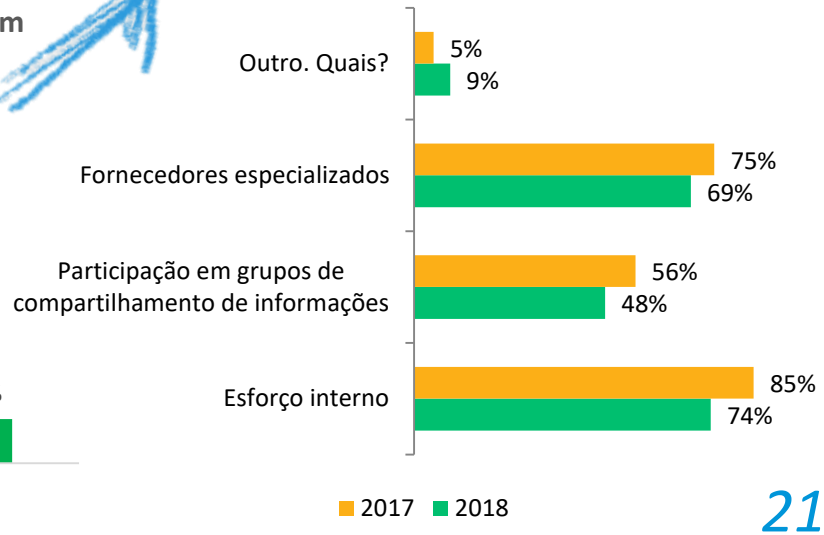
Se sim, qual é a periodicidade (meses)?



Os grupos envolvidos se mantêm atualizados?



Se grupos se mantêm atualizados, como a instituição obtém essas informações?



3.5 Reciclagem e Revisão

Elementos e ações específicas

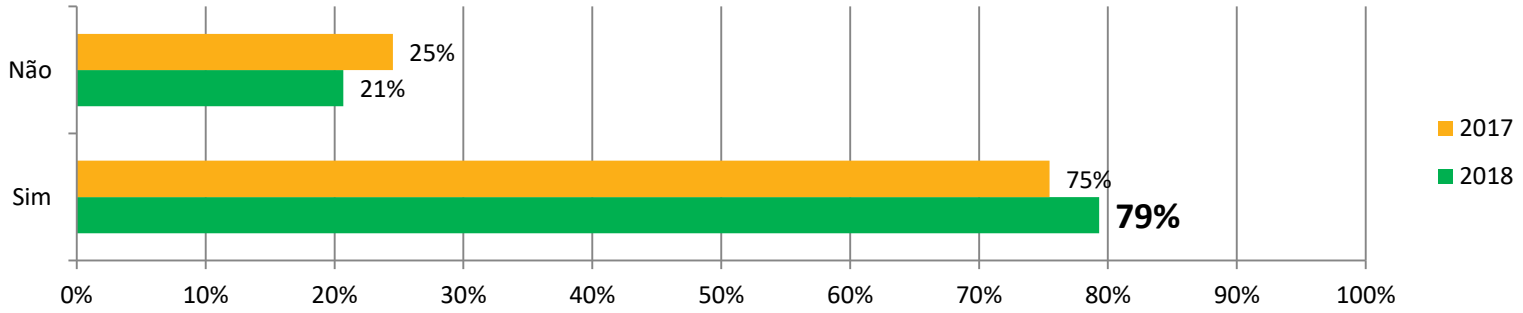
	2017	2018	Δ2018/2017 em p .p
Como parte de ações de conscientização, tem política de uso adequado da **estrutura tecnológica**, de forma independente ou como parte de um documento mais abrangente	87%	80%	↓ -7
Promove e dissemina uma cultura de segurança, com a criação de canais de comunicação internos para divulgar o programa de segurança cibernética e treinamentos	76%	75%	↓ -1
Define e mantém **indicadores de desempenho** (*key performance indicators*) que podem corroborar a conscientização e o envolvimento da alta administração e demais órgãos da instituição	30%	37%	↑ 7
O Programa de Segurança Cibernética é **divulgado também aos prestadores de serviços a terceiros**	-	47% (Asset – 37%)	

