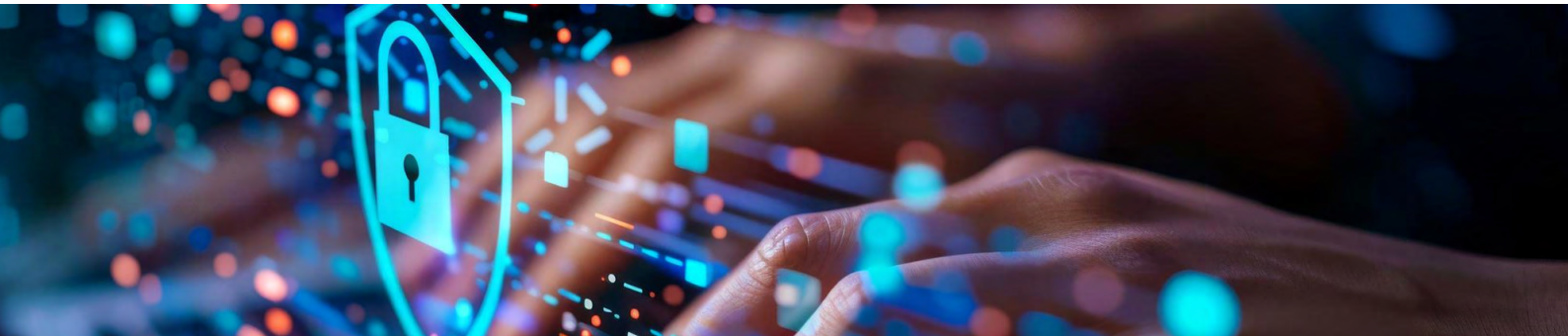
ANBIMA

Guia de Cibersegurança

4ª Edição | 2025

SUMÁRIO



SOBRE O GUIA DE **CIBERSEGURANÇA**

Este Guia de Cibersegurança tem o objetivo de orientar as organizações atuantes nos mercados financeiro e de capitais na implementação de um programa de segurança cibernética, contribuindo para a integridade desses mercados e sua maior resiliência frente às crises motivadas por incidentes. A estruturação de um programa de segurança cibernética é de extrema importância frente à evolução das ameaças e emergência de tecnologias e sua incorporação na rotina das organizações. Observando-se a legislação e regulação[1] vigentes e dentro do limite de suas atribuições, as organizações devem, no desenvolvimento de seus programas de segurança cibernética, considerar minimamente os requisitos da política de cibersegurança, ou documento análogo, conforme previsto nas Regras e Procedimentos de Deveres Básicos da Anbima[2].

Além das normas, as organizações podem basear-se em padrões nacionais e/ou internacionais existentes para desenvolver e manter atualizado seu programa de segurança cibernética, adaptando-o às suas características, necessidades e atividades. A Anbima disponibiliza guias técnicos e materiais que reúnem recomendações e orientações técnicas relacionadas a tópicos específicos de segurança da informação e cibernética, além de um ambiente especial dedicado ao tema: o **#EspaçoCiber**. Referências adicionais podem ser consultadas na seção Base de Conhecimento deste Guia.

[1] **BRASIL. Resolução CMN 4.893/21. Disponível em:** https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893.

BRASIL. Resolução CVM 35/21. Disponível em: https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol035consolid.pdf.

[2] **Anbima. Regras e procedimentos de deveres básicos.** Disponível em: https://www.anbima.com.br/data/files/61/B3/06/B3/EBEA591036202959B82BA2A8/6.%20Regras%20e%20Procedimentos%20de%20Deveres%20Basicos_v_25_02_2025.pdf.

SOBRE O GUIA DE CIBERSEGURANÇA

A segurança cibernética está estreitamente conectada à segurança da informação e é fundamental para proteger os dados e a privacidade dos usuários nos ambientes digitais, em conformidade com a LGPD (Lei Geral de Proteção de Dados)[3].

Para assegurar os ativos das organizações, é imprescindível que todas as pessoas vinculadas a elas, incluindo fornecedores e prestadores de serviços terceirizados, sejam abarcadas pelos programas de segurança cibernética. Assim, recomenda-se o envolvimento de diversas áreas na criação e gestão desses programas, além da promoção de ações e campanhas periódicas de capacitação e conscientização sobre o tema.

Acompanhando o desenvolvimento tecnológico e a evolução das ameaças, as práticas de cibersegurança exigem atualização e adaptação contínuas pelas organizações. Neste sentido, este guia, cuja primeira edição foi publicada em 2016, é revisado e/ou complementado periodicamente. Outras duas edições foram publicadas em 2017 e 2021, e esta é a quarta edição.

Este guia não integra ou se caracteriza como documento da autorregulação Anbima. O seu conteúdo não é vinculante para quaisquer organizações, associadas ou não, e limita-se, tão somente, a difundir melhores práticas e orientar técnicas para melhor consecução de atividades relacionadas à segurança cibernética, sem prejuízo

[3] **BRASIL. Lei 13.709/18. Disponível em:** https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

a futuras discussões sobre o tema. O disposto aqui 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.

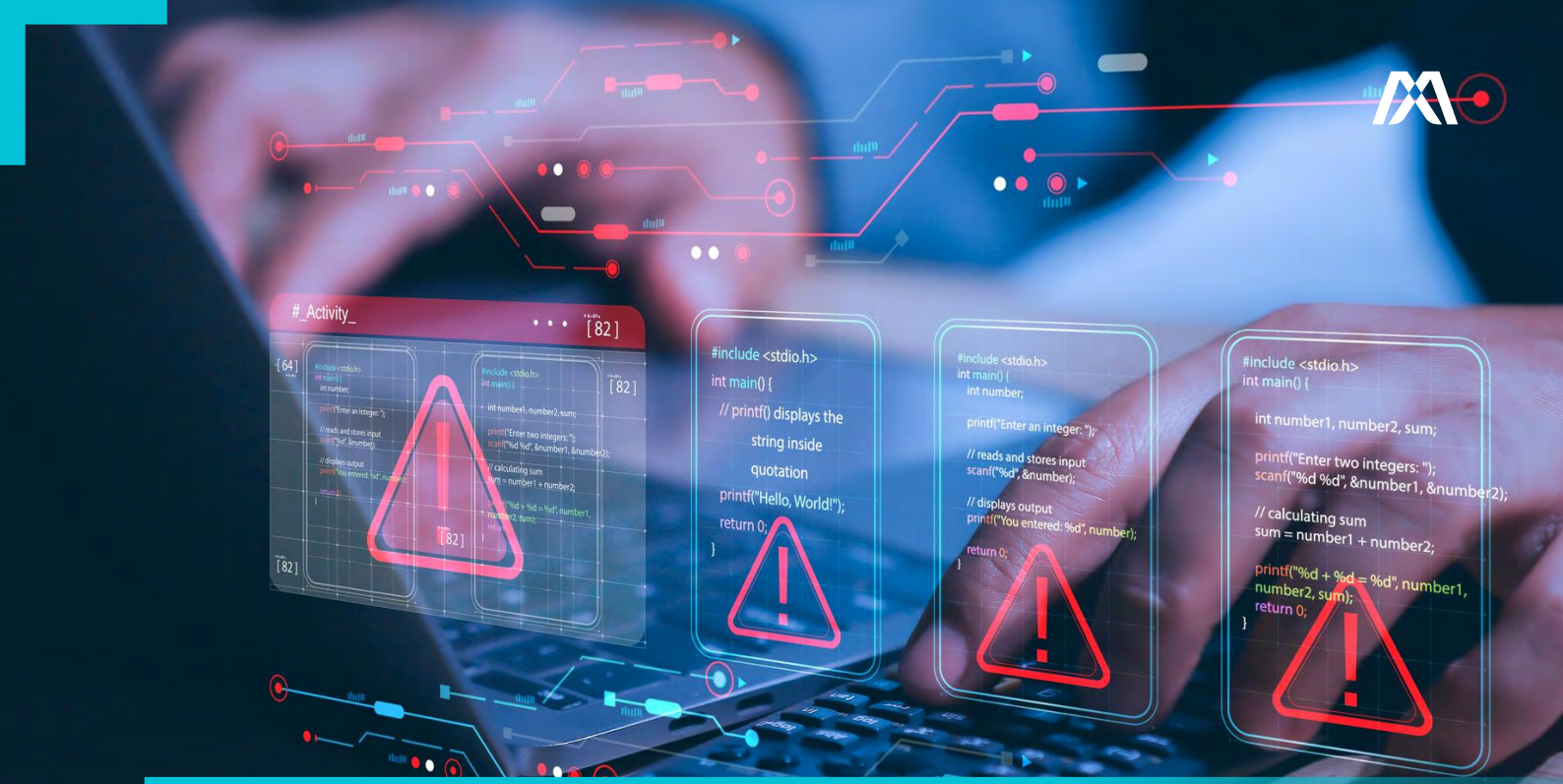
Este guia não se caracteriza como documento da autorregulação Anbima e oferece recomendações e exemplos de práticas para orientar as organizações e contribuir para o aprimoramento da segurança cibernética nos mercados financeiro e de capitais brasileiros.

