POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Iniciador

INICIADOR.COM.BR

Data
01.2026

Classificação
Pública

Versão
5.0

Tipo de Documento
Política

SUMÁRIO

1. APRESENTAÇÃO E OBJETIVO 3
2. DEFINIÇÕES 3
3. ABRANGÊNCIA 4
4. RESPONSABILIDADES 4
5. DIRETRIZES 5
6. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA 6
6.1. Gestão de Ativos 6
6.2. Autenticação 6
6.3. Autorização 6
6.4. Segmentação de Rede 7
6.5. Classificação da Informação 7
6.6. Controle de Acesso 7
6.7. Gestão de Riscos 7
6.8. Gestão de Fornecedores 9
6.9. Segurança Física do Ambiente 9
6.10. Backup e Gravação de LOG 9
6.11. Proteção Contra Vírus, Arquivos e Softwares Maliciosos 9
6.12. Testes de Varredura Para Detecção de Vulnerabilidade 9
6.13. Criptografia 10
6.14. Plano de Continuidade 10
6.15. Mecanismos de Rastreabilidade 11
6.16. Registro de Impacto 11
6.17. Treinamentos e Conscientização 11
7. INCIDENTES DE SEGURANÇA 11
7.1. Classificação de Relevância dos Incidentes 11
7.2. Gestão de Incidentes 12
7.3. Plano de Compartilhamento de Incidentes 12
7.4. Plano de Ação e Resposta a Incidentes 12
7.5. Relatório Anual de Incidentes 12
8. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM 13
8.1. Contratação de Terceiros 13
8.2. Execução de Aplicativos pela Internet 14
8.3. Serviços de Computação em Nuvem 14
8.4. Contratação de Serviços de Computação em Nuvem no Exterior 15
8.5. Contrato de Prestação de Serviços 15
9. ARQUIVAMENTO DE INFORMAÇÕES 17
10. DISPOSIÇÕES GERAIS 17
11. NORMAS APLICÁVEIS 18

1. APRESENTAÇÃO E OBJETIVO

A presente Política de Segurança da Informação e Segurança Cibernética tem o objetivo de estabelecer diretrizes que permitem o **INICIADOR INSTITUIÇÃO DE PAGAMENTO LTDA** (“INICIADOR”), preservar e proteger as informações de seus clientes, funcionários, prestadores de serviços, partes interessadas e do próprio INICIADOR contra ameaças e riscos relacionados à segurança da informação e cibernética, bem como implementar controles e procedimentos que visam a reduzir a vulnerabilidade da Instituição a incidentes; dispõe, também, sobre os requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem.

Ademais, esta política será compatível com:

a. O porte, o perfil de risco e o modelo de negócio do INICIADOR;
b. A natureza das atividades do INICIADOR e a complexidade dos produtos e serviços oferecidos; e
c. A sensibilidade dos dados e das informações sob responsabilidade do INICIADOR.

O Diretor de Tecnologia será responsável por esta Política e pela execução do plano de ação e de resposta a incidentes, o qual poderá desempenhar outras funções no INICIADOR, desde que não haja conflito de interesses.

2. DEFINIÇÕES

Ativos: 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: Formada pelos diretores institucionais do **INICIADOR INSTITUIÇÃO DE PAGAMENTO LTDA** (“INICIADOR”).

Bacen / BCB: Banco Central do Brasil.

Gestão de Ativos: são as boas práticas utilizadas pelo INICIADOR 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: informações que têm valor estratégico para o desenvolvimento dos negócios e das operações do INICIADOR, ganhando tangibilidade por meio de

transações, processamentos, bancos de dados, entre outras formas, e que serão tratados com base no legítimo interesse do INICIADOR, 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 do INICIADOR.

Segurança Cibernética: conjunto de tecnologias e processos desenvolvidos para proteger os sistemas internos, computadores, redes e dados do INICIADOR contra ataques, danos, ameaças ou acesso não autorizado.

3. ABRANGÊNCIA

Esta Política se aplica à Alta Administração, colaboradores e empresas prestadoras de serviço[1] do INICIADOR cujas atividades sejam desempenhadas visando ao desenvolvimento das operações atinentes a esta Política.

4. RESPONSABILIDADES

A implementação, execução e manutenção da presente Política será realizada pelos responsáveis seguintes.