Principais temas tratados na pesquisa

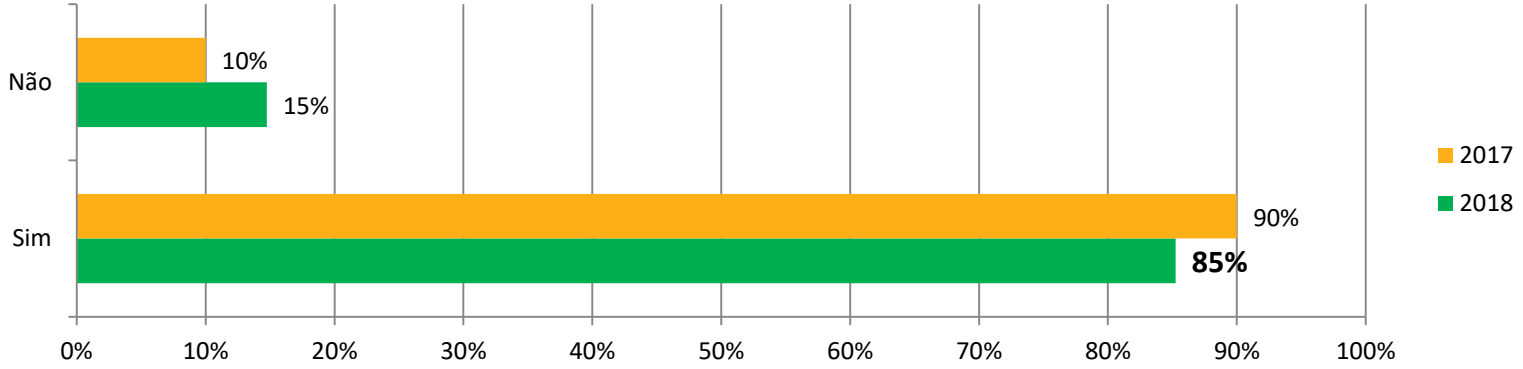
1. Perfil das instituições
2. Programa, política ou formalização de procedimentos de segurança cibernética – Informações Gerais
3. Componentes do programa de segurança cibernética
    1. Avaliação de riscos
    2. Ações de prevenção e proteção
    3. Monitoramento e testes
    4. Criação do plano de resposta a incidentes
    5. Reciclagem e revisão
4. **Computação em nuvem**
5. Testes
6. Regulação

Computação em nuvem

Possui algum serviço ou ativo da instituição localizdo externamente em nuvem? - Todas as intituições

