Grupo Técnico de Cibersegurança

1°Pesquisa ANBIMA de Cibersegurança | 2017

ANBIMA

Resultados da Pesquisa em Cibersegurança junto aos Associados

Aplicação da pesquisa – ação realizada pelo *subgrupo 2*

- Envio para 262 instituições (*30/8 a 22/9*);
  - *Assets (117 instituições) envio de 2 pesquisas* (*3° Ed. da pesquisa IOSCO/AMCC-ICI);*

***Estrutura do questionário -** Guia de Cibersegurança ANBIMA reformulado como benchmark*

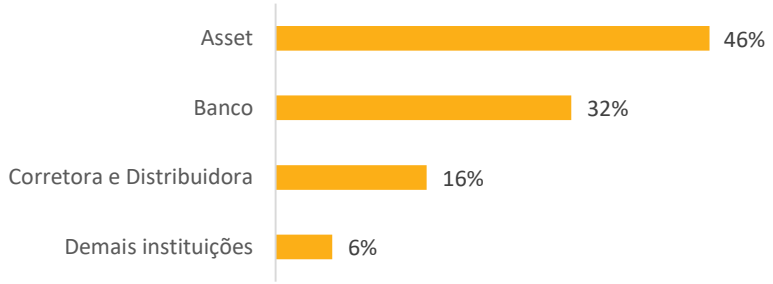
- *Dados da instituição;*
- *Programa de Segurança Cibernética – Informações Gerais*
- *Programa de Segurança Cibernética - Componentes:*
  - *1 - Identificação / Avaliação de riscos;*
  - *2 - Ações de Prevenção e Proteção;*
  - *3 - Monitoramento e Testes;*
  - *4 - Criação do Plano de Resposta; e*
  - *5 - Reciclagem e Revisão*

Resultados da Pesquisa em Cibersegurança junto aos Associados

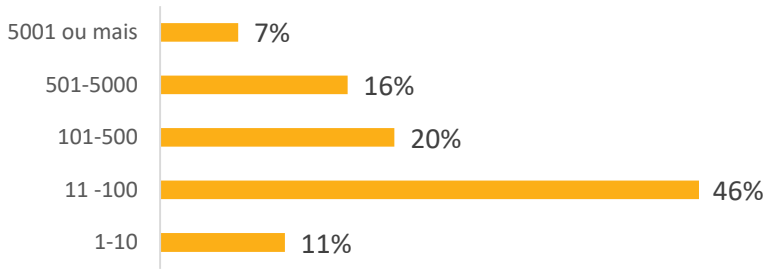
(1) Dados da Instituição

- ***151 respondentes*** *(**58%** do total de 262 instituições que receberam a pesquisa)*

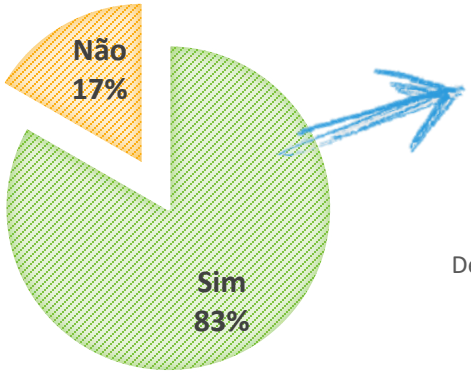
Tipo de instituição



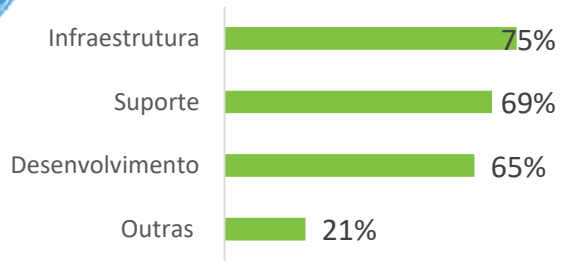
Porte (n° de funcionários)



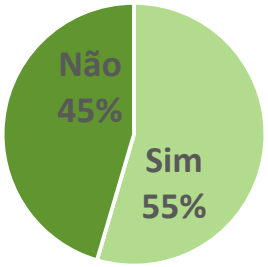
Sua instituição contrata serviços terceirizados de TI?



Se SIM, em quais áreas?



