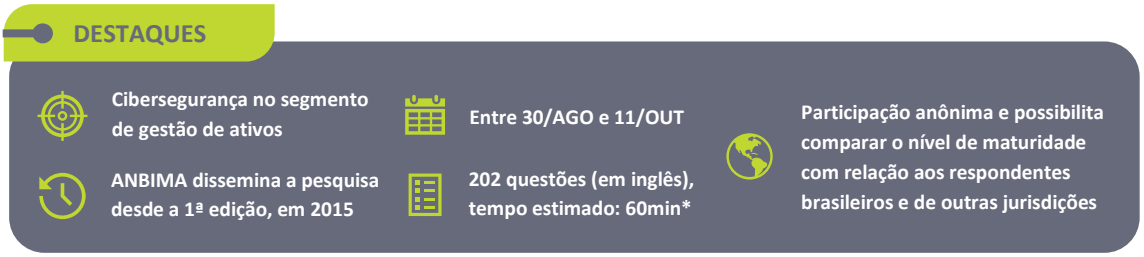
Manual para preenchimento da pesquisa internacional anual de cibersegurança da Iosco

Edição – 2024

ANBIMA

Sumário

Informações gerais



*Tempo estimado para preenchimento do questionário com informações prontamente disponíveis.

O risco cibernético é uma das principais preocupações das instituições financeiras e tem ganhado cada vez mais destaque em diversos fóruns nacionais e internacionais. Desde 2015, O Comitê Consultivo dos Membros Afiliados (AMCC, na sigla em inglês) da *International Organization of Securities Commissions* (Iosco)[1], organiza, em parceria com o *Investment Company Institute (*ICI)[2], realiza a *Asset Management Cybersecurity Benchmarking Survey* (pesquisa de benchmarking de segurança cibernética na gestão de ativos). Aplicada em diversos países (exceto os Estados Unidos, que conta com pesquisa apartada), a pesquisa coleta informações a fim de apoiar esforços focados na segurança e solidez das políticas e práticas de segurança cibernética e auxiliar os participantes em suas avaliações independentes de suas respectivas políticas e práticas, consistentes com seus deveres fiduciários e os melhores interesses dos seus clientes.

A participação nesta pesquisa é voluntária e todas as respostas devem ser direcionadas apenas ao ICI. Os resultados da pesquisa não devem ser usados para qualquer outro propósito em coordenação com outros participantes da pesquisa ou de outra forma. As respostas individuais das empresas serão mantidas confidenciais e os resultados da pesquisa serão agregados e anonimizados de acordo com essa confidencialidade. Informações gerais sobre as instituições respondentes, tais como endereço de e-mail, nome da empresa e país, são exigidos apenas para fins administrativos pela equipe da ICI para garantir que seus resultados estejam completos e não haja duplicatas. O campo obrigatório "região geográfica" será utilizado para fins de agregação de dados e relatórios.

A ANBIMA apoia a Iosco na disseminação da pesquisa para as instituições brasileiras desde a primeira edição, em 2015, orientando os participantes e acompanhando os envios, e não possui acesso às respostas individualmente. A Associação também elabora materiais para o melhor aproveitamento das informações resultantes da pesquisa e para contribuir com o amadurecimento das práticas de cibersegurança no mercado local.

A pesquisa cobre uma ampla gama de tópicos para fornecer uma compreensão completa do cenário de segurança cibernética nas empresas de gestão de ativos. As seções principais incluem:

- **Detalhes da empresa:** nome da empresa, e-mail, país/jurisdição, região geográfica, número de funcionários e localização dos escritórios (Q1-Q5);
- **Programa de Segurança da Informação:** apoio financeiro e de pessoal, gastos per capita e atividades orçamentárias (T6-Q12);
- **Pessoal de Segurança da Informação:** número de funcionários, funções, recrutamento e certificações (Q13-Q26);

[1] Iosco: https://www.iosco.org/.
[2] ICI: https://www.ici.org/.

