querocred

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

Comentado [1]: As alterações realizadas nessa versão da PSI visam tornar o documento seguro para compartilhamento público, em cumprimento do art. 5º da Resolução CMN n° 4.893 de 26/2/2021.
Nesse sentido, foram retiradas informações internas referentes a divisão de responsabilidades, grupos operacionais, ferramentas e sistemas utilizados.
As informações excluídas da "versão pública" não implicam em retirada da sua versão completa, para uso interno ou para parceiros (mediante assinatura de NDA).

Sumário

POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

1. OBJETIVO

Em atenção à Resolução nº 4.893, de 26 de fevereiro 2021, do Conselho Monetário Nacional e à Lei n. 13.709/2018, este documento apresenta de forma pública o resumo contendo as linhas gerais dos princípios, conceitos, valores e práticas a serem adotados visando assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2. PÚBLICO-ALVO

Este documento será aplicado a todos os sócios, administradores, colaboradores, empregados ou não, menores aprendizes, estagiários, correspondentes, prestadores de serviços a terceiros e todas e quaisquer pessoas que tenham acesso aos dados da instituição ou por ela controlados e aos sistemas por ela utilizados.

3. REFERÊNCIAS NORMATIVAS

A presente Política deve ser lida e interpretada em conjunto com os seguintes documentos:

3.1. Normas Externas:

I. Resolução nº 4.557, de 23 de fevereiro de 2017, do Conselho Monetário Nacional: Dispõe sobre a estrutura de gerenciamento de riscos, a estrutura de gerenciamento de capital e a política de divulgação de informações.

II. LEI Nº 12.414, DE 9 DE JUNHO DE 2011: Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

III. LEI Nº 12.527, DE 18 DE NOVEMBRO DE 2011: Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5

de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências.

IV. DECRETO Nº 8.771, DE 11 DE MAIO DE 2016: Regulamenta a Lei nº 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações.

V. LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990: Dispõe sobre a proteção do consumidor e dá outras providências.

VI. LEI Nº 12.965, DE 23 DE ABRIL DE 2014: Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

VII. LEI N º 10.406, DE 10 DE JANEIRO DE 2002: Institui o Código Civil.

VIII. LEI COMPLEMENTAR Nº 105, DE 10 DE JANEIRO DE 2001: Dispõe sobre o sigilo das operações de instituições financeiras e dá outras providências

IX. Resolução CMN n° 4.893 de 26/2/2021: 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 autorizadas a funcionar pelo Banco Central do Brasil.

3.2. Normas Internas

I. Código de Ética e Conduta;

II. Plano de Continuidade de Negócios;

III. Política de Gerenciamento de Risco e Gerenciamento de Capital;

IV. Declaração de Apetite ao Risco (RAS);

4. DOS PRINCÍPIOS

As ações da Instituição regem-se pelos seguintes princípios:

I. Confidencialidade: princípio de segurança da informação que garante que a informação seja acessada somente por pessoas ou processos que tenham autorização para acessá-las. Pressupõe a limitação do acesso à informação, sendo permitido o acesso somente às

pessoas autorizadas e em circunstâncias que se apresentem efetivamente necessário o acesso, protegendo informações que devem ser acessíveis apenas por um determinado grupo de usuários contra acessos não autorizados.

II. Disponibilidade: princípio de segurança da informação que garante que as informações estejam acessíveis às pessoas e aos processos autorizados, no momento requerido. Pressupõe a garantia de acesso das pessoas devidamente autorizadas à informação sempre que o acesso for necessário, prevenindo interrupções das operações da Instituição por meio de um controle físico e técnico das funções dos sistemas de dados, assim como a proteção dos arquivos, seu correto armazenamento e a realização de cópias de segurança.

III. Integridade: princípio de segurança da informação que garante a não-violação das informações com intuito de protegê-las contra alteração, gravação ou exclusão acidental ou proposital. Pressupõe a garantia da veracidade, fidelidade e integridade da informação e dos métodos de seu processamento e eventual tratamento da informação, pois esta não deve ser alterada enquanto está sendo transferida ou armazenada, impedindo que a informação fique exposta ao manuseio por uma pessoa não autorizada e impedindo, também, alterações não aprovadas e sem o controle do controlador (corporativo ou privado) da informação.

