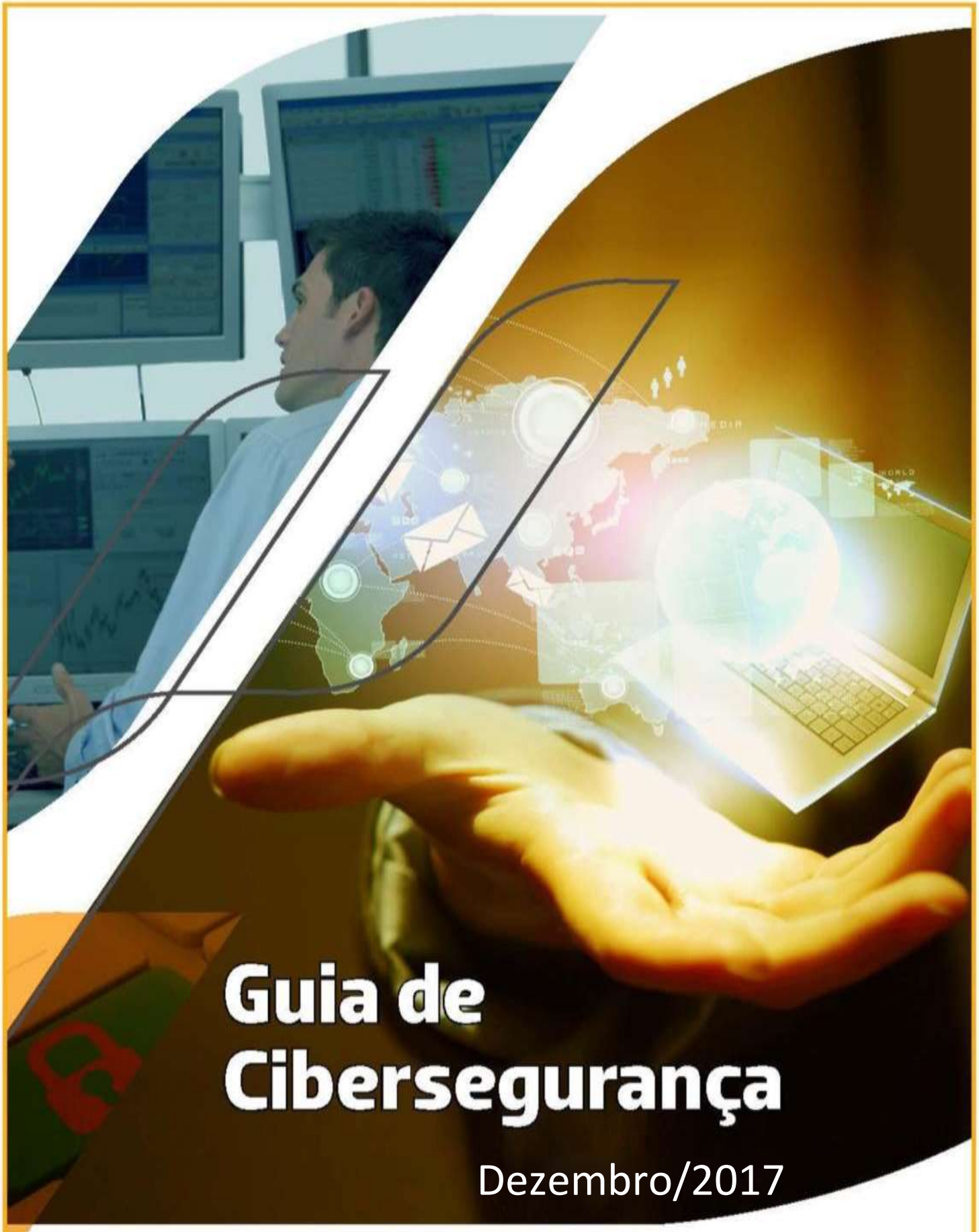


Guia de Cibersegurança

Dezembro/2017

ANBIMA

Sumário

Esta 2ª edição do Guia foi publicada em 6 de dezembro de 2017 (1ª edição publicada em 3/8/16). O objetivo é contribuir para o aprimoramento das práticas de segurança cibernética nos mercados financeiro e de capitais do Brasil, **sendo facultativa a adesão**. O guia não deve servir como fonte única e exaustiva. As instituições devem sempre consultar a legislação e a regulamentação vigentes.