As práticas descritas neste guia não constituem uma lista única e exaustiva das iniciativas que as organizações podem tomar para reforçar a cibersegurança.

Existem várias fontes e recursos que podem contribuir, de forma complementar a este guia, para o desenvolvimento do programa de segurança cibernética das organizações. Consulte referências adicionais na seção Base de conhecimento.

A implementação das recomendações depende das características e das necessidades de cada organização.

A Anbima também disponibiliza guias técnicos, estudos e ferramentas relacionados a tópicos específicos de segurança da informação e cibernética. Consulte-os no #EspaçoCiber.



O RISCO CIBERNÉTICO

A definição do risco cibernético é essencial para a estruturação de um programa de segurança cibernética. Identificar e avaliar os riscos permite que as organizações desenvolvam estratégias de prevenção, proteção, controle, monitoramento, testagem e resposta adequadas. Isso é fundamental para garantir a segurança de usuários, redes, dispositivos, aplicações (softwares), processos, informações, serviços e sistemas.

Esse risco, com base na definição[4] dada pelo Nist (Instituto Nacional de Padrões e Tecnologia), dos Estados Unidos, está diretamente relacionado à perda de confidencialidade, integridade, controle ou disponibilidade de informações ou tecnologias com possíveis impactos adversos a operações, atividades, funções, ativos, indivíduos, organizações ou nações. Os incidentes cibernéticos, que estão associados à realização dos riscos, podem ser caracterizados de forma não exaustiva, como:

[4] **NIST. Developing cyber-resilient systems: a systems security engineering approach (2021). Disponível em:** https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

Malware (e.g. ransomware, vírus, worms, trojans, spyware, adware, rootkits, screenlogger, bots) – softwares desenvolvidos para corromper computadores e redes.

Engenharia social (e.g. clickjacking; phishing, quishing, smishing, vishing, deepfake) – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito.

Ataques de DoS (Negação de Serviços), DDoS (Negação de Serviço Distribuída) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da organização, no caso das botnets, o ataque vem de muitos computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

Intrusões (e.g. ataque de força bruta e MitM – Man in the Middle, em que um invasor se insere entre duas partes que estão se comunicando, interceptando e, potencialmente, modificando a comunicação sem que nenhuma das partes saiba) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Existem diversas razões para que ataques sejam realizados por diferentes agentes (organizações criminosas ou hackers individuais, organismos de Estado, terroristas, colaboradores, competidores etc.), por exemplo:

- Roubar, manipular ou adulterar informações.
- Obter vantagens competitivas e informações confidenciais de organizações concorrentes.

- Fraudar, sabotar ou expor a organização invadida.
- Promover ideias políticas e/ou sociais.
- Espionar, promover guerra cibernética e praticar terrorismo.
- Enfrentar desafios, ter adoração por hackers famosos e chamar atenção.

A título de referência, as **Orientações para o treinamento de colaboradores em cibersegurança**[5] reúnem exemplos de ameaças cibernéticas e dos métodos mais comuns utilizados para ataques, além de conceitos importantes e boas práticas em cibersegurança.

[5] **Anbima. Orientações para o treinamento de colaboradores em cibersegurança (2024). Disponível em:** https://www.anbima.com.br/data/files/67/25/31/3D/483B49100054FA49B82BA2A8/Orientacoes_treinamento_de_colaboradores_em_ciber.pdf.

IMPLEMENTANDO UM PROGRAMA DE SEGURANÇA CIBERNÉTICA

Um programa eficiente contra ameaças cibernéticas deve conter minimamente cinco funções bem definidas:

- **IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS**
- **AÇÕES DE PREVENÇÃO E PROTEÇÃO**
- **CONTROLE, MONITORAMENTO E TESTES**
- **PLANO DE RESPOSTA**
- **GESTÃO**

IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Identificar os riscos internos e externos, os ativos de hardware e software, bem como processos que precisam de proteção.

AÇÕES DE PREVENÇÃO E PROTEÇÃO

Estabelecer um conjunto de medidas cujo objetivo é mitigar e minimizar a concretização dos riscos identificados no item anterior, ou seja, buscar impedir previamente a ocorrência de um ataque cibernético, incluindo a programação e implementação de controles.

CONTROLE, MONITORAMENTO E TESTES

Detectar as ameaças em tempo hábil, reforçando os controles, caso necessário, e identificar possíveis anomalias no ambiente tecnológico, incluindo a presença de usuários, componentes ou dispositivos não autorizados.

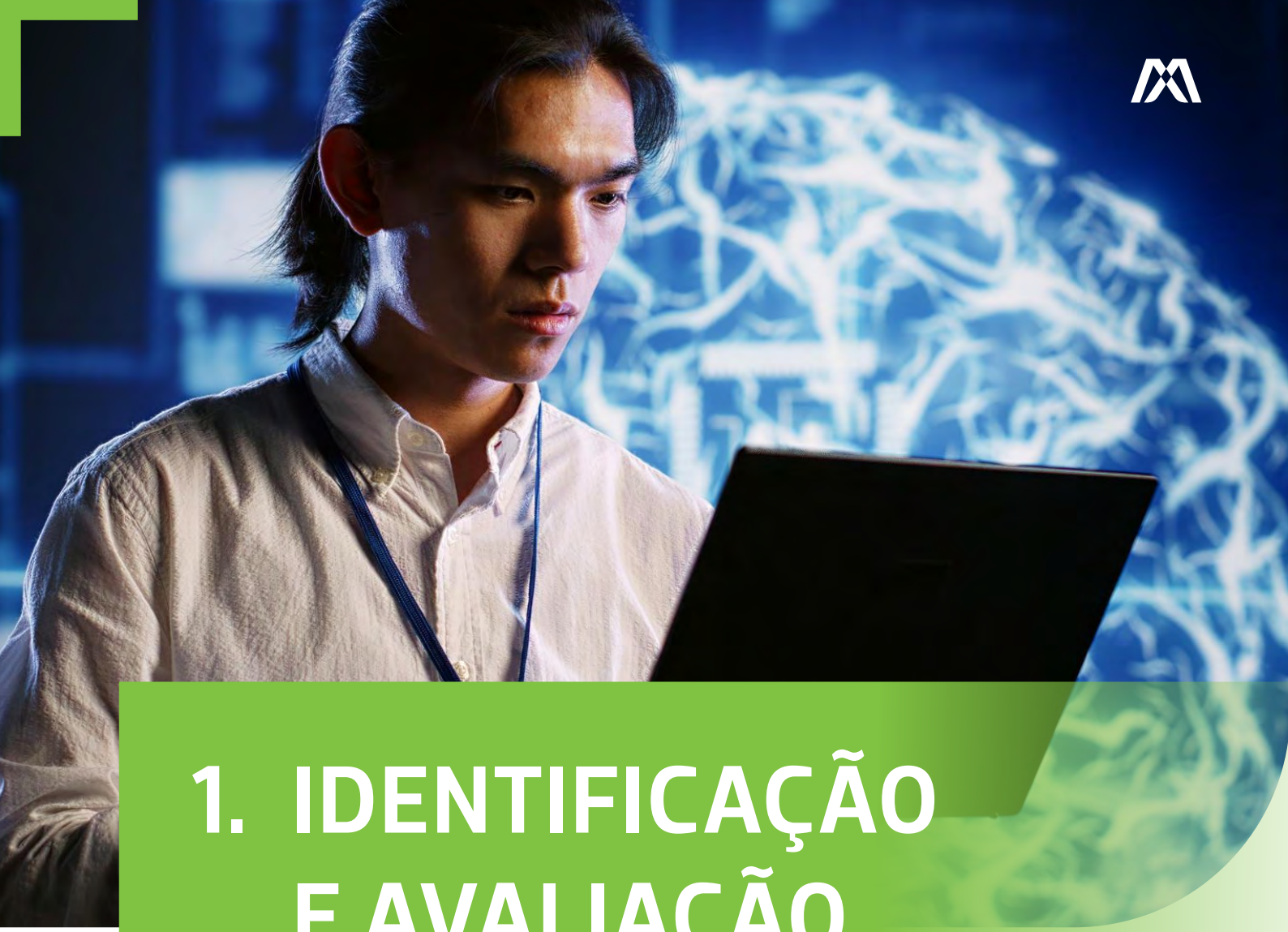
PLANO DE RESPOSTA

Manter um plano de resposta, tratamento e recuperação de incidentes e considerar a manutenção de um plano de comunicação interna e externa.