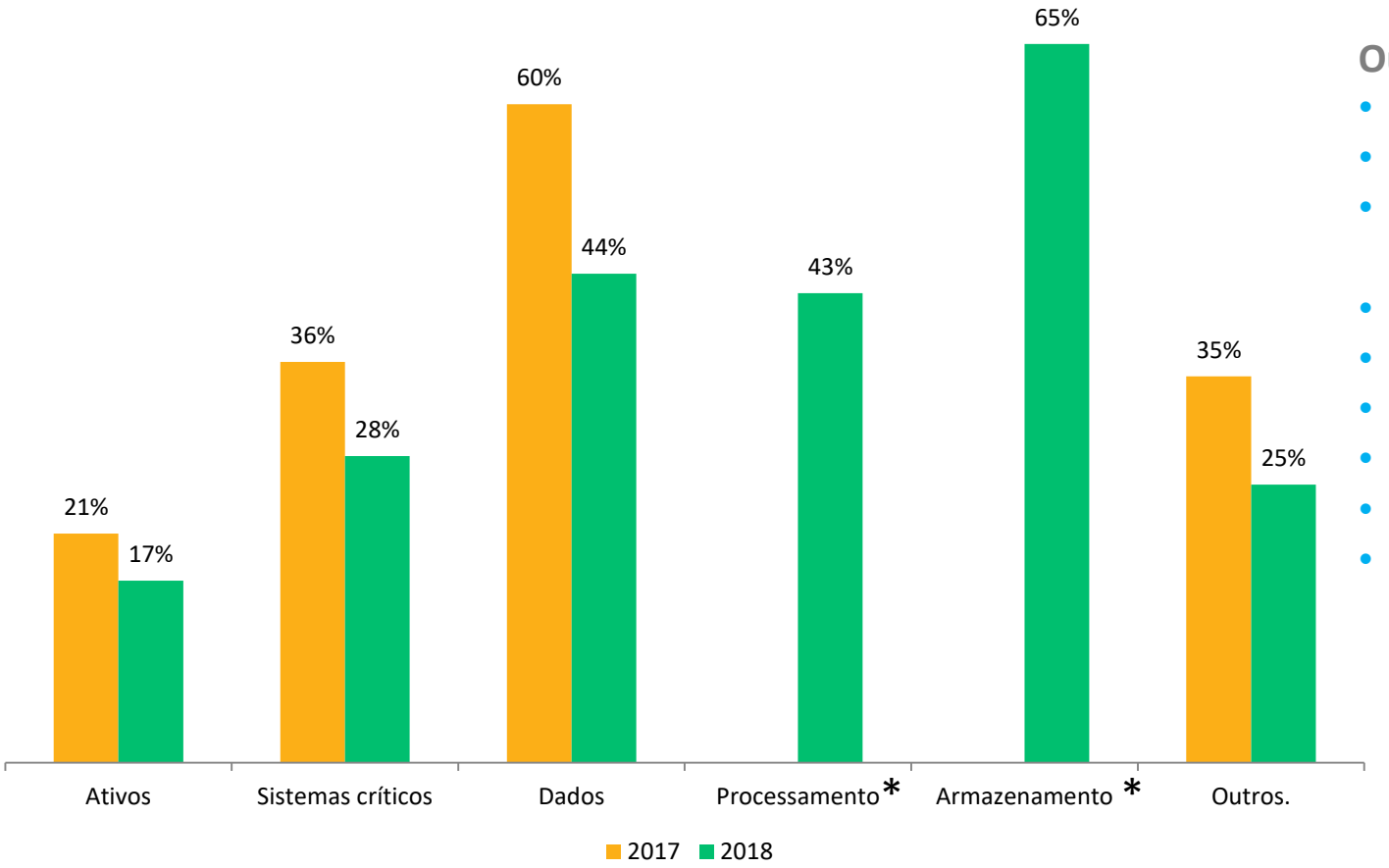


*Para **Assets** valor ainda maior:*



Computação em nuvem (continuação)

Se possui algum serviço ou ativo localizado em nuvem, quais são?



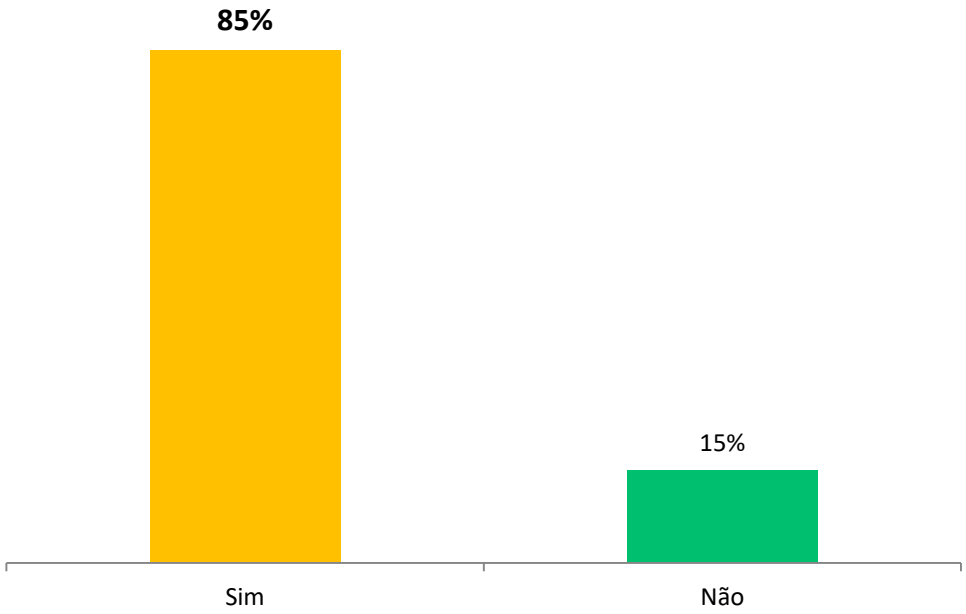
Outros, como:

- Backup de arquivos;
- E-mail;
- Serviços executados com sistemas de terceiros;
- Servidores;
- Sistema;
- Sistemas não críticos;
- Website;
- Controles Financeiros;
- Contingência.