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 em 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 avaliar suas práticas e definir elementos relevantes na construção e no desenvolvimento do seu programa.

Em 2016, de forma a auxiliar as instituições participantes dos Códigos de Regulação e Melhores Práticas, a ANBIMA lançou este guia, que tem como objetivo descrever 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[2], essa primeira versão do documento foi reformulada e atualizada levando a esta segunda edição do Guia.

[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] Para maiores informações ver: http://www.anbima.com.br/pt_br/representar/grupos-de-trabalho/ciberseguranca/ciberseguranca.htm

Esta 2ª edição do Guia foi publicada em 6 de dezembro de 2017 (1ª edição publicada em 3/8/16). O objetivo é contribuir para o aprimoramento das práticas de segurança cibernética nos mercados financeiro e de capitais do Brasil, **sendo facultativa a adesão**. O guia não deve servir como fonte única e exaustiva. As instituições devem sempre consultar a legislação e a regulamentação vigentes.

Como as práticas e soluções de cibersegurança evoluem rapidamente, exigindo constante adaptação das instituições, este guia também 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 progridam na implementação do programa de segurança cibernética.**
- **A implementação das recomendações depende das características e das necessidades de cada instituição.**

Esta 2ª edição do Guia foi publicada em 6 de dezembro de 2017 (1ª edição publicada em 3/8/16). O objetivo é contribuir para o aprimoramento das práticas de segurança cibernética nos mercados financeiro e de capitais do Brasil, **sendo facultativa a adesão**. O guia não deve servir como fonte única e exaustiva. As instituições devem sempre consultar a legislação e a regulamentação vigentes.

O risco cibernético

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 avanços. Por outro lado, 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[3]:

- 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.
- Engenharia social – métodos de manipulação para obter informações confidenciais, como senhas, dados pessoais e número de cartão de crédito:

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

  - *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, vulnerabilidade e informações/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 também da rápida detecção e resposta após a identificação do ataque[4]. Tanto instituições grandes como pequenas podem ser impactadas.

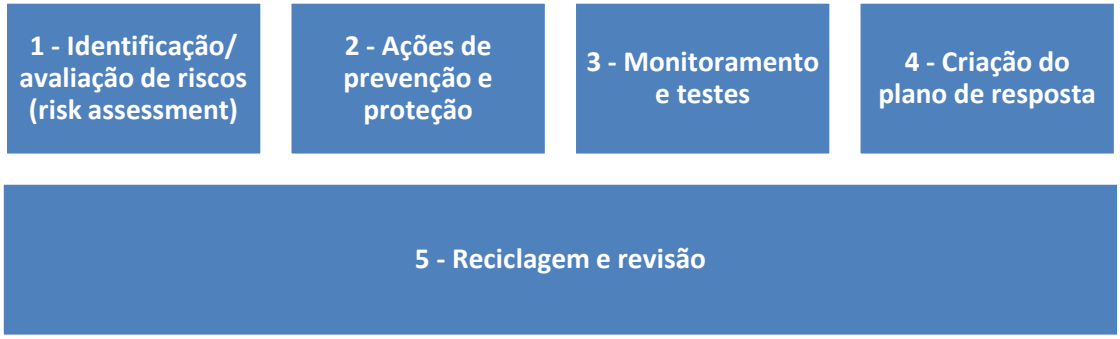
- **Instituições financeiras não podem ignorar o risco cibernético.**
- **Ataques ameaçam a confidencialidade, a integridade ou a disponibilidade dos dados e dos sistemas das instituições.**
- **Reguladores estão focando na identificação de pontos fracos em segurança cibernética nos mercados de capital.**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

Esta 2ª edição do Guia foi publicada em 6 de dezembro de 2017 (1ª edição publicada em 3/8/16). O objetivo é contribuir para o aprimoramento das práticas de segurança cibernética nos mercados financeiro e de capitais do Brasil, **sendo facultativa a adesão**. O guia não deve servir como fonte única e exaustiva. As instituições devem sempre consultar a legislação e a regulamentação vigentes.

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 e 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. **Reciclagem e revisão** – manter o programa de segurança cibernética continuamente atualizado, identificando novos riscos, ativos e processos e reavaliando os riscos residuais.