5. RESPONSABILIDADES

As atribuições e divisões de responsabilidades nos procedimentos e processos de Segurança Cibernética são realizados conforme determinado pel o art. 3º §2º da Resolução nº 4.893 do Banco Central do Brasil.

6. DAS DIRETRIZES DE SEGURANÇA CIBERNÉTICA

A Segurança Cibernética na Instituição segue as seguintes diretrizes:

a) As informações da Instituição, dos clientes e do público em geral devem ser tratadas de forma ética e sigilosa e de acordo com as leis vigentes e normas internas, evitando-se mau uso e exposição indevida.

b) As informações e os dados devem ser utilizados de forma transparente e apenas para as finalidades para as quais foram coletadas.

c) Os procedimentos e os controles deverão abranger 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 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.

d) A identificação daqueles que têm acesso às informações da Instituição deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas.

e) Somente deve ter concedido acesso às informações e recursos de informação imprescindíveis para o pleno desempenho das suas atividades do indivíduo autorizado

f) A senha é utilizada como assinatura eletrônica, sendo pessoal e intransferível, e deve ser mantida secreta, sendo proibido seu compartilhamento.

g) Devem ser reportados à área de Tecnologia da Informação da Instituição os riscos às informações, bem como eventuais fatos ou ocorrências que possam colocar em risco tais informações, que será responsável pelo registro e controle dos efeitos de incidentes relevantes.

h) As responsabilidades quanto à Segurança Cibernética devem ser amplamente divulgadas a todos aqueles considerados público-alvo desta política, que devem entender e assegurar o cumprimento do aqui disposto.

6.1. Das diretrizes para tratamento da Informação

A informação deve receber proteção adequada em observância aos princípios e diretrizes da Segurança Cibernética e da Informação da Instituição em todo o seu ciclo de vida, que compreende: Geração, Manuseio, Armazenamento, Transporte e Descarte.

6.2. Das diretrizes para classificação de dados e das informações

As informações e os dados sob responsabilidade da instituição serão classificados para adequação das estruturas organizacional e operacional aos princípios e às diretrizes da política de segurança cibernética, considerando a relevância, a confidencialidade e as proteções necessárias.

A divulgação desses dados é proibida, salvo se solicitada por órgãos fiscalizadores competentes, tais como o Banco Central do Brasil, a Receita Federal do Brasil e a Comissão de Valores Mobiliários ou por decisão judicial.

Os dados pessoais sensíveis deverão ser protegidos de forma mais rígida, incluindo inciativas de rastreabilidade da informação e controle de acesso diferenciado, devendo ser compatível com as funções desempenhadas e com a sensibilidade das informações. Para isso, devem ser consideradas as necessidades relacionadas ao negócio, o compartilhamento ou restrição de acesso e os impactos no caso de utilização indevida das informações.

Uma vez classificada a informação deve ser protegida e receber tratamento e armazenamento adequados.

6.3. Das diretrizes para a elaboração de cenários de incidentes considerados nos testes de continuidade de negócios:

Deverão ser elaborados, no âmbito dos testes de continuidade de negócios, cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados pela instituição, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição.

Deverão ser consideradas para a elaboração desses cenários a ausência de ativos, humanos ou tecnológicos, que assegurem à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados.

6.4. Das diretrizes para a definição de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços

Na elaboração de procedimentos e de controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços, considerando as características do serviço a ser prestado e níveis de complexidade, abrangência e precisão, deverão ser analisados cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados.

Uma vez identificados os possíveis cenários serão analisados os controles voltados à prevenção e ao tratamento dos incidentes já utilizados pela prestadora, e, caso necessário, deverão ser estabelecidos com a respectiva prestadora de serviços outros procedimentos e controles prevenção e ao tratamento dos incidentes a serem adotados, de forma a suprir as possíveis lacunas relativas à prevenção, detecção e

redução da vulnerabilidade a incidentes relacionados com o ambiente cibernético.