GESTÃO

Gestão do programa de segurança cibernética, que deve ser continuamente atualizado, garantindo a retroalimentação das estratégias definidas com ações, processos e indicadores.

Veja a seguir o detalhamento das cinco funções, com recomendações fundamentais, não exaustivas, para assegurar a efetividade dos programas de segurança cibernética.



1. IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

O programa de segurança cibernética deve ser compatível com as atividades, as características, as necessidades, os objetivos e os stakeholders das organizações, bem como abranger a elaboração e gestão de uma avaliação de riscos (risk assessment). Além disso, os recursos de defesa e as respostas definidos devem ser proporcionais e adequados aos riscos identificados.

Recomendações

1.1. Identificar e manter inventário atualizado de todos os ativos críticos da organização (espaços físicos, equipamentos, sistemas, redes, dados, processos e serviços), desde as etapas iniciais da avaliação de riscos.

1.2. Avaliar as vulnerabilidades e o grau de exposição dos ativos críticos da organização às diversas ameaças possíveis identificadas.

1.3. Avaliar os riscos cibernéticos identificados, adotando-se, a exclusivo critério das organizações e conforme considerarem adequado, os parâmetros definidos nas referências disponíveis na seção Base de Conhecimento.

1.4. Contemplar as atividades desenvolvidas por prestadores de serviços terceirizados, incluindo serviços de nuvem, na avaliação de riscos.

1.5. Criar regras e procedimentos específicos para a classificação das informações geradas, coletadas, tratadas e armazenadas pela organização, permitindo a implementação de processos para tratamento, armazenamento, transporte e descarte adequados dessas informações.

1.6. Mensurar a probabilidade de realização de eventos que comprometam a segurança cibernética da organização, considerando os possíveis impactos financeiros, operacionais e reputacionais.

2. AÇÕES DE PREVENÇÃO E PROTEÇÃO

Recomendações

2.1. Controlar e assegurar acesso interno e externo adequado aos ativos críticos da organização, considerando:

a. Adotar procedimentos de identificação, autenticação e autorização dos usuários, dispositivos e/ou sistemas no acesso aos ativos críticos das organizações.

b. Assegurar que os acessos, quando concedidos, sejam limitados aos recursos necessários para a adequada utilização dos ativos críticos da organização, que possam ser rapidamente revogados quando necessário.

c. Estabelecer política de senhas que defina minimamente:

I. Padrões de complexidade das senhas, tais como: mínimo de 12 caracteres, sendo estes alfabéticos (diferenciando letras maiúsculas e minúsculas), numéricos e especiais (símbolos).

II. Período para troca obrigatória da senha inferior a 90 dias para usuários administrativos e/ou 120 para usuários em geral.

III. Proibição ao reaproveitamento de senhas anteriores.

IV. Critérios para adoção de aplicação (software) de gerenciamento de senhas, quando aplicável.

V. Critérios para adoção de MFA (Autenticação Multifator), quando aplicável.

VI. Critérios para adoção de autenticação biométrica, quando aplicável.

d. Estabelecer procedimentos auditáveis e rastreáveis de gestão de eventos relacionados ao processo de acesso (login) aos ativos críticos da organização.

e. Estabelecer política de acesso de dispositivos aos ativos críticos da organização, considerando:

I. Adotar modelo de confiança zero para acesso de dispositivos às redes internas.

II. Definir regras e procedimentos específicos para utilização de dispositivos pessoais de colaboradores (BYOD – Bring Your Own Device), quando aplicável, abrangendo minimamente: controles para mitigar riscos identificados, critérios de responsabilização e procedimentos relacionados às situações de desligamento do colaborador.

III. Implementar as Orientações de cibersegurança para implementação de política de BYOD[6].

[6] **Anbima. Orientações de cibersegurança para implementação de política de BYOD (2025). Disponível em:** https://www.anbima.com.br/data/files/EC/C0/6B/DA/956A991047E93799BA2BA2A8/Orientacoes_para_implementacao_de_politica_de_BYOD.pdf

f. Estabelecer política de acesso remoto aos ativos críticos da organização, que defina minimamente:

I. Regras e procedimentos específicos para trabalho remoto.

II. Regras e procedimentos específicos para viagens a trabalho.

III. Critérios para adoção de ferramenta de rede privada virtual (VPN – Virtual Private Network), quando aplicável.

g. Estabelecer política de acesso a espaços físicos da organização, que defina minimamente:

I. Regras e procedimentos para adequada manutenção de credenciais físicas de liberação de acesso (crachás), quando aplicável.

II. Critérios de restrição de acesso a áreas sensíveis de espaços físicos.

h. Estabelecer regras e procedimentos de controle de acesso a ativos (sistemas, redes, dados, processos e serviços) de uso restrito a equipes de colaboradores específicos, quando aplicável.

I. Estabelecer regras e procedimentos para gestão de questões de segurança e controles de acesso nas instalações de contingência, físicas ou em nuvem, e adotar configurações seguras para serviços de contingência em nuvem.

2.2. Implementar ações que assegurem equipamentos, sistemas e aplicações (softwares) da organização, inclusive em produção, considerando, quando aplicável:

a. Garantir que os recursos sejam configurados adotando os padrões que conferem maior segurança.

b. Realizar testes em ambientes de homologação.

c. Realizar provas de conceito prévias de ativos em produção.

d. Adotar procedimentos para remoção de vulnerabilidades e implementação de medidas de proteção adicionais (hardening) aos sistemas.

e. Criar logs e trilhas de auditoria sempre que os sistemas permitam.

f. Abranger questões de segurança já durante as fases de pré-projeto e desenvolvimento de novos sistemas, softwares ou aplicações, considerando:

I. Abordar a adoção de práticas DevOps e implementação de programa DevSecOps.

II. Abordar a adoção de modelagem de ameaças, como Sast (Teste Estático de Segurança de Aplicativos) e Dast (Teste Dinâmico de Segurança de Aplicações), análise de composição de softwares, testes manuais, treinamentos etc.

III. Implementar as **Orientações Anbima para o desenvolvimento seguro de aplicações (softwares)**[7].

g. Implementar segurança de borda, nas redes de computadores, por meio de firewalls e outros mecanismos de filtros de pacotes.

h. Implementar recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais.

i. Impedir a instalação e execução de software e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de allowlist).

j. Abordar a realização de análises internas de malware.

k. Abordar o rastreio e a correção de protocolos e algoritmos obsoletos ou inseguros.

2.3. Implementar ações de tratamento, armazenamento, transporte e descarte seguro de dados e informações, considerando:

a. Implementar serviço de cópia de segurança (backup), preferencialmente apartado da rede interna, dos diversos ativos da organização.

b. Implementar segregação de serviços sempre que possível, restringindo o tráfego de dados apenas entre os equipamentos relevantes.

c. Definir critérios para adoção de modelo que considera a privacidade dos dados desde o início do desenvolvimento de um sistema, produto ou serviço (Privacy By Design).

