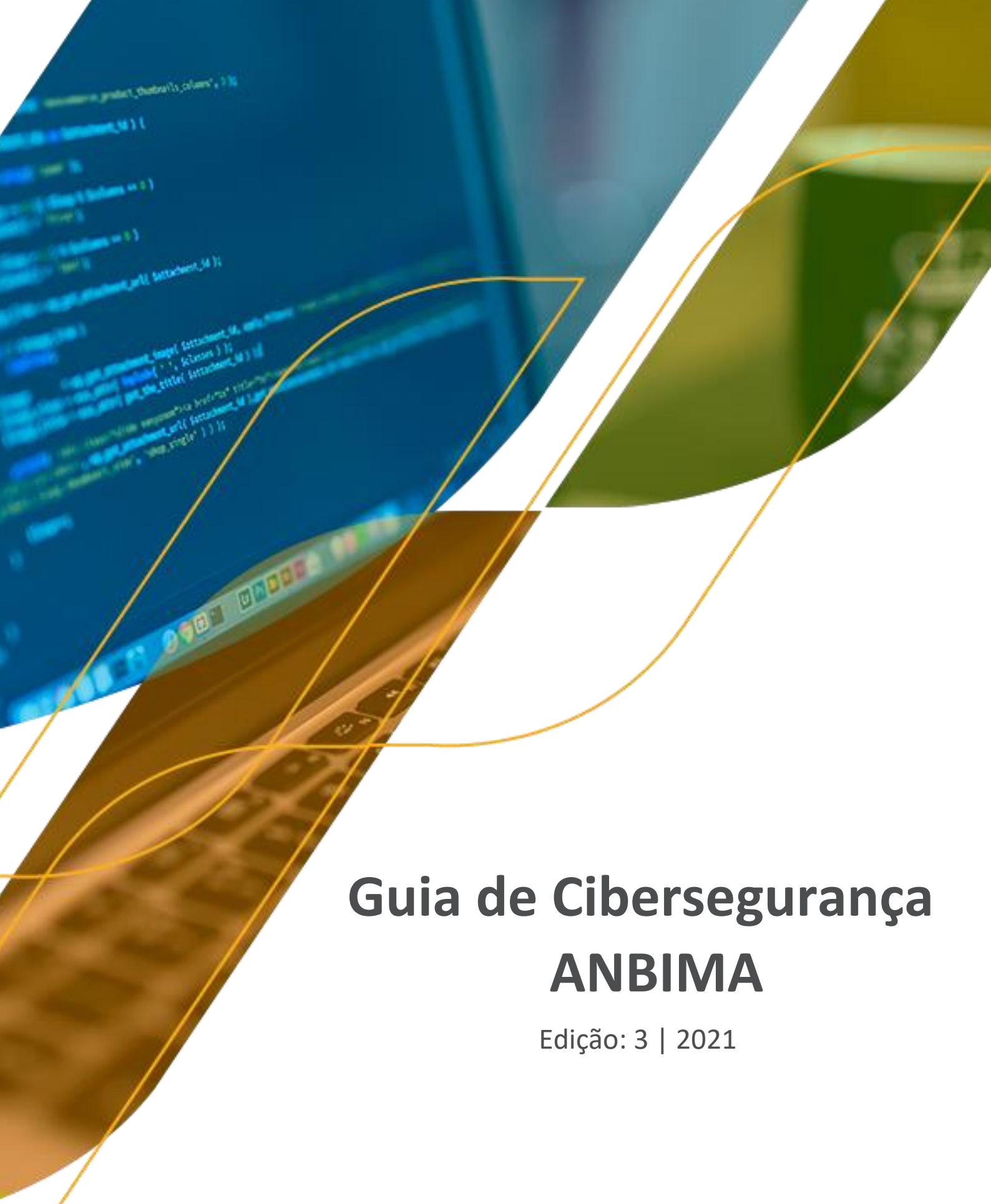


# Guia de Cibersegurança ANBIMA

Edição: 3 | 2021

ANBIMA

# Sumário

# Apresentação

Com o aumento exponencial das ameaças cibernéticas nos últimos anos, tanto em volume quanto em sofisticação, reguladores e autorreguladores têm voltado maior atenção para esse assunto com o objetivo de orientar as instituições em seus respectivos mercados e verificar se suas estruturas estão preparadas para identificar e mitigar riscos cibernéticos, assim como para se recuperar de possíveis incidentes.

Nesse sentido, a ANBIMA entende que é de extrema importância que as instituições estruturem um programa de segurança cibernética. Esse programa pode, a critério de cada instituição, ser incluído na política de segurança da informação, documento exigido por alguns dos Códigos de Regulação e Melhores Práticas da ANBIMA[1].