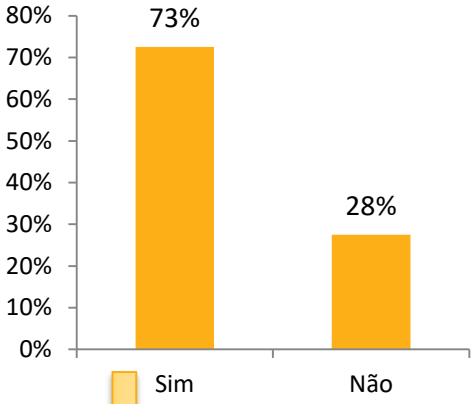
Se SIM, exige relatório periódico para acompanhamento de qualidade?



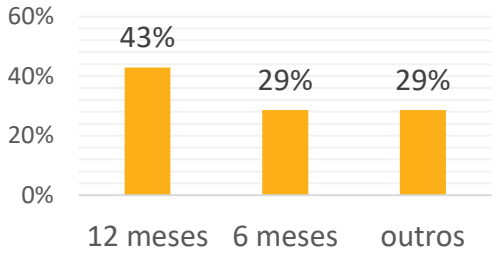
Resultados da Pesquisa em Cibersegurança junto aos Associados

(2) Programa de Segurança Cibernética – Informações Gerais

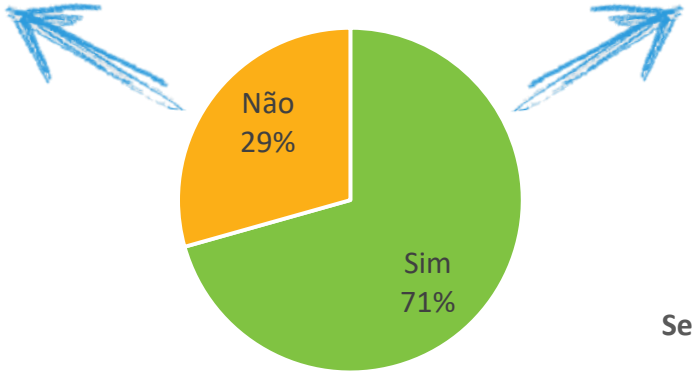
Se NÃO, ele está no planejamento da instituição ou em fase de elaboração?



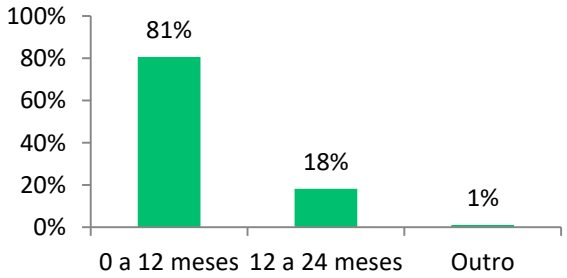
Em quantos meses será implementado?



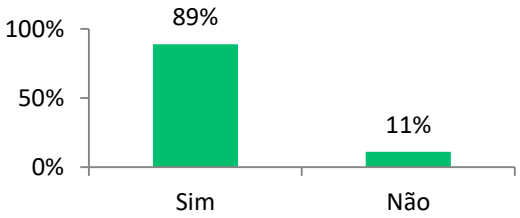
Sua instituição tem um programa formal de segurança cibernética?



Se SIM, qual foi a data da última atualização?



Se SIM, há alguma periodicidade de revisão?

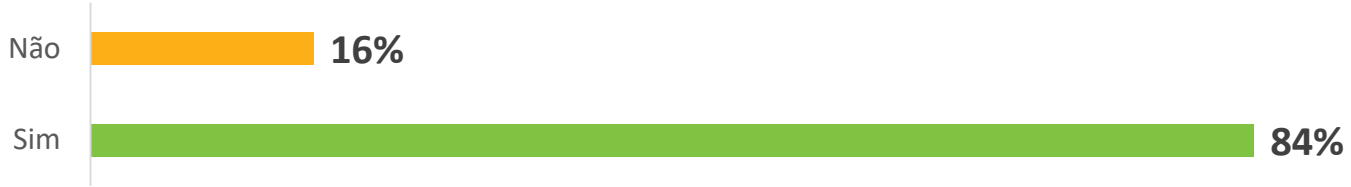


0 a 12 meses	79%
12 a 24 meses	19%
Outro	1%

Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 1 - Avaliação de riscos (Risk assessment)

Sua empresa realiza processo de Avaliação de Riscos?



