Política de Segurança Cibernética

Sumário

1. INTRODUÇÃO 3
2. OBJETIVOS.....3
3. DIRETRIZES 3
4. IMPLEMENTAÇÃO.....4
5. PROCEDIMENTOS E CONTROLE.....4
9. MECANISMOS DE ACOMPANHAMENTO E DE CONTROLE.....10
10. CONSIDERAÇÕES FINAIS.....10

1. INTRODUÇÃO

A informação representa um dos bens mais valiosos de uma organização, garantindo a continuidade dos negócios, minimizando os riscos de perdas financeiras e a imagem no mercado. Em muitos segmentos a informação possibilita novas oportunidades de negócio e agilidade no atendimento aos clientes.

A Resolução CMN n° 4.893/2021 dispõe sobre a Política de Segurança Cibernética e sobre os requisitos necessários para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, os quais deverão ser observados pela Cooperativa.

2. OBJETIVOS

O objetivo desta política é orientar os usuários da informação e definir os procedimentos e controles da COOPERATIVA em relação à segurança cibernética, os requisitos mínimos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem, estando em conformidade com a legislação vigente. Destaca-se que além dos fornecedores de nuvem, os fornecedores de tecnologia da informação relevantes devem estar em conformidade com esta Política.

3. DIRETRIZES

A Segurança da informação da Cooperativa estabelece os principais controles, denominados diretrizes:

- As informações da Cooperativa, dos cooperados e de todos envolvidos 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;
- A informação deve ser utilizada de forma transparente e apenas para a finalidade para a qual foi coletada;
- Todo processo, durante o seu ciclo de vida, deve garantir a segregação de funções, por meio da participação de mais de um colaborador, para que a atividade não seja executada e controlada por uma única pessoa;
- O acesso às informações e recurso só deve ser feito se devidamente autorizado;
- A identificação de qualquer colaborador deve ser única, pessoal e intransferível, qualificando-o como responsável pelas ações realizadas;
- A concessão de acessos deve seguir critérios de menor privilégio, no qual os usuários têm acesso somente aos recursos e informações imprescindíveis para o pleno desempenho de suas atividades;
- A senha é utilizada como assinatura eletrônica e deve ser mantida secreta, sendo proibido seu compartilhamento;
- Os riscos às informações da Cooperativa devem ser reportados ao Diretor(a) que é responsável pela área de Segurança da Informação “BACEN”;
- As responsabilidades quanto à segurança da Informação devem ser amplamente divulgadas aos colaboradores, que devem entender e assegurar estas diretrizes;

- Processamento de dados, armazenamento de dados, infraestrutura de redes e outros recursos computacionais que permitam a Cooperativa implantar ou executar softwares, que podem incluir sistemas operacionais e aplicativos internos adquiridos;
- Implantação ou execução de aplicativos desenvolvidos ou adquiridos pela Cooperativa utilizando recursos computacionais de seus prestadores de serviços;
- Execução por meio de Internet de aplicativos implantados ou desenvolvidos por prestadores de serviços da Cooperativa, com utilização de recursos computacionais do próprio prestador de serviços contratado pela Cooperativa;
- Análise de informações e de recursos adequados ao monitoramento dos serviços;
- Confiabilidade, integridade, disponibilidade, segurança e sigilo em relação aos serviços contratados junto a Prestadores de Serviços;
- Cumprimento da legislação e da regulamentação vigente.

4. IMPLEMENTAÇÃO

A implementação desta Política considera as seguintes compatibilidades da Cooperativa:

- O porte, perfil de risco e o modelo de nossos negócios;
- A natureza das operações e a complexidade dos produtos, serviços, atividades e processos atuais;
- A sensibilidade dos dados e das informações sob responsabilidade da Cooperativa.

Os ambientes, sistemas, computadores e redes da Cooperativa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

Caberá todos os colaboradores conhecer e adotar as disposições desta política e deverão proteger as informações contra acesso, modificação, destruição ou divulgação não autorizada, assegurando que os recursos tecnológicos à sua disposição sejam utilizados apenas para as finalidades de suas atividades.

5. PROCEDIMENTOS E CONTROLE

No intuito de registrar procedimentos e controles para reduzir a vulnerabilidade da Cooperativa a incidentes e atender aos demais objetivos de segurança cibernética, e através disso prover controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis, apresentamos a seguir as principais orientações para manter seu computador seguro:

- Manter os softwares de detecção e proteção (anti vírus), atualizados, capazes de proteger eficientemente o ambiente corporativo;
- Manter atualizados os softwares e aplicativos de uso na rede;
- Somente instale programas legítimos, de fonte confiáveis;

- Não abra e-mails e arquivos enviados de fontes desconhecidas;
- Ao compartilhar recursos do seu computador, estabeleça senhas para os compartilhamentos e permissões de acesso adequadas;
- Fique atendo aos endereços acessados no seu navegador;
- Ao realizar compras pela internet procure por sites reconhecidamente seguros;
- Na utilização de internet banking procure pelos sinais de segurança;
- Troque suas senhas com freqüência, ela é pessoal e intransferível, e, criada de acordo com as funções permitidas para o exercício das suas atividades;
- Ao detectar algum erro é importante que seja rastreado, através das tecnologias disponíveis todo o caminho do processo, para, assim, corrigir o ponto onde o erro aconteceu ou iniciou;
- Realize backup periodicamente de todos os arquivos e sistemas.

