POLÍTICA

DE

SEGURANÇA DA INFORMAÇÃO

E

SEGURANÇA CIBERNÉTICA

Índice

1. Tabela Sinótica 4
2. Propósito 5
3. Escopo 5
4. Responsabilidades referentes a esta política 6
5. Definições e Princípios 7
5.1. Definições 7
5.2. Princípios 8
6. Diretrizes Gerais 8
6.1. Gestão de Ativos 10
6.2. Autenticação 10
6.3. Segmentação de rede 10
6.4. Classificação da Informação 11
6.5. Controle de acesso 11
6.6. Gestão de Riscos 12
6.7. Gestão de Fornecedores 13
6.8. Segurança física do ambiente 13
6.9. Backup e gravação de LOG 14
6.10. Proteção contra vírus, arquivos e softwares maliciosos 14
6.11. Testes de varredura para detecção de vulnerabilidade 14
6.12. Criptografia 14
6.13. Plano de continuidade 15
6.14. Incidentes de segurança 15
6.15. Mecanismos de rastreabilidade 17
6.16. Registro de impacto 17
6.17. Treinamentos e conscientização 17
6.18. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem 18
6.19. Continuidade de negócios 23

6.20. Arquivamento de informações 24

7. Versões 25

1. Tabela Sinótica

aprovador final:
Diretoria

data da elaboração/revisão:
03/06/2025

área mantenedora:
Gestão de Riscos e Compliance

abrangência
- Todos os colaboradores

políticas relacionadas:
- Política de Governança
- Política de Compliance

Regulação
- Res. CMN 4.893 de 2021 – Política de Segurança Cibernéticas Instituições Autorizadas.

2. Propósito

Este documento define a estrutura de segurança de informação e segurança cibernética da Instituição.

Esta Política de Segurança da Informação e Segurança Cibernética ("Política") tem o objetivo de estabelecer diretrizes que permitem a Instituição preservar e proteger as informações de seus clientes, colaboradores, partes interessadas e da própria Instituição contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implantar controles e procedimentos que visam reduzir a vulnerabilidade da Instituição a incidentes, e também dispõe sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

3. Escopo

A Instituição deve implantar e manter esta Política formulada com base em princípios e diretrizes que busquem assegurar a confidencialidade, a integridade, a autenticidade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Esta Política será compatível com:

- O porte, o perfil de risco e o modelo de negócio da Instituição;
- A natureza das atividades da Instituição e a complexidade dos produtos e serviços oferecidos; e
- A sensibilidade dos dados e das informações sob a responsabilidade da Instituição.

A Instituição designará diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes.

- O diretor designado poderá desempenhar outras funções na Instituição, desde que não haja conflito de interesses.

A Política se aplica a todos os diretores (coletivamente "Alta Administração"), funcionários e empresas prestadoras de serviço da Instituição (coletivamente, "Colaboradores") cujas atividades sejam desempenhadas visando ao desenvolvimento das operações da Instituição.

4. Responsabilidades referentes a esta política

São deveres e responsabilidades de implantação, execução e manutenção desta Política:

- Diretor responsável pela execução e manutenção desta Política: responsável pela implantação, execução e manutenção da política;
- Usuários: Alta Administração e Colaboradores da Instituição, que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações da Instituição, e que devem, no que couber: (i) cumprir as normas e procedimentos relacionados ao uso de informações e sistemas associados, em conformidade com o estabelecido nesta Política; (ii) informar, imediatamente, às áreas responsáveis, qualquer falha em dispositivos, serviços ou processos relacionados à Segurança da Informação e Segurança Cibernética, para que sejam tomadas ações de forma tempestiva; (iii) utilizar as informações relacionadas à esta Política, como patrimônio da Instituição, e mantê-las seguras, integras e disponíveis, conforme sua classificação e necessidade. A manutenção desta política está a cargo do responsável pela área de Gestão de Riscos e Compliance, que deve mantê-la atualizada e submetê-la a revisão e reaprovação no mínimo anualmente, ou quando houver alterações que o justifiquem. Seu conteúdo é de responsabilidade integral da Diretoria.