Para desenvolver um programa de segurança cibernética, as instituições podem basear-se em padrões nacionais ou internacionais existentes (ver referências). Esses padrões podem focar especificamente a cibersegurança ou tratar de modo mais abrangente a governança e o gerenciamento das tecnologias da informação dentro das instituições. Eles podem servir como pontos de referência e ajudar as instituições a avaliarem suas práticas e definirem elementos relevantes na construção e no desenvolvimento do seu programa.

Ao elaborar e implementar um programa de segurança cibernética, é fundamental levar em consideração que todas as pessoas ligadas à instituição fazem parte do processo de segurança dos ativos dela. Sob essa ótica, a preocupação com a segurança cibernética não é matéria exclusiva da área de Segurança da Informação ou áreas correlatas. Sendo assim, recomenda-se que, ao desenvolver um programa de segurança cibernética, deve-se considerar formas de envolvimento de todas as pessoas vinculadas à instituição, inclusive prestadores de serviços terceirizados relevantes. Esse engajamento pode ocorrer, por exemplo, em treinamentos periódicos que envolvam toda a hierarquia da instituição, além de campanhas periódicas de conscientização a respeito do tema.

Ainda como etapa inicial da elaboração de um programa de segurança cibernética, e à luz da Lei Geral de Proteção de Dados, deve-se considerar que a segurança cibernética é um dos componentes para que a privacidade do titular[2] seja assegurada por mecanismos de proteção de

[1] Código ANBIMA de Regulação e Melhores Práticas para o Mercado de FIP e FIEE; Código ANBIMA de Regulação e Melhores Práticas da ANBIMA de Fundos de Investimento; Código ANBIMA de Regulação e Melhores Práticas para a Atividade de Private Banking no Mercado Doméstico; e Código ANBIMA de Regulação e Melhores Práticas dos Serviços Qualificados ao Mercado de Capitais.

[2] Lei 13.709 (LGPD), art. 5º, V- Titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento.

dados. Dessa forma, destaca-se a importância do envolvimento de diversas áreas na elaboração e no tratamento do programa de segurança cibernético para que este contemple e enderece preocupações que perpassam as áreas de tecnologia.

Em 2016, de forma a auxiliar as instituições participantes dos Códigos de Regulação e Melhores Práticas, a ANBIMA lançou este guia, que descreve práticas efetivas para orientar a implantação de um programa de segurança cibernética e, com isso, contribuir para o aprimoramento da segurança cibernética nos mercados financeiro e de capitais do Brasil. Em 2017, a partir dos trabalhos desenvolvidos pelo Grupo Técnico de Cibersegurança ANBIMA, a primeira versão do documento foi reformulada e atualizada, levando à segunda edição do guia. Em 2020, a governança para tratar de segurança cibernética na ANBIMA foi reestruturada, e o Grupo Técnico deu lugar ao Grupo Consultivo[3] à Diretoria, responsável por propor e conduzir a agenda de segurança cibernética da Associação. A pandemia de COVID-19, que marcou o ano de 2020, trouxe aprendizados que foram incorporados nesta edição do guia, muito em função da maior incidência do trabalho remoto. Neste sentido, o guia passa a contar com recomendações relacionadas à avaliação de risco destacada para prestadores de serviços terceirizados, incluindo nuvem, recomendações a respeito de Bring Your Own Device (BYOD), além de novos aspectos relacionados ao Plano de Resposta a Incidente. É importante destacar que a nova edição do guia não traz exclusivamente assuntos referentes à pandemia; também atualiza o documento com evoluções das melhores práticas desde sua última atualização.

Como as práticas e soluções de cibersegurança evoluem rapidamente, exigindo constante adaptação das instituições, este guia será reavaliado e atualizado ou complementado por diretrizes e matérias adicionais ao longo do tempo.

- **O guia oferece exemplos e recomendações para orientar as instituições e contribuir para o aprimoramento da segurança cibernética nos mercados brasileiros.**
- **As práticas descritas neste guia não constituem uma lista única e exaustiva das iniciativas que as instituições podem tomar para reforçar a cibersegurança.**
- **Existem várias fontes e recursos disponíveis que podem também auxiliar as instituições à medida que progridem na implementação do programa de segurança cibernética.**
- **A implementação das recomendações depende das características e das necessidades de cada instituição.**

[3] Para mais informações, ver: http://www.anbima.com.br/pt_br/representar/grupos-detrabalho/ciberseguranca/ciberseguranca.htm.

# O risco cibernético

Por um lado, os avanços tecnológicos criam facilidades e possibilitam o uso de novas ferramentas para a atuação das instituições, permitindo agilidade na construção e disponibilização de serviços, ampliação dos meios de comunicação, entre outros. Por outro, o aumento do uso de tais ferramentas potencializa os riscos de ataques cibernéticos, ameaçando a confidencialidade, a integridade e a disponibilidade dos dados ou dos sistemas das instituições.

