

Orientações para Cibersegurança na Gestão de Continuidade de Negócios

1ª Edição | 2024

The logo for ANBIMA, featuring a stylized 'A' composed of two overlapping shapes in green and orange, positioned above the word 'ANBIMA' in a bold, black, sans-serif font. The logo is set against a white, rounded rectangular background.

ANBIMA

Sumário

Sobre o Guia Técnico.....	3
Introdução.....	4
Gestão de continuidade de negócios.....	5
1. Estratégia de contingência de cibersegurança	5
2. Dicas para o gerenciamento de crises	7
3. Dicas adicionais.....	7
Conclusão	9
Expediente.....	10

Sobre o Guia Técnico

Este Guia Técnico de Orientações para Cibersegurança na Gestão de Continuidade de Negócios é resultado do trabalho conjunto da ANBIMA - Associação Brasileira das Entidades dos Mercados Financeiro e de Capitais com participantes de mercado reunidos no Grupo Consultivo de Cibersegurança. O material traz orientações e informações que visam disseminar boas práticas de segurança cibernética às instituições atuantes nos mercados financeiro e de capitais com o objetivo de contribuir para sua integridade e maior resiliência frente às crises motivadas por incidentes cibernéticos.

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

O conteúdo deste material também não deve ser interpretado de forma a contrariar, mitigar ou se opor a nenhum normativo da legislação, regulação¹ e autorregulação², aplicáveis aos mercados financeiro e de capitais, limitando-se, tão somente, a orientar técnicas para melhor consecução de atividades ao mercado.

¹ BRASIL. Resolução CMN Nº 4.893/2021. Disponível em:

<<https://www.bcb.gov.br/estabilidadefinanceira/exibnormativo?tipo=Resolu%C3%A7%C3%A3o%20CMN&numero=4893>>.

BRASIL. Resolução CVM Nº 35/2021. 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/1E/42/14/73/BB3EF810B99A0EF8B82BA2A8/Regras%20e%20Procedimentos%20de%20Deveres%20Basico%20vigente%20a%20partir%20de%2003.06.24_.pdf>.

Introdução

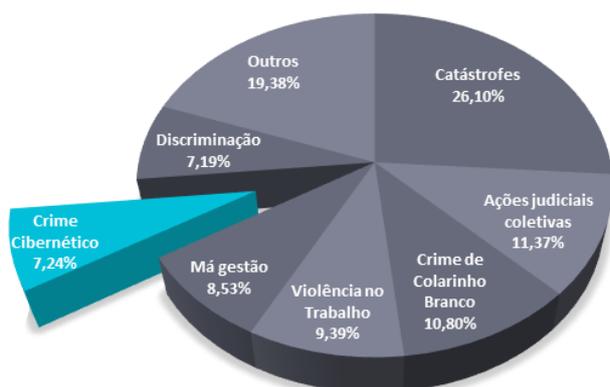
ICM ANNUAL CRISIS REPORT 2023



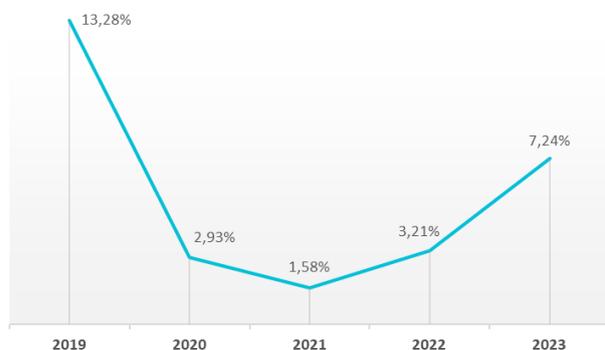
1.977.722 de crises de negócios contabilizadas no mundo, 7,24% decorrentes de crimes cibernéticos

Conceito de crise:

Qualquer questão, problema ou perturbação que desencadeia reações negativas das partes interessadas que pode impactar a reputação da organização e a solidez empresarial e financeira.



As crises decorrentes de **Crimes Cibernéticos** contabilizadas em 2023 mais que dobraram com relação a 2022, mas ainda se mantêm abaixo dos níveis anteriores à pandemia da COVID-19.