*Questão Ausente em 2017

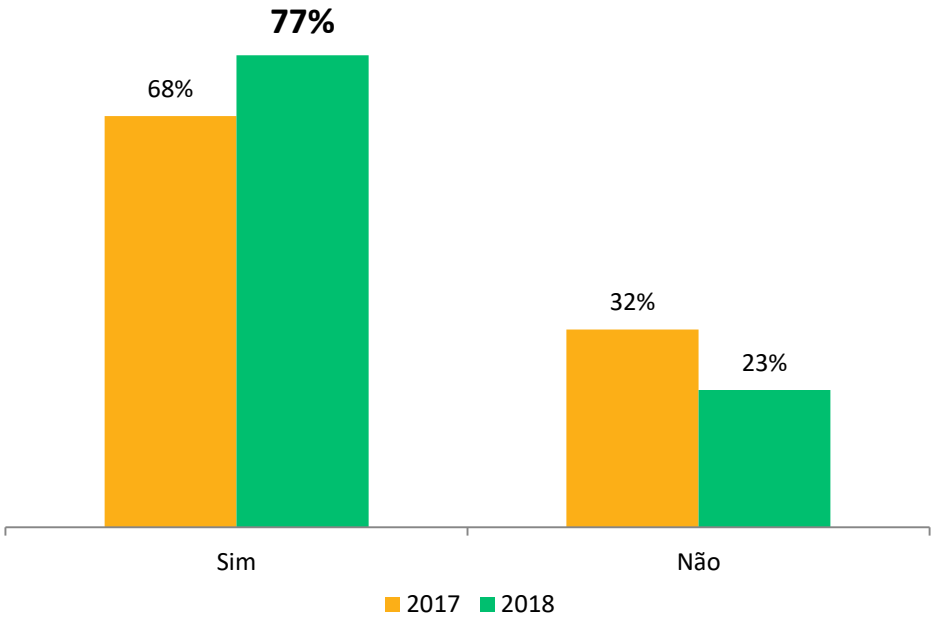
Computação em nuvem (continuação)

Ao contratar serviço em nuvem, garante que sejam feitas configurações seguras de seus recursos?



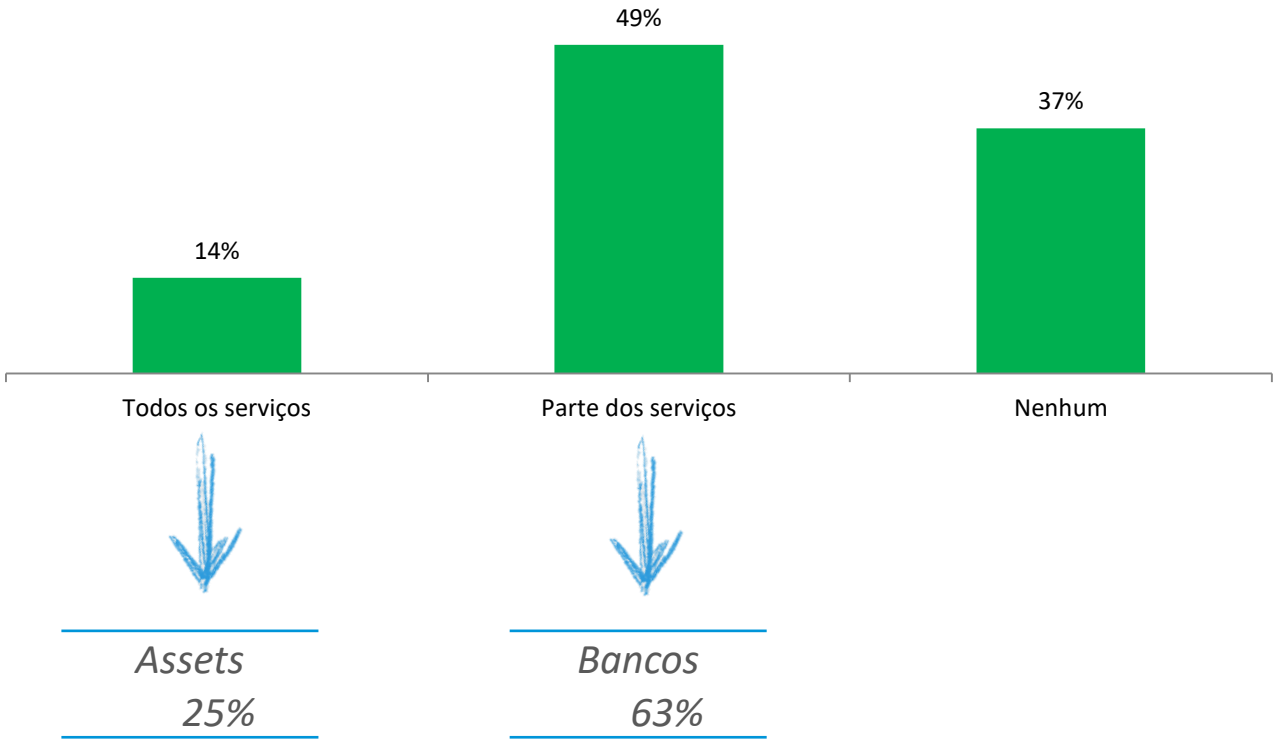
Similar à 2017!