Área de *Compliance*: responsável, em conjunto com o diretor responsável pela execução e manutenção desta Política, pela sua aprovação e atualização periódica.

Diretor de Tecnologia: responsável pela implementação, execução e manutenção da política e pela execução do plano de ação e de resposta a incidentes.

Usuários: Alta Administração e Colaboradores do INICIADOR, que direta ou indiretamente utilizam ou suportam os sistemas, a infraestrutura ou as informações do INICIADOR, 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 do INICIADOR, e mantê-las seguras, íntegras e disponíveis, conforme sua classificação e necessidade.

[1] Quaisquer terceiros que atuem em nome do INICIADOR, tais como Auditoria Externa, Tecnologia da Informação, Infraestrutura de TI, dentre outras.

5. DIRETRIZES

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

a. 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 no INICIADOR;
b. 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. O INICIADOR adotará mecanismos que visam a assegurar a utilização segura de senhas;
c. Qualquer risco à informação deverá ser imediatamente reportado pelo Colaborador por meio dos canais e procedimentos indicados pelo INICIADOR;
d. 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;
e. Assegurar que as informações sejam utilizadas somente para a finalidade para a qual foram coletadas e que o acesso esteja condicionado à autorização;
f. 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, os mecanismos de criptografia, os mecanismos de prevenção e detecção de intrusão, os mecanismos de prevenção de vazamento de informações, os mecanismos de proteção contra softwares maliciosos, os mecanismos de rastreabilidade, a gestão de cópias de segurança dos dados e das informações, a avaliação e a correção de vulnerabilidades dos recursos computacionais e dos sistemas de informação, os controles de acesso, a definição e implementação de perfis de configuração segura de ativos de tecnologia, os mecanismos de proteção de rede, a gestão de certificados digitais, os requisitos de segurança para a integração de sistemas de informação por meio de interfaces eletrônicas e as ações de inteligência no ambiente cibernético, incluindo o monitoramento de informações de interesse da instituição, na Deep Web e na Dark Web, além de grupos privados de comunicação;
g. Assegurar que os controles específicos, incluindo os voltados para a rastreabilidade da informação, garantam, no melhor nível possível, a segurança das informações sensíveis;
h. Assegurar o registro, análise da causa e o impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do INICIADOR;
i. Assegurar a elaboração de cenários de incidentes considerados nos testes de continuidade dos serviços de pagamento prestados;

j. 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 do INICIADOR;
k. Classificar os dados e as informações quanto à relevância;
l. Definir os parâmetros a serem utilizados na avaliação da relevância dos incidentes;
m. Assegurar os mecanismos para disseminação da cultura de segurança cibernética, incluindo (i) a implementação de programas de capacitação e de avaliação periódica de pessoal; (ii) a prestação de informações a usuários finais sobre precauções na utilização de produtos e serviços oferecidos;
n. Estimular iniciativas para compartilhamento de informações sobre incidentes relevantes, com Instituições de Pagamento, instituições financeiras e demais instituições autorizadas a funcionar pelo Bacen;
o. Manter o registro, análise da causa e do impacto, bem como o controle dos efeitos de incidentes de informações recebidas de empresas prestadoras de serviços a terceiros; e
p. Contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pelo INICIADOR e por esta Política.

6. PROCESSO DE SEGURANÇA DA INFORMAÇÃO E CIBERNÉTICA

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, o INICIADOR adotará as seguintes políticas e procedimentos.

6.1. Gestão de Ativos

Os Ativos são 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, por meio de mecanismos de autenticação e autorização de acesso, destinados a impedir o acesso de indivíduos não autorizados.

Os Ativos devem ser utilizados tão somente para a finalidade devidamente autorizada. O INICIADOR 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.

Ainda, a definição e implementação de perfis de configuração segura de ativos de tecnologia preverá:

a. A gestão do ciclo de vida dos recursos computacionais da Instituição;

b. A aplicação regular de correções de segurança;
c. A configuração adequada dos serviços a serem suportados pelos recursos computacionais; e
d. A alteração de senhas e de outros padrões que possam ser utilizados para acessos indevidos aos recursos computacionais.