Existem diversas razões para que esses ataques sejam realizados por vários agentes (organizações criminosas ou hackers individuais, organismos de Estado, terroristas, colaboradores, competidores etc.). Os principais motivos identificados são:

- Obter ganho financeiro.
- Roubar, manipular ou adulterar informações.
- Obter vantagens competitivas e informações confidenciais de empresas concorrentes.
- Fraudar, sabotar ou expor a instituição invadida, podendo ter como motivo acessório a vingança.
- Promover ideias políticas e/ou sociais.
- Praticar o terror e disseminar pânico e caos.
- Enfrentar desafios e/ou ter adoração por hackers famosos.

Os invasores podem utilizar vários métodos para os ataques cibernéticos. Destacam-se os mais comuns[4]:

- Malware – softwares desenvolvidos para corromper computadores e redes:
  - vírus: software que causa danos a máquina, rede, softwares e banco de dados;
  - cavalo de Troia: aparece dentro de outro software e cria uma porta para a invasão do computador;
  - spyware: software malicioso para coletar e monitorar o uso de informações; e
  - ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja reestabelecido.[5]

[4] Ver SANS, *Glossary of Terms*, para definições dos termos mais usados. Disponível em: https://www.sans.org/security-resources/glossary-of-terms.

[5] Ver posicionamento do Departamento do Tesouro dos EUA nas referências.

- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:
  - pharming: direciona o usuário para um site fraudulento, sem o seu conhecimento;
  - phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável que envia comunicação eletrônica oficial para obter informações confidenciais;
  - vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais;
  - smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais; e
  - acesso pessoal: pessoas localizadas em lugares públicos como bares, cafés e restaurantes que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

- Ataques de DDoS (Distributed Denial of Services) e botnets – ataques visando negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos botnets, o ataque vem de um grande número de computadores infectados utilizados para criar e mandar spam ou vírus, ou inundar uma rede com mensagens resultando na negação de serviços.

- Invasões (advanced persistent threats) – ataques realizados por invasores sofisticados, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

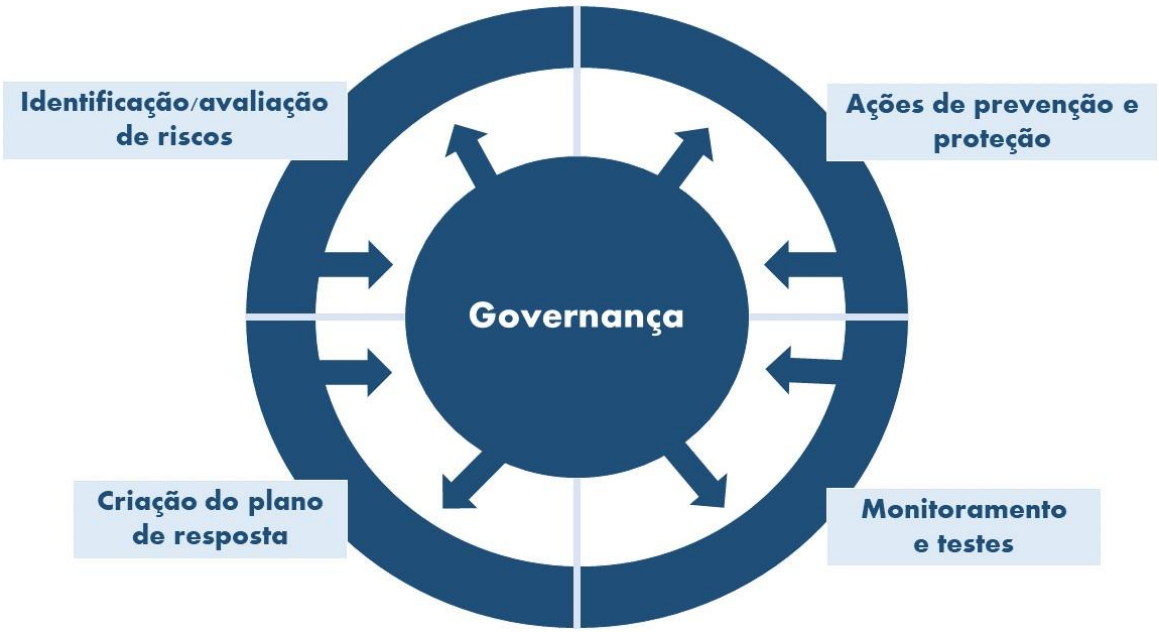
As ameaças cibernéticas podem variar de acordo com a natureza, a vulnerabilidade e as informações ou os bens de cada organização. As consequências para as instituições podem ser significativas em termos de risco de imagem, danos financeiros ou perda de vantagem concorrencial, além de riscos operacionais. Os possíveis impactos dependem ainda da rápida detecção e resposta após a identificação do ataque[4]. Tanto instituições grandes como pequenas podem ser impactadas.

