POLÍTICA DE SEGURANÇA CIBERNÉTICA E DA INFORMAÇÃO

1. Objetivo

Em atenção à Resolução nº 4.658 do Banco Central do Brasil e à Lei n. 13.709/2018, este documento estabelece os princípios, conceitos, valores e práticas a serem adotados na Instituição visando assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados, além de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados à segurança da informação, ao ambiente cibernético e proteger os direitos fundamentais de liberdade, de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

2. Público-Alvo

A Política de Segurança Cibernética e da Informação é dirigida a todos os acionistas, administradores, correspondentes, colaboradores, prestadores de serviço, parceiros e quaisquer outros que tenham ou venham a ter acesso aos dados controlados pela instituição ou aos sistemas de informação da instituição.

3. Definições

Além daquilo que está armazenado nos computadores, a informação, para fins da Política de Segurança Cibernética e da Informação abrange, também, mas não somente, conteúdos impressos e conteúdos repassados através de conversas nos ambientes interno e externo.

Os serviços, procedimentos e processos descritos na Política de Segurança Cibernética e da Informação podem ser terceirizados no todo ou em parte por empresas de total confiança e credibilidade, que deverão conhecer e respeitar a Política de Segurança Cibernética e da Informação.

4. Ciclo de vida da informação

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

5. Princípios

As ações da instituição regem-se pelos seguintes princípios:

- **Confidencialidade:** 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.
- **Disponibilidade:** 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.
- **Integridade:** 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 alterações não aprovadas e sem o controle do proprietário (corporativo ou privado) da informação.

6. Classificação dos dados

As informações e os dados sob responsabilidade da instituição serão classificados conforme análise de impacto, considerando a relevância, a confidencialidade e as proteções necessárias, nos seguintes níveis:

I - Dado não pessoal.

II - Dado pessoal.

III - Dado pessoal sensível.

A divulgação desses dados é proibida, salvo se solicitada por órgão fiscalizador competente (BACEN, Receita Federal, por exemplo) ou por decisão judicial.

7. Diretrizes

A Segurança Cibernética seguirá as seguintes diretrizes:

a) As informações da Instituição, dos clientes e do público em geral devem ser tratadas de forma ética, 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, 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 deverá ser concedido acesso às informações e recursos de informação imprescindíveis para o pleno desempenho das 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 responsável, os riscos às informações e eventuais fatos ou ocorrências que possam colocar em risco tais informações, que será responsável pelo registro e controle dos efeitos de incidentes relevantes;

h) Os parâmetros a serem utilizados na avaliação da relevância dos incidentes serão frequência e Impacto.

i) As responsabilidades quanto à Segurança Cibernética devem ser amplamente divulgadas a todos aqueles considerados público-alvo da Política de Segurança Cibernética e da Informação, que devem entender e assegurar o cumprimento da Política de Segurança Cibernética e da Informação;

j) A Instituição disponibilizará no seu site informações de boas práticas a clientes sobre precauções na utilização de produtos e serviços financeiros;

k) Os recursos que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na

Instituição. Somente se houver permissão formal poderão ser utilizados tais recursos para outros fins.

l) Os conteúdos acessados e transmitidos através dos recursos de tecnologia da Instituição devem ser legais, inclusive de acordo com o Código de Ética e Conduta da instituição, e devem contribuir para as atividades profissionais do usuário.

m) O uso dos recursos de tecnologia da Instituição pode ser examinado, auditado ou verificado pela Instituição.

n) Os recursos de tecnologia da Instituição, disponibilizados para os usuários, é de uso pessoal e intransferível e não podem ser repassados para outra pessoa interna ou externa à organização.

o) Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (*softwares*) instalados.

p) O usuário é responsável por cumprir com as normas estabelecidas na Política de Segurança Cibernética e da Informação e atentar para os perigos do uso de programas não homologados, para a necessidade de se manter o programa de antivírus instalado, atualizado e ativo no equipamento computacional e verificar, com o programa de antivírus, os arquivos recebidos por correio eletrônico ou por outro meio, como pen-drive, logo após o seu recebimento.

q) Os Diretores e Coordenadores são responsáveis por garantir que todos estejam cientes das responsabilidades atribuídas a eles pela Política de Segurança Cibernética e da Informação, garantir que as normas aqui estabelecidas sejam comunicadas e compreendidas por todas as pessoas envolvidas, zelar pelo cumprimento das normas estabelecidas neste documento e comunicar à área responsável, a necessidades de revisão e atualização do conteúdo estabelecido na Política de Segurança Cibernética e da Informação.

r) O Supervisor de TI da instituição alertará todos os usuários que a instalação ou utilização de *software* não autorizados constitui em crime contra a propriedade intelectual, de acordo com a Lei 9.609/1998, sujeitando os infratores à pena de detenção e multa. A Instituição não se responsabiliza por qualquer ação individual que esteja em desacordo com a Lei mencionada acima.