[7] **Anbima. Orientações para o desenvolvimento seguro de aplicações (softwares) (2025). Disponível em:** https://www.anbima.com.br/data/files/A3/36/31/78/7563A910C35D53A9BA2BA2A8/Orientacoes_Desenvolvimento_Seguro_de_Aplicacoes.pdf.

d. Abordar a criptografia em nível de mensagem e exigir que as transmissões externas de e-mail sejam criptografadas.

e. Utilizar de recursos de DRM (Gerenciamento de Direitos Digitais).

2.4. Realizar diligência na contratação de serviços de terceiros, inclusive serviços em nuvem, considerando:

a. Avaliar a adequação a legislações e regulações vigentes.

b. Adotar cláusulas de confidencialidade e exigência de controles de segurança na própria estrutura dos terceiros.

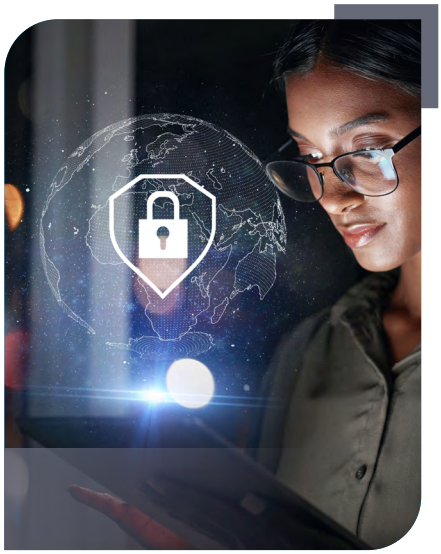
c. Adotar o **questionário Anbima de due diligence para contratação de terceiros e serviços em nuvem**[8], bem como as **Orientações Anbima para contratação de terceiros e nuvem**[9].

d. Abordar ações e procedimentos de segurança a serem adotados no momento da migração de dados para a nuvem, evitando a exportação de vulnerabilidades prévias.

e. Abordar a utilização de corretores de acesso à nuvem para impor políticas de segurança, requisitos de conformidade e proteção contra ameaças.

f. Abordar a realização de processo de sanitização de dados para repositórios de dados de computação em nuvem, de verificações regulares de vulnerabilidades em IaaS (Infraestrutura como Serviço), PaaS (Platforma como Serviço), SaaS (Software como Serviço) e de testes de penetração regulares.

g. Abordar a criptografia dos dados mantidos por provedor de serviços de armazenamento (SSP – Storage Service Provider), quando contratados.



[8] **Anbima. Questionário Anbima de due diligence para contratação de terceiros e serviços em nuvem (2024). Disponível em:** https://www.anbima.com.br/data/files/D7/43/BD/84/6AE569104D404569B82BA2A8/2024.05.13%20QDD%20Contratacao%20de%20Terceiros%20e%20Nuvem.docx.

[9] **Anbima. Orientações para contratação de terceiros e nuvem (2022).** https://www.anbima.com.br/data/files/85/60/2A/F9/3B8C4810272519486B2BA2A8/Guia%20para%20Contratacao%20de%20Terceiros%20e%20Nuvem.pdf.

3. CONTROLE, MONITORAMENTO E TESTES

Recomenda-se que a organização busque estabelecer mecanismos e sistemas de monitoramento para cada um dos controles existentes.

Recomendações

3.1 Recomenda-se que a organização busque estabelecer mecanismos e sistemas de monitoramento para cada um dos controles existentes.

- **a.** Definir critérios para a adoção de controles mais rígidos conforme o nível de risco.
- **b.** Estabelecer procedimentos que atendam às características e necessidades da organização.

3.2. Manter inventários atualizados de hardware e software, verificando-os com frequência para identificar elementos estranhos à organização, por exemplo, computadores não autorizados ou software não licenciado (destacadamente para o caso de adoção de trabalho remoto por período prolongado).

3.3. Manter os sistemas operacionais e softwares sempre atualizados, garantindo que atualizações sejam instaladas assim que disponibilizadas pelos fornecedores, mesmo para o contexto de trabalho remoto ou de adoção de política de BYOD.

3.4. Monitorar diariamente as rotinas de backup, executando testes regulares de restauração dos dados.

3.5. Estruturar rotina de simulação e testagem que permita avaliar a eficácia do programa de segurança cibernética da organização, identificar oportunidade de desenvolvimento e respostas apropriadas a incidentes e aumentar a conscientização sobre riscos, considerando, de forma não exaustiva:

- **a.** Realizar exercício de simulação do tipo tabletop, que envolve a discussão de um cenário de crise ou incidente para planejamento colaborativo da resposta.
- **b.** Realizar teste de intrusão (Pentest), que simula ataques reais a sistemas, redes e aplicações para identificar e explorar vulnerabilidades.
- **c.** Realizar teste de phishing, que simula este tipo de ataque através de comunicações falsas, porém realistas, com o objetivo de aumentar a conscientização sobre ameaças e avaliar a prontidão da organização em identificá-las e reportá-las.
- **d.** Realizar teste do plano de resposta a incidentes, que simula os cenários especificados durante sua criação e a eficácia das estratégias de contingência.

3.6. Realizar análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.

3.7. Realizar a gestão de eventos de segurança da informação, analisando regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, internos ou externos, e considerando:

- **a.** Adotar ferramentas de centralização e correção de logs, por exemplo Siem (Gerenciamento de Informações e Eventos de Segurança).
- **b.** Adotar ferramentas para aprimoramento do Siem, tais como Ueba (Análise de Comportamento de Usuários e Entidades) e Soar (Orquestração, Automação e Resposta de Segurança).

3.8. Adotar a prática de compartilhamento de informações sobre incidentes de segurança da informação e cibernética através de plataformas especializadas (por exemplo, Misp, FS-Isac, entre outras), considerando:

- **a.** Implementar as **Orientações Anbima para compartilhamento de informações de incidentes cibernéticos**[10].

[10] **Anbima. Orientações para compartilhamento de informações de incidentes cibernéticos (2022). Disponível em:** https://www.anbima.com.br/data/files/82/F7/69/66/351B281016078A28882BA2A8/Ebook_Orientacoes_para_Compartilhamento_de_Informacoes_de_Incidentes_Ciberneticos.pdf.

4. PLANO DE RESPOSTA

Recomendações

4.1. Definir e desenvolver estratégia de contingência de cibersegurança que inclua plano de resposta, considerando:

a. Observar o disposto na seção IV e o inciso IV do art. 13 das **Regras e procedimentos de deveres básicos** da Anbima[11].

b. Implementar as recomendações do **Orientações Anbima para cibersegurança na gestão de continuidade de negócios**[12].

[11] **Anbima. Orientações para compartilhamento de informações de incidentes cibernéticos (2022). Disponível em:** https://www.anbima.com.br/data/files/82/F7/69/66/351B281016078A28882BA2A8/Ebook_Orientacoes_para_Compartilhamento_de_Informacoes_de_Incidentes_Ciberneticos.pdf.

[12] **Anbima. Regras e procedimentos de deveres básicos (2025). Disponível em:** https://www.anbima.com.br/data/files/61/B3/06/B3/EBEA591036202959B82BA2A8/6.%20Regras%20e%20Procedimentos%20de%20Deveres%20Basicos_v_25_02_2025.pdf.