- **Instituições financeiras não podem ignorar o risco cibernético.**
- **Ataques ameaçam a confidencialidade, a integridade ou a disponibilidade dos dados e dos sistemas das instituições.**
- **Reguladores estão focando na identificação de pontos fracos em segurança cibernética nos mercados de capital.**
- **Clientes e parceiros têm questionado cada vez mais a segurança das instituições.**

# Implementando um programa de segurança cibernética

A ANBIMA recomenda que um programa eficiente contra ameaças cibernéticas deve, no mínimo, conter cinco funções bem definidas:

1. **Identificação/avaliação de riscos (risk assessment)** – identificar os riscos internos e externos, os ativos de hardware, software e processos que precisam de proteção.
2. **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.
3. **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.
4. **Criação do plano de resposta** – ter um plano de resposta, tratamento e recuperação de incidentes, incluindo um plano de comunicação interna e externa, caso necessário.
5. **Governança** – manter o programa de segurança cibernética continuamente atualizado garantindo que ações, processos e indicadores sejam regularmente executados, retroalimentando a estratégia definida.




Veja o detalhamento das cinco funções, com recomendações consideradas fundamentais para a efetividade dos programas de cada uma das instituições, mas não se limitando a elas.

## 1 – Identificação/avaliação de riscos (risk assessment)

É recomendado que as instituições implementem um programa de segurança cibernética baseado em suas necessidades, elaborando e mantendo uma avaliação de riscos (ou risk assessment) atualizada. Os esforços devem ser compatíveis com as características e o tamanho da instituição, bem como os recursos de defesa e as respostas, proporcionais aos riscos identificados. A avaliação deve levar em conta o ambiente da instituição, seus objetivos, seus stakeholders e suas atividades.

**Recomendações:**

1. Durante a avaliação de risco inicial[6], devem-se identificar todos os ativos relevantes da instituição (sejam equipamentos, sejam sistemas, processos ou dados) usados para seu correto funcionamento.
2. Recomenda-se a criação de regras para a classificação das informações geradas pela instituição, permitindo com isso a implementação de processos para o devido manuseio, armazenamento, transporte e descarte dessas informações.
3. As vulnerabilidades dos ativos em questão devem ser avaliadas, identificando-se as possíveis ameaças e o grau de exposição dos ativos a elas. Vários cenários devem ser considerados nessa avaliação.[7]
4. Devem ser considerados os possíveis impactos financeiros, operacionais e reputacionais, em caso de evento de segurança, assim como a expectativa de tal evento ocorrer.
5. O processo de avaliação de riscos deve contemplar as atividades desenvolvidas por prestadores de serviços terceirizados, incluindo serviços de nuvem.
6. Uma vez definidos os riscos, ações de prevenção e proteção devem ser tomadas.
7. Existem várias metodologias para avaliação de risco cibernético, adequadas a diferentes instituições. Alguns exemplos estão indicados nas referências.

[6] Para melhor entendimento a respeito da elaboração de uma avaliação de risco inicial no contexto de segurança cibernética, ver, por exemplo: CSA, *Guide to conducting Cybersecurity risk assessment for critical information infrastructure* (dados completos disponíveis na seção de referências).

[7] Para melhor compreensão da probabilidade e do impacto de ocorrências, recomenda-se usar informações de ameaças cibernéticas de fonte interna e externa, como o framework estabelecido pelo NIST (e.g. ID.RA-3, disponível em: https://nvd.nist.gov/800-53/Rev4/control/RA-3, e ID.RA-5, disponível em: https://nvd.nist.gov/800-53/rev4/control/ra-5).