Realiza diligência na contratação de serviços de computação em nuvem?



Computação em nuvem no exterior

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

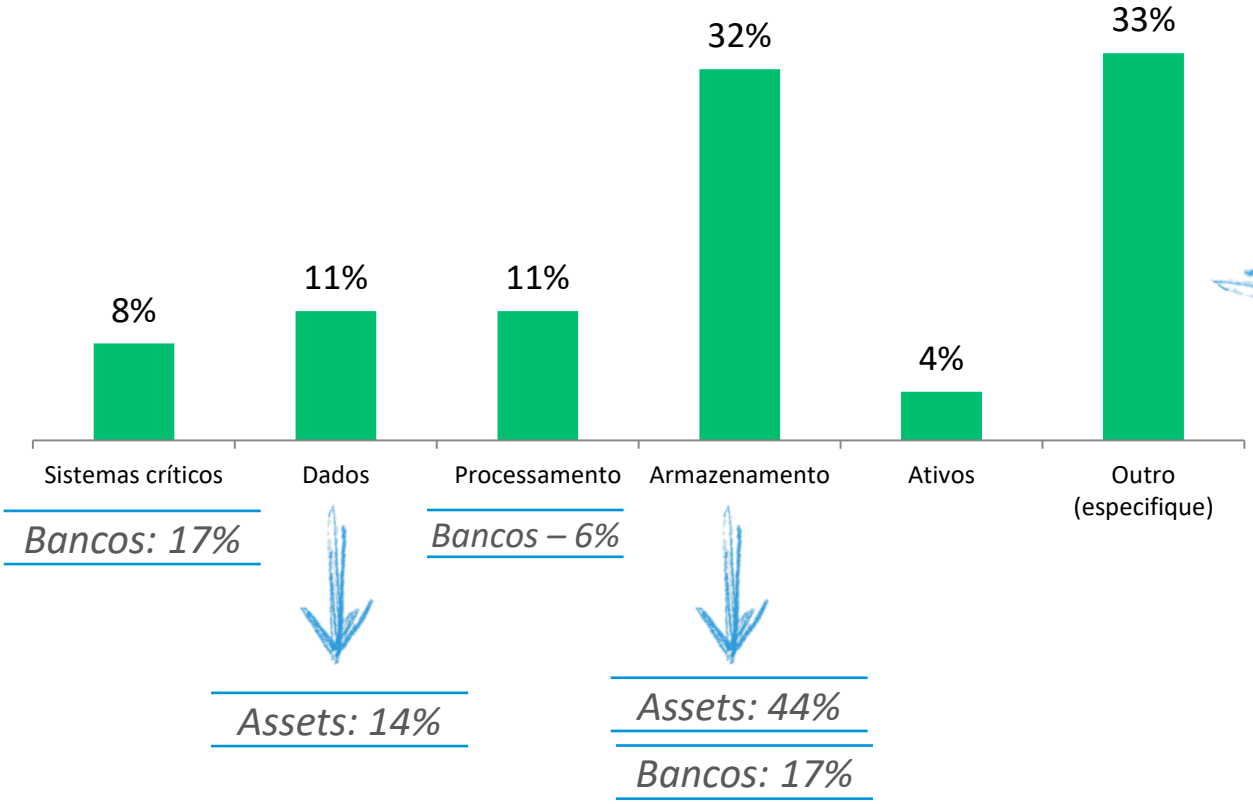


Exterior, como:

- Estados Unidos (maioria);
- Reino Unido;
- Portugal;
- Matriz (não especificado)

Computação em nuvem no exterior (continuação)

Qual parte do serviço o prestador é responsável?



Outros, como:

- Infraestrutura;
- Contingência;
- Processamento & Armazenamento;
- Sistemas não críticos;
- Site;
- E-mail.

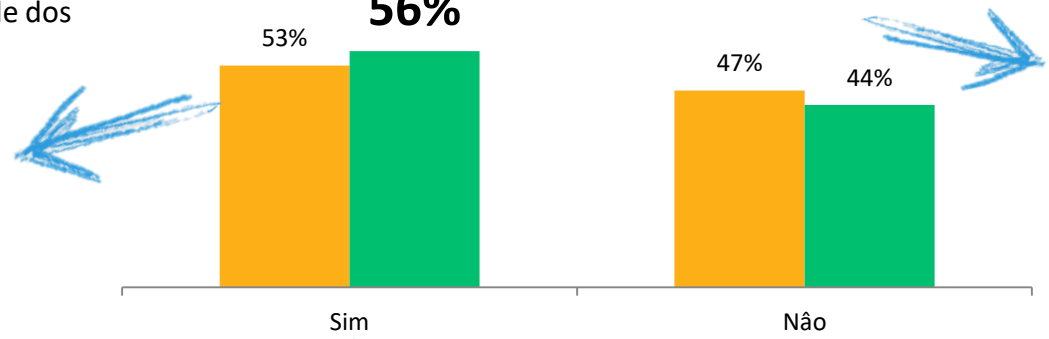
Principais temas tratados na pesquisa

1. Perfil das instituições
2. Programa, política ou formalização de procedimentos de segurança cibernética – Informações Gerais
3. Componentes do programa de segurança cibernética
    1. Avaliação de riscos
    2. Ações de prevenção e proteção
    3. Monitoramento e testes
    4. Criação do plano de resposta a incidentes
    5. Reciclagem e revisão
4. Computação em nuvem
5. **Testes**
6. Regulação

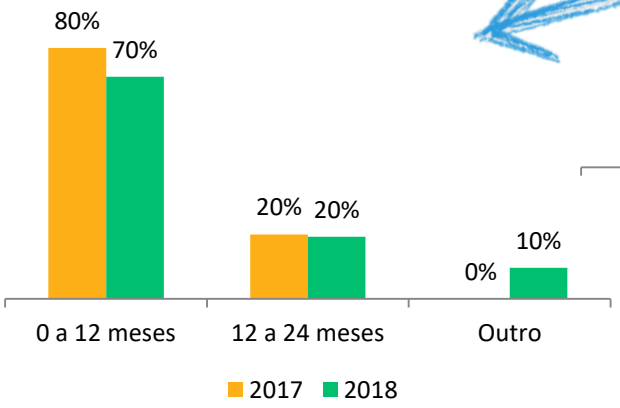
Monitoramento e Testes

Sua instituição já realizou **testes externos de penetração** no último ano?