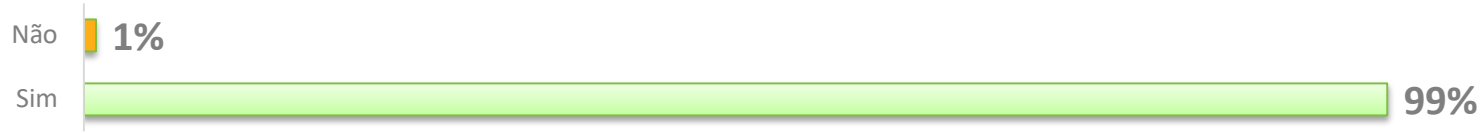
Identifica todos os ativos relevantes da instituição (equipamentos, sistemas, dados ou processos)	80%
Avalia as vulnerabilidades dos ativos em questão, identificando as possíveis ameaças e o grau de exposição dos ativos a elas.	80%
Mensura os possíveis impactos financeiros, operacionais e reputacionais, e expectativa de tais eventos.	59%
Determina e utiliza metodologia para avaliações de risco cibernético	48%
Elabora regras para a classificação das informações geradas pela instituição, permitindo com isso a implementação de processos para o devido manuseio, armazenamento, transporte e descarte dessas informações.	48%
Desenvolveu um comitê, fórum ou grupo específico para tratar de cibersegurança	42%

Asset – 27%

Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 2 - Ações de Prevenção e Proteção

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

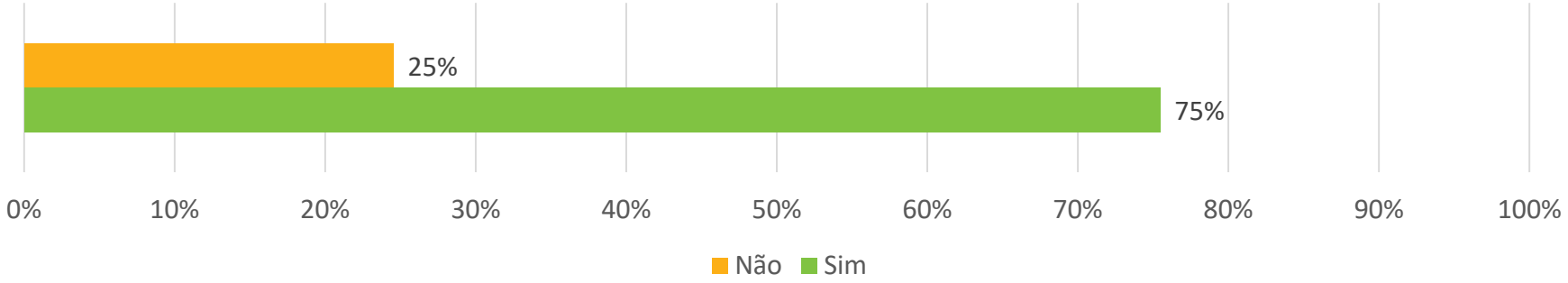


• Implementa serviço de backup dos diversos ativos da instituição.	99%
• Controle de acesso aos ativos das instituições	96%
• Segurança de borda, nas redes de computadores, através de firewalls e outros mecanismos de filtros de pacotes.	95%
• Implementa recursos anti-malware nas estações e servidores de rede, como antivírus e firewalls pessoais.	95%
• Restrição de acesso físico nas áreas com informações críticas/sensíveis.	92%
• Cria logs e trilhas de auditoria sempre que os sistemas permitem.	90%
• Regras mínimas na definição de senhas de acesso a dispositivos corporativos, sistemas e rede	89%
• Concessão de acesso limitado a apenas recursos relevantes para o desempenho das atividades.	89%
• Concessão de acesso implementada de forma a ser revogada rapidamente quando necessário.	85%
• Os eventos de logins e alteração de senhas são auditáveis e rastreáveis.	81%
• Realiza teste em ambientes de homologação e de prova de conceito, antes do envio à produção.	81%
• Implementa segregação de serviços sempre que possível, restringindo-se o tráfego de dados apenas entre os equipamentos relevantes.	80%
• Ao incluir novos equipamentos e sistemas em produção, garante que sejam feitas configurações seguras de seus recursos.	78%
• Controles visando impedir a instalação e execução de software e aplicações não autorizadas	74%
• Considera questões de segurança já durante as fases, pré-projeto e o desenvolvimento de novos sistemas, softwares ou aplicações.	73%
• **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%**
• Utiliza gerenciador de senhas para evitar o uso da mesma senha para facilitar a memorização em vários serviços.	44%