6.5. Das diretrizes para definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes

Os parâmetros a serem utilizados na avaliação da relevância dos incidentes deverão considerar a frequência e o impacto dos cenários de incidentes que impliquem em dano ou perigo de dano à confiabilidade, à integridade, à disponibilidade, à segurança e ao sigilo dos dados e dos sistemas de informação utilizados, que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição.

6.6. Dos critérios para configuração de situação de crise

A Instituição adota os critérios, independente de cumulação, para configuração de situação de crise conforme disposto no parágrafo único do art. 20 da Resolução CMN n° 4.893 de 26/2/2021.

Critérios relacionados à segurança e ao sigilo dos dados e dos sistemas de informação utilizados

A Instituição adota os critérios estabelecidos no art. 48 da LGPD para avaliação da situação de crise e incidentes de segurança relacionados à segurança e ao sigilo dos dados e dos sistemas de informação utilizados.

7. PROCEDIMENTOS E OS CONTROLES

Para reduzir a vulnerabilidade da instituição a incidentes e atender aos demais objetivos de segurança cibernética, a instituição, inclusive, no desenvolvimento de sistemas de informação seguros e na adoção de novas tecnologias, adotará os seguintes procedimentos e os controles:

7.1. Autenticação

Em segurança da informação, a autenticação é um processo que busca verificar a identidade digital do usuário de um sistema, normalmente, no momento em que ele requisita um log in (acesso) em um programa ou computador. A autenticação normalmente depende de um ou mais "fatores de autenticação".

7.2. Criptografia

A criptografia é um conjunto de técnicas que transformam dados em códigos que só podem ser decifrados por quem tenha a chave de acesso.

Assim, a criptografia garante a proteção dessas informações e permite que apenas quem tem direito

cedido de acesso (autenticação) consiga visualizar seu conteúdo.

7.3. Prevenção e detecção de intrusão

Os Sistemas de Detecção de Intrusão (IDS) analisam o tráfego da rede em busca de assinaturas que correspondam a ciberataques conhecidos. Os Sistemas de Prevenção de Intrusões (IPS) também analisam pacotes, mas podem impedir que esses pacotes sejam entregues com base nos tipos de ataques detectados – ajudando a interromper o ataque.

Basicamente, ambos são partes da infraestrutura de rede e comparam pacotes de rede em um banco de dados de ameaças cibernéticas, contendo assinaturas conhecidas e sinaliza todos os pacotes correspondentes.

A principal diferença entre eles é que o IDS é um sistema de monitoramento, enquanto o IPS é um sistema de controle de intrusão. O IDS não altera os pacotes de rede de nenhuma maneira, já o IPS impede que o pacote seja entregue com base em seu conteúdo, da mesma forma como um firewall impede o tráfego por endereço IP.

7.4. Prevenção de vazamento de informações

Esta instituição também utiliza política de prevenção contra perda de dados (DLP) para prevenção de vazamento de informações bem como todos mecanismos de sigilo e proteção de dados em datas centers homologados pelo Bacen, com atendimento a todas as regras normativas de compliance e segurança da informação.

7.5. Testes e varreduras periódicos para detecção de vulnerabilidades

Esta instituição conta com varreduras periódicas verificando controle de dispositivos e web.

7.6. Proteção contra software malicioso

Esta instituição conta com procedimentos para proteção contra ameaça de arquivo, proteção contra ameaça de web, proteção contra ameaça de rede e proteção AMSI.

7.7. Mecanismos de rastreabilidade para informações sensíveis

O acesso e o uso de todos os sistemas de informação, diretórios de rede, bancos de dados e demais recursos devem ser restritos a pessoas autorizadas responsáveis conforme a necessidade mínima ao cumprimento de suas funções e são rastreados através de logs fornecidos pelos Sistemas de

Informação e mecanismos de prevenção a vazamentos de dados.

7.8. Controles de acesso

Esta Instituição utiliza mecanismos de controle de acesso por autenticação, permitindo que apenas usuários autorizados possam acessar as informações devidamente autorizad as.