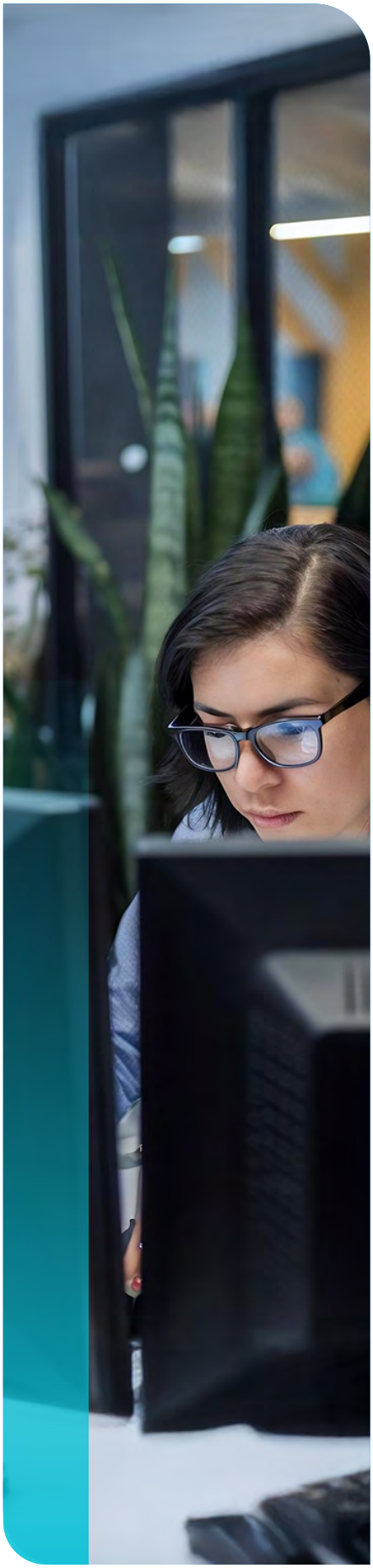
4.2. Implementar e realizar a gestão de plano de resposta, considerando minimamente:

a. Abordar os riscos identificados na etapa de identificação e avaliação de riscos, descrevendo vulnerabilidades a ameaças, suscetibilidade probabilística a incidentes de segurança cibernética e potenciais impactos negativos previstos na ocorrência desses incidentes.

b. Definir e descrever as táticas e medidas de contingência específicas e adequadas para as diferentes ameaças e vulnerabilidades e para cada equipamento, sistema, rede, dado, processo, serviço ou atividade (ou conjuntos deles, quando aplicável) identificados e avaliados como críticos, considerando também suas dependências e redundâncias.

c. Definir critérios e processos de ativação para colocar em prática as estratégias de contingência de cibersegurança, indicando responsáveis por cada etapa e fornecendo alternativas para processar os dados em tempo hábil (considerando a possibilidade de automatização) e para assegurar as operações de TI (Tecnologia da Informação), essencial para a resposta ao incidente cibernético.

d. Constituir comitês multidisciplinares de gerenciamento de crise (compostos, por exemplo, de representantes das áreas de TI, SI (Segurança da Informação), Compliance, Assessoria de Comunicação, Riscos, Sucesso do Cliente, Relações Institucionais, Jurídico etc.) para deliberar sobre as ações a serem tomadas, diretamente pela organização e/ou por eventuais fornecedores terceiros contratados, durante e após o enfrentamento ao incidente de cibersegurança, considerando os diferentes impactos que esse tipo de evento pode gerar ao negócio.



e. Garantir a eliminação da infecção ou neutralização da ameaça, prevenir-se de eventuais novos ataques, proteger as evidências do incidente e adotar as medidas cabíveis com relação à privacidade e proteção de dados e de comunicação do incidente às autoridades e autarquias competentes.

f. Analisar, arquivar, documentar informações e considerar elaborar relatórios sobre incidentes de segurança e o funcionamento do plano de resposta, a fim de servir como evidência em eventuais auditorias e contribuir para a prevenção de reincidências.

g. Revisar e atualizar o plano de continuidade de negócios com relação às estratégias de contingência de cibersegurança anualmente ou sempre que ocorrerem mudanças significativas que possam alterar as condições de segurança da organização.

4.3. Realizar exercícios e testes periódicos levando em consideração a comunicação interna (com os colaboradores) e externa (terceiros contratados, mídias, autoridades, público em geral), bem como treinar e capacitar adequadamente as equipes para essas situações.

5. GOVERNANÇA

Recomendações

5.1. Implementar governança adequada para estruturação e gestão do programa de segurança cibernética da organização, considerando:

a. Revisar e atualizar o programa de segurança cibernética periodicamente (em período inferior a um ano), mantendo sempre atualizadas suas avaliações de risco, implementações de proteção, planos de resposta a incidentes e monitoramento dos ambientes.

b. Criar política, controles internos ou procedimentos de uso adequado da estrutura tecnológica da organização, de forma independente ou como parte de um documento mais abrangente.

c. Criar política, controles internos ou procedimentos de uso adequado, de forma independente ou como parte de um documento mais abrangente, de tecnologias emergentes e/ou específicas, tais como e não exaustivamente:

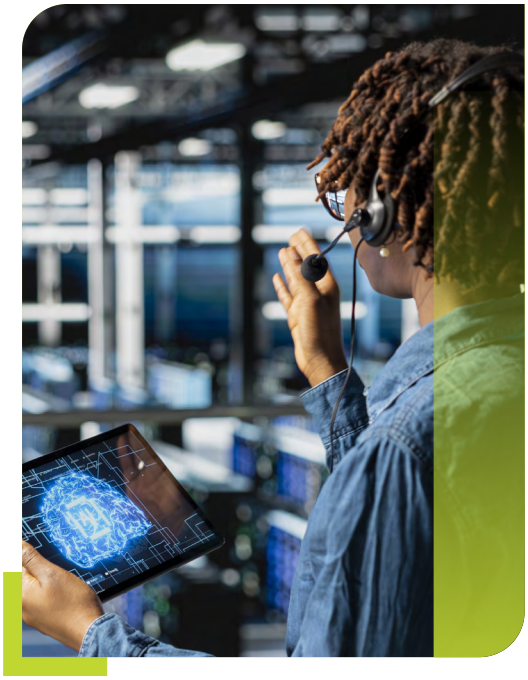
I. IA (Inteligência Artificial) e modelos de linguagem de grande escala (LLM – Large Language Model), considerando, conforme aplicável, as recomendações do Guia orientativo Anbima de boas práticas para o uso de sistemas de inteligência artificial nos mercados financeiro e de capitais[13].

II. Internet das Coisas (IoT – Internet of Things).

III. Recursos de Finanças Descentralizadas (DeFi – Decentralized Finance).

IV. Plataformas de desenvolvimento de software (por exemplo, low-code/no-code).

V. Plataformas de compartilhamento de informações (tais como, Isac – Information Sharing and Analysis Center e Misp – Malware Information Sharing Platform).



d. Estruturar governança específica para terceiros, abrangendo parceiros, fornecedores e prestadores de serviço contratados, conforme aplicável.

5.2. Estruturar governança adequada para administração e operação do programa de segurança cibernética, considerando:

a. Nomear pessoa integralmente dedicada, capaz de deliberar em nome da organização e de assumir responsabilidades legais, encarregada de liderar as equipes diretamente

[13] **Anbima. Guia orientativo: boas práticas para o uso de sistemas de inteligência artificial nos mercados financeiro e de capitais (2024). Disponível em:** https://www.anbima.com.br/data/files/63/74/15/39/F12C091039E04909EA2BA2A8/Guia_orientativo_boas_praticas_para_o_uso_de_sistemas_de_inteligencia_artificial.pdf.

responsáveis pela segurança cibernética, por exemplo, uma pessoa diretora de segurança da informação (CISO – Chief Information Security Officer).

b. Estruturar equipe diretamente responsável pela segurança cibernética, adotando, quando aplicável:

I. Escala contínua de trabalho (24×7);

II. Critérios para exigência de qualificação profissional que considerem experiências acadêmicas e profissionais, bem como certificações, tais como os seguintes exemplos não exaustivos: CISSP, CISM, CISA, CCSP/CCSK, CEH.

III. Acordos de Nível de Serviço (SLAs – Service Level Agreements) adequados para operações de segurança, prevendo ações para evitar e tratar a superação dos prazos estabelecidos e buscando equilibrá-los com as operações de negócio.

c. Criar um comitê, fórum ou grupo específico multidisciplinar para tratar de segurança cibernética dentro da organização.

d. Definir e realizar a gestão de Indicadores de Desempenho Chave (KPIs – Key Performance Indicators) que sejam utilizados em relatórios periódicos para apresentação aos conselhos de administração da organização e/ou demais órgãos consultivos e deliberativos.

5.3. Realizar ações de conscientização e estruturar programa de treinamento de colaboradores, incluindo terceiros, conforme aplicável, considerando:

a. Adotar programa de treinamento periódico adequado voltado a todos os colaboradores da organização, incluindo terceiros, conforme aplicável, sobre segurança cibernética, que seja capaz de:

I. Promover conscientização e disseminar conhecimentos importantes relacionados à segurança cibernética.

II. Desenvolver competências e habilidades para identificar e reportar ameaças cibernéticas ou situações suspeitas e para classificar as informações.