Esta Política foi elaborada pelo Diretor responsável pela segurança da informação e cibernética em conjunto com a área de Compliance, e aprovada pela Alta Administração, e será revisada com a periodicidade mínima anual.

A Política também poderá ser alterada, a qualquer momento, para contemplar quaisquer alterações regulatórias e outras obrigações legais.

Os Colaboradores da Instituição, a ela devem aderir formalmente por meio de um termo em que se comprometem a agir de acordo com esta Política.

Os contratos celebrados com terceiros pela Instituição e que tratem de Ativos de informação referentes a esta Política devem possuir cláusula que assegure a segurança das informações.

Esta Política está acompanhada de um Termo de Adesão à Política de Segurança da Informação e Segurança Cibernética e Termo de Adesão às Alterações da Política de Segurança da Informação e Segurança Cibernética, que deverão ser assinados pela Alta Administração e pelos Colaboradores, e no que couber, os prestadores de serviços, fornecedores, provedores e parceiros.

Esta Política está disponível em local acessível a todos Colaboradores, em linguagem clara e acessível. É possível acessá-la no site bezz.com.br.

5. Definições e Princípios

5.1. Definições

- Ativos de informação: todas as formas de tratamento de informações. Os Ativos podem ser documentos impressos, sistemas, softwares, banco de dados, arquivos digitais, dispositivos móveis etc.
- Alta Administração: formado por todos os diretores da Instituição.
- Bacen: Banco Central do Brasil.
- Gestão de Ativos: são as boas práticas utilizadas pela Instituição em seu processo de controle de ativos tangíveis e intangíveis (equipamentos, contratos, marcas, ferramentas e materiais, know-how), que buscam alcançar um resultado desejado e sustentável para a operação.
- Informações Sensíveis: que tem valor estratégico para o desenvolvimento dos negócios e das operações da Instituição, ganhando tangibilidade por meio de transações, processamentos, bancos de dados, entre outras formas, e que serão tratadas com base no legítimo interesse da Instituição, estritamente necessários para a finalidade pretendida nos termos desta Política e da legislação em vigor.
- Log: registro de eventos de um sistema.
- Segurança da Informação: conjunto de conceitos, mecanismos e estratégias que visam a proteger os Ativos da Instituição.
- Segurança Cibernética: conjunto de práticas, tecnologias e processos desenvolvidos para proteger as informações e os sistemas internos, computadores, redes, softwares e dados da Instituição de ataques cibernéticos, danos, ameaças ou acesso não autorizado.

5.2. Princípios

A Instituição tem como compromisso garantir a segurança e o tratamento adequado das informações, sistemas internos, computadores, redes, softwares e dados. Para tanto, adota atividades que se baseiam nos seguintes princípios:

- Autenticidade: garantia de identificar e autenticar usuários, entidades, sistemas ou processos com acesso à informação;
- Confidencialidade: garantia de que somente pessoas autorizadas terão acessos às informações e apenas quando houver necessidade;
- Disponibilidade: garantia de que a informação estará disponível somente às pessoas autorizadas e sempre que for necessário;
- Integridade: garantia de que as informações permanecerão exatas e completas e não serão modificadas indevidamente.

6. Diretrizes Gerais

Com o objetivo de garantir os objetivos desta Política, os procedimentos de Segurança da Informação e Segurança Cibernética seguirão as seguintes diretrizes:

- Assegurar que não haja acessos indevidos, modificações, destruições ou divulgações não autorizadas das informações. Para tanto, o acesso do Colaborador deve ser pessoal, intransferível e restrito aos recursos necessários para realizar suas atribuições na Instituição.
- Cada Colaborador, quando aplicável, receberá uma senha pessoal de acesso e ficará responsável por manter sua senha em sigilo para evitar acesso indevido às informações que estão sob sua responsabilidade. A Instituição adotará mecanismos que visem assegurar a utilização segura de senhas.
- Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pela Instituição.
- Assegurar que todas as informações sejam tratadas de maneira ética e sigilosa e que sejam adotadas medidas capazes de evitar ou, ao menos, registrar acessos indevidos, modificações, destruições ou divulgações não autorizadas.

- Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização.
- Assegurar o cumprimento dos procedimentos e controles adotados para reduzir a vulnerabilidade a incidentes e atender aos demais objetivos de Segurança Cibernética, tais como, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção de vulnerabilidades, a proteção contra softwares maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações.
- Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam, no melhor nível possível, a segurança das informações sensíveis.
- Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos negócios;
- Definir os procedimentos e controles voltados à prevenção e ao tratamento dos incidentes que devem ser adotados pelos prestadores serviços e terceiros que manuseiem dados ou informações sensíveis ou que sejam relevantes para a condução das atividades operacionais da Instituição;
- Classificar os dados e as informações quanto à relevância;
- Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;
- Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo:
    - A implantação de programas de capacitação e de avaliação periódica de pessoal;
    - A prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços financeiros oferecidos.
- Estimular iniciativas para compartilhamento de informações sobre incidentes relevantes, com as demais instituições autorizadas a funcionar pelo Bacen.
- Manter o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Instituição, inclusive de informações recebidas de empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis.

- Assegurar que os prestadores de serviço utilizem procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela Instituição e por esta Política.

A fim de assegurar que todas as diretrizes acima sejam cumpridas e que os princípios de Segurança da Informação e de Segurança Cibernética sejam devidamente seguidos, a Instituição adotará procedimentos para os processos elencados nos tópicos a seguir.

6.1. Gestão de Ativos

Os Ativos devem ser inventariados e protegidos de acessos indevidos ou ameaças que possam comprometer o negócio. Para tanto, o acesso às salas com armazenagem de documentos físicos deve ser restrito e limitado, destinados a impedir o acesso de indivíduos não autorizados.

Os Ativos devem ser utilizados tão somente para a finalidade devidamente autorizada. A Instituição deve assegurar proteção aos Ativos durante todo o seu ciclo de vida, a fim de garantir que os princípios da autenticidade, confidencialidade, disponibilidade e integridade sejam cumpridos integralmente.

6.2. Autenticação

A Instituição adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas aos indivíduos autorizados, bem como deverá prever processos de autorização levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

6.3. Segmentação de rede

A Instituição deve adotar mecanismos internos para a segmentação de rede para proteger seus dados de ataques cibernéticos e determinar que todos os computadores conectados à rede corporativa não estejam acessíveis diretamente pela Internet.

Caso o Colaborador queira criar, alterar ou excluir regras nos firewalls e Ativos de rede deverá enviar uma requisição à estrutura de tecnologia da informação, que fará análise e aprovação.

6.4. Classificação da Informação

As informações devem ser classificadas segundo sua criticidade e sensibilidade para o negócio e seus clientes. Portanto, a Instituição deve adotar a seguinte classificação:

- Informação Pública: aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados divulgados ao mercado e dados promocionais;
- Informação Interna: aquela que pode ser acessada somente por Colaboradores da Instituição. São exemplos de Informação Interna: normas, procedimentos e formulários da Instituição;
- Informação Restrita: aquela que pode ser acessada somente por Colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: contratos, sistemas e documentos estratégicos da Instituição.
- Informação Confidencial: aquela que pode ser acessada somente por Colaboradores que tenham permissão de acesso ou que necessitem dela para um propósito específico. São exemplos de Informação Confidencial: plano estratégico e informações de clientes.

6.5. Controle de acesso

A Instituição deve adotar controles de acesso em toda infraestrutura para evitar que indivíduos não autorizados tenham acesso aos ambientes segregados, aos sistemas internos e as informações que não sejam de livre acesso e sem permissão prévia. Desta forma, a Instituição deve implantar mecanismos para a autenticação de usuários, manutenção de segregação de funções, rastreabilidade de acesso e aprovação de acesso, quando aplicável, de forma a garantir procedimentos internos adequados e consistentes.

6.6. Gestão de Riscos

A Instituição possui processo para análise de vulnerabilidades, ameaças e impactos sobre os Ativos de informação para, diante de um incidente, adotar as medidas adequadas para minimizar os danos causados.

Os processos de gestão de riscos englobam os controles de mudanças no ambiente de tecnologia da Instituição, que são estruturados e aplicados através de um conjunto de processos que vão atuar em todas as áreas potencialmente impactadas, bem como a capacitação e o engajamento dos Colaboradores diretamente envolvidos nas ações mitigatórias dentro da Instituição, com o objetivo da preparação para essas situações.

