Relatório comparativo: pesquisa internacional de cibersegurança na gestão de ativos

(2023 - 2024)

1ª Edição | 2025

ANBIMA

Sumário

Sobre o relatório

Este Relatório comparativo sobre a pesquisa internacional de cibersegurança na gestão de ativos, a *2024 AMCC Cyber Security Asset Management Benchmarking Survey*, é resultado do trabalho conjunto da ANBIMA - Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais com participantes de mercado reunidos no Grupo Consultivo de Cibersegurança. A elaboração do material contou também com o apoio técnico do *Investment Company Institute* (ICI)[1], que organiza a pesquisa para o Comitê Consultivo dos Membros Afiliados (AMCC, na sigla em inglês) da *International Organization of Securities Commissions* (Iosco)[2].

O material analisa os resultados da pesquisa visando disseminar informações e dados comparativos que contribuam para fomentar o amadurecimento das práticas de cibersegurança entre as instituições atuantes nos mercados financeiro e de capitais brasileiros. Além disso, traz orientações para o melhor aproveitamento desses resultados pelas gestoras de ativos a fim de que estas possam definir, atualizar e aprimorar suas estratégias de segurança cibernética.

Vale ressaltar que o conteúdo deste documento não é vinculante para quaisquer instituições, associadas ou não à ANBIMA, e não integra documento da nossa autorregulação. Ainda, o disposto aqui não se caracteriza, de nenhum modo, como documento da autorregulação ANBIMA. O presente documento reflete tão somente análises e orientações técnicas, e, sob nenhuma hipótese, vincula as instituições e a ANBIMA a futuras discussões sobre o tema que forem tratadas no âmbito da autorregulação.

O conteúdo deste material também não deve ser interpretado de forma a contrariar, mitigar ou se opor a nenhum normativo da legislação, regulação e autorregulação, aplicáveis aos mercados financeiro e de capitais, limitando-se, tão somente, a disseminar informações e orientar técnicas para melhor consecução das atividades do mercado relativa à cibersegurança.

[1] **ICI.** Acesse aqui: <https://www.ici.org/>.
[2] **Iosco.** Acesse aqui: <https://www.iosco.org/>.

Introdução

A ANBIMA, como membro do AMCC-Iosco, atua na disseminação da *Cyber Security Asset Management Benchmarking Survey* desde 2015, quando sua primeira edição foi realizada. A pesquisa, que vem crescendo em número de participantes e de jurisdições representadas, está em constante atualização para abranger temas emergentes, como novas tecnologias, ameaças e melhores práticas, bem como para oferecer informações que auxiliem a medir a resiliência cibernética das gestoras de ativos e possibilitar análises comparativas de níveis de maturidade a nível global. Este relatório faz parte da agenda da Associação para contribuir com a divulgação da pesquisa e para o melhor aproveitamento dos resultados e visa fomentar o amadurecimento das práticas de cibersegurança entre as instituições atuantes nos mercados financeiro e de capitais brasileiros.

A última edição da pesquisa foi realizada entre agosto e outubro de 2024, com participação de 88 gestoras de ativos em 18 países, incluindo o Brasil. O questionário cobriu uma abrangente variedade de tópicos para fornecer uma compreensão completa do cenário de segurança cibernética das instituições participantes, cujas respostas são confidenciais e mantidas pela organizadora, a ICI. A ANBIMA possui acesso, desde a edição de 2023, aos resultados anonimizados da pesquisa e, com base nessas informações, foi construído este relatório comparativo a fim de auxiliar as instituições em suas avaliações independentes de suas políticas e práticas de cibersegurança, consistentes com seus deveres fiduciários e os melhores interesses dos seus clientes.

Em função das atualizações promovidas pela organizadora no questionário da pesquisa entre 2023 e 2024, seções adicionadas à última edição, como a que trata de Inteligência Artificial (IA) e grandes modelos de linguagem (LLM, da sigla em inglês), ainda não são passíveis de análise comparativa com dados anteriores, mas também são discutidas neste documento dada a relevância dos temas. Em 2023, 170 perguntas compunham o questionário e, na edição de 2024, foram 202 perguntas. Dentre as seções temáticas correlacionadas, foram identificadas **12 categorias** principais que serão analisadas neste relatório, conforme detalhado a seguir.

1 Equipes de segurança da informação

Fatores analisados:

- O número total de funcionários dedicados ou contratados que trabalham na segurança da informação;
- O número total de funcionários ou contratados que desempenham funções de segurança da informação como parte de suas responsabilidades;
- A porcentagem de contratados em relação aos funcionários internos dedicados à segurança da informação;
- A empresa possui um CISO (Chief Information Security Officer) em tempo integral.

2 Autenticação

Fatores analisados:

- Políticas de senha, como comprimento mínimo e complexidade exigida;
- Uso de software de gerenciamento de senhas;
- Implementação de autenticação biométrica e baseada em risco;
- Frequência de mudança de senhas para administradores e não administradores;
- Exigência de autenticação multifator para acessos internos e externos;
- Uso de autenticação de dispositivos e serviços de verificação de identidade de terceiros.

3 Dispositivos

Fatores analisados:

- Restrição de acesso a mídias removíveis em dispositivos de clientes;
- Utilização de *firewalls* pessoais ou proteção equivalente em endpoints;
- Criptografia de discos rígidos dos dispositivos de computação dos usuários finais;
- Detecção/Prevenção de intrusão em *hosts* em dispositivos de computação dos usuários finais;
- Utilização de solução de detecção e resposta de endpoint em dispositivos de computação dos usuários finais;
- Adoção de modelo de confiança zero para acesso à rede interna.

4 Segurança de rede

Fatores analisados:

- Adoção de modelo de confiança zero para acesso remoto à rede;
- Controle de acesso a sites externos usando servidores proxy ou outros controles baseados em rede;
- Segmentação da rede interna usando *firewalls* ou outras capacidades de controle;
- Detecção de intrusão na conexão com a Internet;
- Uso de sistemas de detecção de anomalias, como Análise de Comportamento do Usuário, para detectar atividades internas maliciosas;
- Exigência de TLS v1.2 ou superior para comunicações voltadas para a internet;
- Uso de tecnologia de *firewall* de próxima geração, que adiciona inspeção profunda de pacotes e capacidades de inspeção de aplicativos.

5 Políticas e procedimentos

Fatores analisados:

- Conformidade e Governança;
- Avaliação e gestão de riscos, inclusive de terceiros;
- Gestão da continuidade de negócios prevendo planos de resposta a incidentes cibernéticos e procedimentos de escalonamento para eventos cibernéticos;
- Treinamento de segurança da informação e exercícios de simulação de phishing;
- Métricas de eficácia da segurança de TI e ambientes de teste e desenvolvimento;
- Inventário de dispositivos físicos e softwares, autenticação de identidade e controles de acesso;
- Seguro cibernético.

6 Criptografia

Fatores analisados:

- Criptografia de backups externos, e-mails e dados em movimento;
- Compartilhamentos internos de arquivos, bancos de dados internos e uso de provedores de serviços de armazenamento;
- Gerenciamento de direitos digitais e senhas e monitoramento de acessos.

7 Prioridades de segurança da informação

Fatores analisados:

- Desempenho da estratégia de segurança da informação e avaliação de riscos;
- Resultados em testes e auditorias;
- Manutenção de informações sobre incidentes, testes, *benchmarks*;
- Métricas e progresso dos indicadores-chave de risco;
- Conselho de cibersegurança.

8 Supervisão regulatória (terceiros)

Fatores analisados:

- Governança que aborda especificamente fornecedores terceirizados.

9 Segurança externa

Fatores analisados:

- Processo de revisão de terceiros que impõe requisitos contratuais de habilitação e revisão para estabelecer SLAs de segurança, incluindo SLAs de tempo de notificação de violação com terceiros e quartos.

10 Operações de segurança

Fatores analisados:

- Operação da equipe de defesa cibernética (incluindo período de funcionamento) e acordos de nível de serviço (SLAs) para correção de vulnerabilidades;
- Uso de ferramentas SIEM, UEBA ou SOAR e de tecnologia de engano, análise de malware interna, revisão ativa de inteligência de ameaças cibernéticas e automação de funções de segurança;
- Gestão de riscos de segurança de aplicativos;
- Rastreamento e remediação de protocolos e algoritmos obsoletos ou inseguros;
- Programas DevSecOps.

