CREDITAR S.A.

CRÉDITO | FINANCIAMENTO | INVESTIMENTO

POLÍTICA DE SEGURANÇA CIBERNÉTICA

Sumário

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.

Os dados sensíveis deverão ser protegidos de forma mais rígida, incluindo inciativas de rastreabilidade da informação e controle de acesso, devendo ser compatível com as funções desempenhadas e com a sensibilidade das informações.

7. Diretrizes

A Segurança Cibernética na Financeira 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, 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;

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 Compliance 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 Financeira 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 Financeira;
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. 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.

12. Aprovação da Diretoria

A Política de Segurança Cibernética e da Informação foi aprovada pela Diretoria da instituição em 25/11/2020.