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, e 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, devem-se identificar todos os processos e ativos relevantes da instituição (sejam equipamentos, sejam sistemas 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.
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. Deve ser criado um comitê, fórum ou grupo específico para tratar segurança cibernética dentro da instituição, com representação e governança apropriados.
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.

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 senhas de acesso a dispositivos corporativos, sistemas e rede – complexidade, periodicidade e autenticação de múltiplos fatores – em função da relevância do ativo acessado.
3. Segregar senhas entre serviços. É atualmente mais recomendado o uso de um gerenciador de senhas do que o uso da mesma senha para facilitar a memorização em vários serviços.
4. 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.
5. Os eventos de *login* e alteração de senhas devem ser auditáveis e rastreáveis.
6. 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. Para mais referências sobre configurações seguras na nuvem consulte as referências.
7. 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.

8. Restringir o acesso físico às áreas com informações críticas/sensíveis.
9. Implementar serviço de backup dos diversos ativos da instituição.
10. Criar logs e trilhas de auditoria sempre que os sistemas permitam.
11. 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.
12. Considerar questões de segurança já durante as fases e pré-projeto e desenvolvimento de novos sistemas, softwares ou aplicações.
13. Implementar segurança de borda, nas redes de computadores, por meio de firewalls e outros mecanismos de filtros de pacotes.
14. Implementar recursos *anti-malware* em estações e servidores de rede, como antivírus e firewalls pessoais.
15. Implementar segregação de serviços sempre que possível, restringindo-se o tráfego de dados apenas entre os equipamentos relevantes.
16. Impedir a instalação e execução de software e aplicações não autorizadas por meio de controles de execução de processos (por exemplo, aplicação de *whitelisting*).

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, deve-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. Por exemplo, computadores não autorizados ou software não licenciado.
3. Deve-se manter os sistemas operacionais e softwares de aplicação sempre atualizados, instalando as atualizações sempre que forem disponibilizadas.
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. É sugerido, 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[5], sejam externos. O uso de ferramentas de centralização e análise de logs é especialmente recomendado.

4 – Criação de plano de resposta

Recomendações:

1. Recomenda-se o envolvimento de várias áreas da instituição na elaboração do plano formal, além da área de segurança tecnológica, como departamentos jurídico, de compliance e de comunicação.
2. Deve haver definição de papéis e responsabilidades dentro do plano de ação, prevendo acionamento dos colaboradores-chaves e contatos externos relevantes.
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 duplicação de equipamentos para a continuidade dos serviços, até o uso de instalações de contingência em casos mais severos. Nesses casos, o plano deve prever também o processo de retorno às instalações originais após o término do incidente.
5. Deve-se atentar para questões de segurança e controles de acesso também nas instalações de contingência.
6. Recomenda-se o devido arquivamento de documentações relacionadas ao gerenciamento dos incidentes e ao plano de continuidade de negócios para servir como evidência em eventuais questionamentos.

5 – Reciclagem e revisão

Recomendações:

1. 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.
2. 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.
3. 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

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

treinamentos e repassar novas orientações.

4. 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.
5. 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.

Deve-se orientar usuários a ter atenção especial antes de clicar em links recebidos, mesmo vindos de pessoas conhecidas. Este é um dos principais vetores atuais de invasão.