11 Segurança na nuvem

Fatores analisados:

- Segurança e conformidade da empresa em relação ao uso de infraestrutura de nuvem pública (IAAS ou PAAS);
- Utilização de corretores de acesso à nuvem para impor políticas de segurança, requisitos de conformidade e proteção contra ameaças;
- Realização de varreduras regulares de vulnerabilidades na infraestrutura de nuvem pública;
- Realização de testes de penetração regulares na infraestrutura de nuvem pública;
- Exigência de tecnologias de autenticação local (autenticação multifator ou em duas etapas) para acesso administrativo às plataformas de nuvem públicas;
- Restrição de acesso a serviços de nuvem pública não relacionados aos negócios;
- Processo de sanitização de dados para repositórios de dados de computação em nuvem.

12 Trabalho remoto (Home Office)

Fatores analisados:

- Relaxamento de algum controle de segurança para efetivamente habilitar o trabalho remoto/híbrido;
- Política de classificação de dados;
- Medidas de segurança com o acesso a inteligências artificiais (ChatGPT).

Metodologia

A partir dos resultados de 2023 e 2024 da AMCC Cyber Security Asset Management Benchmarking Survey, compartilhados pela ICI (organizadora da pesquisa) com a ANBIMA, este relatório comparativo foi elaborado considerando as 12 categorias de análise supracitadas. Estas, que foram definidas pela equipe técnica da Associação com base nos tópicos em comum identificados nas perguntas dos questionários das edições analisadas da pesquisa.

Foi atribuída uma classificação por nota a cada uma das perguntas comparadas, na escala de 0 (zero) a 10 (dez) pontos. A nota máxima foi atingida pelas instituições participantes que incluíram ou assinalaram as respostas associadas às melhores práticas de segurança cibernética dentro do tema abordado. Quando aplicável, notas intermediárias também foram incluídas em bandas de valores simétricos para consideração, por exemplo, de adoção parcial das melhores práticas pelas participantes. As notas mínimas somente foram imputadas às gestoras que responderam não adotar nenhuma prática dentro do tema abordado, quando isso significava prejuízo à cibersegurança.

A partir do cálculo da média aritmética das notas obtidas pelas gestoras de ativos em cada uma das perguntas consideradas dentro das categorias de análise, obteve-se a média das instituições dentro das categorias. Assim, foi possível determinar as médias aritméticas das instituições para cada categoria, das instituições brasileiras para cada categoria (denominadas “BRASIL” nos resultados a seguir) e das instituições das demais jurisdições (denominadas “MUNDO” nos resultados a seguir) para cada categoria, bem como a média geral de todas as instituições participantes da pesquisa em todas as categorias de análise.

A ANBIMA realiza ações para apoiar as instituições brasileiras no preenchimento da pesquisa, como a disponibilização de manuais[3] e o compartilhamento de informações gerais[4]. Porém, é importante ressaltar que a participação na pesquisa pelas gestoras de ativos é voluntária e as respostas não são verificáveis, pela ANBIMA ou pela ICI (organizadora).

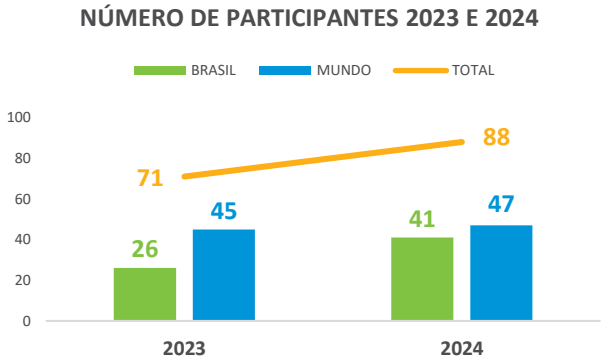
[3] **ANBIMA.** *Manual para preenchimento da pesquisa internacional anual de cibersegurança da Iosco* (2024). Acesse aqui: <https://www.anbima.com.br/data/files/F8/C5/D0/32/DA4749107AF1F649EA2BA2A8/Manual_Pesquisa_Ciberseguranca_IOSCO.pdf>.

[4] **ANBIMA.** *Cibersegurança: participe da 10ª edição da pesquisa internacional da Iosco* (2024). Acesse aqui: <https://www.anbima.com.br/pt_br/noticias/ciberseguranca-participe-da-10-edicao-da-pesquisa-internacional-da-iosco.htm>.

Resultados

Aumento de 23,94% do número de participantes da pesquisa

Em 2024, **88** instituições participaram da pesquisa, enquanto, em 2023, **71** gestoras haviam respondido o questionário. A maior representatividade em ambas as edições é das instituições brasileiras. Foram **26** (36,61% do total) e **41** (46,59% do total) gestoras pelo Brasil, nos respectivos levantamentos, um aumento de 57,69%. Enquanto o número de participantes de outras jurisdições aumentou apenas 4,44%.

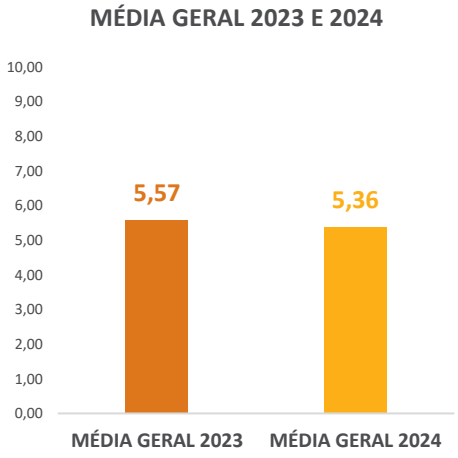


Em 2024, gestoras de 18 países completaram o questionário

Na última edição da pesquisa, além do Brasil (com **41** representantes), participaram instituições pela Austrália (**8**), Alemanha (**7**), Reino Unido (**5**), Eslovênia (**4**), Coréia do Sul (**3**), Estados Unidos (**3**), Portugal (**3**), África do Sul (**2**), Bulgária (**2**), França (**2**), Irlanda (**2**), Bélgica (**1**), Canadá (**1**), Dinamarca (**1**), Espanha (**1**), Itália (**1**) e Japão (**1**).

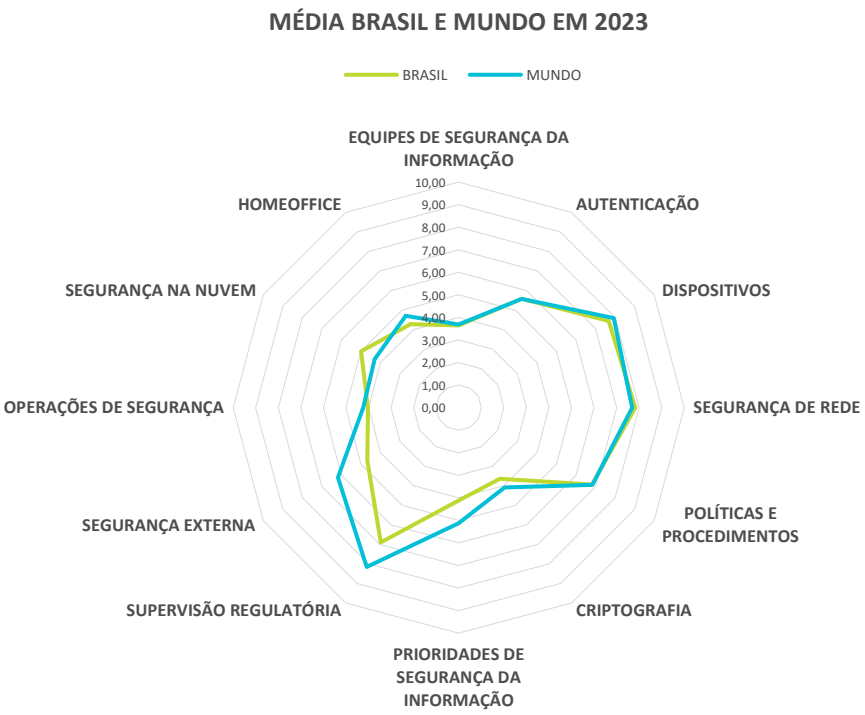
A média geral das gestoras teve redução de 3,78%