Neste processo, será levado em conta: (i) o levantamento dos impactos organizacionais; (ii) a priorização das ações de mudanças no ambiente de tecnologia da Instituição; (iii) o planejamento; (iv) os testes; (v) a mobilização; (vi) a comunicação; e (vii) os treinamentos contínuos para a devida capacitação das pessoas diretamente envolvidas no processo de gestão de riscos e controle dos respectivos ambientes de tecnologia da Instituição, da seguinte forma:

i. O levantamento dos impactos organizacionais irá detalhar quais áreas da Instituição podem vir a ser impactadas direta e/ou indiretamente;

ii. A priorização das ações de mudanças no ambiente de tecnologia irá avaliar e elencar todas as mudanças que precisam ser implantadas, definindo quais demandas serão tratadas com prioridade e quais poderão ser mitigadas;

iii. O planejamento irá definir os planos de implantação, impactos e correções, visando maximizar a segurança e integridade dos ambientes de tecnologia, e minimizar ao máximo os riscos de ações ineficientes e ineficazes;

iv. Os testes irão monitorar todo o processo e se certificar que tudo está acontecendo conforme o planejamento realizado. Através dos testes serão elaborados relatórios que descreverão os resultados, funcionalidades e correções;

v. A mobilização irá, através do Diretor responsável por esta Política e pela execução do plano de ação e de resposta a incidentes, direcionar a Instituição e todos os Colaboradores ao

encontro do objetivo deste processo da gestão de riscos e de controles de mudanças no ambiente de tecnologia da Instituição;

vi. A comunicação irá informar e detalhar os objetivos da mudança através dos canais de comunicação e do desenvolvimento do plano de comunicação, para que todos os Colaboradores da Instituição tenham conhecimento da relevância e da necessidade do engajamento para o alcance de todas as medidas adequadas e mitigatórias, para neutralizar ou minimizar os eventuais ou potenciais danos;

O treinamento contínuo irá garantir a transferência e o nivelamento de conhecimentos relacionados ao trabalho desenvolvido no processo da gestão de riscos e de controles de mudanças no ambiente de tecnologia da Instituição.

6.7. Gestão de Fornecedores

A Instituição verifica o grau de comprometimento com relação a controles de Segurança da Informação e Segurança Cibernética de todos os seus prestadores de serviços, fornecedores, provedores e parceiros que processam e armazenam dados da Instituição, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

A Instituição deve disponibilizar um canal para que seus prestadores de serviços, fornecedores, provedores e parceiros comuniquem incidentes de Segurança da Informação e Segurança Cibernética que estejam relacionados às informações da Instituição.

6.8. Segurança física do ambiente

A Instituição deve implantar sistema para controle de acesso dos Colaboradores, prestadores de serviços, fornecedores, provedores e parceiros aos locais restritos. Os equipamentos e instalações de processamento de informação crítica ou sensível devem ser mantidos em áreas seguras, com níveis de controle de acesso apropriados, incluindo proteção contra ameaças físicas e ambientais.

6.9. Backup e gravação de LOG

A Instituição deve adotar uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.

A Instituição também deve realizar gravação de logs de dados que permitam a rastreabilidade do acesso e a identificação do criador, data, meios de acessos e informações acessadas. As informações dos logs devem ser protegidas contra alterações e acessos não autorizados.

6.10. Proteção contra vírus, arquivos e softwares maliciosos

A Instituição adotará mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (*phishing, spam* etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a Instituição a vulnerabilidades.

6.11. Testes de varredura para detecção de vulnerabilidade

A Instituição se preocupa em identificar e eliminar as vulnerabilidades de seus sistemas e servidores para assegurar a integridade do ambiente dos processos de negócio. Para tanto, deve promover monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

A Instituição adota processo de atualização periódica de segurança no parque tecnológico, de forma a prevenir vulnerabilidades que possam ocasionar brechas de segurança para ataque de vírus e outros tipos de software, que se propaguem nos computadores, sistemas e servidores da Instituição.