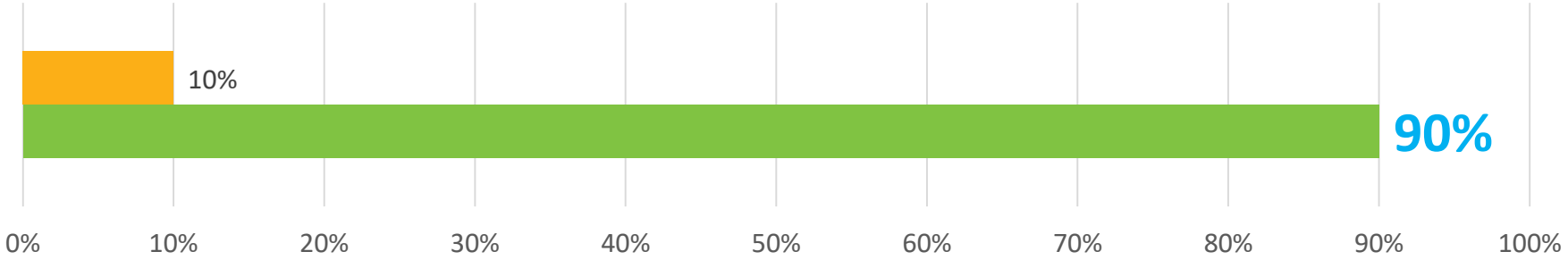
Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 2 - Ações de Prevenção e Proteção

Possui algum serviço ou ativo da instituição localizado externamente **em nuvem**?
- ***Todas as instituições***



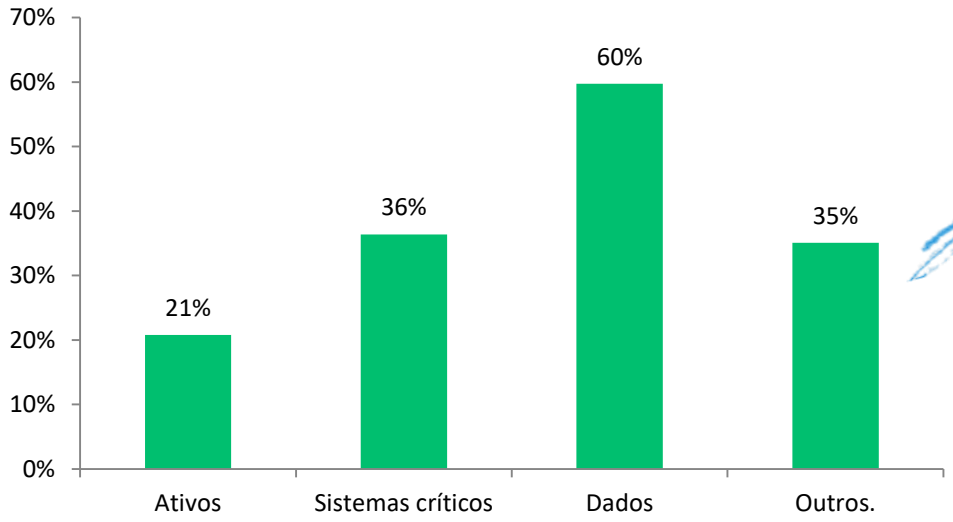
Para Assets valor ainda maior:



Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 2 - Ações de Prevenção e Proteção

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



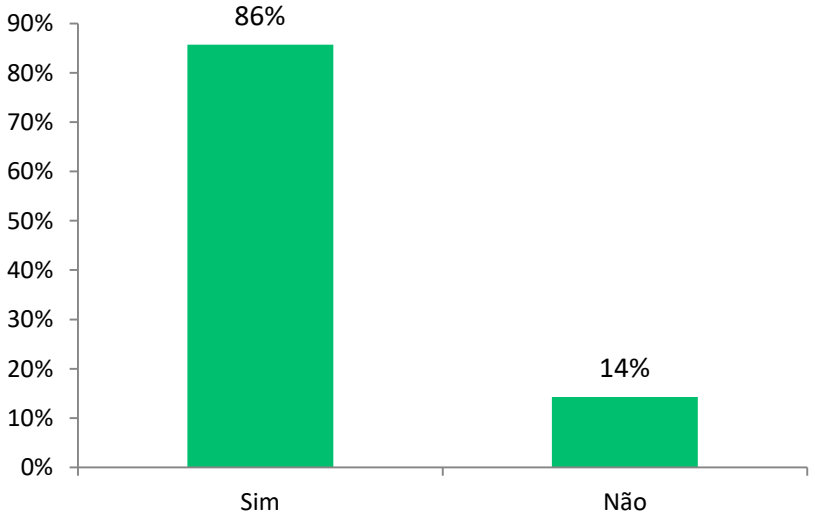
Outros, como:

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

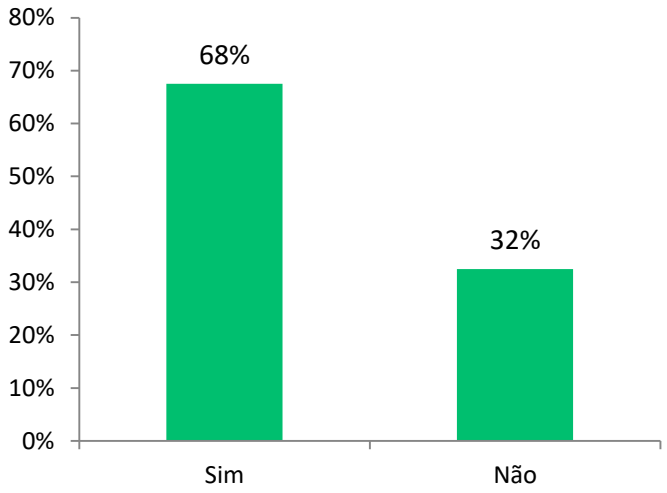
Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 2 - Ações de Prevenção e Proteção

Ao contratar serviço em nuvem, garante que sejam feitas configurações seguras de seus recursos (por exemplo "Hardening")?

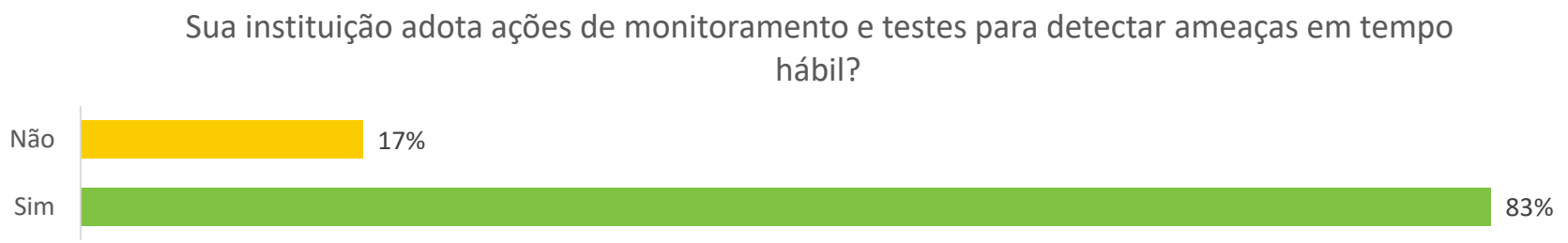


Ao contratar serviço em nuvem, realiza diligência com terceiros na nuvem?



Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 3 - Monitoramento e Testes

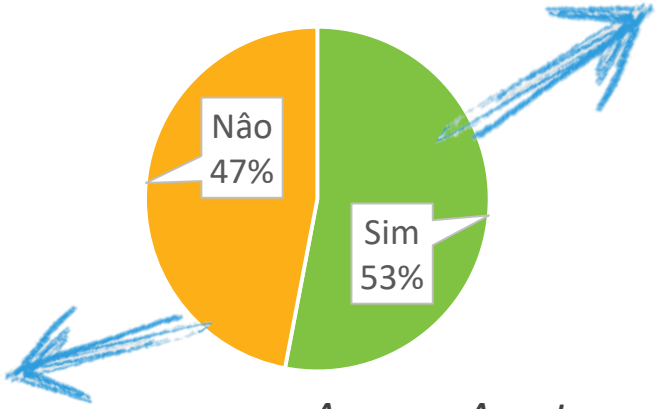


- Mantém os sistemas operacionais e softwares de aplicação sempre atualizados. 91,57%
- Monitora diariamente as rotinas de backup, executando testes regulares de restauração dos dados. 90,36%
- Mantém inventários atualizados de hardware e software, e os verifica com frequência 80,72%
- Cria mecanismos de monitoramento de todas as ações de proteção implementadas. 74,70%
- Analisa logs e trilhas de auditoria criados 68,67%
- Testa o plano de resposta a incidentes, simulando os cenários especificados durante sua criação. 50,60%
  - Se SIM, qual a periodicidade?
    14% entre 1 a 3 meses;
    43% em 6 meses;
    43% em 12 meses
- Utiliza ferramentas de centralização e análise de logs. 45,78%

Resultados da Pesquisa em Cibersegurança junto aos Associados

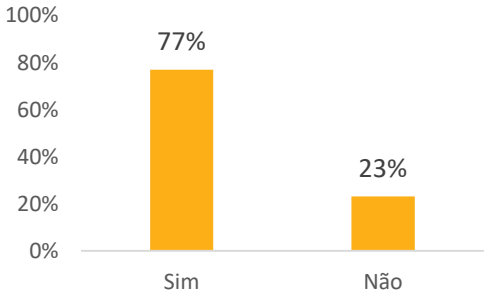
(3) Componentes do Programa: 3 - Monitoramento e Testes

Sua instituição já realizou testes <u>externos</u> de penetração no último ano?