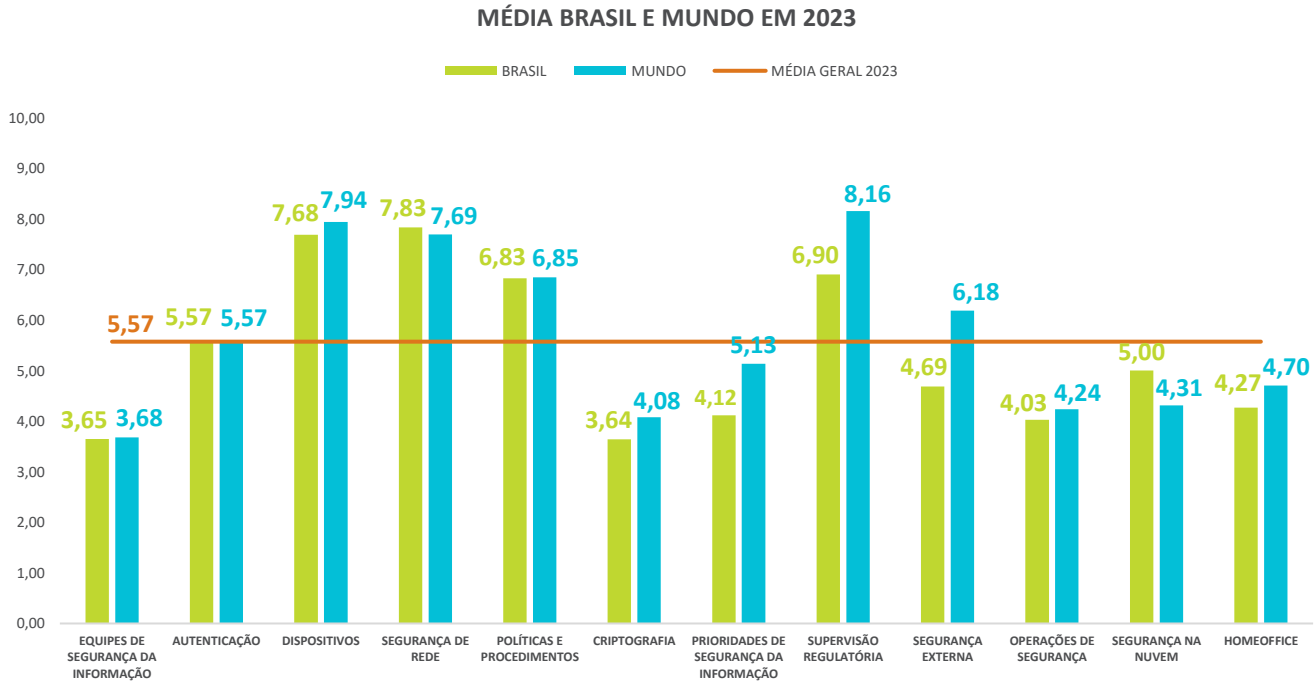
Um ponto de atenção revelado pelo estudo é a queda da nota geral das instituições participantes da pesquisa na análise conjunta de todas as categorias. Em 2023, a média das gestoras era **5,57** e, em 2024, atingiu **5,36**.

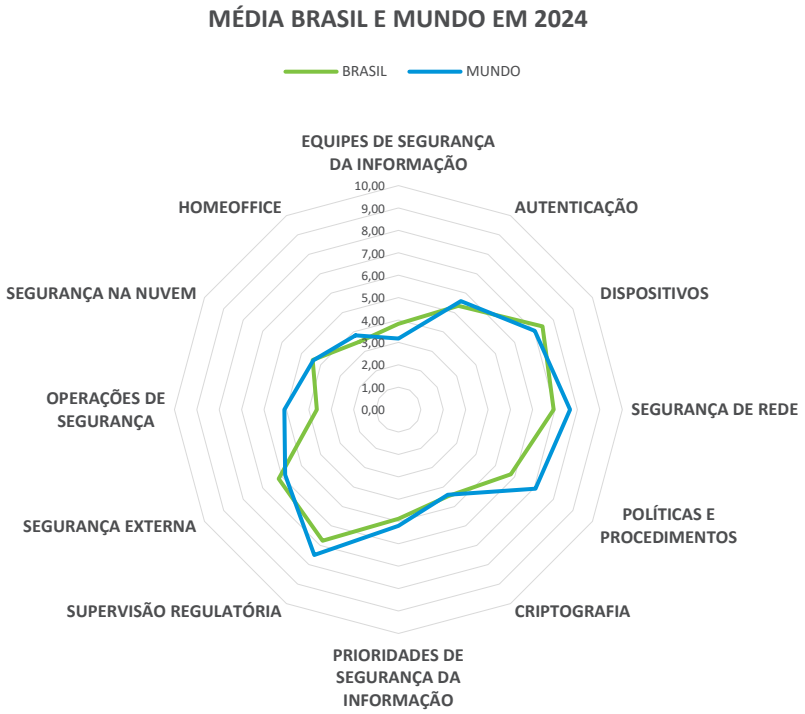


Em 2023, o BRASIL teve médias inferiores à geral em 7 categorias

As gestoras brasileiras ficaram abaixo de média geral (**5,57**) nas categorias: Equipes de segurança da informação, Criptografia, Prioridades de segurança da informação, Segurança externa, Operações de segurança, Segurança na nuvem e Trabalho remoto. Uma categoria a mais que as instituições das demais jurisdições, que ficaram abaixo da média geral em **6** categorias. Diferentemente do **BRASIL**, Segurança externa não foi uma categoria que o **MUNDO** pontuou abaixo da média.

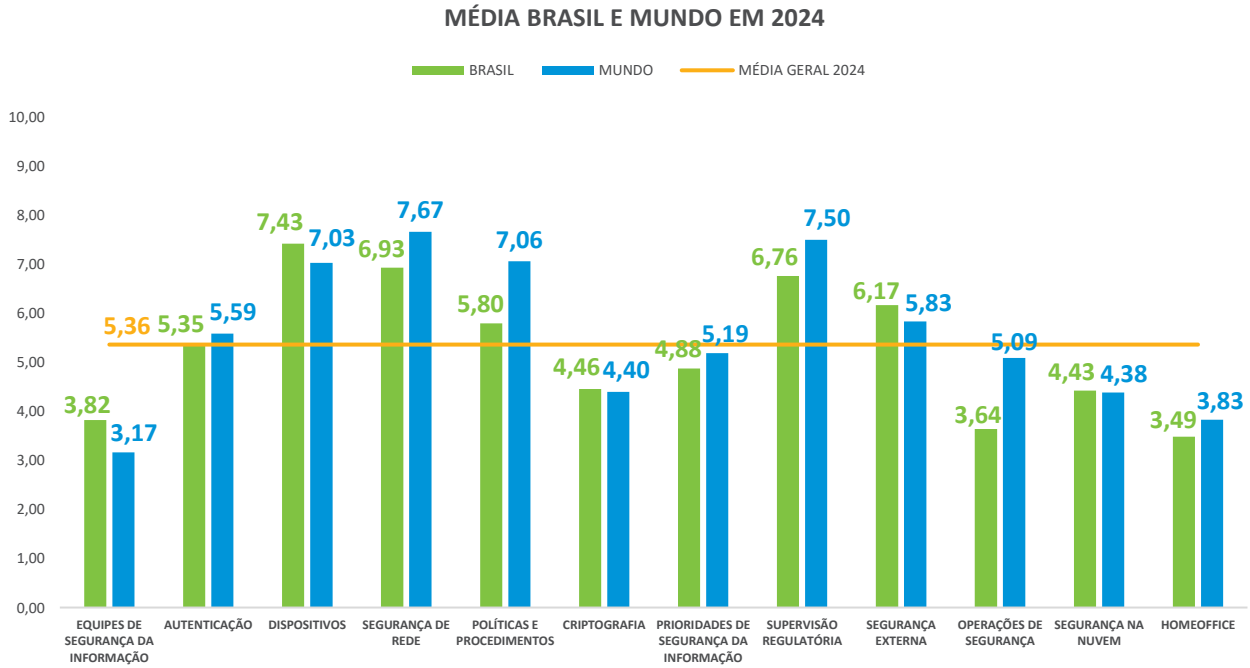






Em 2024, o BRASIL manteve médias inferiores à geral em 7 categorias

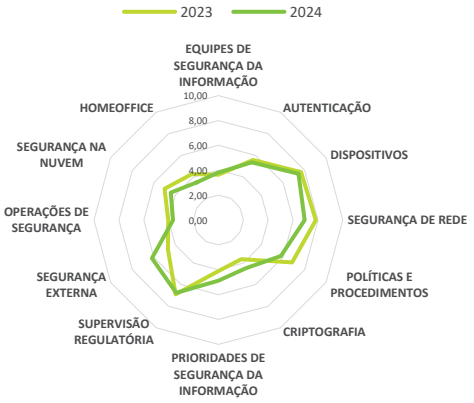
Com Segurança externa passando para cima da média geral (**5,36**) e Autenticação para baixo, as gestoras brasileiras registraram uma manutenção do número de categorias abaixo da média geral, em comparação com os resultados de 2023. No entanto, é importante ressaltar que a média geral sofreu redução de **3,78%** entre os dois levantamentos. O **MUNDO** também manteve o número de médias das categorias inferiores à geral (**6**).