7.9. Segmentação da rede de computadores

A segmentação de rede é uma estratégia de segurança muito utilizada para proteger os dados de ataques cibernéticos. Ela permite a divisão da rede em subseções para que seja possível controlar a concessão de acessos dos usuários de acordo com suas necessidades no trabalho.

7.10. Manutenção de cópias de segurança dos dados e das informações

Esta instituição instituiu a política de backup, para uso interno, na qual são registradas todas as decisões sobre armazenamento de dados. Assim são definidos:

- quais são os dados a serem copiados;
- frequência de realização do processo;
- tipo de backup a ser realizado;
- métricas de avaliação do processo;
- funcionários envolvidos no processo.

7.11. Registro, análise da causa e do impacto e controle dos efeitos de incidentes relevantes

Para que seja possível a melhoria contínua dos procedimentos relacionados à segurança cibernética, permitindo que sejam realizadas as adequações necessárias à correção de vulnerabilidades nas medidas e procedimentos relativos à segurança cibernética, deve ser realizado o registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição, abrangendo, inclusive, informações recebidas de empresas prestadoras de serviços a terceiros, sendo elaborado relatório próprio pela área responsável.

7.12. Gestão de Prestadores de Serviço

Quando da contratação de prestadores de serviço, inclusive serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, a instituição confirmará que a prestadora mantém o cumprimento das conformidades mínimas exigidas.

7.12.1. Abrangência

Devem ser consideradas para fins de aplicação do disposto nesta política aquelas empresas prestadoras de serviços a terceiros que tiverem acesso:

I. aos dados da instituição, ou por ela controlados; ou
II. aos sistemas por ela utilizados; ou
III. aos ambientes físicos ou tecnológicos, que possam ser utilizados para acessar aos dados e sistemas de que tratam os incisos I e II.

7.12.2. Cláusulas contratuais

Os contratos com empresas prestadoras de serviços a terceiros deverão conter cláusulas de confidencialidade e responsabilidades entre as partes, bem como cláusulas que garantam que os profissionais das empresas prestadoras de serviços a terceiros:

I. Protejam e zelem pelo sigilo das informações da Instituição.
II. Tenham conhecimento e cumpram esta política.
III. Cumpram as leis e normas que regulamentam a propriedade intelectual e a proteção de dados, especialmente a Lei nº 13.709/18 (Lei Geral de Proteção de Dados Pessoais) e a Resolução nº 4.893 do Banco Central do Brasil.
IV. Utilizem os dados da instituição, ou por ela controlados, os sistemas por ela utilizados, bem como os ambientes físico e tecnológico da Instituição, apenas para as finalidades objeto do contrato de prestação de serviço.
V. Comuniquem imediatamente qualquer violação desta Política e/ou outras Normas.

7.12.3. Procedimentos e controles voltados à prevenção e ao tratamento dos incidentes a serem adotados por empresas prestadoras de serviços a terceiros

A instituição somente contratará prestadores de serviços que demonstrarem a adoção dos seguintes mecanismos de prevenção e tratamento de incidentes:

1. Adoção de software de proteção contra softwares maliciosos, mantendo-o sempre ativado e atualizado;
2. Adoção de Firewall, mantendo-o sempre ativado e atualizado;
3. Adoção de processo de manutenção de cópias de segurança dos dados e das informações, seja ele realizado para servidor físico ou em nuvem, a ser executado no mínimo

semanalmente;

4. Adoção de mecanismos de controles de acesso e de autenticação que permitam identificar e rastrear o usuário que tiver acesso aos sistemas ou dados da instituição e seus clientes no ambiente cibernético;
5. Adoção de mecanismos de criptografia que permitam criptografar os dados pessoais de clientes e os dados pertencentes à instituição armazenados pelo prestador de serviço ou enviado por meios de comunicação;
6. Adoção de mecanismos de segmentação da rede pela qual o prestador de serviço acessa aos sistemas ou dados da instituição ou dos clientes da instituição;

8. TESTES DE INSTRUSÃO (PENTEST)

A Instituição deverá realizar testes de intrusão (pentests) como controle técnico obrigatório de sua estratégia de segurança cibernética, em conformidade com a Resolução CMN nº 4893/2021, conforme atualizada.