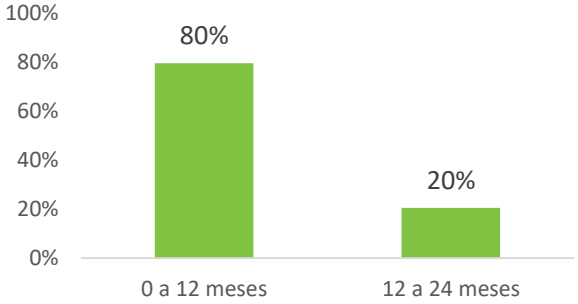


Apenas Assets:
*- **SIM: 37%***
- NÃO: 63%

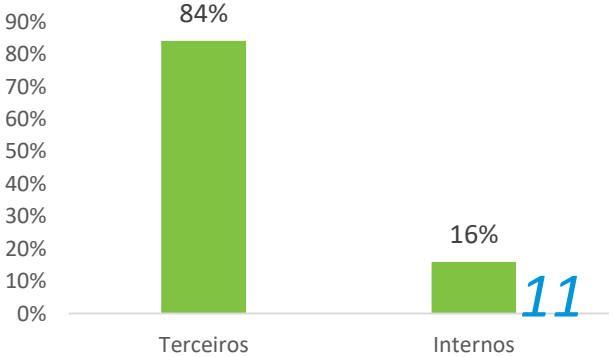
Se NÃO, há algum plano prevendo a realização desse teste?



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



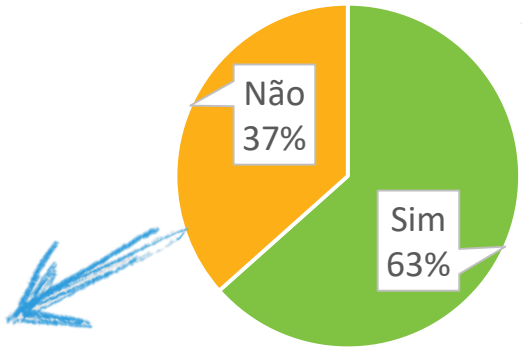
Se SIM, o teste foi realizado por:



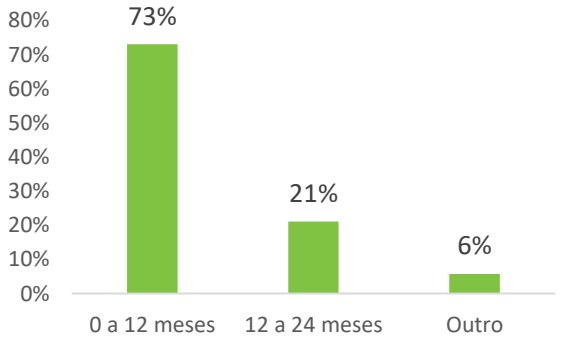
Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 3 - Monitoramento e Testes

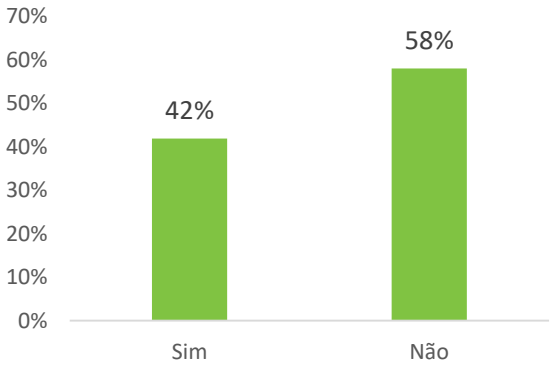
Sua instituição já realizou testes <u>internos</u> de penetração?



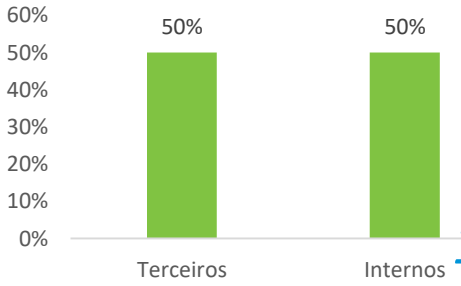
Se SIM, qual é a periodicidade dos testes de penetração?