Os ataques cibernéticos representam o 6º maior fator gerador de crises nos negócios globalmente. É o que aponta o relatório³ anual do *Institute for Crisis Management* – ICM, publicado em julho de 2024. O estudo revela que 7,24% das quase 2 milhões de crises registradas em 2023 foram decorrentes de cibercrimes; percentual que supera a medição de 2022 em mais que o dobro. Este cenário reforça a importância de as organizações desenvolverem estratégias, políticas e processos definidos e documentados, além de coordenar o investimento de recursos a fim de preservar a integridade dos mercados, garantir a manutenção da confiança de clientes e stakeholders e a continuidade de seus negócios frente a contingências de cibersegurança.

Este material reúne estratégias e orientações que visam auxiliar as instituições na gestão de seu plano de continuidade de negócios, a fim de que estejam preparadas para lidar com eventuais cenários que exijam sua estratégia de contingência de cibersegurança.

Para se aprofundar no tema e saber mais sobre as melhores práticas, a regulação e autorregulação relacionadas à segurança cibernética e da informação, consulte nossa página especial de cibersegurança em:

<http://anbi.ma/espacociber>

³ ICM. "Annual Crisis Report" (2024). Disponível em: <<https://crisisconsultant.com/icm-annual-crisis-report/>>.

Gestão de continuidade de negócios

No cenário atual, em que a tecnologia se tornou indispensável tanto para o funcionamento das empresas quanto para o dia a dia das pessoas, a segurança cibernética desponta como uma prioridade fundamental. Com a digitalização de processos e a crescente dependência de sistemas informatizados, as organizações enfrentam um desafio constante: proteger seus dados e operações contra ameaças cibernéticas cada vez mais sofisticadas. Por isso, realizar uma adequada gestão da continuidade de negócios para resguardar as instituições de disrupções relacionadas à cibersegurança é mais que uma necessidade operacional, é uma questão de preservação da confiança dos clientes e stakeholders e de sobrevivência nos mercados.

1. Estratégia de contingência de cibersegurança

A estratégia de contingência de cibersegurança pode ser definida, dentro dos planos de continuidade de negócios, pela coordenação de processos e recursos para manter ou retomar as atividades de uma instituição em caso de disrupção relacionada a incidente cibernético. O objetivo é reduzir os danos causados por eventos desse tipo, proteger dados sensíveis, garantir a continuidade dos serviços críticos, restabelecer a normalidade das operações e identificar oportunidades de melhoria da segurança para prevenir novos incidentes.

Apresentamos abaixo boas práticas a serem consideradas pelas instituições para a desenvolvimento de sua estratégia de contingência de cibersegurança:

- 1 Definir os **objetivos**, o **escopo**, os **recursos aplicáveis**, os **responsáveis** e os **requisitos regulatórios** a serem atendidos;
- 2 Identificar e avaliar os riscos relacionados aos diferentes **equipamentos, sistemas, redes, dados, processos e serviços críticos**, inclusive às diversas **atividades essenciais exercidas** pela organização (considerando informações e dados gerados, coletados, tratados e armazenados em cada uma delas), descrevendo suas vulnerabilidades a ameaças, suscetibilidade probabilística a incidentes de segurança cibernética e potenciais impactos negativos previstos na ocorrência destes incidentes;
- 3 Identificar e avaliar as **dependências e redundâncias** entre equipamentos, sistemas, redes, processos, serviços e atividades críticos para melhor identificar vulnerabilidades e potenciais impactos que o comprometimento de uma etapa pode desencadear em outras numa reação em cadeia;
- 4 Definir e descrever as **táticas e medidas de contingência específicas e adequadas** para as diferentes ameaças e vulnerabilidades 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;

- 5 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 Tecnologia da Informação – TI** (essencial para a resposta ao incidente cibernético);
- 6 **Identificar e avaliar o incidente cibernético** em caso de interrupção, buscando mensurar a extensão de eventual infecção e implementar as táticas e medidas mais adequadas a serem utilizadas para **recuperação e mitigação dos impactos**;
- 7 Constituir **comitês multidisciplinares** de gerenciamento de crise (compostos, por exemplo, por representantes das áreas de TI, Segurança da Informação – SI, *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 este tipo de evento pode gerar ao negócio;
- 8 **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**;
- 9 Analisar o incidente e considerar **elaborar relatórios** sobre as vulnerabilidades exploradas na interrupção e, a fim de evitar a reincidência, **propor soluções e aprimoramentos** para:
 - as políticas e controles de segurança cibernética;
 - as políticas e controles de segurança da informação;
 - o plano de continuidade de negócios e as estratégias de contingência de cibersegurança;
 - as regras e procedimentos que contemplem a contratação de terceiros e de serviços em nuvem (no caso de eventualidade envolvendo o risco de terceiros);
 - as regras e procedimentos que contemplem o desenvolvimento de aplicações e sistemas (na eventualidade de incidentes envolvendo, por exemplo, a segurança dos softwares); e
 - os processos e rotinas de treinamento, validação e testagens (considerando intensificar testagens, cuja recorrência recomendada é, no mínimo, anual ou em prazo inferior ao exigido pela regulação em vigor).
- 10 **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.