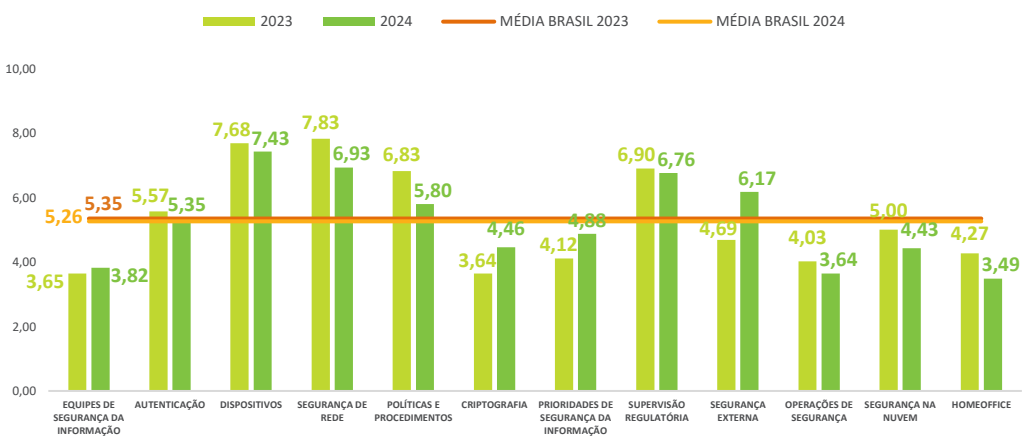
O BRASIL de 2023 para 2024

A média das gestoras brasileiras, considerando todas as categorias agregadas, foi de **5,35** em 2023 para **5,26** em 2024, uma variação negativa de 1,68%. Uma variação baixa, considerando o aumento de 57,69% do número de participantes do Brasil (de 26 para 41).

MÉDIA DO BRASIL EM 2023 E 2024



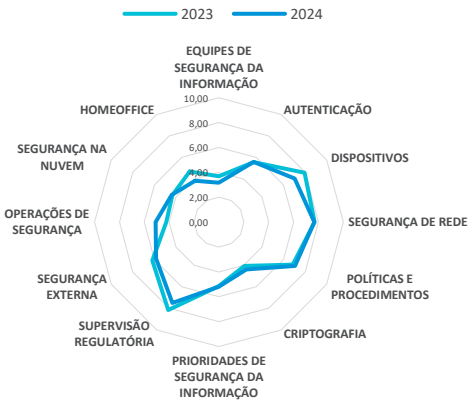
MÉDIA DO BRASIL EM 2023 E 2024



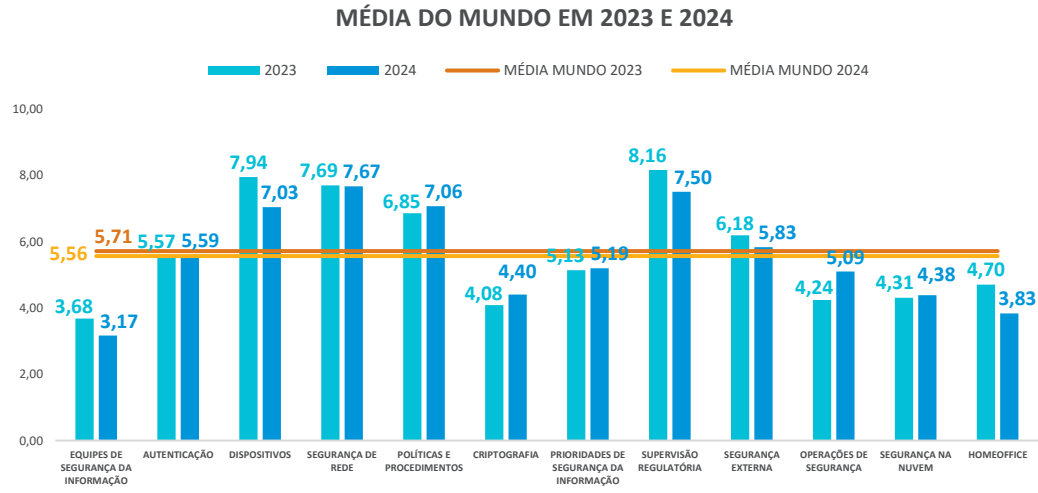
O MUNDO de 2023 para 2024

Já a média das gestoras não locais, considerando todas as categorias agregadas, foi de **5,71** em 2023 para **5,56** em 2024, uma variação negativa de 2,63%. Com aumento de apenas 4,44% do número de participantes de outras jurisdições além do Brasil (de 46 para 47).

MÉDIA DO MUNDO EM 2023 E 2024



MÉDIA DO MUNDO EM 2023 E 2024



Equipes de segurança da informação

BRASIL: 3,65 (2023) – 3,82 (2024) | **MUNDO:** 3,68 (2023) – 3,17 (2024)

Ter um time dedicado em tempo integral para a segurança da informação (SI) permite uma resposta mais ágil e eficiente a incidentes, além de garantir uma vigilância constante sobre possíveis ameaças. Os resultados da pesquisa apontam para uma melhora significativa dos resultados obtidos pelas gestoras brasileiras nessa categoria. O BRASIL atingiu uma média neste tópico específico de 5,17, número 29,3% maior que a média de 2023, que foi 4,00. Isso significa que a maior parte das gestoras brasileiras que responderam ao questionário na última pesquisa possuem ao menos 4% do total de seus colaboradores dedicados à SI. As gestoras brasileiras estão mais bem posicionadas neste aspecto em comparação com o MUNDO, que teve médias iguais a 3,38 em 2023 e 3,19 em 2024, uma queda de 5,6%.

A terceirização dessas funções pode complementar a equipe interna, fornecendo expertise adicional e recursos especializados. Porém, isso também exige uma gestão mais robusta para coordenação dos recursos e dos riscos adicionais relativos aos fornecedores. Com relação à terceirização das funções das equipes de SI, o BRASIL registrou uma média de 6,15 em 2023 e de 6,24 em 2024, enquanto o MUNDO atingiu 5,20 e 5,83, respectivamente nas duas pesquisas. A maior parte das gestoras locais como as das outras jurisdições possuem menos de 50% dos times dedicados à SI terceirizados. Inclusive, as brasileiras, em sua maioria, possuem uma taxa de terceirização menor que 28,3%.

Ainda nesta categoria, um ponto de atenção foi a variação negativa acentuada do BRASIL no tópico que trata da nomeação de um Chief Information Security Officer (CISO) dedicado em tempo integral para liderança do time de SI dentro das organizações. Em 2023, 54% das gestoras brasileiras possuíam um CISO, enquanto em 2024 este percentual caiu para 29%. O MUNDO apresentou estabilidade dessas taxas: 40% e 43%, respectivamente. A presença de um CISO é uma prática amplamente recomendada por especialistas e reguladores, pois este profissional não apenas coordena as atividades do time, mas também alinha as estratégias de cibersegurança com os objetivos dos negócios da organização, garantindo uma abordagem holística e proativa na mitigação de riscos.

As certificações mais comuns exigidas pelas gestoras de ativos, em 2024, dos profissionais responsáveis pela segurança da informação e cibernética são: CISSP (62,96%), CISM (44,44%), CISA (33,33%), CCSP/CCSK (11,11%), CEH (11,11%), CompTIA Security+ (7,41%), ITIL (7,41%) e outras (37%).

Autenticação

BRASIL: 5,57 (2023) – 5,35 (2024) | **MUNDO:** 5,57 (2023) – 5,59 (2024)

Políticas de senha rigorosas são a primeira linha de defesa, estabelecendo diretrizes sobre a complexidade, a extensão e a frequência de troca de senhas para dificultar o acesso não autorizado. Os resultados da pesquisa demonstram que grande parte das gestoras, tanto locais como de outras jurisdições, exige que os colaboradores definam senhas complexas (por exemplo: alfabéticas + numéricas + caracteres especiais). Enquanto a extensão das senhas adotadas pelas respondentes do BRASIL ficou um pouco abaixo da observada entre as demais respondentes. A maioria das gestoras brasileiras adota senhas de 8 caracteres para colaboradores em geral e de 9 a 12 caracteres para administradores (usuários com acessos privilegiados). Situação que se manteve estável nas edições de 2023 e 2024 da pesquisa, com uma leve melhora na última edição. Por sua vez, o MUNDO tende a exigir, em sua maioria, senhas um pouco mais longas: 9 a 12 caracteres

para colaboradores em geral e 12 a 15 caracteres para administradores. A frequência de troca das senhas para as gestoras locais e de outras jurisdições se manteve entre 90 e 120 dias, para usuários com ou sem acesso privilegiado, em ambos os levantamentos. O uso de software de gerenciamento de senhas facilita a criação e o armazenamento de senhas fortes, reduzindo a possibilidade de reutilização de credenciais comprometidas. As gestoras brasileiras utilizam essas ferramentas mais que as gestoras de outras jurisdições e, em geral, a maioria das respondentes adota a prática ou está considerando implementar nos próximos anos.