III. Estimular o engajamento dos colaboradores e garantir que todos assinem termos associados a políticas, regras e procedimentos de segurança cibernética adotados pela organização, conforme aplicável.

IV. Contribuir para a mitigação dos riscos identificados e a melhoria da segurança da organização.

b. Considerar definir planos de treinamento específicos para:

I. Colaboradores recém-contratados.

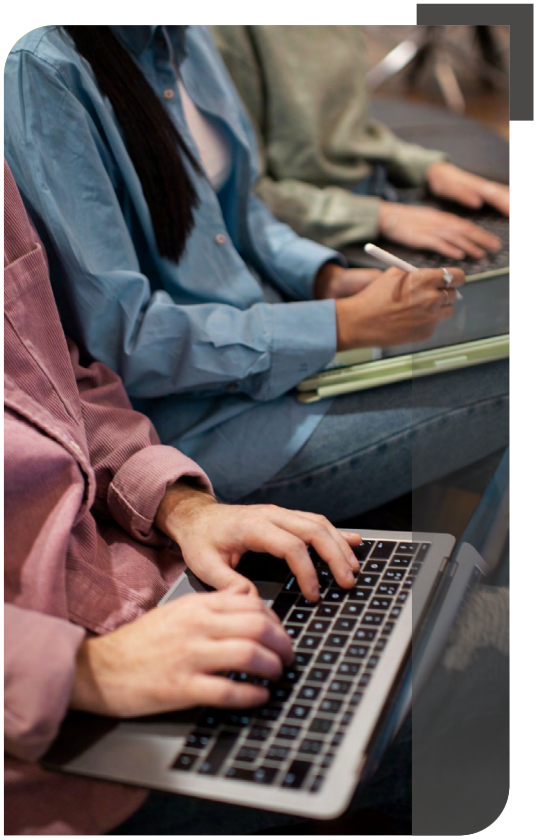
II. Colaboradores que trabalham remotamente.

III. Colaboradores que foram vítimas de incidente cibernético.

IV. Colaboradores com desempenho insuficiente em testes de cibersegurança.

V. Colaboradores que atuam em áreas sensíveis.

VI. Terceiros, abrangendo colaboradores de parceiros, fornecedores e prestadores de serviço contratados, conforme aplicável.



c. Promover e disseminar a cultura de segurança cibernética, considerando criar canais de comunicação internos que sejam eficientes para divulgar o programa de segurança cibernética, assim como conscientizar sobre os riscos e as práticas de segurança e informar sobre novas orientações.

d. Avaliar a implementação das Orientações para treinamento de colaboradores em cibersegurança[14].

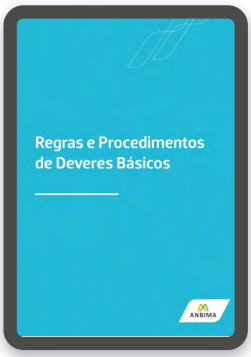
5.4. Avaliar a possibilidade de contratação de seguros de segurança cibernética.

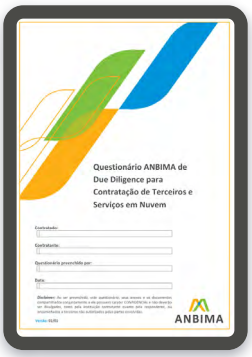
[14] **Anbima. Orientações para treinamento de colaboradores em cibersegurança (2024). Disponível em:** https://www.anbima.com.br/data/files/67/25/31/3D/483B49100054FA49B82BA2A8/Orientacoes_treinamento_de_colaboradores_em_ciber.pdf.

BASE DO **CONHECIMENTO**

#ESPAÇOCIBER

AUTORREGULAÇÃO





ORIENTAÇÕES TÉCNICAS

PESQUISAS E ESTUDOS

Para se aprofundar nos tópicos relacionados à segurança da informação e cibernética, acesse o QR Code ao lado e consulte nossa página especial.

#ESPAÇOCIBER

1. ANBIMA

1. Anbima. **#ESPAÇOCIBER. Disponível em:** https://www.anbima.com.br/pt_br/especial/cibersegurança.htm.

2. Anbima. **Grupo Consultivo de Cibersegurança.** https://www.anbima.com.br/pt_br/representar/grupos-consultivos-para-temas-emergentes/cibersegurança/cibersegurança.htm.

3. Anbima. **Regras e procedimentos de deveres básicos: Capítulo II – Regras Estruturais, Seção VI – Segurança Cibernética (2025). Disponível em:** https://www.anbima.com.br/data/files/61/B3/06/B3/EBEA591036202959B82BA2A8/6.%20Regras%20e%20Procedimentos%20de%20Deveres%20Basicos_v_25_02_2025.pdf.

4. Anbima. **Questionário Anbima de due diligence para contratação de terceiros e serviços em nuvem (2024). Disponível em:** https://www.anbima.com.br/data/files/D7/43/BD/84/6AE569104D404569B82BA2A8/2024.05.13%20QDD%20Contratacao%20de%20Terceiros%20e%20Nuvem.docx.

5. Anbima. **Orientações para contratação de terceiros e nuvem (2022). Disponível em:** https://www.anbima.com.br/data/files/85/60/2A/F9/3B8C4810272519486B2BA2A8/Guia%20para%20Contratacao%20de%20Terceiros%20e%20Nuvem.pdf.

6. Anbima. **Orientações para compartilhamento de informações de incidentes cibernéticos** (2022). Disponível em: https://www.anbima.com.br/data/files/82/F7/69/66/351B281016078A28882BA2A8/Ebook_Orientacoes_para_Compartilhamento_de_Informacoes_de_Incidentes_Ciberneticos.pdf.

7. Anbima. **Orientações para o treinamento de colaboradores em cibersegurança** (2024). Disponível em: https://www.anbima.com.br/data/files/67/25/31/3D/483B49100054FA49B82BA2A8/Orientacoes_treinamento_de_colaboradores_em_ciber.pdf.

8. Anbima. **Orientações para cibersegurança na gestão de continuidade de negócios** (2024). Disponível em: https://www.anbima.com.br/data/files/03/74/D7/D3/

A94749107AF1F649EA2BA2A8/Orientacoes_ciberseguranca_na_continuidade_de_negocios.pdf.

9. Anbima. **Orientações de cibersegurança para implementação de política de BYOD** (2025). Disponível em: https://www.anbima.com.br/data/files/EC/C0/6B/DA/956A991047E93799BA2BA2A8/Orientacoes_para_implementacao_de_politica_de_BYOD.pdf.

10. Anbima. **Orientações para o desenvolvimento seguro de aplicações** (softwares) (2025). Disponível em: https://www.anbima.com.br/data/files/A3/36/31/78/7563A910C35D53A9BA2BA2A8/Orientacoes_Desenvolvimento_Seguro_de_Aplicacoes.pdf.

11. Anbima. **Checklist de desenvolvimento seguro de aplicações** (softwares) (2025). Disponível em: https://www.anbima.com.br/data/files/42/E3/C8/18/D103A910C8D0A1A9BA2BA2A8/Checklist_de_Desenvolvimento_Seguro_de_Aplicacoes.xlsx.

12. Anbima. **Modelo de política de desenvolvimento seguro de aplicações (softwares)** (2025). Disponível em: https://www.anbima.com.br/data/files/CA/C6/14/E6/8103A910C8D0A1A9BA2BA2A8/Politica_Modelo_Desenvolvimento_Seguro_de_Aplicacoes.pdf.

13. Anbima. **Guia orientativo: boas práticas para o uso de sistemas de inteligência artificial nos mercados financeiro e de capitais** (2024). Disponível em: https://www.anbima.com.br/data/files/63/74/15/39/F12C091039E04909EA2BA2A8/Guia_orientativo_boas_praticas_para_o_uso_de_sistemas_de_inteligencia_artificial.pdf.

14. Anbima. **Governança de IA: integrando boas práticas ao longo do ciclo de vida da inteligência artificial** (2025). Disponível em: https://www.anbima.com.br/data/files/D0/42/D1/7F/35EC991040E49C99BA2BA2A8/guia_ia_boas_praticas_ciclo_vida.pdf.