- **Governança e Maturidade:** níveis de maturidade de governança, estrutura de relatórios e tecnologias emergentes (Q26);
- **Autenticação e gerenciamento de acesso:** políticas de senha, autenticação multifatorial e autenticação biométrica (Q27-Q49);
- **Segurança de dispositivos e redes:** restrições sobre mídia removível, criptografia e segmentação de rede (Q50-Q67);
- **Políticas e Procedimentos:** gestão de identidade e acesso, testes de conformidade e estruturas de segurança cibernética (Q68-Q112);
- **Terceirização:** funções de TI terceirizadas, como desenvolvimento de aplicativos, defesa cibernética e recuperação de desastres (Q113);
- **Práticas de criptografia:** criptografia de mídia de backup, dispositivos móveis e bancos de dados (Q114-Q125);
- **Acesso Administrativo:** utilização de gerenciadores de senhas e autenticação multifator (Q126-Q131);
- **Prioridades de segurança de dados:** preocupações com diferentes categorias de dados e informações no nível do conselho (Q132-Q134);
- **Supervisão Regulatória:** jurisdições e agências que impactam o programa de segurança (Q135-Q136);
- **Segurança de Terceiros:** governança de fornecedores terceirizados e acordos de segurança (Q137-Q140);
- **Operações de segurança:** equipes de resposta a incidentes, serviços de segurança gerenciados e ferramentas SIEM (Q141-Q162);
- **Segurança na nuvem:** uso de serviços de nuvem pública, verificações de vulnerabilidades e autenticação federada (Q163-Q174);
- **Controles de acesso remoto e trabalho em casa:** controles de segurança para trabalho remoto, classificação de dados e prevenção de ransomware (Q175-Q183);
- **Inteligência Artificial (IA) generativa e grandes modelos de linguagem:** políticas para uso de IA e áreas de aplicação (Q184-Q190);
- **Gestão de Riscos Internos:** escopo de programas de riscos internos e verificações de antecedentes (Q191-Q196); e
- **Comunicação e troca de dados:** uso de anexos de e-mail para detalhes financeiros (Q201-Q202).

O questionário conta 202 perguntas em inglês e a plataforma SurveyMonkey[3] será utilizada para a realização desta edição da pesquisa. Esta plataforma suporta os seguintes navegadores: Chrome, Firefox, Safari e Microsoft Edge. O hyperlink para acesso será disponibilizado pela ANBIMA às gestoras associadas e aderentes no dia 30 de agosto e as instituições poderão enviar respostas até às 13:00 (GMT-3) do dia 11 de outubro. Qualquer alteração de cronograma será comunicada pela Associação tempestivamente.

É importante que cada instituição envie apenas uma resposta e preenchimento do questionário seja realizado preferencialmente por um único profissional das áreas de Tecnologia da Informação (TI), Segurança da Informação (SI), Risco ou Compliance, designado para execução desta atividade por Diretor de Segurança da Informação (CISO) ou executivo responsável equivalente. Dada a diversidade de temas abordados pela pesquisa, poderá ser necessário envolver diferentes equipes no preenchimento. Portanto, é recomendável todos os envolvidos estejam cientes da pesquisa, dos temas abordados nela e do prazo para envio de respostas. Além disso, as empresas participantes devem investir os melhores esforços para que o hyperlink

[3] SurveyMonkey: https://surveymonkey.com/.

que dá acesso ao questionário não seja utilizado indevidamente por colaboradores ou compartilhado com pessoas externas.

O tempo estimado para preenchimento do questionário é de 60 minutos com as informações prontamente disponíveis. A pesquisa pode ser realizada apenas uma vez no mesmo dispositivo e será salva se utilizado o mesmo navegador. Ao tentar responder à pesquisa novamente depois de concluí-la, usando o mesmo navegador, aparecerá mensagem informando que a pesquisa já foi respondida. Caso necessário acessar novamente o questionário preenchido para fazer alterações após o envio de sua resposta, entre em contato com a instituição organizadora através de e-mail para ICIcybersurvey@ici.org.

Este manual tem como objetivo reunir informações e orientações que possam auxiliar as instituições a se prepararem para o preenchimento do questionário, realizarem o envio adequado de sua resposta e aproveitarem melhor os resultados da pesquisa. Além do passo-a-passo a seguir, a Associação está à disposição para eventuais dúvidas e sugestões neste *e-mail*: Distribuição@anbima.com.br.

Boa leitura!