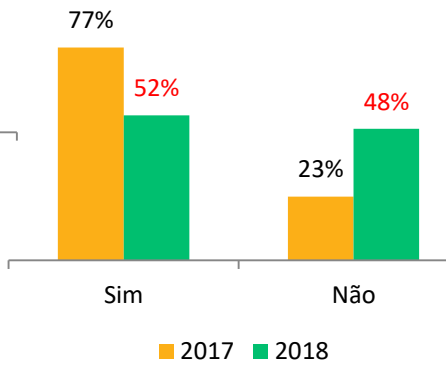
56%



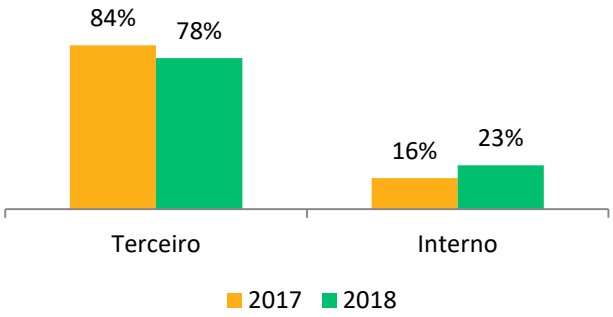
Se SIM, qual é a periodicidade dos testes de penetração?



Se NÃO, há algum plano prevendo a realização desse teste?



Se SIM, o teste foi realizado por:



*Entre Assets (2017: 37%; 2018: **40%**)*

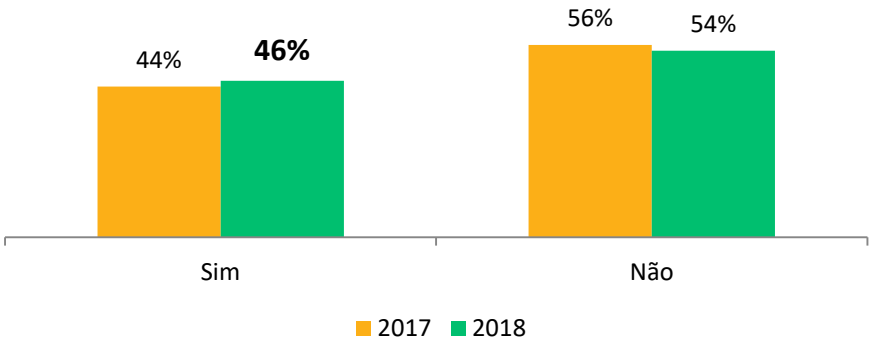
3 p. p.

*Entre Corretoras (2017:**44%**; 2018: 35%)*

-9 p. p.

Monitoramento e Testes (continuação)

Sua instituição realizou exercício de ***phishing*** no último ano?



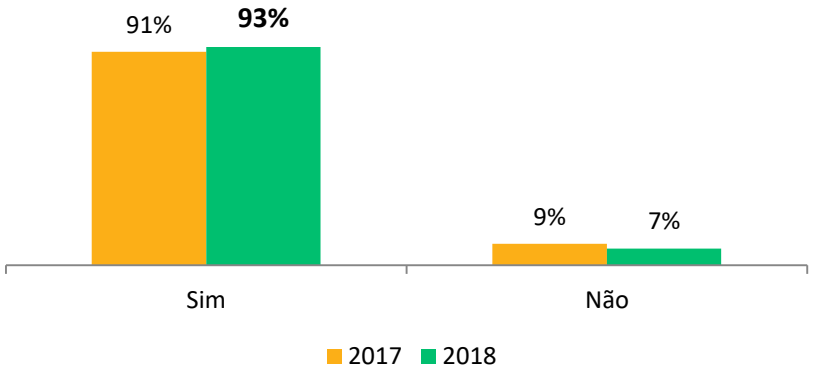
Assets (2018):
- 2017: 29%
*- 2018: **40%***

⬆ 11 p. p.

Corretoras (2018):
*- 2017: **47%***
- 2018: 19%

⬇ 28 p. p.

Há alguma orientação aos usuários quanto a ter **atenção especial antes de clicar em links recebidos**, mesmo vindos de pessoas conhecidas?