6.12. Criptografia

Os Ativos de informação da Instituição devem possuir criptografia adequada, conforme a classificação da informação, em todo tráfego que ocorrer em rede pública, a fim de se garantir

proteção em todo o ciclo de vida da informação, em conformidade com os padrões de segurança dos órgãos reguladores.

6.13. Plano de continuidade

A Instituição realiza plano de continuidade dos serviços prestados a partir da adoção de um conjunto preventivo de estratégias e planos de ação para garantir que os serviços essenciais da Instituição sejam devidamente identificados e preservados após a ocorrência de uma contingência.

Para tanto, a Instituição realizará o mapeamento de processos críticos, análise de impacto nos negócios e inventário dos cenários de crises cibernéticas relacionados aos incidentes de segurança.

Devem ser aplicados testes de continuidade de negócios e realização testes periódicos para garantir a eficácia e segurança dos processos. O teste deve ser conduzido em um ambiente controlado que permita que a Instituição certifique a conformidade dos planos desenvolvidos com os objetivos da Instituição e requisitos legais.

6.14. Incidentes de segurança

a. Classificação de relevância dos incidentes

A Instituição classificará os incidentes de segurança segundo sua relevância e conforme a classificação das informações envolvidas e o impacto na continuidade de negócios da Instituição.

b. Gestão de incidentes

Todos os incidentes ou suspeita de incidentes identificados por um Colaborador ou cliente devem ser imediatamente comunicados à área responsável. A comunicação deverá ser feita através do e-mail segurança@bezz.com.br.

Os incidentes reportados serão classificados segundo o risco que representam para a Instituição e o impacto na continuidade de negócios da Instituição. Além disso, devem ser devidamente registrados, tratados e comunicados. A Instituição adotará procedimentos para mitigar os efeitos dos incidentes relevantes e a interrupção dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados.

c. Plano de compartilhamento de incidentes

Sem prejuízo do dever de sigilo e da livre concorrência, a Instituição deve adotar iniciativas para o compartilhamento de informações sobre incidentes relevantes com as demais instituições autorizadas a funcionar pelo Bacen, por meio dos canais adotados pelas instituições.

As informações compartilhadas também estarão disponíveis ao Bacen.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, a Instituição comunicará o Bacen e adotará medidas necessárias para que as suas atividades sejam reiniciadas, informando o prazo para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos, estabelecendo e documentando os critérios que configuraram a situação de crise.

d. Plano de ação e de resposta a incidentes

A Instituição deve estabelecer plano de ação e de resposta a incidentes visando à implantação desta Política, que abrange, minimamente:

- As ações a serem desenvolvidas para adequar as estruturas organizacional e operacional às diretrizes desta Política;
- As rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes.

e. Relatório anual de incidentes

A Instituição deve elaborar relatório anual sobre a implantação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro. O relatório abordará:

- A efetividade da implantação das ações de adequação de suas estruturas organizacional e operacional;
- O resumo dos resultados obtidos na implantação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta Política;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
- Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

O relatório anual de incidentes deve ser apresentado à Alta Administração da Instituição até 31 de março do ano seguinte ao da data-base.

6.15. Mecanismos de rastreabilidade

A Instituição deve adotar controles específicos para promover a rastreabilidade da informação, principalmente que busquem garantir a segurança das informações sensíveis.

6.16. Registro de impacto

A Instituição deve realizar registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da Instituição, que devem abranger inclusive informações recebidas de empresas prestadoras de serviços a terceiros.

6.17. Treinamentos e conscientização

A Instituição preza por uma cultura de Segurança da Informação e Segurança Cibernética. Dessa forma, devem ser adotados políticas e procedimentos para a difusão dos princípios e diretrizes integrantes desta Política, garantindo-se a capacitação e conscientização para toda a Alta Administração e todos os seus Colaboradores.

A Instituição promoverá a ampla divulgação desta Política a todos os seus Colaboradores e o público em geral, bem como às empresas prestadoras de serviços a terceiros, no que couber, mediante linguagem clara, acessível e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, incluindo a prestação de informações aos usuários finais sobre medidas de precaução para a utilização dos produtos e serviços oferecidos.