## 2 – Ações de prevenção e proteção

**Recomendações:**

1. Controlar o acesso adequado aos ativos das instituições. A implementação desses controles passa pela identificação, autenticação e autorização dos usuários, ou sistemas, aos ativos das instituições.
2. Estabelecer regras mínimas na definição de acesso a dispositivos corporativos, definindo senhas com alta complexidade.
3. Disponibilizar autenticação de múltiplos fatores, sempre que possível.
4. Evitar o reaproveitamento de senhas. É atualmente mais recomendado o uso de um gerenciador de senhas do que a repetição da mesma senha, por mais sofisticada que seja, para facilitar a memorização em vários serviços.
5. Limitar o acesso, uma vez concedido, a apenas recursos relevantes para o desempenho das atividades. A concessão de acesso deve ser implementada de forma a ser revogada rapidamente quando necessário.
6. Os eventos de *login* e alteração de senhas devem ser auditáveis e rastreáveis.
7. É importante notar que os ativos das instituições podem estar localizados interna ou externamente ao ambiente da instituição, muitas vezes em nuvem. Um controle adequado deve prever acessos locais ou remotos a ativos também locais ou remotos e prever a possibilidade de uso de dispositivos pessoais nesses casos (*Bring Your Own Device* - BYOD).[8]
8. Recomenda-se que o acesso remoto seja realizado por meio de ferramenta que contenha criptografia e múltiplos fatores de autenticação.
9. Ao incluir novos equipamentos e sistemas em produção, garantir que sejam feitas configurações seguras de seus recursos. É altamente recomendável o teste em ambientes de homologação e de prova de conceito antes do envio à produção. Apenas como referência, o chamado "hardening" pode ser aplicado a sistemas operacionais, aplicativos, na restrição de serviços disponíveis em rede e na criptografia de dados em trânsito, assim como na configuração das estruturas de nuvem, entre outros.
10. Restringir o acesso físico às áreas com informações críticas/sensíveis.
11. Implementar serviço de backup dos diversos ativos da instituição. Recomenda-se que o serviço de backup esteja apartado da rede da instituição.

[8] Para mais informações sobre configurações seguras em casos de BYOD, consulte as referências. Ver, por exemplo: NCSC, *Guidance for organisations on enabling staff to use their own smartphones, tablets, laptops and desktop PCs to access work information* (dados completos disponíveis na seção de referências).

12. Criar logs e trilhas de auditoria sempre que os sistemas permitam.
13. Realizar diligência na contratação de serviços de terceiros, inclusive serviços em nuvem. Adequação a questões jurídicas devem ser avaliadas. Cláusulas de confidencialidade e exigência de controles de segurança na própria estrutura dos terceiros são desejáveis. Para proposição de modelo de diligência com terceiros, consulte as referências.
14. Considerar questões de segurança já durante as fases de pré-projeto e desenvolvimento de novos sistemas, softwares ou aplicações.
15. Implementar segurança de borda, nas redes de computadores, por meio de firewalls e outros mecanismos de filtros de pacotes.
16. Implementar recursos anti-malware em estações e servidores de rede, como antivírus e firewalls pessoais.
17. Implementar segregação de serviços sempre que possível, restringindo o tráfego de dados apenas entre os equipamentos relevantes.
18. Impedir a instalação e execução de software e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de whitelisting).
19. Estabelecer controles para mitigação de riscos e garantir a responsabilidade sobre os eventuais riscos se as instituições optarem por permitir o uso de dispositivos BYOD para acessar seus sistemas e informações.
20. Ter política de controle sobre os dados da instituição nos dispositivos BYOD, garantindo seu acionamento no processo de desligamento de funcionários.

## 3 – Monitoramento e testes

Em geral, recomenda-se que a instituição busque estabelecer mecanismos e sistemas de monitoramento para cada um dos controles existentes.

**Recomendações:**

1. Como regra geral, devem-se criar mecanismos de monitoramento de todas as ações de proteção implementadas para garantir seu bom funcionamento e efetividade.
2. Deve-se manter inventários atualizados de hardware e software, bem como verificá-los com frequência para identificar elementos estranhos à instituição, inclusive em momento de acesso e/ou trabalho remoto prolongado. Por exemplo, computadores não autorizados ou software não licenciado.

3. Devem-se manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas. Essa recomendação deve valer também para o ambiente de trabalho remoto, incluindo em casos de BYOD.
4. Deve-se monitorar diariamente as rotinas de backup, executando testes regulares de restauração dos dados.
5. Deve-se realizar, periodicamente, testes de invasão externa e phishing.
6. Deve-se realizar análises de vulnerabilidades na estrutura tecnológica, periodicamente ou sempre que houver mudança significativa em tal estrutura.
7. Sugere-se, periodicamente, testar o plano de resposta a incidentes, simulando os cenários especificados durante sua criação.
8. Deve-se analisar regularmente os logs e as trilhas de auditoria criados, de forma a permitir a rápida identificação de ataques, sejam internos[9], sejam externos. O uso de ferramentas de centralização e correlação de logs é especialmente recomendado (e.g. Security Information and Event Management, SIEM).
9. Recomenda-se o compartilhamento de dados de ataque por meio de ferramentas ou organizações, como o MISP, FS-ISAC, entre outros[10]. O compartilhamento de incidentes de ataque em plataformas especializadas tem o potencial de beneficiar a indústria em geral, ao possibilitar que as instituições avaliem antecipadamente e respondam aos ataques atuais.
10. O monitoramento dos controles de segurança deve ser implementado adotando uma abordagem baseada em risco e intensificado de acordo com o nível de risco, levando em consideração o contexto no qual a instituição está inserida e as necessidades emergentes.