Os testes de penetração devem ser conduzidos por profissionais ou empresas especializadas independentes, sem vínculo funcional ou comercial com as equipes responsáveis pela infraestrutura avaliada, garantindo a imparcialidade técnica dos resultados. A contratação de executores externos deverá observar os critérios de gestão de terceiros estabelecidos nesta Política, incluindo a assinatura de acordos de confidencialidade (NDA) e cláusulas de responsabilidade.

9. PROCEDIMENTO DE CONTRATAÇÃO DE SERVIÇOS RELEVANTES DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM

Quando da contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, além das práticas de governança corporativa e de gestão referidas acima, a instituição adotará as práticas de governança corporativa e de gestão estabelecidas no art. 12 da Resolução CMN n° 4.893 de 26/2/2021.

Além dos serviços relevantes de processamento e armazenamento de dados, para fins desta política os serviços de computação em nuvem abrangem a disponibilidade à instituição, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

I. processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam à instituição contratante implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos desenvolvidos pela

instituição ou por ela adquiridos;

II. implantação ou execução de aplicativos desenvolvidos pela instituição contratante, ou por ela adquiridos, utilizando recursos computacionais do prestador de serviços; ou

III. 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.

Devem ser documentadas as práticas de governança corporativa e de gestão adotadas em relação a cada prestador de serviço contratado, proporcionais à relevância do serviço a ser contratado e aos riscos aos quais a instituição se expõe.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem deve ser comunicada ao Banco Central do Brasil, nos termos do art. 15 da Resolução CMN n° 4.893 de 26/2/2021.

10. COMUNICAÇÃO DE INCIDENTES DE SEGURANÇA À AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS

A instituição comunicará à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares dos dados a ocorrência de incidente de segurança, seja ele relativo ao ambiente cibernético ou não, que possa acarretar risco ou dano relevante aos titulares.

A referida comunicação deverá ser feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, conforme disposto no art. 48 da LGPD, no mínimo:

I. a descrição da natureza dos dados pessoais afetados;

II. as informações sobre os titulares envolvidos;

III. a indicação das medidas técnicas e de segurança utilizadas para a proteção dos dados, observados os segredos comercial e industrial;

IV. os riscos relacionados ao incidente;

V. a causa do incidente;

VI. o impacto do incidente;

VII. os motivos da demora, no caso de a comunicação não ter sido imediata; e

VIII. as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do incidente.

11. COMUNICAÇÃO DE INCIDENTES RELEVANTES RELACIONADOS AO AMBIENTE CIBERNÉTICO AO BANCO CENTRAL DO BRASIL

A instituição comunicará ao Banco Central do Brasil as ocorrências de incidentes relevantes e das interrupções dos serviços relevantes que configurem uma situação de crise pela instituição financeira, bem como das providências para o reinício das suas atividades, mencionando, no mínimo, os itens descritos no item 9 desta política.

12. MECANISMOS PARA DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA NA INSTITUIÇÃO

Para a disseminação da cultura de segurança cibernética a instituição adotará os seguintes mecanismos:

I. a instituição promoverá a disseminação dos princípios e diretrizes da Segurança Cibernética por meio de programas de conscientização, capacitação e avaliação periódicas de pessoal.

II. a política e as regras de segurança da informação e segurança cibernética serão divulgadas e compartilhadas com todo o público alvo desta política, e devem ser disponibilizadas de maneira que seu conteúdo possa ser consultado a qualquer momento, protegidas contra alterações.

III. a prestação, na página da instituição na internet, de informações a clientes e usuários sobre precauções na utilização de produtos e serviços financeiros

IV. a divulgação ao público, na página da instituição na internet, de resumo contendo as linhas gerais da política de segurança cibernética.