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



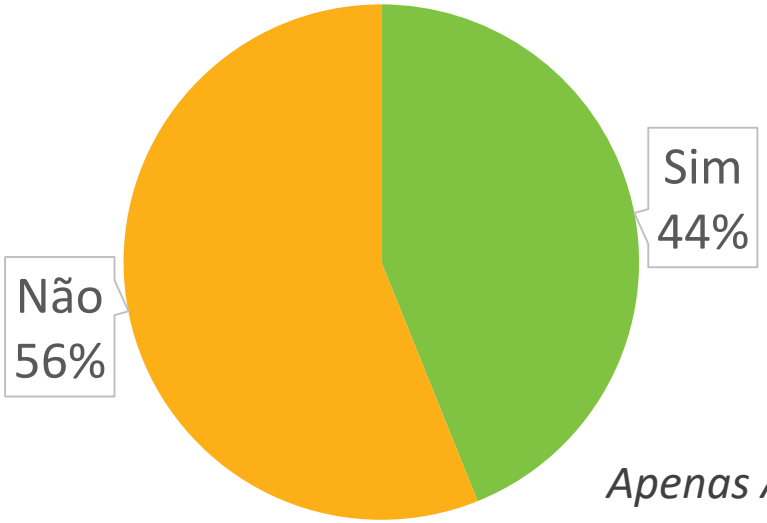
Se SIM, o teste foi realizado por:



Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 3 - Monitoramento e Testes

Sua instituição realizou exercício de phishing no último ano?

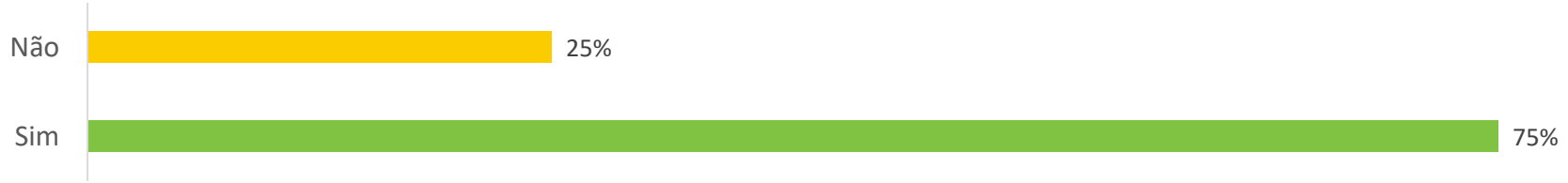


Apenas Assets:
*- **SIM: 29%***
- NÃO: 71%

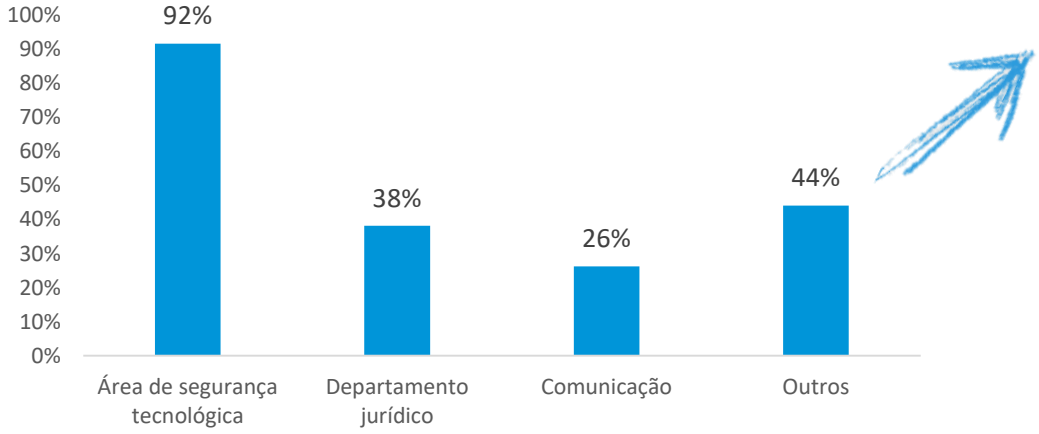
Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 4 - Criação do Plano de Resposta

A sua instituição conta com plano de resposta para incidentes ou ataques cibernéticos?



Quais são as áreas envolvidas na elaboração do plano?