6.2. Autenticação

O INICIADOR adotará mecanismos para garantir que o acesso às informações e ambientes tecnológicos seja permitido apenas a indivíduos autorizados.

6.3. Autorização

Há processos de autorização levando em consideração o princípio do menor privilégio, a segregação de funções e a classificação da informação.

6.4. Segmentação de Rede

O INICIADOR adota 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 ao departamento de tecnologia da informação, que fará análise e aprovação.

Ainda, haverá o monitoramento de conexões, o qual deverá:
a. Evitar tentativas de conexão com sistemas de informação provenientes de ativos de tecnologia localizados fora da rede corporativa da Instituição;
b. Estabelecer critérios para o estabelecimento e o monitoramento de conexões com ambientes externos, em especial em horário noturno e em dias não úteis;
c. Identificar e prevenir conexões indevidas com ambientes externos à instituição oriundas de recursos tecnológicos da instituição;
d. Realizar a implementação e manutenção de processos e ferramentas para identificação, análise, tratamento e controle de eventos atípicos no ambiente de produção da instituição, abrangendo, como exemplos, o estabelecimento de virtual private networks – VPN e tentativas de acesso privilegiado a recursos computacionais, especialmente em horário noturno e em dias não úteis; e
e. Estabelecer medidas para restringir o acesso a redes corporativas apenas a dispositivos ou ativos de tecnologia devidamente autorizados.

6.5. Classificação da Informação

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

a. **Informação Pública**: aquela que pode ser acessada por todos, sem restrição. São exemplos de Informação Pública: dados divulgados ao mercado e dados promocionais;
b. **Informação Interna**: aquela que pode ser acessada somente por Colaboradores do INICIADOR. São exemplos de Informação Interna: normas, procedimentos e formulários do INICIADOR;
c. **Informação Restrita**: aquela que pode ser acessada somente por colaboradores que precisam dela para desempenhar suas atribuições. São exemplos de Informação Restrita: contratos e documentos estratégicos do INICIADOR; e
d. **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.

6.6. Controle de Acesso

O INICIADOR 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, implementará:

a. Mecanismos para limitar o acesso à rede corporativa a usuários credenciados e a dispositivos autorizados;
b. Revisão periódica e tempestiva das permissões de acesso, em especial de colaboradores terceirizados com acesso aos recursos computacionais da instituição; e
c. Implementação de múltiplos fatores de autenticação para acesso à rede corporativa a partir de ambientes externos à instituição.

6.7. Gestão de Riscos

O INICIADOR 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 do INICIADOR, 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 do INICIADOR, 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 do INICIADOR; (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 do INICIADOR, da seguinte forma:

a. O levantamento dos impactos organizacionais irá detalhar quais áreas do INICIADOR podem vir a ser impactadas direta e/ou indiretamente;
b. A priorização das ações de mudanças no ambiente de tecnologia irá avaliar e elencar todas as mudanças que precisam ser implementadas, definindo quais demandas serão tratadas com prioridade e quais poderão ser mitigadas;
c. O planejamento irá definir os planos de implementação, impactos e correções, visando maximizar a segurança e integridade dos ambientes de tecnologia, e minimizar ao máximo riscos de ações ineficientes e ineficazes;
d. Os testes irão monitorar todo o processo e se certificar que tudo está acontecendo conforme o planejamento realizado. Através dos testes serão elaborados relatórios, os quais serão revisados pelo Diretor responsável pela execução e manutenção desta Política, que descreverão os resultados, funcionalidades e correções;
e. A mobilização irá, através do Diretor responsável por esta Política de segurança cibernética e pela execução do plano de ação e de resposta a incidentes, direcionar o INICIADOR e todos os Colaboradores ao encontro do objetivo deste processo da gestão de riscos e de controles de mudanças no ambiente de tecnologia do INICIADOR; e
f. 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 do INICIADOR 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 do INICIADOR.

6.8. Gestão de Fornecedores

O INICIADOR 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 do

INICIADOR, com a finalidade de verificar o nível de maturidade dos controles de segurança e o plano de tratamento de incidentes adotados.

6.9. Segurança Física do Ambiente

O INICIADOR possui 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.

6.10. Backup e Gravação de LOG

O INICIADOR adota uma rotina de backup e restauração de dados para assegurar a disponibilidade das informações relevantes para o pleno funcionamento de suas atividades.