2. LEGISLAÇÃO E REGULAÇÃO

15. BRASIL. ANPD – Autoridade Nacional de Proteção de Dados. **Resolução CD/ANPD 2/22**. Regulamento de aplicação da LGPD para agentes de tratamento de pequeno porte. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/institucional/atos-normativos/regulamentacoes_anpd/resolucao-cd-anpd-no-2-de-27-de-janeiro-de-2022.

16. BRASIL. ANPD. **Resolução CD/ANPD 15/24**. Regulamento de comunicação de incidente de segurança da informação. Disponível em: https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024.

17. BRASIL. BC – Banco Central do Brasil. **Resolução BC 498/25**. Procedimentos e condições para o credenciamento de PSTI (Provedor de Serviços de Tecnologia da Informação). Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20BCB&numero=498.

18. BRASIL. CMN – Conselho Monetário Nacional. **Resolução CMN 4.893/21. Política de segurança cibernética**. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893.

19. BRASIL. CVM – Comissão de Valores Mobiliários. **Resolução CVM 35/21: Capítulo XII – Segurança da Informação, Seção III – Segurança Cibernética**. Disponível em: https://conteudo.cvm.gov.br/export/sites/cvm/legislacao/resolucoes/anexos/001/resol035consolid.pdf.

20. BRASIL. **Decreto 11.856/23**. Institui a PNCiber (Política Nacional de Cibersegurança) e o CNCiber (Comitê Nacional de Cibersegurança). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm.

21. BRASIL. **Decreto 12.573/25**. Institui a Estratégia Nacional de Cibersegurança (E-Ciber). Disponível em: https://www.in.gov.br/en/web/dou/-/decreto-n-12.573-de-4-de-agosto-de-2025-646200784.

22. BRASIL. GSI – Gabinete de Segurança Institucional. **Portaria GSI/PR 148/25**. Diretriz de estímulo à criação e operação de Centros de Análise e Compartilhamento de Informações (ISACs – Information Sharing and Analysis Centers). Disponível em: https://www.in.gov.br/web/dou/-/portaria-gsi/pr-n-148-de-8-de-abril-de-2025-622872170.

23. BRASIL. **Lei 13.709/18. LGPD** (Lei Geral de Proteção de Dados Pessoais). Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm.

3. REFERÊNCIAS

BRASIL

24. BRASIL. ANPD. **Comunicação de incidente de segurança da informação.** Disponível em: https://www.gov.br/anpd/pt-br/canais_atendimento/agente-de-tratamento/comunicado-de-incidente-de-seguranca-cis.

25. BRASIL. **GSI**. Disponível em: https://www.gov.br/gsi/pt-br.

26. BRASIL. GSI. **Glossário de Segurança da Informação.** Disponível em: https://www.gov.br/gsi/pt-br/seguranca-da-informacao-e-cibernetica/glossario-de-seguranca-da-informacao-1.

27. BSM SUPERVISÃO DE MERCADOS. **CE BSM 04/24**. Norma de Supervisão sobre Segurança da Informação. Disponível em: https://www.bsmsupervisao.com.br/documents/1266368/1723432/04-2024-Norma-de-Supervisao-sobre-Seguranca-da-Informacao.pdf/5f769301-aa83-c813-41fe-6ad7e740bb1e?version=1.0&t=1725906925155&&objectDefinitionExternalReferenceCode=6983da10-9877-ce3d-046d-d31627e56f16&objectEntryExternalReferenceCode=e4437c98-8b26-d311-935e-a877f6e95a22.

28. B3 – Brasil, Bolsa, Balcão. **Política de Segurança da Informação** (2025). Disponível em: https://api.mziq.com/mzfilemanager/v2/d/5fd7b7d8-54a1-472d-8426-eb896ad8a3c4/e04d777f-1c9d-adb5-6c84-d0a4fa6cd25d?origin=1.

29. CERT – NIC.br. MISP – Malware Information Sharing Platform. **Plataforma de software livre para compartilhamento de dados de inteligência de ameaças**. Disponível em: https://cert.br/misp/.

30. CERT. Cartilha de Segurança para Internet – fascículos. Disponível em: https://cartilha.cert.br/fasciculos/.

31. FEBRABAN – Federação Brasileira de Bancos. **Guia de boas práticas de Segurança da Informação** (2024). Disponível em: https://portal.febraban.org.br/pagina/3360/52/pt-br/guiaboaspraticas-segurancainformacao.

MUNDO

32. AIMA – Alternative Investment Management Association. **Guide to sound practices for cybersecurity** (2022). Disponível, somente para membros, em: https://www.aima.org/sound-practices/guides-to-sound-practices/guide-to-sound-practices-for-cyber-security-2022.html.

33. AITEC; AIMA. **AITEC-AIMA vendor technology and cyber security DDQ** (2025). Disponível em: https://www.aima.org/event/webinar--aima---aitec-ddq-launch.html.

34. AMF – Autorité des Marchés Financiers. S**tock market cybercrime: definition, cases and perspectives** (2020). Disponível em: https://www.amf-france.org/sites/default/files/2020-02/study-stock-market-cybercrime-_-definition-cases-and-perspectives.pdf.

35. CFTC – Commodities and Futures Trading Commission. **Recommendations on DCO system safeguards standards for third party service providers** (2024). Disponível em: https://www.cftc.gov/media/11666/mrac121024_DCOThirdPartySystemSafeguards/download.

36. CIRO – Canadian Investment Regulatory Organization. **Cybersecurity & technology: guides and resources**. Disponível em: https://www.ciro.ca/firms/educational-resources/cybersecurity-technology/guides-and-resources.

37. CIS – Center for Internet Security. **CIS critical security controls** – v8.1 (2024). Disponível em: https://learn.cisecurity.org/cis-controls-download.

38. CISA – Cybersecurity & Infrastructure Security Agency. **CPGs (Cybersecurity Performance Goals)**. Disponível em: https://www.cisa.gov/cybersecurity-performance-goals-cpgs.

39. CISA. **Cybersecurity best practices**. Disponível em: https://www.cisa.gov/topics/cybersecurity-best-practices.

40. CISA. **#StopRansomware guide** (2020). Disponível em: https://www.cisa.gov/stopransomware/ransomware-guide.

41. CPMI – Committee on Payments and Market Infrastructures (BIS); IOSCO – International Organization of Securities Commissions. **Guidance on cyber resilience for financial market infrastructures** (2016). Disponível em: https://www.ecb.europa.eu/paym/pol/shared/pdf/CPMI_IOSCO_Guidance_on_cyber_resilience_for_FMIs.pdf.

42. CSA – Cyber Security Agency of Singapore. **Cybersecurity education and learning guidebook** (2024). Disponível em: https://www.csa.gov.sg/resources/publications/cybersecurity-education-and-learning-guidebook.

43. CSA. **Guidelines and companion guide on securing AI systems** (2024). Disponível em: https://www.csa.gov.sg/resources/publications/guidelines-and-companion-guide-on-securing-ai-systems.

44. 44. CSA. **Singapore's operational technology cybersecurity masterplan 2024** (2024). Disponível em: https://www.csa.gov.sg/resources/publications/singapore-s-operational-technology-cybersecurity-masterplan-2024.

45. DFS – **New York State Department of Financial Services. Cybersecurity regulation, 23 NYCRR Part 500** (2023). Disponível em: https://www.dfs.ny.gov/industry_guidance/regulations/final_adoptions_fs/rf_fs_2amend23NYCRR500_text_20231101_alt.

46. DFS. **Cybersecurity resource center**. Disponível em: https://www.dfs.ny.gov/industry_guidance/cybersecurity.

47. EBA – European Banking Authority. **Orientações sobre medidas de segurança para gerir os riscos operacionais e de segurança ao abrigo da Diretiva (UE)**

2015/2366 (PSD2) – Tradução em português (2018). Disponível em: https://www.eba.europa.eu/documents/10180/2081899/f2ef7577-439f-46e6-b64a-cf548e0a4a0d/Guidelines%20on%20the%20security%20measures%20under%20PSD2%20(EBA-GL-2017-17)_PT.pdf.

48. EIOPA – European Insurance and Occupational Pensions Authority. **Guidelines on information and communication technology security and governance** (2020). Disponível em: https://www.eiopa.europa.eu/system/files/2020-10/eiopa-bos-20-600-guidelines-ict-security-and-governance.pdf.