Referências

Segue abaixo 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.
- ANBIMA, Grupo Técnico de Cibersegurança, *Referência técnica para configuração segura de ambiente em nuvem* (4/12/17) – http://www.anbima.com.br/data/files/50/F7/30/E0/D9C206101703E9F5A8A80AC2/Tecnica-para-nuvem-Referencia.pdf
- ANBIMA, Grupo Técnico de Cibersegurança, *Modelos de diligência com terceiros* – incluindo provedores de serviços em nuvem (4/12/17) – http://www.anbima.com.br/data/files/84/B7/86/09/B9C206101703E9F5A8A80AC2/Modelo-de-Diligencia-com%20Terceiros-Referencia.pdf
- Banco Central do Brasil, Edital de Consulta Pública BC 57/2017 – Publicada em 19/9/2017 (*Dispõe sobre a política de segurança cibernética e sobre os requisitos para a contratação de serviços de processamento, armazenamento de dados e de computação em nuvem, a serem observados pelas instituições financeiras e demais instituições autorizadas a funcionar pelo BCB)*. Disponível em: https://www3.bcb.gov.br/audpub/HomePage?1
- BM&FBovespa, Programa de Qualificação Operacional, Roteiro básico. Disponível em: http://www.bmfbovespa.com.br/pt_br/regulacao/programa-de-qualificacao-operacional-pqo/roteiros/
- Câmara dos Deputados, Projeto de Lei 5276/16 (*Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural*). Disponível em: http://www.camara.gov.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378
- Central Bank of Ireland, *Review of the Management of Operational Risk Around Cybersecurity within the Investment Firm and Fund Service Industry*, set. 2015. Disponível em: https://www.centralbank.ie/regulation/industry-sectors/investment-firms/mifid-firms/Documents/Industry%20Letter%20-%20Thematic%20Review%20of%20Cyber-Security%20and%20Operational%20Risk.pdf.
- Comissão Parlamentar de Inquérito dos Crimes Cibernéticos, *Relatório final,* maio 2016. Disponível em: http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-temporarias/parlamentar-de-inquerito/55a-legislatura/cpi-crimes-ciberneticos
- Commodities and Futures Trading Commission (CFTC), *Recommended Best Practices for the Protection of Customer Records and Informations*, fev. 2014. Disponível em: http://www.cftc.gov/idc/groups/public/@lrlettergeneral/documents/letter/14-21.pdf

Esta 2ª edição do Guia foi publicada em 6 de dezembro de 2017 (1ª edição publicada em 3/8/16). O objetivo é contribuir para o aprimoramento das práticas de segurança cibernética nos mercados financeiro e de capitais do Brasil, **sendo facultativa a adesão**. O guia não deve servir como fonte única e exaustiva. As instituições devem sempre consultar a legislação e a regulamentação vigentes.

- Financial Industry Regulatory Authority (FINRA), *Report on Cybersecurity Practices*, jan. 2015. Disponível em: https://www.finra.org/sites/default/files/p602363%20Report%20on%20Cybersecurity%20Practices_0.pdf
- Hedge Fund Standards Board (HSFB), *Cybersecurity Toolbox for Hedge Funds Managers*, out. 2015. Disponível em: http://www.hfsb.org/sites/10377/files/regulators_on_cybersecurity.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*, Disponível em: http://www.iosco.org/library/pubdocs/pdf/IOSCOPD528.pdf
- 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.
- National Institute of Standards and technology (NIST), *Cloud Computing Program* – NCCP. Disponível em (acesso em 13/9/17): https://www.nist.gov/programs-projects/nist-cloud-computing-program-nccp
- New York State Department of Financial Services (DFS), *Cybersecurity Requirements for Financial Services Companies* – 23 NYCRR Part 500 (28/12/16). Disponível em: http://www.dfs.ny.gov/about/press/pr1612281.htm
- New York State Department of Financial Services (DFS), *Cybersecurity*. Disponível em: http://www.dfs.ny.gov/about/cybersecurity.htm
- SANS Institute. Disponível em: http://www.sans.org.

- Securities Industry and Financial Markets Association (SIFMA), *Insider Threat Best Practices Guide*. Disponível em: https://www.sifma.org/wp-content/uploads/2017/08/insider-threat-best-practices-guide.pdf
- Securities Industry and Financial Markets Association (SIFMA), *Cybersecurity Resource Center*. Disponível em: http://www.sifma.org/issues/operations-and-technology/cybersecurity/resources.
    - SIFMA, *Guidance for small firms*, jul. 2014;
    - SIFMA, *Best practices for insider threat*, jul. 2014; e
    - SIFMA, *Third Party Management Program Implementation Tips*.
- SIFMA, Best Practices for Insider Threats. Disponível http://www.sifma.org/uploadedFiles/Issues/Technology_and_Operations/Cyber_Security/insider-threat-best-practices-guide.pdf?n=45727
- Senado Federal, Projeto de Lei do Senado 330/13 (*Dispõe sobre a proteção, o tratamento e o uso dos dados pessoais, e dá outras providências*). Disponível em: https://www25.senado.leg.br/web/atividade/materias/-/materia/113947
- US Securities and Exchange Commission (SEC), *Observations from Cybersecurity Examination*, 7/8/2017. 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.