Passo-a-passo

1. Como se preparar para responder o questionário

Neste sentido, sugerimos considerar os seguintes passos para preparação para o preenchimento:

- **Garantir** que o Diretor de Segurança da Informação (CISO) ou executivo responsável equivalente, a única pessoa designada para o preenchimento do questionário e as equipes que contribuirão para a coleta das informações necessárias (TI, SI, Risco, Compliance, Financeiro, Recursos Humanos, possivelmente outras) estejam cientes da pesquisa, dos temas abordados nela e do prazo para envio de respostas;
- **Designar**, o Diretor de Segurança da Informação (CISO) ou executivo responsável equivalente, uma (única) pessoa responsável por preencher o questionário pela instituição, considerando que é recomendável que esta ação seja executada, no mesmo computador e usando o mesmo navegador com *cookies* ativados, por profissionais proficientes na língua inglesa e das áreas de TI, SI, Risco ou Compliance;
- **Agendar** reuniões internas com representantes das equipes que contribuirão para o preenchimento do questionário dentro do prazo para envio de respostas à pesquisa a fim de reunir as informações necessárias; e
- **Checar**, na data de início da pesquisa (30 de agosto), o recebimento de comunicação da ANBIMA (via e-mail ou circular – enviados aos Representantes ANBIMA e/ou contatos institucionais cadastrados) informando a abertura do questionário para envio de respostas, contendo o hyperlink para acesso.

2. Preenchendo o questionário

Para um preenchimento adequado do questionário, sugerimos considerar os seguintes passos:

- **Compartilhar** com as equipes que contribuirão para o preenchimento do questionário as perguntas que demandarão informações específicas não diretamente acessíveis pela pessoa responsável por preencher o questionário pela instituição;
- **Realizar** reuniões internas com representantes das equipes que contribuirão para o preenchimento do questionário dentro do prazo para envio de respostas à pesquisa, a fim de reunir as informações necessárias;
- **Consolidar** as informações necessárias em um material de apoio para o momento do preenchimento do questionário;
- **Reservar**, o profissional responsável pelo preenchimento do questionário, ao menos 60 minutos para a realização da atividade;
- **Garantir** que somente o profissional responsável por preencher o questionário pela instituição insira informações na resposta a ser enviada e realize esta atividade a partir do mesmo computador e navegador, com o salvamento de *cookies* ativado; e
- **Certificar-se**, caso precise sair do questionário e retornar mais tarde durante o preenchimento, de que:
    i. Completou o preenchimento da página da última seção respondida e clicou sobre “Next”;

ii. Utilizará, ao retornar, o mesmo computador, navegador e hyperlink para acesso ao questionário; e
iii. Não desabilitou o salvamento de *cookies*.

→ **Investir os melhores esforços** para que o hyperlink que dá acesso ao questionário não seja utilizado indevidamente por colaboradores ou compartilhado com pessoas externas.

3. Enviando sua resposta

Antes de concluir o questionário e enviar sua resposta, sugerimos considerar os seguintes passos:

→ **Repassar** por todas as seções para eventuais revisões necessárias;
→ **Verificar** se todas as perguntas foram respondidas;
→ **Registrar** também suas respostas em arquivo interno para manutenção de histórico de sua participação na pesquisa, que possibilite acompanhamento da evolução da maturidade de sua organização nas práticas de cibersegurança ao longo dos anos; e
→ **Certificar-se** que clicou em "Done" antes de sair da página do questionário, para salvar e enviar sua resposta.

4. Aproveitando melhor os resultados

Após a divulgação do resultado, a ANBIMA compartilhará materiais para o melhor aproveitamento das informações resultantes da pesquisa pelas gestoras de recursos participantes e a fim de contribuir com o amadurecimento das práticas de cibersegurança no mercado brasileiro. No entanto, é recomendável que as instituições que enviarem respostas invistam num histórico interno de suas participações para acompanharem a evolução de sua maturidade em segurança cibernética. Isso possibilitará também que comparem seus resultados com as médias brasileira e internacional e identifiquem prioridades e oportunidades de aprimoramento de suas políticas e procedimentos.

Conclusão

Esperamos que este manual tenha contribuído para melhor entendimento do funcionamento da Pesquisa Internacional Anual de Cibersegurança da Iosco e para a preparação para o preenchimento do questionário, o envio adequado das respostas e o aproveitamento dos resultados. Esperamos poder contar com sua participação na pesquisa todos os anos e estamos à disposição para eventuais dúvidas e sugestões neste *e-mail*: Distribuição@anbima.com.br.

Agradecemos o tempo investido na leitura e parabenizamos o engajamento nesta iniciativa que visa o fortalecimento da segurança cibernética no mercado de gestão de recursos!