A implementação de autenticação baseada em risco adiciona uma camada extra de segurança, garantindo que apenas usuários legítimos possam acessar os sistemas. Grande parte das gestoras respondentes adota ou está considerando a implementação de práticas de autenticação baseada em risco, destacadamente com relação a acessos remotos. Atualmente, essas práticas são mais difundidas entre as gestoras não locais. A prática de autenticação mais difundida entre as participantes da pesquisa e implementada pela maioria delas é a exigência de autenticação multifator (MFA) para acessos internos e externos, que combina fatores como senhas, tokens e biometria. A autenticação biométrica, como utilização de reconhecimento facial ou de impressão digital para acesso a dispositivos corporativos, ainda não é amplamente aplicada local ou globalmente.

Dispositivos

BRASIL: 7,68 (2023) – 7,43 (2024) | **MUNDO:** 7,94 (2023) – 7,03 (2024)

Adotar um modelo de confiança zero para acesso à rede interna é uma abordagem que consiste em não considerar automaticamente nenhum dispositivo como confiável e verificar rigorosamente todos os acessos, reduzindo a superfície de ataque. Segundo a pesquisa, o BRASIL apresentou evolução na adoção deste modelo entre 2023 e 2024, com suas médias partindo de 3,8 e atingindo 4,9 neste tópico específico. Enquanto o MUNDO apresentou queda da adoção desta prática, com médias iguais a 4,5 e 3,6, respectivamente para os dois levantamentos.

A utilização de firewalls ou soluções de proteção equivalentes em endpoints, que auxilia no controle do tráfego e bloqueio de atividades suspeitas, demonstrou-se uma prática amplamente difundida local e globalmente, com quase todas as respondentes da pesquisa afirmando adotá-la. A detecção e prevenção de intrusão em hosts, bem como a utilização de soluções de detecção e resposta de endpoint, que são fundamentais para monitorar atividades maliciosas e responder rapidamente a incidentes, também apresentaram altas taxas de implementação pelas gestoras. No entanto, o BRASIL teve significativa redução da aplicação de restrições de acesso a mídias removíveis em dispositivos de clientes, com médias nos levantamentos de 8,2 e 6,8, respectivamente, enquanto o MUNDO se manteve estável para este fator, com médias iguais a 7,3 e 7,5.

Ressalta-se ainda, que, em 2024, 24,39% das respondentes afirmaram adotar política que permite aos colaboradores utilizarem seus dispositivos pessoais para acessar a rede corporativa (Bring Your Own Device – BYOD). Estão considerando implementar essa política 8,54% das participantes e 67,07% não têm planos nesse sentido.

Segurança de rede

BRASIL: 7,83 (2023) – 6,93 (2024) | **MUNDO:** 7,69 (2023) – 7,67 (2024)

O controle de acesso a sites externos utilizando servidores proxy ou outros controles baseados em rede é essencial para monitorar e restringir atividades potencialmente maliciosas. Enquanto a segmentação da rede interna com firewalls ou outras capacidades de controle limita a movimentação lateral de atacantes, confinando possíveis brechas. A adoção de tecnologia de firewall de próxima geração, que oferece inspeção profunda de pacotes e capacidades de inspeção de aplicativos, também é recomendável para uma defesa abrangente contra ameaças cibernéticas avançadas. Todas essas práticas apresentaram altas taxas de adoção entre todas as respondentes nos levantamentos de 2023 e 2024 da pesquisa.

Resultado semelhante para a detecção de intrusão e interceptação na conexão com a internet. Porém, o uso de sistemas de detecção de anomalias, como a Análise de Comportamento do Usuário (User Behavior Analytics), pelas gestoras não locais teve significativa variação negativa. As médias do MUNDO para este tópico específico caíram de 8,2 em 2023 para 6,8 em 2024. Enquanto o BRASIL registrou estabilidade, com médias iguais a 7,6 e 7,3, respectivamente. Outro destaque é a adoção de políticas de confiança zero para redes remotas de acesso, onde as gestoras brasileiras tiveram algum avanço, mas ainda desempenharam bastante abaixo da média na categoria, com resultados iguais a 4,7 em 2023 e 5,5 em 2024. Enquanto as gestoras não locais obtiveram 6,4 e 5,9, respectivamente.

Políticas e procedimentos

BRASIL: 6,83 (2023) – 5,80 (2024) | **MUNDO:** 6,85 (2023) – 7,06 (2024)

A definição de políticas e procedimentos para segurança da informação e cibernética é um requisito regulatório às instituições atuantes nos mercados financeiros e de capitais no Brasil. A conformidade rigorosa com regulamentações e padrões internacionais, aliada a uma governança eficaz, garante uma implementação eficaz das melhores práticas do setor para cibersegurança, incluindo a proteção de dados, avaliação e gestão de riscos (inclusive relacionados a terceiros), gestão da continuidade de negócios, capacitação e atualização dos colaboradores, realização de testes e exercícios de simulação, definição de métricas de eficácia etc. Na tabela a seguir, destacam-se os principais resultados das instituições participantes da pesquisa nesta categoria.

POLÍTICAS E PROCEDIMENTOS	BRASIL		MUNDO		OBSERVAÇÃO
	2023	2024	2023	2024	
Programa de gerenciamento de identidade e acesso (Identity and Access Management – IAM)	6,7	6,3	7,0	6,8	
Testes de conformidade para os controles estabelecidos	5,4	5,7	5,1	4,6	

Plataforma de Governança, Risco e Conformidade (excluindo Excel) para gerenciar e monitorar riscos e conformidade	5,3	5,6	5,7	6,3	
Revisões periódicas de acesso (access reviews)	10,0	8,5	9,1	9,4	
Utilização de frameworks de segurança como base para o programa de cibersegurança	9,6	8,8	9,1	10,0	NIST Cybersecurity Framework e ISO-IEC27K são os mais utilizados
Avaliações de risco periódicas (risk assessments)	8,8	7,9	8,8	8,9	
Exigência de treinamento de SI dos colaboradores	7,5	8,3	8,4	9,0	A maioria das gestoras respondentes realiza esses treinamentos anualmente
Exercícios simulados de phishing	7,9	7,8	8,7	9,2	
Exigência de assinatura anual de declaração de consentimento com a política de segurança da informação e cibernética da empresa	6,8	8,1	6,5	6,0	
Manutenção de inventário periódico de todos os dispositivos físicos, software e aplicativos	9,6	8,1	8,2	7,3	
Exercícios práticos periódicos (tabletop) para preparar a equipe para responder a um evento ou desastre	6,3	6,1	7,3	7,8	A maioria das gestoras respondentes realiza esses exercícios anualmente
Plano detalhado de resposta a incidentes	8,1	8,5	9,2	9,3	
Procedimento de escalonamento claro para relatar eventos cibernéticos	8,7	8,5	8,5	9,8	
Seguro cibernético	1,5	2,3	6,3	6,9	A principal faixa de valor de cobertura dos seguros contratados é de 1 a 5 milhões de dólares americanos
Ambiente de teste e desenvolvimento de software e aplicativos separado do ambiente de produção	9,3	8,1	8,6	8,6	

Exigência de avaliações de risco de segurança cibernética de prestadores de serviços terceirizados	6,5	5,9	8,0	7,3	
Backups dos principais sistemas de negócios	7,9	7,7	6,5	6,4	

Questões envolvendo a adoção de políticas formais descrevendo como e onde tecnologias como AI e LLMs podem ser utilizadas passaram a compor o levantamento a partir de 2024. Portanto, ainda não é possível realizar uma análise comparativa. Nesta última edição da pesquisa, o BRASIL pontuou 2,88, enquanto o MUNDO registrou 4,83. A média neste tópico foi de 4,01. Entre as gestoras respondentes, 32,05% possuem políticas formais definidas para essas tecnologias.

Criptografia

BRASIL: 3,64 (2023) – 4,46 (2024) | **MUNDO:** 4,08 (2023) – 4,40 (2024)

A criptografia garante que dados sensíveis, como backups externos, e-mails e dados em movimento, estejam protegidos contra acessos não autorizados, mantendo a privacidade e a integridade das informações. A implementação de criptografia robusta em compartilhamentos internos de arquivos e bancos de dados internos é crucial para prevenir vazamentos e acessos indevidos, enquanto o uso de provedores de serviços de armazenamento deve ser cuidadosamente gerido para assegurar que os dados permaneçam cifrados e seguros. Além disso, o gerenciamento de direitos digitais e senhas, aliado ao monitoramento contínuo de acessos, previne que informações críticas sejam comprometidas, permitindo uma resposta rápida a qualquer tentativa de violação. Na tabela a seguir, destacam-se os principais resultados das instituições participantes da pesquisa para diferentes aplicações da criptografia.