Sendo assim, realiza 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.

6.11. Proteção Contra Vírus, Arquivos e Softwares Maliciosos

O INICIADOR adota mecanismos para prevenir que vírus e outros tipos de software e condutas maliciosas (e.g., *phishing*, *spam* etc.) se propaguem nos computadores, sistemas e servidores internos ou exponham a Instituição a vulnerabilidades. Para tanto, os softwares de segurança, como o antivírus, devem estar instalados e atualizados em toda a rede interna do INICIADOR.

6.12. Testes de Varredura Para Detecção de Vulnerabilidade

O INICIADOR se preocupa em identificar e eliminar as vulnerabilidades de seus sistemas e servidores para assegurar a integridade do ambiente dos processos de negócio. Assim, através de alertas, *dashboards* e ferramentas para verificar vulnerabilidades e variabilidades, promove monitoramento constante e condução de testes e varredura para detecção de vulnerabilidades, avaliação de riscos e determinação de medidas de correção adequadas.

Ressalta, ainda, que tais procedimentos e controles abrangem, dentre outros, os seguintes requisitos: 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.

Adota, também, 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 do INICIADOR.

6.13. Criptografia

Os Ativos de informação do INICIADOR 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.

6.14. Plano de Continuidade

O INICIADOR 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 do INICIADOR sejam devidamente identificados e preservados após a ocorrência de uma contingência.

Para tanto, o INICIADOR realizará:

a. Testes e análises periódicos para detecção de vulnerabilidades em sistemas de informação;
b. Varreduras periódicas dos recursos tecnológicos com o objetivo de identificar dispositivos indevidamente conectados à rede corporativa que possam estabelecer conexão com ativos de tecnologia externos à instituição;
c. Análises periódicas dos recursos tecnológicos com o objetivo de identificar vulnerabilidades que possam comprometer a segurança dos ativos de tecnologia da instituição;
d. Testes de intrusão; e
e. Correção tempestiva das vulnerabilidades identificadas.

6.15. Mecanismos de Rastreabilidade

O INICIADOR adota controles específicos para promover a rastreabilidade da informação, principalmente buscando garantir a segurança das informações sensíveis.

Os mecanismos de rastreabilidade devem abranger a rastreabilidade de transações e operações, contemplando, no mínimo:

a. Trilhas de auditoria do processamento fim a fim dos dados e das informações, incluindo a definição e a geração de logs que possibilitem identificar falhas de processamento ou comportamentos atípicos, bem como subsidiar análises;
b. Definição de tempo de retenção de informações de acordo com o tipo de processamento realizado; e
c. Retenção segura das trilhas de auditoria.

6.16. Registro de Impacto

O INICIADOR realiza o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades do INICIADOR, abrangendo, inclusive, informações recebidas de empresas prestadoras de serviços a terceiros.

6.17. Treinamentos e Conscientização

O INICIADOR preza por uma cultura de Segurança da Informação e Segurança Cibernética. Dessa forma, são 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.

O INICIADOR 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 do INICIADOR 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 relacionado à Segurança da Informação e Segurança Cibernética.

7. INCIDENTES DE SEGURANÇA

7.1. Classificação de Relevância dos Incidentes

O INICIADOR classifica os incidentes de segurança segundo sua relevância, bem como a classificação das informações envolvidas e o impacto na continuidade de seus negócios.

Assim, no dia a dia da Instituição, são utilizados diversos parâmetros para a avaliação de incidentes, tais como: (i) falta de conectividade; (ii) acesso negado; (iii) *ransomware*; (iv) entre outros.

7.2. Gestão de Incidentes

Todos os incidentes ou suspeitas de incidentes identificados por um Colaborador, cliente, prestador de serviços, fornecedor, provedor ou parceiro devem ser imediatamente comunicados à área responsável. A comunicação deverá ser feita por meio dos canais indicados pelo INICIADOR ou através do e-mail security@iniciador.com.br

Os incidentes reportados serão classificados segundo o risco que representam para o INICIADOR e o impacto na continuidade de seus negócios. Além disso, devem ser devidamente registrados, tratados e comunicados.

O INICIADOR 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.