## 4 – Criação de plano de resposta

**Recomendações:**

1. Recomenda-se o envolvimento de múltiplas áreas da instituição na elaboração do plano formal e no tratamento de incidentes, incluindo a alta gestão. Além da área de segurança tecnológica e de riscos, pois trata-se de risco operacional, devem ser incluídos departamentos como

[9] Para boas práticas na prevenção e no monitoramento dos ataques internos, ver, por exemplo: SIFMA, *Best Practices for Insider Threats* (dados completos disponíveis na seção de referências).

[10] A menção às ferramentas especificadas ocorre meramente com caráter exemplificativo e não representa uma avaliação prévia da Associação. É de responsabilidade de cada instituição realizar avaliação própria para utilização de qualquer ferramenta de compartilhamento de informação de incidentes cibernéticos.

Jurídico, de Compliance e de Comunicação. Para melhor tratamento de resposta, os eventos e incidentes já incorridos devem ser reportados à governança e avaliados por comitês internos formados pelas múltiplas áreas.

2. O plano de ação deve contar com mecanismos que assegurem a comunicação imediata para todos os colaboradores relevantes com relação a incidentes que possam gerar riscos à empresa. Deve haver definição de papéis e responsabilidades, prevendo o acionamento dos colaboradores-chaves e contatos externos relevantes, inclusive de reguladores, considerando critérios e prazos vigentes, quando aplicável.
3. O plano deve levar em consideração os cenários de ameaças previstos na avaliação de risco.
4. Deve haver critérios para classificação dos incidentes, por severidade. Eles podem requerer desde uma simples redundância de equipamentos para a continuidade dos serviços, a criação de uma estrutura para acesso remoto, em casos de restrições de acesso físico aos escritórios, ou até mesmo a implementação de instalações de contingência, físicas ou em nuvem, em casos mais severos. Nestes, o plano deve prever também o processo de retorno às instalações originais após o término do incidente.
5. Deve-se atentar a questões de segurança e controles de acesso também nas instalações de contingência, físicas ou em nuvem, e configurações seguras para serviços de contingência em nuvem.
6. Recomenda-se o devido arquivamento de documentações relacionadas ao gerenciamento dos incidentes e ao plano de resposta a incidentes para servir como evidência em eventuais questionamentos.

## 5 – Governança

### Recomendações

1. Deve ser criado um comitê, fórum ou grupo específico para tratar de segurança cibernética dentro da instituição, com representação e governança apropriados.
2. O programa de segurança cibernética deve ser revisado periodicamente mantendo sempre atualizadas suas avaliações de risco, implementações de proteção, planos de resposta a incidentes e monitoramento dos ambientes. Sugere-se que a revisão do programa seja realizada anualmente.
3. Os grupos envolvidos com o programa devem manter-se atualizados com novas vulnerabilidades e ameaças identificadas que possam alterar a exposição da instituição aos riscos avaliados originalmente. Isso pode ser feito, entre outras formas, por meio de

participação em grupos de compartilhamento de informações, ou via fornecedores especializados.

4. As instituições devem promover e disseminar a cultura de segurança com a criação de 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, dar treinamentos e repassar novas orientações.
5. Iniciativas como a definição e manutenção de indicadores de desempenho (key performance indicators) podem corroborar a conscientização e o envolvimento da alta administração e dos demais órgãos da instituição.
6. Como parte dos mecanismos para conscientização sobre o assunto, é importante a criação de uma política de uso adequado da estrutura tecnológica da instituição, de forma independente ou como parte de um documento mais abrangente.
7. Deve-se orientar usuários a terem atenção especial antes de clicar em links recebidos, mesmo vindos de pessoas conhecidas. Esse é um dos principais vetores atuais de invasão.
8. Recomenda-se que o programa de segurança cibernética contenha disposição quanto ao treinamento periódico sobre segurança da informação. Ele deve incidir periodicamente sobre todos os funcionários, além de haver um plano de treinamentos especiais para funcionários recém-contratados, no momento do onboarding.
9. Os treinamentos e as campanhas de conscientização devem ser intensificados para os funcionários que trabalham remotamente e para os funcionários que foram vítimas de incidente cibernético.
10. Serviços online, como aplicativos de mensagens instantâneas e envio de mensagens diretas em mídias sociais, podem ser usados em uma tentativa irregular de extrair informações dos colaboradores. Para evitar essa situação, os colaboradores devem ser informados sobre o que constitui o contato suspeito por meio de serviços online e como relatá-lo à organização.