Além disto, a Alta Administração da Instituição deverá difundir a cultura de Segurança da Informação e Segurança Cibernética para promover melhorias contínuas em seus processos internos, a fim de evitar quaisquer incidentes relacionados à Segurança da Informação e Segurança Cibernética.

6.18. Contratação de serviços de processamento e armazenamento de dados e computação em nuvem

a. Seleção de terceiros

O processamento e armazenamento de dados e computação em nuvem serão realizados por meio de terceiros localizados no Brasil ou no exterior. A contratação de terceiros deve ser realizada por meio da aferição da capacidade do prestador de serviço para realizar as atividades em cumprimento com a legislação e regulamentação aplicável. Desta forma, a Instituição deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

- O cumprimento da legislação e da regulamentação em vigor;
- O acesso da Instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;
- A confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;
- A aderência do prestador de serviço a certificações exigidas pela Instituição para a prestação do serviço a ser contratado;

- O acesso da Instituição aos relatórios elaborados por empresa de auditoria especializada independente contratada pelo prestador de serviço, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados;
- O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A identificação e a segregação dos dados dos usuários finais da Instituição por meio de controles físicos ou lógicos;
- A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos usuários finais da Instituição.

Na avaliação da relevância do serviço a ser contratado, a Instituição também deve considerar a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado. Todos os procedimentos devem ser documentados.

Ademais, a Instituição deve adotar recursos e medidas necessários para a adequada gestão dos serviços a serem contratados, inclusive para análise de informações e uso dos recursos providos pelo potencial prestador de serviços.

b. Execução de aplicativos pela internet

No caso da execução de aplicativos por meio da internet, a Instituição deve assegurar que o potencial prestador dos serviços adote controles que mitiguem os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

c. Serviços de computação em nuvem

Os serviços de computação em nuvem disponibilizados a Instituição, sob demanda e de maneira virtual, deverão incluir um ou mais serviços conforme descritos abaixo:

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a Instituição implantar ou executar

softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela Instituição ou por ela adquiridos;

- Implantação ou execução de aplicativos desenvolvidos pela Instituição, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços;
- Execução, por meio da internet, dos aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

A Instituição é responsável, em conjunto com o prestador de serviços, pela confiabilidade, pela integridade, pela disponibilidade, pela segurança e pelo sigilo em relação aos serviços contratados, bem como pelo cumprimento da legislação e da regulamentação em vigor.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada pela Instituição ao Bacen.

d. Contratação de serviços de computação em nuvem no exterior

Em caso de contratação de serviços de processamento, armazenamento de dados e de computação em nuvem no exterior, a Instituição deverá observar os seguintes requisitos:

- Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços serão prestados;
- Verificação de que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação do Bacen;
- Definição dos países e regiões em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados. Essa definição deverá ocorrer antes da contratação dos serviços;
- Previsão de alternativas para a continuidade de negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

Caso não haja convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países em que os serviços serão prestados, a Instituição solicitará autorização do Bacen para a contratação do serviço. O prazo para solicitar autorização é de 60 dias anteriores à contratação. Caso haja alterações contratuais que impliquem em modificação das informações, a Instituição deverá solicitar autorização 60 dias antes da alteração contratual.

A Instituição deve assegurar que a legislação e a regulamentação nos países em que os serviços serão prestados não restrinjam ou impeçam o acesso da Instituição e do Bacen aos dados e às informações. A comprovação do atendimento aos requisitos e o cumprimento desta exigência deverão ser documentados.

e. Contrato de prestação de serviços

A Instituição deve assegurar que os contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem prevejam:

- A indicação dos países e da região em cada país em que os serviços serão prestados e os dados armazenados, processados e gerenciados;
- A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
- A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos usuários finais;
- Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou a Instituição, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.
- O acesso da Instituição às informações fornecidas pela empresa contratada; bem como as informações relativas às certificações e aos relatórios de auditoria especializada e informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
- A obrigação da empresa contratada notificar a Instituição sobre a subcontratação de serviços relevantes para a Instituição;