2. Dicas para o gerenciamento de crises

Em tempos de crise, a capacidade de resposta rápida e coordenada pode determinar o sucesso na preservação dos ativos empresariais e na manutenção da confiança dos stakeholders e dos clientes. Mesmo que não seja possível uma rápida recuperação das atividades e operações, é muito importante que, reunidas as condições para que seja colocada em prática a estratégia de contingência de cibersegurança prevista no plano de continuidade de negócios, isso seja feito o quanto antes pelas organizações. Realizando ações suficientes para sinalizar que o problema está sendo tratado e uma comunicação transparente com o comprometimento de toda a equipe.

Realizar exercícios e testes periódicos levando em consideração a comunicação interna e externa com os colaboradores, que devem receber treinamento adequado para essas situações, é fundamental. Recomenda-se manter os canais de comunicação com o público (nas diferentes plataformas utilizadas oficialmente pela instituição) abertos, trazendo atualizações crescentes sobre o enfrentamento da crise até a recuperação total.

A definição de porta-vozes para essas comunicações e o treinamento de mídia, são ações que contribuem para evitar posicionamentos individuais que possam gerar confusão ou expor a instituição diante do público geral. Outra medida para reduzir o risco de imagem, é manter modelos padronizados de comunicados, informes a autoridades e reguladores, notas à imprensa, mensagens, publicações em redes sociais etc. que podem servir como base para a comunicação no momento da crise.

Após a recuperação, além dos relatórios internos de análise detalhada da crise, a divulgação de um relatório ao público geral ou algum documento análogo capaz de explicar o incidente, descrever as respostas adotadas para recuperação e mitigação de impactos e definir as ações que serão tomadas para prevenção e melhoria da segurança é uma prática que contribui significativamente para a manutenção da imagem da instituição e de seus negócios.

3. Dicas adicionais

Apresentamos abaixo algumas dicas adicionais que contribuem para a prevenção, o tratamento e a mitigação de impactos de interrupções relacionadas a incidentes de cibersegurança:

-  **Investir o tempo adequado para uma recuperação total:** em caso de contingência de cibersegurança, a prioridade é garantir que as vulnerabilidades exploradas tenham sido identificadas e as intrusões e/ou ameaças neutralizadas e, em segundo lugar, garantir a retomada segura das atividades o mais rápido possível;
-  Realizar o **treinamento dos colaboradores** em cibersegurança para promover a conscientização, o engajamento e a capacitação, visando a redução dos riscos e melhoria da segurança da organização (considerar as melhores práticas definidas no documento *Orientações*

para o treinamento de colaboradores em cibersegurança⁴, que inclui a definição de conceitos importantes e das principais ameaças cibernéticas);

-  No caso de contingência associada a ataque cibernético do tipo **ransomware**, recomenda-se não realizar o pagamento de resgates aos criminosos;
-  Desenvolver sistemas e processos de **recuperação de dados** e realizar **backups** com regularidade, considerando automatizar esse processo (quando aplicável) e manter cópias em dispositivos externos seguros e/ou cópias criptografadas em nuvem, e realizando testes periódicos dos sistemas e processos de recuperação e backup;
-  Observar os requisitos regulatórios e adotar as melhores práticas (considerar as definidas no documento *Orientações para contratação de terceiros e nuvem*⁵) para administrar o **risco associado a contratação de terceiros e serviços em nuvem** (no exterior ou dentro de país em que a instituição opera);
-  Utilizar **ferramenta de detecção e resposta de endpoint (EDR)** para identificação de processos suspeitos relacionados, por exemplo, a ataques de dia zero, ataques direcionados (APT), ransomwares ou violações das políticas internas da empresa;
-  Observar as melhores práticas para o **desenvolvimento seguro de aplicações e sistemas** (considerar orientações contidas no documento *Segurança no desenvolvimento de aplicações – CEGSIC 2009-2011*⁶, os princípios da OWASP⁷ de codificação segura e a estrutura de desenvolvimento seguro de software do NIST⁸);
-  Aderir a práticas de **cooperação** entre entidades participantes dos mercados financeiro e de capitais, entre outras, para troca de informações e experiências que contribuam para o amadurecimento da capacidade de cibersegurança e maior resiliência das instituições e coordenação de ações de prevenção e recuperação e mitigação de impactos no caso de contingências (considerar adesão à prática descrita no documento *Orientações para compartilhamento de informações sobre incidentes cibernéticos*⁹);