# Referências

Segue uma lista, não exaustiva, de referências para aprofundamento nos assuntos tratados neste guia:


- Alternative Investment Management Association (AIMA), *Guide to Sound Practices for Cybersecurity* (disponível para membros da AIMA), out. 2015.
- Autoridade Nacional de Proteção de Dados (ANPD), *Comunicação de incidentes de segurança*, mar. 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/incidente-de-seguranca/.
- Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA) – Grupo Técnico de Cibersegurança, *Referência técnica para configuração segura de ambiente em nuvem*, dez. 2017. Disponível em: https://www.anbima.com.br/data/files/50/F7/30/E0/D9C206101703E9F5A8A80AC2/Tecnica-para-nuvem-Referencia.pdf.
- Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais (ANBIMA) – Grupo Técnico de Cibersegurança, *Modelos de diligência com terceiros – incluindo provedores de serviços em nuvem*, dez. 2017. Disponível em: https://www.anbima.com.br/data/files/84/B7/86/09/B9C206101703E9F5A8A80AC2/Modelo-de-Diligencia-com%20Terceiros-Referencia.pdf.
- Autorité des marchés financiers (AMF), *Stock Market Cybercrime – Definition, cases and perspectives*, fev. 2020. Disponível em: https://www.amf-france.org/sites/default/files/2020-02/study-stock-market-cybercrime-_-definition-cases-and-perspectives.pdf.
- Brasil, Lei 13.709, de 14 de agosto de 2018. *Lei Geral de Proteção de Dados.* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.
- Brasil, Bolsa e Balcão, *Programa de Qualificação Operacional*, jan. 2019. Disponível em: http://www.b3.com.br/pt_br/antigo/s_regul-antigo/programa-de-qualificacao-operacional-pqo/roteiros/.
- Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, *Relatório final*, mai. 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra;

jsessionid=214D61B364D3F74027CAB7F56C3E0C39.proposicoesWeb2?codteor=1455189&filename=REL+4/2016+CPICIBER+%3D>+RCP+10/2015.

- Commodities and Futures Trading Commission (CFTC), *Recommended Best Practices for the Protection of Customer Records and Information*, fev. 2014. Disponível em: http://www.cftc.gov/idc/groups/public/@lrlettergeneral/documents/letter/14-21.pdf.

- Conselho Monetário Nacional (CMN), Resolução 4.893, de 26 de fevereiro de 2021, *que dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem a serem observados pelas instituições autorizadas a funcionar pelo Banco Central do Brasil*. Disponível em: https://www.bcb.gov.br/estabilidadefinanceira/exibenormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893.

- Cyber Security Agency of Singapore (CSA), *Guide to conducting Cybersecurity risk assessment for critical information infrastructure,* dez. 2019. Disponível em: https://www.csa.gov.sg/-/media/csa/documents/legislation_supplementary_references/guide_to_conducting_cybersecurity_risk_assessment_for_cii.pdf.

- Cyber Security Agency of Singapore (CSA), *Singapore's Operation Technology Cybersecurity Masterplan 2019*, out. 2019. Disponível em: https://www.csa.gov.sg/news/publications/ot-cybersecurity-masterplan.

- Department of The Treasury, *Advisory on Potential Sanctions Risks for Facilitating Ransomware Payments*, out. 2020. Disponível em: https://home.treasury.gov/system/files/126/ofac_ransomware_advisory_10012020_1.pdf.

- European Insurance and Occupational Pensions Authority (EIOPA), *Guidelines on outsourcing to cloud service providers*, fev. 2020. Disponível em: https://www.eiopa.europa.eu/content/guidelines-outsourcing-cloud-service-providers_en.

- European Securities and Markets Authority (ESMA), *Guidelines on outsourcing to cloud service providers*, dez. 2020. Disponível em: https://www.esma.europa.eu/sites/default/files/library/esma50-157-2403_cloud_guidelines.pdf.

- European Systemic Risk Board (ESRB), *Systemic cyber risk*, fev. 2020. Disponível em: https://www.esrb.europa.eu/news/pr/date/2020/html/esrb.pr200219~61abad5f20.en.html.
- Federal Financial Institutions Examination Council's (FFIEC), *Cybersecurity Assessment Tool*, jun. 2015. Disponível em: https://www.ffiec.gov/pdf/cybersecurity/FFIEC_CAT_May_2017_All_Documents_Combined.pdf.
- Federal Reserve (FED), *Sound Practices to Strengthen Operational Resilience*, out. 2020. Disponível em: https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20201030a1.pdf.
- Financial Conduct Authority (FCA), *Cyber resilience*, out. 2020. Disponível em: https://www.fca.org.uk/firms/cyber-resilience.
- Financial Conduct Authority (FCA), *Cyber Security – industry insights*, mar. 2019. Disponível em: https://www.fca.org.uk/publications/research/cyber-security-industry-insights.
- Financial Industry Regulatory Authority (FINRA), *Observations on Cybersecurity*, out. 2019. Disponível em: https://www.finra.org/rules-guidance/guidance/reports/2019-report-exam-findings-and-observations/cybersecurity.
- Financial Industry Regulatory Authority (FINRA), *Report on Selected Cybersecurity Practices*, dez. 2018. Disponível em: https://www.finra.org/rules-guidance/guidance/reports/2018-cybersecurity-report.
- Financial Industry Regulatory Authority (FINRA), *Small Firm Cybersecurity Checklist*, jun. 2020. Disponível em: https://www.finra.org/compliance-tools/cybersecurity-checklist.
- Financial Stability Board (FSB), *Effective Practices for Cyber Incident Response and Recovery*, out. 2020. Disponível em: https://www.fsb.org/wp-content/uploads/P191020-1.pdf.
- Global Financial Markets Association (GFMA), *Framework for the Regulatory Use of Penetration Testing in the Financial Services Industry*, abr. 2018. Disponível em: https://www.gfma.org/correspondence/updated-gfma-framework-for-the-regulatory-use-of-penetration-testing-in-the-financial-services-industry/.
- Government Digital Service (Gov.UK), *Cyber security incentives & regulation review*, ago. 2020. Disponível em: https://www.gov.uk/government/publications/cyber-security-incentives-regulation-review-government-response-to-the-call-for-evidence.