- A permissão de acesso do Bacen aos contratos e acordos firmados para a prestação de serviços, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso aos dados e informações;
- A adoção de medidas pela Instituição, em decorrência de determinação do Bacen;
- A obrigação de a empresa contratada manter a Instituição permanentemente informado sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Em caso de decretação de regime de resolução da Instituição pelo Bacen, o contrato de prestação de serviços deve prever:

- A obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, acordos, documentação e informações referentes aos serviços prestados, dados armazenados e informações sobre seus processamentos, cópias de segurança dos dados e das informações, bem como códigos de acesso, que estejam em poder da empresa contratada;
- A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços. A notificação deverá ocorrer com 30 dias de antecedência da data prevista para a interrupção dos serviços prestados e deverá determinar que:
    - A empresa contratada se obriga a aceitar eventual pedido de prazo adicional de 30 dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução;
    - A notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da Instituição.

f. Comunicação ao Bacen

A comunicação ao Bacen, referente a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, deve conter as seguintes informações:

- O nome da empresa a ser contratada;
- Os serviços relevantes a serem contratados;
- No caso de contratação no exterior, indicação dos locais onde os serviços serão prestados e os dados armazenados, processados e gerenciados.

O prazo para comunicação é de 10 dias, contados a partir da contratação dos serviços. Caso haja alterações contratuais que impliquem em modificação das informações, a comunicação ao Bacen deverá ocorrer em 10 dias contados da alteração contratual, salvo na hipótese prevista no item 18 “d”.

6.19. Continuidade de negócios

No tocante à continuidade de negócios, a Instituição deve assegurar:

- O tratamento dos incidentes relevantes relacionados com o ambiente cibernético;
- Os procedimentos a serem seguidos no caso de interrupção de serviços de processamento e armazenamento de dados e de computação em nuvem contratados, abrangendo cenários que considerem a substituição da empresa contratada e o reestabelecimento da operação normal da Instituição;
- Os cenários de incidentes considerados nos testes de continuidade de negócios.
- O tratamento para mitigar os efeitos dos incidentes relevantes da interrupção dos serviços de processamento, armazenamento de dados e de computação em nuvem contratados;
- O prazo estipulado para reinício ou normalização das suas atividades ou dos serviços relevantes interrompidos;
- A comunicação tempestiva ao Bacen das ocorrências de incidentes relevantes e das interrupções dos serviços, que configurem uma situação de crise pela Instituição, bem como das providências para o reinício das suas atividades;
- Estabelecer e documentar os critérios que configurem a situação de crise.

A Instituição deve instituir mecanismos de acompanhamento e de controle visando a assegurar a implantação e a efetividade desta Política, do plano de ação e de resposta a incidentes e dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Os mecanismos de acompanhamento e controle devem incluir a definição de processos, testes e trilhas de auditoria, bem como a definição de métricas e indicadores adequados e a identificação e a correção de eventuais deficiências.

6.20. Arquivamento de informações

A Instituição deve armazenar em meio físico ou digital, pelo prazo de 5 anos, as seguintes informações:

- O documento relativo à política de Segurança Cibernética;
- O documento relativo ao plano de ação e de resposta a incidentes;
- A ata da reunião com a aprovação da Alta Administração referente a esta Política e ao plano de ação e de resposta a incidentes;
- O relatório anual sobre a implantação do plano de ação e de resposta a incidentes;
- A documentação sobre os procedimentos desta Política;
- A documentação com os critérios que configurem uma situação de crise;
- A documentação no caso de serviços prestados no exterior;
- Os contratos de prestação de serviços;
- Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle, a partir da implantação dos mecanismos mencionados.

7. Versões

versão	data da elaboração/revisão	Alterações
1ª	31/10/2022	Versão inicial
2ª	07/02/2023	Adequação aos requisitos de negócio
3ª	03/06/2024	Revisão anual
4ª	03/06/2025	Revisão anual

Documento aprovado digitalmente por:

Fernando Henrique Schneider

Data da aprovação: 20/10/2025 08:30:23

1783fd3a821428b27b46a4e1da23e9c559bb7a04

Leonardo Conde Villar Schneider

Data da aprovação: 07/11/2025 13:31:23

96fb3ebd6d53b047359082e0bda1cbae49a8405f