8. Critérios de decisão quanto à contratação de empresas e parceiros para prestação de serviços

Em linhas gerais, a instituição estabelece como **critérios de decisão quanto à contratação de empresas e parceiros para prestação de serviços**, no país ou no exterior:

- **I.** A potencial contribuição do serviço para o posicionamento do negócio, considerando a criticidade do serviço e a sensibilidade das informações e dados a serem processados, armazenados e gerenciados pelo contratado, levando em conta, inclusive, a classificação dos dados;
- **II.** A relação do serviço com a estratégia do negócio;
- **III.** Capacidade da contratada de assegurar à instituição contratante o cumprimento da legislação e da regulamentação em vigor, bem como a capacidade da contratada de assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

9. 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 confidencialidade, à integridade e à disponibilidade dos dados e dos sistemas de informação utilizados e que tenham ou possam ter a capacidade de causar interrupção nos processos de negócios da instituição.

Deverão ser consideradas para a elaboração desses cenários as ausências de ativos humanos ou tecnológicos causadas por:

- desastres e catástrofes, naturais ou não;
- danos físicos relevantes a instalações ou equipamentos críticos, intencionais ou não;
- problemas relacionados a software, banco de dados, servidor de aplicação, rede, incluindo vazamento de dados/informações Indisponibilidade de recursos computacionais, quebra da integridade dos dados, via alteração ou injeção fraudulenta de dados/informações em sistemas e/ou bases de dados, fraudes eletrônicas, incluindo a realização de transações fraudulentas em sistemas de informação da instituição;
- problemas relacionados à segurança cibernética e da informação;
- falhas no fornecimento de energia elétrica; ausência de colaboradores por greves; ausência de colaboradores chave por licença médica ou maternidade / paternidade.

10. Gestão de Terceiros

Os contratos com prestadores de serviço que tiverem acesso aos dados controlados pela instituição ou aos sistemas de informação da instituição deverão conter cláusulas que assegurem a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela prestadores de serviço.

Esses contratos deverão conter, também, cláusulas que responsabilizem os prestadores de serviço perante a instituição, devendo, ainda, os prestadores de serviço assegurarem que seus profissionais:

a) Tenham conhecimento e cumpram a Política de Segurança Cibernética e da Informação;
b) Cumpram as leis e normas que regulamentam a propriedade intelectual;
c) Protejam e zelem pelo sigilo das informações da Instituição;
d) Que a utilização das informações, sistemas e ambiente físico e tecnológico da instituição sejam apenas para finalidades previamente aprovadas;
e) Comuniquem imediatamente qualquer violação desta Política e/ou outras Normas.

11. 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 adotará as seguintes práticas de governança corporativa e de gestão:

11.1. 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.

11.2. 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:

f) Protejam e zelem pelo sigilo das informações da Instituição.

g) Tenham conhecimento e cumpram esta política.

h) 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 4.658 do Banco Central do Brasil.

i) 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.

j) Comuniquem imediatamente qualquer violação desta Política e/ou outras Normas.

11.3. 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 de 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;

12. 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 seguintes práticas de governança corporativa e de gestão:

12.1. Abrangência

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.

12.2. Avaliação da relevância do serviço a ser contratado

Previamente à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem deve ser avaliada a relevância do serviço a ser contratado, considerando:

I. os riscos a que estará exposta;

II. considerando a criticidade do serviço;

III. sensibilidade dos dados e das informações a serem processados, armazenados e gerenciados pelo contratado;

IV. classificação da informação a ser tratada pelo prestador.

12.3. Critérios de decisão quanto à contratação

A instituição estabelece como critérios de decisão quanto à contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, no país ou no exterior, a capacidade do potencial prestador de serviço de assegurar:

I. o cumprimento da legislação e da regulamentação em vigor;

II. o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

III. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processadas ou armazenadas;

IV. a sua aderência às certificações exigidas por lei para a prestação do serviço a ser contratado;

V. 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 contratados;

VI. provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados

VII. a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos;

VIII. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

IX. o acesso da instituição às informações a serem fornecidas pelo prestador de serviço, visando verificar o cumprimento do disposto nas cláusulas referentes à:

a) indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

b) adoção de medidas de segurança para a transmissão e armazenamento dos dados;

c) manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;

d) aderência do prestador de serviço às certificações exigidas por lei;

e) concessão de acesso 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 aqui contratados, quando aplicável;

f) concessão de acesso às informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

g) confidencialidade, integridade e disponibilidade dos dados da instituição, bem como pelo cumprimento da legislação e da regulamentação em vigor;

h) prestação dos serviços, armazenamento, processamento e gerenciamento dos dados unicamente nos países e regiões previamente estabelecidos e comprometendo-se a não mudar a localização indicada sem a prévia autorização.