⁴ ANBIMA. “Orientações para o treinamento de colaboradores em cibersegurança”. Disponível em:

<https://www.anbima.com.br/data/files/14/E0/43/F8/4BCD0910D8866C09B82BA2A8/Orientacoes_treinamento_de_colaboradores_em_ciber.pdf>

⁵ ANBIMA. “Orientações para contratação de terceiros e nuvem”. Disponível em:

<<https://www.anbima.com.br/data/files/85/60/2A/F9/3B8C4810272519486B2BA2A8/Guia%20para%20Contratacao%20de%20Terceiros%20e%20Nuvem.pdf>>.

⁶ BRASIL. CEGSIC 2009-2011. “Segurança no desenvolvimento de aplicações”. Disponível em:

<https://www.trf3.jus.br/documentos/rget/seguranca/CLRI/GSIC701_Seguranca_Desenvolvimento_Aplicacoes.pdf>.

⁷ OWASP. “OWASP Top Ten”. Disponível em: <<https://owasp.org/Top10/>>.

⁸ NIST. “Secure Software Development Framework (SSDF) Version 1.1”. Disponível em:

<<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218.pdf>>.

⁹ ANBIMA. “Orientações para compartilhamento de informações sobre incidentes cibernéticos”. Disponível em:

<https://www.anbima.com.br/data/files/82/F7/69/66/351B281016078A28882BA2A8/Ebook_Orientacoes_para_Compartilhamento_de_Informacoes_de_Incidentes_Ciberneticos.pdf>.

- ✓ Observar as exigências regulatórias¹⁰ específicas com relação à **privacidade e proteção de dados**, tais como a comunicação às autoridades competentes dos incidentes de segurança envolvendo dados pessoais e a manutenção de registros desses casos por, ao menos, 5 anos; e
- ✓ Considerar as **externalidades e impactos socioeconômicos** que as contingências podem causar na identificação e avaliação dos riscos à imagem e ao negócio da instituição.

Conclusão

Conforme exposto neste material, estruturar estratégias de contingência de cibersegurança e o gerenciamento de crises dentro do plano de continuidade de negócios é essencial para manter ou retomar as atividades das instituições em caso de interrupções relacionadas a incidentes cibernéticos e para reduzir e mitigar os impactos às organizações e pessoas. As orientações apresentadas visam contribuir para a implementação de planos estruturados, consistentes e alinhados às melhores práticas nacionais e internacionais, sem prejuízo à observação das regulações e autorregulações vigentes. Garantindo a superação das crises cibernéticas e aproveitando a oportunidade de aprendizado quando elas ocorrem é que se garante, não apenas a continuidade dos negócios, mas também a manutenção da confiança dos clientes e stakeholders nas empresas e a integridade dos mercados.

¹⁰ BRASIL. Resolução CD/ANPD Nº 15/2024. Disponível em: <<https://www.in.gov.br/en/web/dou/-/resolucao-cd/anpd-n-15-de-24-de-abril-de-2024-556243024>>.

Expediente

GUIA TÉCNICO

Orientações para
Cibersegurança na Gestão de
Continuidade de Negócios

Gerência de Representação de Distribuição de Produtos de Investimentos

Luiz Henrique de Carvalho

Redação

Augusto Brisola

Divulgação

Paula Lepinski

Presidência

Carlos André

Diretoria

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

Comitê Executivo

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

Grupo Consultivo de Cibersegurança

Adonai Bernardes, Ana Paula Godoy, Anderson Mota, Andre Bastos, Clemer Arantes, Denise Ornellas, Fabio Nacajune, Frederico Neres, Ismar Leite, João Gabriel Lisanti, Jorge Matsumoto, Kenia Carvalho, Lilian Celeri, Luciano Kahn, Luiz Leme, Mauricio Rodrigues, Rodrigo Fusco, Rogério Malgor, Simone de Grandis

Endereço

Rio de Janeiro

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

São Paulo

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

www.anbima.com.br