- Hedge Fund Standards Board (HSFB), *Cybersecurity Toolbox for Hedge Funds Managers*, out. 2015. Disponível em: http://www.sbai.org/wp-content/uploads/2016/04/Cybersecurity-HFSB-Toolbox.pdf.
- Investment Company Institute (ICI), *Information Security Resource Center*. Disponível em: https://www.ici.org/info_security.
- Investment Industry Regulatory Organization of Canada (IIROC), *Cybersecurity Best Practices Guide for IIROC Dealers Members*, mar. 2016. Disponível em: http://www.iiroc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf.
- Investment Industry Regulatory Organization of Canada (IIROC), *Cybersecurity Incident Management Planning Guide*, mar. 2016. Disponível em: http://www.iiroc.ca/industry/Documents/CyberIncidentManagementPlanningGuide_en.pdf.
- International Organization of Securities Commissions (IOSCO), *Cyber Security in Securities Markets – An International Perspective*, abr. 2016. Disponível em: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf.
- National Cyber Security Centre (NCSC), *Guidance for organizations on enabling staff to use their own smartphones, tablets, laptops and desktop PCs to access work information*, Disponível em: https://www.ncsc.gov.uk/collection/mobile-device-guidance/bring-your-own-device.
- National Cyber Security Centre (NCSC), *Effective steps to cyber exercise creation*, fev. 2020. Disponível em: https://www.ncsc.gov.uk/guidance/effective-steps-to-cyber-exercise-creation.
- National Cyber Security Centre (NCSC), *10 steps to cyber security*, nov. 2018. Disponível em: https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security.
- National Futures Association (NFA), *Information Security Programs*, out. 2015. Disponível em: http://www.nfa.futures.org/nfamanual/NFAManual.aspx?RuleID=9070&Section=9.
- National Institute of Standards and Technology (NIST), *Cybersecurity Framework*. Disponível em: http://www.nist.gov/cyberframework.
- New York State Department of Financial Services (DFS), *Cybersecurity Requirements for Financial Services Companies – 23 NYCRR Part 500,* dez. 2016. Disponível em: https://govt.westlaw.com/nycrr/Browse/Home/NewYork/NewYorkCodesRulesandRegula

tions?guid=I5be30d2007f811e79d43a037eefd0011&originationContext=documenttoc&transitionType=Default&contextData=(sc.Default).

- New York State Department of Financial Services (DFS), *Cybersecurity*. Disponível em: https://www.dfs.ny.gov/industry_guidance/cybersecurity.
- SANS Institute, *Securing the Human*. Disponível em: https://www.sans.org/security-resources/posters/securing-the-human.
- Securities Industry and Financial Markets Association (SIFMA), *Insider Threat Best Practices Guide*, fev. 2018. Disponível em: https://www.sifma.org/wp-content/uploads/2018/02/insider-threat-best-practices-guide.pdf.
- Securities Industry and Financial Markets Association (SIFMA), *Cybersecurity Resource Center*. Disponível em: https://www.sifma.org/resources/cybersecurity-resources/.
    - SIFMA, *Data Protection Principles*, jan. 2020;
    - SIFMA, *Guidance for small firms*, jul. 2014;
    - SIFMA, *Best practices for insider threat*, jul. 2014; e
    - SIFMA, *Third Party Management Program Implementation Tips*.
- US Securities and Exchange Commission (SEC), *Observations from Cybersecurity Examination*, ago. 2017. Disponível em: https://www.sec.gov/files/observations-from-cybersecurity-examinations.pdf.
- US Securities and Exchange Commission (SEC), *Investment Management Cybersecurity Guidance*, abr. 2015. Disponível em: https://www.sec.gov/investment/im-guidance-2015-02.pdf.