i) transferência dos dados recebidos para a prestação do serviço ao novo prestador de serviços ou à instituição em caso de extinção do contrato e a excluir os dados recebidos para a prestação do serviço, após a transferência dos dados e a confirmação da integridade e da disponibilidade;

j) não promoção de subcontratação de serviços sem autorização prévia.

k) concessão de acesso do Banco Central do Brasil aos contratos e aos acordos firmados para a prestação dos 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.

l) obrigação de mantê-la permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

m) obrigação de, em caso de decretação de regime de resolução da instituição pelo Banco Central do Brasil:

I. o prestador de serviço conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, 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 códigos de acesso aos dados e às informações, que estejam em poder do prestador de serviço;

II. o prestador de serviço notificar previamente ao responsável pelo regime de resolução sobre a intenção de interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

1. o prestador de serviço obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

2. a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da instituição.

12.4. Cláusulas contratuais

Os contratos para prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

I. a indicação dos países e da região em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados;

II. a adoção de medidas de segurança para a transmissão e armazenamento dos dados;

III. a manutenção, enquanto o contrato estiver vigente, da segregação dos dados e dos controles de acesso para proteção das informações dos clientes;

IV. a obrigatoriedade, em caso de extinção do contrato, de:

a) transferência dos dados ao novo prestador de serviços ou à instituição contratante; e

b) exclusão dos dados pela empresa contratada substituída, após a transferência dos dados prevista na alínea "a" e a confirmação da integridade e da disponibilidade dos dados recebidos;

V. o acesso da instituição contratante a:

a) informações fornecidas pela empresa contratada, visando a verificar o cumprimento dessas obrigações;

b) informações relativas às certificações e aos relatórios de auditoria especializada; e

c) informações e recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

VI. a obrigação de a empresa contratada notificar a instituição contratante sobre a subcontratação de serviços relevantes para a instituição;

VII. a permissão de acesso do Banco Central do Brasil 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;

VIII. a adoção de medidas pela instituição contratante, em decorrência de determinação do Banco Central do Brasil; e

IX. a obrigação de a empresa contratada manter a instituição contratante permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e da regulamentação em vigor.

Os **contratos** devem prever, ainda, cláusulas específicas para o caso de decretação de regime de resolução da instituição contratante pelo Banco Central do Brasil:

I. a obrigação de a empresa contratada conceder pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, 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, citados no inciso VII do caput, que estejam em poder da empresa contratada; e

II. a obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção de a empresa contratada interromper a prestação de serviços, com pelo menos trinta dias de antecedência da data prevista para a interrupção, observado que:

a) a empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de trinta dias para a interrupção do serviço, feito pelo responsável pelo regime de resolução; e

b) a notificação prévia deverá ocorrer também na situação em que a interrupção for motivada por inadimplência da contratante.

12.5. Comunicação da contratação ao Banco Central do Brasil

A contratação de serviços relevantes de processamento,

armazenamento de dados e de computação em nuvem deve ser comunicada ao Banco Central do Brasil, devendo a comunicação conter as seguintes informações:

I - a denominação da empresa a ser contratada;

II - os serviços relevantes a serem contratados; e

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,

A referida comunicação deve ser realizada, no máximo, até 10 (dez) dias após a contratação dos serviços e as alterações contratuais que impliquem modificação dessas informações devem ser comunicadas ao Banco Central do Brasil, no máximo, até 10 (dez) dias após a alteração contratual.

Para a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior devem ser observados requisitos dispostos no art. 16 da Resolução 4.658 do BACEN.

12.6. Documentação

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

Da mesma forma, deve ser documentada a verificação da capacidade do potencial prestador de serviço de assegurar:

I. o cumprimento da legislação e da regulamentação em vigor;

II. o acesso da instituição aos dados e às informações a serem processados ou armazenados pelo prestador de serviço;

III. a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviço;

IV. a sua aderência a certificações exigidas pela instituição para a prestação do serviço a ser contratado;

V. o acesso da instituição contratante 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;

VI. o provimento de informações e de recursos de gestão adequados ao monitoramento dos serviços a serem prestados;

VII. a identificação e a segregação dos dados dos clientes da instituição por meio de controles físicos ou lógicos; e

VIII. a qualidade dos controles de acesso voltados à proteção dos dados e das informações dos clientes da instituição.

13. Cultura de segurança cibernética

A instituição promoverá a disseminação dos princípios e diretrizes da Segurança Cibernética por meio de programas de conscientização e capacitação, com o objetivo de fortalecer a cultura de segurança e realizará avaliação periódica dos colaboradores.