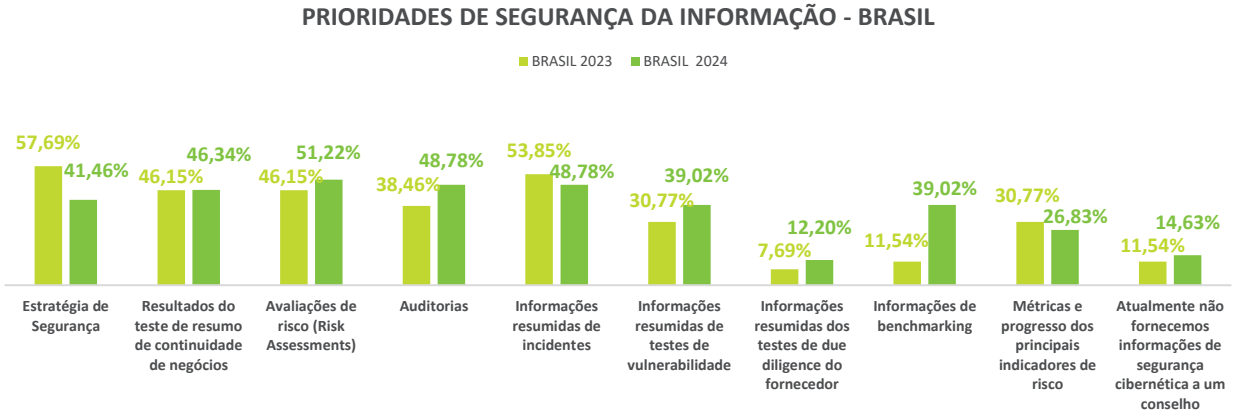
CRIPTOGRAFIA	BRASIL		MUNDO	
	2023	2024	2023	2024
Criptografia de mídia de backup externa	6,8	6,9	7,3	6,9
Criptografia de compartilhamentos de arquivos internos	3,1	5,2	4,0	4,2
Criptografia de bancos de dados internos	3,3	5,7	4,5	4,8
Criptografia dos seus dados pelo provedor de serviços de armazenamento (Storage Service Provider – SSP), quando contratados	6,0	8,0	7,9	5,9

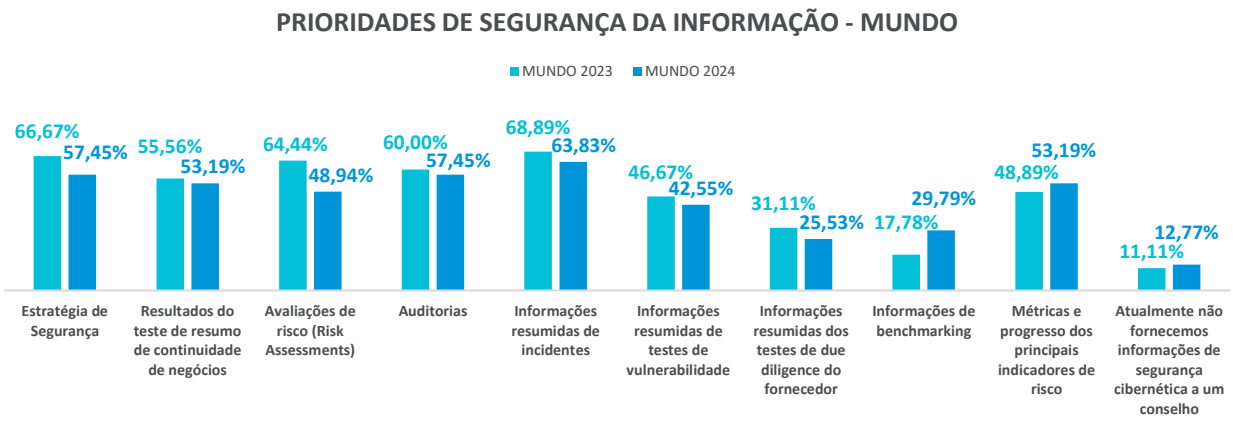
Utilização de Digital Rights Management	1,7	2,4	2,9	3,0
Exigência de que as transmissões externas de e-mail sejam criptografadas	4,7	5,4	5,6	5,5
Criptografia em nível de mensagem para e-mail (por exemplo, por S/MIME, Zixmail)	3,4	4,5	2,4	3,3
Criptografia de dados internos em movimento (data in motion)	5,3	4,5	5,5	5,4

Prioridades de segurança da informação

BRASIL: 4,12 (2023) – 4,88 (2024) | **MUNDO:** 5,13 (2023) – 5,19 (2024)

A preparação das informações que são apresentadas aos conselhos de administração é essencial para a definição eficaz das prioridades de segurança da informação e crucial para que os diretores e/ou conselheiros tenham acesso a dados atualizados sobre o desempenho das estratégias de segurança da organização e da avaliação dos riscos. Resultados de testes e auditorias regulares devem ser compilados e analisados para proporcionar uma visão clara da eficácia das medidas implementadas. Além disso, a manutenção detalhada de registros de incidentes, testes e benchmarks oferece uma base sólida para a rápida identificação e mitigação de vulnerabilidades. Métricas claras e o monitoramento contínuo do progresso dos indicadores-chave de risco são indispensáveis para avaliar a resiliência da organização e ajustar estratégias conforme necessário. Este nível de preparação não só reforça a integridade e confidencialidade dos dados, mas também fortalece o compromisso com a segurança e a conformidade regulatória. Nos gráficos a seguir, destacam-se as proporções de gestoras respondentes que sinalizaram incluir os tópicos descritos entre as informações preparadas para apresentação nos conselhos de administração.





Supervisão regulatória (terceiros)

BRASIL: 6,90 (2023) – 6,76 (2024) | **MUNDO:** 8,16 (2023) – 7,50 (2024)

A terceirização de serviços tecnológicos traz benefícios significativos, mas também aumenta os riscos de segurança que devem ser rigorosamente monitorados. Instituir uma governança específica para fornecedores terceirizados envolve a implementação de processos de revisão de terceiros e a imposição de requisitos contratuais de habilitação. Entre as gestoras brasileiras que responderam à pesquisa, 51,22% afirmaram possuir governança específica para fornecedores terceirizados em 2024, número inferior ao observado em 2023: 61,54%. Enquanto as respondentes de outras jurisdições tiveram resultados um pouco melhores: 70,21% em 2024 e 68,89% em 2023. No primeiro levantamento, 7,94% do total de participantes estava considerando implementar governança voltada à supervisão regulatória de terceiros, número que aumentou para 13,92% na última pesquisa realizada.

Segurança externa

BRASIL: 4,69 (2023) – 6,17 (2024) | **MUNDO:** 6,18 (2023) – 5,83 (2024)

Adotar uma abordagem estruturada de segurança voltada aos terceiros, envolve a implementação de processos de revisão passíveis de monitoramento. Definir acordos de nível de serviço (Service Level Agreement – SLA) de segurança, incluindo tempos de notificação de violação, pode contribuir para assegurar que qualquer vulnerabilidade seja comunicada e abordada prontamente por todos os parceiros e fornecedores, prevenindo incidentes. Os resultados do BRASIL apontam que 53,66% das gestoras locais adotavam essa prática no último levantamento, ao menos para os fornecedores de maior risco. Resultado ligeiramente superior do observado no levantamento anterior, quando metade – 50,00% – das participantes adotavam. Enquanto os resultados do MUNDO foram: 61,70% em 2024 e 57,78% em 2023.

Operações de segurança

BRASIL: 4,03 (2023) – 3,64 (2024) | **MUNDO:** 4,24 (2023) – 5,09 (2024)

O funcionamento contínuo das equipes de segurança da informação acompanhado da adoção das melhores práticas do segmento e a implementação de ferramentas avançadas que contribuam para a eficácia e eficiência das atividades desses times é crucial para antecipar e mitigar riscos e garantir maior resiliência cibernética. Na tabela a seguir, destacam-se os principais resultados das instituições participantes da pesquisa para diferentes operações de segurança da informação e cibernética.