7.3. Plano de Compartilhamento de Incidentes

Sem prejuízo do dever de sigilo e da livre concorrência, o INICIADOR adota iniciativas para o compartilhamento de informações sobre incidentes relevantes com outras Instituições de Pagamento por meio dos canais adotados pelas instituições.

As informações compartilhadas também estarão disponíveis ao Bacen.

Caso haja incidentes relevantes ou interrupção dos serviços relevantes, o INICIADOR 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.

7.4. Plano de Ação e Resposta a Incidentes

O INICIADOR possui plano de ação e de resposta a incidentes visando à implementação desta Política, o qual abrange:

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

7.5. Relatório Anual de Incidentes

O INICIADOR elabora relatório anual sobre a implementação do plano de ação e de resposta a incidentes, com data-base de 31 de dezembro, o qual aborda:

a. A efetividade da implementação das ações de adequação suas estruturas organizacional e operacional, com o objetivo de adequar suas estruturas organizacional e operacional aos princípios e às diretrizes desta Política;
b. O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e das tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as rotinas, os procedimentos, os controles e as tecnologias a serem utilizados na prevenção e na resposta a incidentes, em conformidade com as diretrizes desta Política;
c. Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;
d. Os resultados dos testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes; e
e. Os resultados dos testes de intrusão e dos testes, varreduras e análises periódicas para detecção de vulnerabilidades e os planos de ação estabelecidos para as suas correções.

8. CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E COMPUTAÇÃO EM NUVEM

8.1. Contratação de Terceiros

O processamento e armazenamento de dados e computação em nuvem será realizado 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, o INICIADOR deve adotar procedimentos para verificação da capacidade do potencial prestador de serviço de forma a assegurar:

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

e. O acesso do INICIADOR 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;
f. O provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;
g. A identificação e a segregação dos dados dos clientes e dos usuários finais do INICIADOR por meio de controles físicos ou lógicos; e
h. A qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes e dos usuários finais do INICIADOR.

Na avaliação da relevância do serviço a ser contratado, será considerada a criticidade do serviço e a sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação dos dados e informações quanto à sua relevância. Todos os procedimentos devem ser documentados.

Ademais, o INICIADOR adota os recursos e medidas necessários para a adequada gestão dos serviços contratados ou a serem contratados futuramente, inclusive para análise de informações e uso dos recursos providos pelo potencial prestador de serviços.

8.2. Execução de Aplicativos pela Internet

No caso da execução de aplicativos por meio da internet, qual seja, aqueles implantados ou desenvolvidos pelo prestador de serviço, com a utilização de seus próprios recursos computacionais, o INICIADOR deve assegurará que o potencial prestador dos serviços adote controles que mitigam os efeitos de eventuais vulnerabilidades na liberação de novas versões do aplicativo.

8.3. Serviços de Computação em Nuvem

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

a. Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam ao INICIADOR implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pelo INICIADOR ou por ele adquiridos;
b. Implantação ou execução de aplicativos desenvolvidos pelo INICIADOR, ou por ele adquiridos, utilizando recursos computacionais do prestador de serviços; e/ou

c. Execução, por meio da internet, de aplicativos implantados ou desenvolvidos pelo prestador de serviço, com a utilização de recursos computacionais do próprio prestador de serviços.

O INICIADOR é responsável 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 será comunicada pelo INICIADOR ao Bacen, o qual poderá vetar ou impor restrições para a contratação quando constatar, a qualquer tempo, violação à Regulamentação.

8.4. 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, o INICIADOR deverá observar os seguintes requisitos:

a. Existência de convênio para troca de informações entre o Bacen e as autoridades supervisoras dos países onde os serviços serão prestados;
b. Verificação de que a prestação dos serviços não causará prejuízos ao seu regular funcionamento nem embaraço à atuação do Bacen;
c. Definição, previamente à contratação, dos países e regiões em cada país em que os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;
d. Previsão de alternativas para a continuidade 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, o INICIADOR solicitará, com 60 (sessenta) dias de antecedência, autorização do Bacen para a contratação do serviço. O mesmo se dará no caso de qualquer alteração contratual que implique em modificação de informações referentes: (i) a denominação da empresa contratada; (ii) os serviços relevantes contratados; e/ou (iii) a indicação dos países e das regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados.