Outros, como:

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

Resultados da Pesquisa em Cibersegurança junto aos Associados

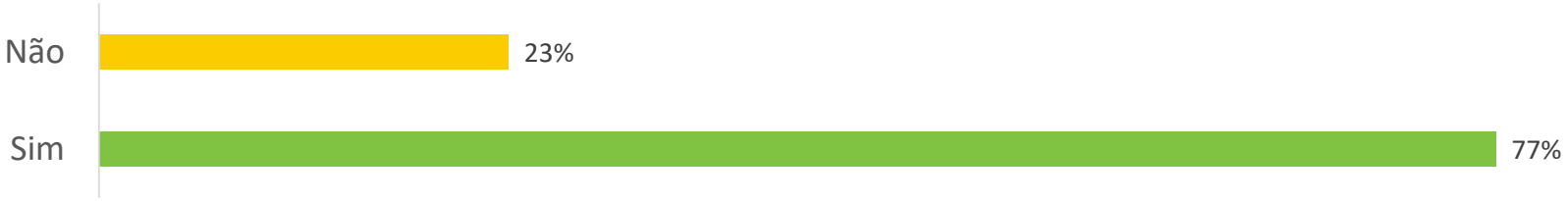
(3) Componentes do Programa: 4 - Criação do Plano de Resposta

Leva em consideração questões de Segurança e controles de acesso também nas instalações de contingência	95,79%
Apresenta plano de continuidade dos negócios e processos de recuperação e remediação	95,65%
Realiza o arquivamento de documentações relacionadas ao gerenciamento dos incidentes e ao plano de continuidade de negócios para servir como evidência em eventuais questionamentos	85,26%
Definição de papéis e responsabilidades dentro do plano de ação	78,02%
O plano leva em consideração os cenários de ameaças previstos na avaliação de risco	74,44%
Há critérios para classificação dos incidentes, por severidade	67,03%

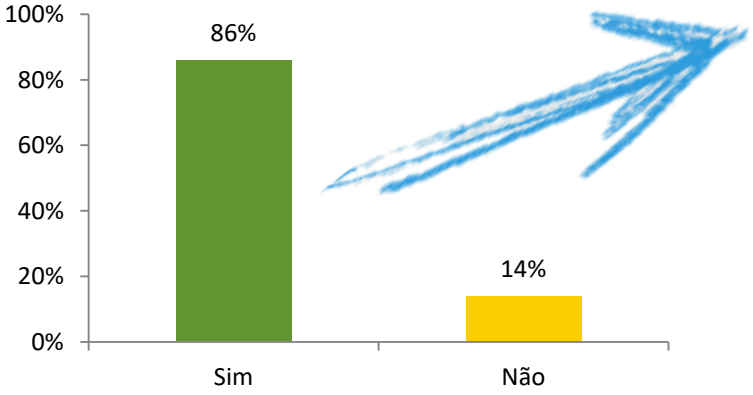
Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 5 - Reciclagem e Revisão

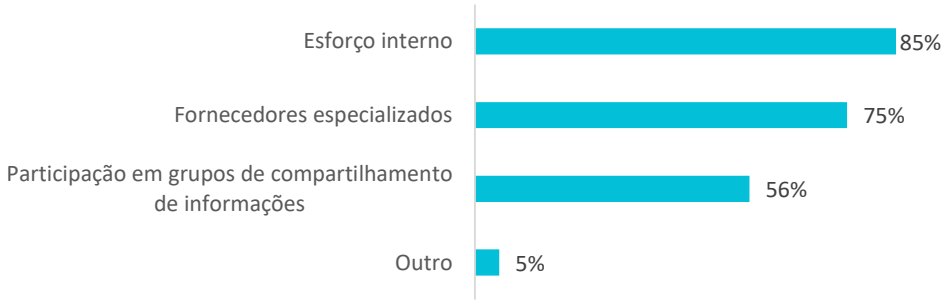
O Programa de Segurança Cibernética é revisado periodicamente, mantendo sempre atualizados as avaliações de risco, as implementações de proteção, os planos de resposta a incidentes e o monitoramento dos ambientes?



Os grupos envolvidos se mantêm atualizados?



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



Resultados da Pesquisa em Cibersegurança junto aos Associados

(3) Componentes do Programa: 5 - Reciclagem e Revisão

Há alguma orientação dos usuários a ter atenção especial antes de clicar em links recebidos	90,82%
Apresenta política de uso adequado da estrutura tecnológica, de forma independente ou como parte de um documento mais abrangente	86,46%
Promove e dissemina uma cultura de segurança, com a criação de canais de comunicação internos para divulgar o programa de segurança cibernética e treinamentos	75,51%
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	29,90%

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