13. PROGRAMA DE SEGURANÇA CIBERNÉTICA

Conforme sua criticidade, o programa de segurança cibernética divide-se em:

Ações críticas: Correções emergências e imediatas para mitigar riscos iminentes.

Ações de Sustentação: Iniciativas de curto / médio prazo, para mitigação de risco no ambiente atual, mantendo o ambiente seguro e permitindo que ações de longo prazo/estruturantes possam ser realizadas.

Ações Estruturantes: Iniciativas de médio / longo prazo que tratam a causa raiz dos riscos, voltadas para o futuro da Instituição.

14. GOVERNANÇA COM AS ÁREAS DE NEGÓCIO E TECNOLOGIA

As iniciativas e projetos das áreas de negócio e tecnologia devem estar alinhadas com as diretrizes e

arquiteturas da Segurança Cibernética, garantindo a confidencialidade, integridade e disponibilidade das informações.

15. SEGURANÇA NO DESENVOLVIMENTO DE SISTEMAS DE APLICAÇÃO

O processo de desenvolvimento de sistemas de aplicação deve garantir a aderência às políticas de segurança da instituição e às boas práticas de segurança.

16. RELATÓRIO ANUAL SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES

A Instituição elaborará relatório anual sobre a implementação do plano de ação e de resposta a incidentes, tendo como data-base o dia 31 de dezembro de cada ano.

17. MANUTENÇÃO DE DOCUMENTAÇÃO

Devem ficar à disposição do Banco Central do Brasil pelo prazo de cinco anos:

I. o documento relativo à política de segurança cibernética;
II. o documento relativo ao plano de ação;
III. o documento relativo ao plano de resposta a incidentes;
IV. os relatórios anuais de que trata esta política;
V. a documentação referente às práticas de governança corporativa e de gestão e a verificação da capacidade do potencial prestador de serviço;
VI. os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem, contado o prazo a partir da extinção do contrato.
VII. os dados, os registros e as informações relativas aos mecanismos de acompanhamento e de controle da implementação e da efetividade:
    a. da política de segurança cibernética, contado o prazo a partir da implementação;
    b. do plano de ação, contado o prazo a partir da implementação;
    c. do plano de resposta a incidentes, contado o prazo a partir da implementação;
    d. dos requisitos para contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, contado o prazo a partir da implementação.

18. DIVULGAÇÃO

A Política de Segurança Cibernética e da Informação e as demais políticas e normas complementares da Instituição aqui referenciadas devem ser divulgadas ao Público-Alvo, mediante linguagem clara, acessível

e em nível de detalhamento compatível com as funções desempenhadas e com a sensibilidade das informações, devendo estar disponíveis em local acessível aos colaboradores e protegidas contra alterações.

Além disso, será divulgado ao público, na página da instituição na internet e/ou e-mail corporativo o resumo contendo as linhas gerais da política de segurança cibernética.

19. DÚVIDAS

Em caso de dúvidas sobre o tema relacionado neste documento, contactar a área de Compliance e Controles Internos, através do e-mail: compliance@querocred.com.br.

20. REVISÃO ANUAL

Esta política será revisada anualmente, ou em casos de alterações na legislação vigente e mudanças na estrutura organizacional ou em processos da Instituição

21. COMPROMETIMENTO DA ALTA ADMINISTRAÇÃO

A Diretoria da instituição, ao aprovar esta Política de Segurança Cibernética e da Informação, institui um compromisso para com a melhoria contínua dos procedimentos relacionados com a segurança cibernética e da informação, buscando sempre manter a instituição em conformidade com normas legais e regulamentares sobre os referidos temas, guiada pelos princípios, conceitos, valores e práticas aqui adotados, com o objetivo de assegurar a confidencialidade, a integridade e a disponibilidade dos dados da instituição ou por ela controlados e dos sistemas de informação por ela utilizados, permitindo à instituição prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação e ao ambiente cibernético e proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

22. APROVAÇÃO E VIGÊNCIA DA POLÍTICA

A versão resumida para publicação desta política foi aprovada pela Diretoria da Instituição em maio de 2026 e permanece vigente até a sua atualização.