O INICIADOR assegurará que a legislação e a regulamentação nos países em que os serviços serão prestados não restrinjam ou impeçam o acesso do INICIADOR e do Bacen aos dados e às informações. A comprovação do atendimento aos requisitos e o cumprimento desta exigência serão devidamente documentados.

8.5. Contrato de Prestação de Serviços

O INICIADOR assegurará que os contratos de prestação de serviços de processamento, armazenamento de dados e computação em nuvem prevejam:

a. A indicação dos países e da região em cada país em que os serviços poderão ser prestados e os dados armazenados, processados e gerenciados;
b. A adoção de medidas de segurança para a transmissão e armazenamento dos dados;
c. A manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes e dos usuários finais;
d. Em caso de extinção do contrato, a obrigatoriedade de transferência dos dados ao novo prestador de serviços ou ao INICIADOR, bem como a exclusão dos dados pela empresa contratada substituída, após a transferência destes e a confirmação da integridade e da disponibilidade dos dados recebidos;
e. O acesso do INICIADOR 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;
f. A obrigação de a empresa contratada notificar o INICIADOR sobre a subcontratação de serviços relevantes para a Instituição;
g. A permissão de acesso do Bacen aos contratos e aos acordos firmados para a prestação de serviços, à documentação e às informações referentes aos serviços prestados, aos dados armazenados e às informações sobre seus processamentos, às cópias de segurança dos dados e das informações, bem como aos códigos de acesso aos dados e às informações;
h. A adoção de medidas pelo INICIADOR, em decorrência de determinação do Bacen;
i. A obrigação de a empresa contratada manter o INICIADOR 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 do INICIADOR pelo Bacen, o contrato de prestação de serviços deve prever:

a. 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; e

b. 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 (i) 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; (ii) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência do INICIADOR.

9. ARQUIVAMENTO DE INFORMAÇÕES

O INICIADOR armazenará, em meio físico ou digital, pelo prazo de 5 (cinco) anos, as seguintes informações:

a. Todas as versões das políticas de Segurança Cibernética aplicadas no período;
b. Todos os Planos de Ação e de Resposta a Incidentes aplicados no período;
c. Todos os relatórios anuais sobre a implementação do plano de ação e de resposta a incidentes apresentados no período;
d. A documentação referente à contratação de serviços relevantes de processamento e armazenamento de dados e computação em nuvem, inclusive aquelas que contemplem o procedimento de verificação da capacidade do prestador de serviço exigidos;
e. No caso de contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a documentação que comprove os requisitos exigidos;
f. Os contratos referentes a prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, sendo contado o prazo do arquivamento a partir de sua extinção;
g. Os dados, os registros e as informações relativas aos mecanismos de acompanhamento e controle para assegurar a implementação e a efetividade da presente 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, sendo contado o prazo do arquivamento a partir de sua implementação; e
h. A documentação referente a ocorrência de incidentes relevantes e interrupções dos serviços relevantes de processamento, armazenamento de dados e de computação em nuvem contratados, que configurem situação de crise.

10. DISPOSIÇÕES GERAIS

Esta Política foi elaborada pela Área de Compliance e aprovada pela Alta Administração, e será revisada com a periodicidade mínima anual.

Os colaboradores do INICIADOR devem aderir formalmente por meio de um termo em que se comprometem a agir de acordo com esta Política.

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

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

Esta Política está disponível em local acessível a todos os colaboradores, em linguagem clara e acessível.

11. NORMAS APLICÁVEIS

Resolução BCB nº 85/2021: 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 de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.

Resolução BCB n° 538/2025: Altera a Resolução BCB nº 85, de 8 de abril 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 de pagamento, pelas sociedades corretoras de títulos e valores mobiliários, pelas sociedades distribuidoras de títulos e valores mobiliários e pelas sociedades corretoras de câmbio autorizadas a funcionar pelo Banco Central do Brasil.

As leis e normas acima são citadas de forma exemplificativa, e não esgotam toda a Legislação Aplicável às atividades do INICIADOR quanto à segurança.

As regras são citadas para o conhecimento dos colaboradores, sendo a Área de *Compliance* responsável por verificar eventuais atualizações, revogações ou a publicação de novas normas. No caso de novas normas virem a demandar alterações a esta Política, o INICIADOR promoverá a sua revisão.