49. ENISA – European Union Agency for Cybersecurity. **ENISA threat landscape 2025** (2025). Disponível em: https://www.enisa.europa.eu/sites/default/files/2025-10/ENISA%20Threat%20Landscape%202025_0.pdf.

50. ESMA – European Securities and Markets Authority. G**uidelines on maintenance of systems and security access protocols under MiCA** (2025). Disponível em: https://www.esma.europa.eu/sites/default/files/2025-02/ESMA75-223375936-6132_Guidelines_on_maintenance_of_systems_and_security_access_protocols_under_MiCA.pdf.

51. ESRB – European Systemic Risk Board. **Systemic cyber risk** (2020). Disponível em: https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

52. EUROPEAN COMMISSION. NIS – Network and Information Systems. **Directive 2022/2555** (2022). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555.

53. EUROPEAN COMMISSION. **DORA – Regulation on digital operational resilience** (2022). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R2554.

54. EUROPEAN COMMISSION. **DORA – implementing and delegated acts**. Disponível em: https://finance.ec.europa.eu/regulation-and-supervision/financial-services-legislation/implementing-and-delegated-acts/digital-operational-resilience-regulation_en?etrans=fr&prefLang=fr.

55. FCA – Financial Conduct Authority. **Operational incident and third party reporting** (2024). Disponível em: https://www.fca.org.uk/publication/consultation/cp24-28.pdf.

56. FCA. **CTPS 4.5 Requirement 4: technology and cyber resilience** (2025). Disponível em: https://www.handbook.fca.org.uk/handbook/CTPS/4/5.pdf.

57. FCA. **Cyber security – industry insights** (2019). Disponível em: https://www.fca.org.uk/publication/research/cyber-security-industry-insights.pdf.

58. FED – Federal Reserve. **Sound practices to strengthen operational resilience** (2020). Disponível em: https://www.federalreserve.gov/supervisionreg/srletters/SR2024a1.pdf.

59. IMF –International Monetary Fund. **Strengthening cybersecurity: lessons from the cybersecurity survey** (2025). Disponível em: https://www.imf.org/-/media/Files/Publications/TNM/2025/English/TNMEA2025006.ashx.

60. FINRA – Financial Industry Regulatory Authority. **2025 FINRA annual regulatory oversight report** (2025). Cybersecurity and Cyber-Enabled Fraud. Disponível em: https://www.finra.org/sites/default/files/2025-01/2025-annual-regulatory-oversight-report.pdf.

61. FINRA. **Core cybersecurity threats and effective controls for small firms** (2024). Disponível em: https://www.finra.org/sites/default/files/2022-05/Core_Cybersecurity_Threats_and_Effective_Controls-Small_Firms.pdf.

62. FINRA. **Quantum computing and the implications for the securities industry** (2023). Section III: Potential Threats to Cybersecurity. Disponível em: https://www.finra.org/sites/default/files/2023-10/2023-quantum-computing-and-the-implications-for-the-securities-industry.pdf.

63. FINRA. **Key topics: cybersecurity**. Disponível em: https://www.finra.org/rules-guidance/key-topics/cybersecurity#overview.

64. FINRA. **Small firm cybersecurity checklist**. Disponível em: https://www.finra.org/sites/default/files/smallfirm_cybersecurity_checklist.xlsx.

65. FSB – Financial Stability Board. **Effective practices for cyber incident response and recovery** (2020). Disponível em: https://www.fsb.org/wp-content/uploads/P191020-1.pdf.

66. GFMA – Global Financial Markets Association. **Framework for the regulatory use of penetration testing in the financial services industry** (2020). Disponível em: https://www.gfma.org/wp-content/uploads/2020/12/gfma-penetration-testing-guidance-for-regulators-and-financial-firms-version-2-december-2020.pdf.

67. GFMA; EBF – European Banking Federation; ISDA – International Swaps and Derivatives Association. **International cybersecurity, data and technology principles** (2020). Disponível em: https://www.gfma.org/wp-content/uploads/0/83/197/211/13187d1e-077f-43c5-85a1-1da370608a2b.pdf.

68. IOSCO – International Organization of Securities Commissions. **Cyber security in securities markets – an international perspective** (2016). Disponível em: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf.

69. ISO – International Organization for Standardization. **ISO/IEC 27001** (2022). Sistemas de gerenciamento de segurança da informação. A norma integra a família ISO/IEC 27000 de gestão da segurança da informação. Disponível em: https://www.iso.org/standard/27001.

70. NCSC – National Cyber Security Centre. **Cyber essentials**. Disponível em: https://www.ncsc.gov.uk/cyberessentials/resources.

71. NCSC. **Annual review 2024**. Disponível em: https://www.ncsc.gov.uk/files/NCSC_Annual_Review_2024.pdf.

72. NIST – National Institute of Standards and Technology. **Cybersecurity framework 2.0 – Tradução em português** (2024). Disponível em: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.por.pdf.

73. NIST. **Developing cyber-resilient systems: a systems security engineering approach** (2021). Disponível em: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-160v2r1.pdf.

74. NFA – National Futures Association. **Information security programs** (2015). Disponível em: https://www.nfa.futures.org/rulebooksql/rules.aspx?RuleID=9070&Section=9.

75. NFA. **Introducing broker (IB) regulatory obligations: cybersecurity**. Disponível em: https://www.nfa.futures.org/members/ib/regulatory-obligations/cybersecurity.html.

76. OWASP – Open Web Application Security Project. **OWASP top ten** (2021). Disponível em: https://owasp.org/www-project-top-ten/.

77. OWASP. **Cyber defense framework**. Disponível em: https://owasp.org/www-project-cyber-defense-framework/.

78. SANS INSTITUTE. **SANS CISO Primer: 4** cyber trends that will move the needle in 2024

(2024). Disponível em: https://www.sans.org/white-papers/ciso-primer-4-cyber-trends-2024/.

79. SANS. **SANS 2024 ICS/OT Survey: the state of ICS/OT cybersecurity** (2024). Disponível em: https://sansorg.egnyte.com/dl/oq4USL3qoA.

80. SANS. **SANS 2024 top attacks and threats report** (2024). Disponível em: https://www.sans.org/white-papers/sans-2024-top-attacks-threats-report/.

81. SEC – Securities and Exchange Commission (US). **Observations from cybersecurity examination** (2017). Disponível em: https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.

82. SIFMA. **Insider threat best practices guide, 3rd Edition** (2024). Disponível em: https://www.sifma.org/wp-content/uploads/2025/03/2024-SIFMA-Insider-Threat-Best-Practices-Guide-FINAL.pdf.

83. SIFMA. **SIFMA data protection principles** (2021). Disponível em: https://www.sifma.org/wp-content/uploads/2017/11/SIFMA-Data-Protection-Principles-March-2021.pdf.

84. SIFMA. **Reconnection framework** (2023). Disponível em: https://www.sifma.org/wp-content/uploads/2024/04/SIFMA-Reconnection-Framework-for-Remediating-Cyber-Events-Nov2023.pdf.

85. WEF – **World Economic Forum. Global cybersecurity outlook** (2025). Disponível em: https://reports.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2025.pdf.

EXPEDIENTE

Guia de Cibersegurança
4ª edição | 2025

Superintendência de Representação de Mercados

Tatiana Itikawa

Gerência de Representação de Distribuição de Produtos de Investimentos

Luiz Henrique de Carvalho

Redação

Augusto Brisola

Divulgação

Paula Lepinski

Projeto Grafico

João Macedo

Presidência

Carlos André

Diretoria

Adriano Koelle, Andrés Kikuchi, Aquiles Mosca, Carlos Takahashi, César Mindof, Eduardo Azevedo, Eric Altafim, Fernanda Camargo, Fernando Rabello, Flavia Palacios, Giuliano De Marchi, Gustavo Pacheco, 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, Denise Ornellas, Fabio Nacajune, Frederico Neres, Hanna Ki, Ismar Marcos Leite, Joao Paulo Santos, Jorge Matsumoto, José Silva, Kenia Carvalho, Leonardo Alonso, Lilian Celeri, Mauricio Corrêa, Patrik Lemos, Rodrigo Fusco, Simone de Grandis e 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, 21° andar, Pinheiros

São Paulo, SP – CEP: 05425-070

Tel.: (11) 3471 4200

www.anbima.com.br