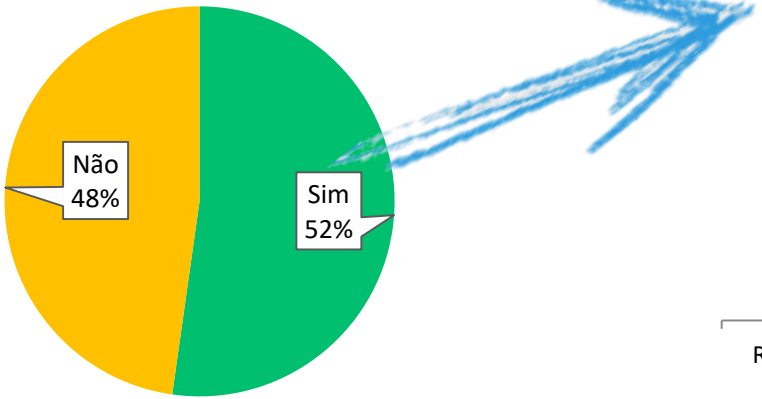


Principais temas tratados na pesquisa

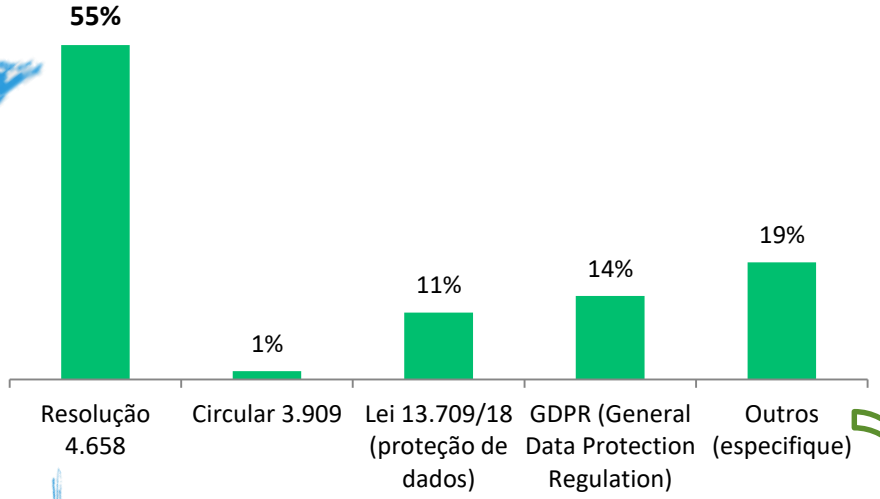
1. Perfil das instituições
2. Programa, política ou formalização de procedimentos de segurança cibernética – Informações Gerais
3. Componentes do programa de segurança cibernética
    1. Avaliação de riscos
    2. Ações de prevenção e proteção
    3. Monitoramento e testes
    4. Criação do plano de resposta a incidentes
    5. Reciclagem e revisão
4. Contratação de serviços terceirizados de TI
5. Computação em nuvem
6. Testes
7. **Regulação**

Regulação

A implementação das políticas de cibersegurança em sua instituição já **contempla** a regulação sobre o tema? (novo em 2018)



Quais?



Bancos: 71%
Intermediários: 80%

Instituições em processo de adaptação às normas

Outros, como:

- Códigos ANBIMA;
- Guia ANBIMA de Cibersegurança;

Principais Conclusões

1. 85% das empresas declararam ter um programa formal de segurança cibernética, atualizado no último ano por 83% destas instituições; 95% adotam ações de prevenção e proteção
2. 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 (aumento no universo de participantes)
3. Iniciativas de **compartilhamento de informações sobre incidentes** cibernéticos ainda é uma questão em evolução para os participantes do mercado local
4. **Testes de penetração externa e *Phishing*** registraram melhora nos indicadores, mas ainda são um ponto de atenção
5. Aumento da utilização do serviço de **computação em nuvem** e também da diligência com esse serviço
6. Há um processo em curso de adaptação às normas de cibersegurança.

Organização

Pesquisa estruturada e conduzida pelo **Grupo Técnico de Cibersegurança** da ANBIMA (*Superintendência de Representação institucional – Gerência de Estudos Regulatórios*)

Para mais informações sobre o GT, acesse:
http://www.anbima.com.br/pt_br/representar/grupos-de-trabalho/ciberseguranca/ciberseguranca.htm

Superintendência de Representação institucional
Gerência de Estudos Regulatórios

Rio de Janeiro
Av. República do Chile, 230 13º andar
20031-170 Rio de Janeiro RJ Brasil
+ 55 21 3814 3800

São Paulo
Av. das Nações Unidas, 8.501 21º andar
05425-070 São Paulo SP Brasil
+ 55 11 3471 4200

ANBIMA