OPERAÇÕES DE SEGURANÇA	BRASIL		MUNDO		OBSERVAÇÃO
	2023	2024	2023	2024	
Horário de funcionamento da equipe de defesa cibernética	6,5	6,5	7,9	5,0	Quanto maior o número de gestoras que adotam o funcionamento 24 x 7, mais próxima a nota de 10,0
Automatização de funções de segurança	4,9	5,9	6,5	6,7	Automatização da resposta a incidentes e de testes (vulnerabilidade, conformidade, penetração, aplicativos etc.)
Análise ativa por colaboradores da inteligência sobre ameaças cibernéticas	6,6	6,7	6,4	5,7	
Prescrição de SLAs para correção de vulnerabilidades de segurança	6,3	5,4	6,6	6,4	Na maioria dos casos, o BRASIL adota SLAs de 7 dias, enquanto o MUNDO adota SLAs entre 48 horas e 7 dias
Restrição a descumprimento de SLAs em função de impactos ou interrupções nas operações de negócios	2,1	3,1	3,6	3,0	
Realização de análises de malware internamente	5,4	6,8	6,1	3,2	
Rastreio e correção de protocolos e algoritmos obsoletos ou inseguros	8,4	7,4	7,6	7,3	Por exemplo: SSL v3, TLS v1.0/1.1
Utilização de ferramenta SIEM (Security Information and Event Management)	6,3	5,6	6,8	7,9	
Utilização de ferramentas UEBA (User and Entity Behavior Analytics) ou SOAR (Security Orchestration, Automation and Response) para SIEM	3,5	3,5	4,2	4,6	Ambas são ferramentas que contribuem para o aprimoramento do SIEM
Gerenciamento de riscos de segurança de aplicações (softwares)	7,8	6,3	6,7	8,3	Adoção de modelagem de ameaças, SAST, DAST, análise de composição de softwares, testes manuais, treinamentos etc.
Adoção de práticas DevOps e implementação de programa DevSecOps	2,2	2,4	2,8	2,0	

Segurança na nuvem

BRASIL: 5,00 (2023) – 4,43 (2024) | **MUNDO:** 4,31 (2023) – 4,38 (2024)

À medida que as organizações ampliam a adoção de serviços de armazenamento de dados em nuvem, torna-se imperativo reforçar as práticas de segurança para proteger a integridade e a confidencialidade das informações. A utilização de infraestruturas de nuvem pública, como IAAS (Infraestrutura como Serviço) e PAAS (Plataforma como Serviço), requer uma vigilância constante e a implementação de medidas robustas de segurança, além de uma preparação prévia à adoção relacionada a eventuais vulnerabilidades preexistentes. Na tabela a seguir, destacam-se os principais resultados das instituições participantes da pesquisa para diferentes práticas de segurança na nuvem.

SEGURANÇA NA NUVEM	BRASIL		MUNDO	
	2023	2024	2023	2024
Utilização de corretores de acesso à nuvem para impor políticas de segurança, requisitos de conformidade e proteção contra ameaças	5,1	6,8	5,6	5,5
Exigência de autenticação multifatorial ou em duas etapas para acesso administrativo a plataformas IAAS ou PAAS de nuvem pública	7,7	6,7	7,1	7,0
Exigência de tecnologias de autenticação locais para nuvem pública	6,7	5,4	5,9	4,2
Restrição de acesso a serviços de nuvem pública não relacionados aos negócios	5,6	6,1	5,9	5,9
Realização de processo de sanitização de dados para repositórios de dados de computação em nuvem	3,1	4,0	3,0	2,3
Realização de verificações regulares de vulnerabilidades na infraestrutura de nuvem pública IAAS ou PAAS	5,2	5,5	4,9	4,3
Realização de testes de penetração regulares em infraestrutura de nuvem pública IAAS ou PAAS	4,7	4,5	4,0	3,8

Trabalho remoto (home office)

BRASIL: 4,27 (2023) – 3,49 (2024) | **MUNDO:** 4,70 (2023) – 3,83 (2024)

Com o avanço do trabalho remoto e híbrido, especialmente pós-pandemia da COVID-19, surgiram novos desafios para a segurança da informação e cibernética. A execução de atividades fora do ambiente tradicional de escritório pode comprometer a eficácia de alguns controles e monitoramentos, tornando essencial mapear e mitigar vulnerabilidades adicionais. É fundamental que as organizações atualizem suas políticas e procedimentos de segurança, abrangendo tópicos como a classificação das informações e o uso de dispositivos e redes. Além disso, prever um tratamento específico para tecnologias emergentes, como o ChatGPT, contribui para prevenir o vazamento de informações confidenciais e/ou restritas.

Os resultados da pesquisa apontam para um maior relaxamento dos controles de segurança para a adoção do trabalho remoto e híbrido no último levantamento em comparação com o anterior. Foram considerados os controles a seguir: controles de acesso; verificação de vulnerabilidades de clientes remotos; sistemas operacionais/patches necessários de clientes de acesso remoto; controles de acesso privilegiado; e restrições que impeçam a impressão remota. Em 2023, a restrição à impressão de documentos em casa e os controles de acesso foram os itens mais flexibilizados pelas instituições. Enquanto, em 2024, a verificação de vulnerabilidades e a exigência de sistemas operacionais/patches para clientes de acesso remoto foram os procedimentos de maior relaxamento. Tanto o BRASIL como o MUNDO tiveram redução expressiva de suas notas neste tópico entre os levantamentos. As gestoras brasileiras saíram de 9,1 para 7,8 e as das demais jurisdições de 9,2 para 6,6.

As instituições respondentes também tiveram redução de suas notas para a adoção de política de classificação das informações. Os resultados do BRASIL foram 7,2 em 2023 e 6,2 em 2024, enquanto o MUNDO registrou 6,8 e 6,7, respectivamente para os levantamentos. A exigência do uso de etiquetas de confidencialidade em documentos é uma prática adotada pela maioria das gestoras locais (notas neste item: 6,1 em 2023 e 7,3 em 2024), enquanto nas demais jurisdições (notas neste item: 5,4 em 2023 e 4,7 em 2024) essa prática deixou de ser empregada pela maioria das respondentes no último levantamento. Já a utilização de ferramentas para identificar e aplicar esses rótulos de classificação e confidencialidade é bastante reduzida ainda, tanto local como globalmente.

Discussão

A Cyber Security Asset Management Benchmarking Survey tem atraído mais participantes ao longo dos anos e maior representação de diferentes jurisdições, bem como se atualizando constantemente para incluir novas tecnologias, ameaças e melhores práticas. Em virtude disso, futuras edições deste relatório poderão apresentar modificações quanto à metodologia de análise dos dados da pesquisa e às 12 categorias de análise propostas.

Os resultados apresentados ao longo deste documento se baseiam em respostas enviadas voluntariamente através de questionário específico pelas instituições participantes à ICI, organizadora da pesquisa, que compartilhou as informações resultantes anonimizadas com a ANBIMA. O foco dessa pesquisa é a atividade de gestão de ativos e, portanto, os resultados oferecem uma visão particular do grau de maturidade de organizações que atuam nos mercados financeiro e de capitais. Generalizações podem incorrer em imprecisões.

A expressiva participação das instituições brasileiras na pesquisa demonstra o engajamento das gestoras locais nas iniciativas voltadas ao amadurecimento das práticas de segurança da informação e cibernética. Contudo, a representatividade relativamente baixa de outras jurisdições implica em uma maior correlação dos resultados gerais com os resultados das gestoras brasileiras. Isso é um fator de atenção que será também observado em eventuais edições posteriores deste relatório em paralelo com o incentivo ao reforço da participação das instituições dos demais países em grupos e fóruns multilaterais que a ANBIMA participa.

A apresentação dos resultados dentro das categorias analisadas traz destaques dos principais fatores que compõem a nota obtida pelas gestoras nas respectivas categorias. Em função da extensão da pesquisa, que nesta última edição contou com 202 questões, não é realizada uma análise exaustiva de todas as perguntas neste relatório, visando a melhor comunicação das informações geradas. Por isso, não há uma relação direta entre a nota obtida pelas instituições participantes nas categorias de análise e as pontuações em tópicos específicos e/ou porcentagens mencionadas dessas categorias.

Este relatório visa, tão somente, oferecer dados comparativos sobre a Cyber Security Asset Management Benchmarking Survey no sentido de contribuir para a disseminação de melhores práticas de segurança da informação e cibernética. Assim, apoiando as instituições atuantes nos mercados financeiro e de capitais na identificação de oportunidades de desenvolvimento de suas estratégias de cibersegurança.

Conclusão

Este relatório sublinha a importância das práticas de segurança da informação e cibernética nos mercados financeiro e de capitais, disseminando as principais, que são abordadas também na Cyber Security Asset Management Benchmarking Survey. O compromisso contínuo com a atualização das políticas e estratégias, o engajamento dos conselhos de administração e a adaptação às novas tecnologias são essenciais para a construção de um ambiente cibernético mais seguro e resiliente. Neste sentido, destacam-se a seguir, de forma não exaustiva, áreas críticas onde há mais espaço para desenvolvimento de maturidade pelas organizações.

- **Liderança das equipes de segurança da informação**

Um dos fundamentos para a eficácia das estratégias de cibersegurança é a dedicação em tempo integral de um time especializado e capacitado, por exemplo, para respostas efetivas a incidentes e vigilância constante de possíveis ameaças. A maior parte das gestoras brasileiras possui um percentual adequado de colaboradores dedicados à segurança da informação e cibernética em relação ao total de funcionários e uma taxa de terceirização menor que 28,3%. Resultados superiores aos observados pelas gestoras dos demais países representados na pesquisa. No entanto, a nomeação de um CISO pelas organizações, que é uma prática essencial não apenas coordenação das atividades do time de SI, mas também para alinhamento das estratégias de cibersegurança com os objetivos dos negócios da organização, demanda mais atenção. No último levantamento, somente 29% das gestoras locais possuíam um CISO, enquanto nas demais jurisdições a taxa média é de 43%.

- **Políticas e controles aplicáveis ao trabalho remoto e híbrido**

A execução de atividades fora das dependências da organização, no trabalho remoto e híbrido, demanda políticas e procedimentos de segurança específicos para lidar com os desafios e ameaças adicionais relacionados à prática. Em contrapartida, a pesquisa evidenciou um relaxamento dos controles de segurança para o home office tanto local como globalmente. Cumpre salientar que muitas empresas estão impondo recentemente mais restrições ao trabalho remoto, mas é crucial, ao adotarem a prática e/ou optarem pela manutenção desta, que garantam a eficácia dos controles de segurança e atualizem suas políticas para abranger tópicos como a classificação das informações e o uso de dispositivos, tecnologias emergentes e redes.

- **Equilíbrio entre as prioridades das operações de negócios e de segurança**

Atualmente, grande parte das gestoras de ativos tolera descumprimentos de SLAs de operações de segurança em função de impactos ou interrupções nas operações de negócios. É recomendável buscar equilibrar com responsabilidade as prioridades dessas operações, considerando a possibilidade de que a não interrupção no curto prazo de determinadas atividades de negócio para ajustes de segurança pode implicar em interrupções mais prolongadas no futuro em caso de incidentes, que podem, inclusive, ter consequências irreversíveis.

- **Otimização do gerenciamento das informações de segurança e de eventos (SIEM)**

A implementação de SIEM pelas gestoras de ativos tem se mantido em níveis aceitáveis, mas há espaço para ampliação da adoção de tecnologias do tipo UEBA, que permitem uma análise mais precisa e automatizada dos comportamentos de usuários e entidades. Bem como de ferramentas capazes de orquestrar e automatizar respostas a incidentes de segurança, do tipo SOAR. Isso resulta em uma detecção mais rápida e eficaz de ameaças, redução de falsos positivos e uma resposta mais ágil a intrusões, promovendo maior proteção e resiliência cibernética entre as instituições.

Práticas e programas de segurança de aplicações

O gerenciamento de riscos de segurança de aplicações é implementado pela maioria das instituições participantes da pesquisa, contudo as práticas DevOps e os programas DevSecOps ainda são pouco difundidos. Essas abordagens contribuem para a integração das equipes de desenvolvimento, operações e segurança ao longo de todo o ciclo de vida do desenvolvimento de software, possibilitando uma identificação e mitigação mais precoce de vulnerabilidades, maior automação de processos de segurança e uma resposta mais rápida a incidentes. Por isso, é recomendável que organizações avaliem, conforme seu contexto específico, considerar essas abordagens em suas estratégias de cibersegurança.

Tratamento dos dados na nuvem e testagem da infraestrutura

Garantir que os dados sejam gerenciados de forma segura e que as plataformas estejam protegidas contra vulnerabilidades é uma responsabilidade das organizações que utilizam serviços de armazenamento de dados em nuvem. A realização de processo de sanitização de dados de repositórios voltados à computação em nuvem, de verificações frequentes de vulnerabilidades na infraestrutura e de testes de penetração regulares são medidas que contribuem para prevenir perda ou acesso não autorizado a informações restritas e para identificação e correção de falhas antes que possam ser exploradas por atacantes. Em contrapartida, essas práticas ainda são adotadas pela minoria das gestoras de ativos respondentes da pesquisa.

Práticas de criptografia para prevenir interceptações e acessos não autorizados

A adoção de práticas de criptografia em e-mails e dados em movimento cria uma barreira de proteção contra interceptações e acessos não autorizados a informações sensíveis. Além de investirem nessas práticas, é recomendável que as gestoras de ativos também considerem a utilização de ferramentas ainda pouco adotadas por elas, como Digital Rights Management (DRM), que utilizam tecnologias de criptografia e autenticação para garantir que apenas usuários autorizados possam acessar, copiar ou distribuir informações protegidas. Isso é fundamental para a proteção de propriedade intelectual, informações estratégicas e conteúdos digitais.

Modelo de confiança zero para acesso à rede interna

Não considerar automaticamente nenhum dispositivo como confiável e verificar rigorosamente todos os acessos a redes internas são práticas que ainda não são implementadas pela maioria das gestoras respondentes da pesquisa, mas são importantes para garantir a segurança da informação e prevenir intrusões.

Governança específica para fornecedores e parceiros

Ainda que a maioria das gestoras brasileiras tenha afirmado possuir governança específica para terceiros no questionário, a proporção com relação ao total de instituições participantes pelo Brasil diminuiu significativamente entre 2023 e 2024. É importante ressaltar, paralelamente, que o número total de respondentes locais aumentou expressivamente no último levantamento, o que tem impacto nessa análise. De qualquer modo, este é um ponto que exige atenção, pois é notório que o risco associado a terceiros é uma das principais preocupações em cibersegurança. Possuir uma governança e procedimentos de diligência bem definidos desde a contratação dos fornecedores e parceiros é crucial para garantir a segurança da informação e cibernética das organizações.

Contratação de seguro cibernético

A contratação de seguros cibernéticos pelas gestoras locais ainda não muito expressiva, enquanto nas demais jurisdições representadas na pesquisa a prática é adotada pela maioria. Esses seguros, para além do pagamento de indenizações, podem oferecer consultoria e suporte técnicos, especialmente quando ocorrem

incidentes cibernéticos, o que contribui para uma resposta mais eficaz e eficiente. Além disso, cobrem custos de violação de dados e oferecem financiamentos para a recuperação e continuidade dos negócios.

Expediente

Relatório comparativo: pesquisa internacional de cibersegurança na gestão de ativos (2023 - 2024)

Gerência de Representação de Distribuição de Produtos de Investimentos
Luiz Henrique de Carvalho

Redação e Análises
Augusto Brisola

Dados e Análises
Antonio Sá

Cibersegurança
Silvio dos Santos

Divulgação
Paula Lepinski

Presidência
Carlos André

Diretoria
Adriano Koelle, Andrés Kikuchi, Aquiles Mosca, Carlos Takahashi, César Mindof, Denisio Liberato, Eduardo Azevedo, Eric Altafim, Fernanda Camargo, Fernando Rabello, Flavia Palacios, Giuliano De Marchi, Gustavo Pires, Julya Wellisch, Pedro Rudge, Roberto Paolino, Roberto Paris, Rodrigo Azevedo, Sergio Bini, Sergio Cutolo, Teodoro Lima e Zeca Doherty

Comitê Executivo
Amanda Brum, Eliana Marino, Francisco Vidinha, Guilherme Benaderet, Lina Yajima, Marcelo Billi, Soraya Alves, Tatiana Itikawa, Thiago Baptista e Zeca Doherty

Grupo Consultivo de Cibersegurança
Adonai Bernardes, Ana Paula Godoy, Anderson Mota, Andre Bastos, Denise Ornellas, Fabio Nacajune, Frederico Neres, Ismar Leite, Jorge Matsumoto, Kenia Carvalho, Lilian Celeri, Luciano Kahn, Luiz Leme, Mauricio Rodrigues, Patrik Lemos, Rodrigo Fusco, Rogério Malgor, Simone de Grandis, William Borges

Endereço

Rio de Janeiro
Praia de Botafogo, 501 - 704, Bloco II, Botafogo,
Rio de Janeiro, RJ - CEP: 22250-911
Tel.: (21) 2104-9300

São Paulo
Av. Doutora Ruth Cardoso, 8501, 21º andar, Pinheiros
São Paulo, SP - CEP: 05425-070
Tel.: (11) 3471 4200
www.anbima.com.br