6. PROCESSOS DE SEGURANÇA DA INFORMAÇÃO

Para assegurar que as informações tratadas estejam adequadamente protegidas, a cooperativa adota os seguintes processos.

Gestão de Ativos da Informação

- Entende-se por Ativos da Informação todos os tipos de dados que se pode criar, processar, armazenar, transmitir, alterar e excluir. Podem ser tecnológicos (“software” e “hardware”) e não tecnológicos (pessoas, processos e dependências físicas);
- Os ativos da informação devem ser identificados de forma individual, inventariado e protegido de acesso indevido, fisicamente e logicamente, ter documentos e planos de manutenção.

Classificação da Informação

- As informações devem ser classificadas de acordo com a confidencialidade e as proteções necessárias, nos seguintes níveis: Restrita, Confidencial, Interna e Pública. 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.

Gestão de Acessos

- As concessões, revisões e exclusões de acesso devem utilizar as ferramentas e os processos da Cooperativa;
- Os acessos devem ser rastreáveis, a fim de garantir que ações são passiveis de auditoria possam identificar individualmente o Colaborador, para que seja responsabilizado por suas ações.

Gestão de Riscos

- Os riscos devem ser identificados por meio de um processo estabelecido para análise de vulnerabilidade, ameaças e impactos sobre os ativos de

informação da Cooperativa, para que sejam recomendadas as proteções adequadas;
- Os cenários de riscos de segurança da informação são escalonados nos setores apropriados, para decisão.

Mitigação dos Riscos

- A Cooperativa oferece aos Colaboradores estrutura tecnológica para o exercício das atividades, sendo responsabilidade de cada Colaborador manter e zelar pela integridade dessas ferramentas de trabalho, e por manter o controle sobre a segurança das informações armazenadas ou disponibilizadas nos equipamentos sob sua responsabilidade (Computador, notebook, acesso à internet, e-mail, etc.);
- Equipamentos e computadores disponibilizados aos Colaboradores devem ser utilizados com a finalidade de atender aos interesses comerciais legítimos da Cooperativa;
- A instalação de cópias de arquivos de qualquer extensão, obtido de forma gratuita ou remunerada, em computadores da Cooperativa depende de autorização do Diretor responsável pela Política de Segurança Cibernética devendo observar os direitos de propriedade intelectual pertinentes, tais como copyright, licenças e patentes;
- As mensagens enviadas ou recebidas através de correio eletrônico corporativo (e-mails corporativos), seus respectivos anexos, e a navegação através da rede mundial de computadores (internet) através de equipamentos da Cooperativa poderão ser monitoradas;
- As senhas de acesso aos dados contidos em todos os computadores, bem como nos e-mails, devem ser conhecidas pelo respectivo usuário de computador e são pessoais e intransferíveis, não devendo ser divulgados para quaisquer terceiros;
- O colaborador poderá ser responsabilizado caso disponibilize a terceiros as senhas acima referidas para quaisquer fins. É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados;
- As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (Word,Excel,etc), não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veiculo, nome de empresa, nome de departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcde”, “12345”, entre outras;
- Os usuários podem alterar a própria senha e devem ser orientados a fazê-lo, caso suspeitem que terceiros obtiveram acesso indevido ao seu login/senha.

Tratamento de Incidentes de Segurança da Informação

Incidentes são interrupções de sistema não planejadas que ocorrem de várias naturezas e que afetam os negócios da Cooperativa, como por exemplo:

- ✓ Queda de energia elétrica;
- ✓ Falha de um elemento de conexão;
- ✓ Servidor fora do ar;

- ✓ Ausência de conexão com internet;
- ✓ Sabotagem/terrorismo;
- ✓ Indisponibilidade de acesso a Cooperativa;
- ✓ Ataques DDOS.

Qualquer colaborador que detectar um incidente deverá comunicar imediatamente ao Diretor Responsável pela Política de Segurança Cibernética.

Segurança Física do Ambiente

- O processo de Segurança Física visa estabelecer controles relacionados à concessão de acesso físico ao ambiente somente a pessoas autorizadas.

Controle de Prestadores de Serviços que manuseiam dados ou informações sensíveis

- Os prestadores de serviços que detenham informações sensíveis ou que sejam relevantes para condução das atividades operacionais da cooperativa, deverão ser tecnicamente capacitados e extremamente envolvidos com as atividades da cooperativa, de forma íntegra e responsabilizados sobre qualquer dano ou vazamento de informações de acordo com contrato de prestação de serviço e políticas internas da cooperativa. O acesso a qualquer informação deverá ser solicitado formalmente por e-mail, ao Responsável na Cooperativa.

7. EXIGÊNCIAS PARA CONTRATAÇÃO DE SERVIÇOS EM NUVEM

A Cooperativa ao realizar contratações de serviços relevantes e armazenamento de dados e de computação em nuvem, no país ou no exterior deverá adotar procedimentos visando certificar-se de que a empresa contratada atende as seguintes exigências:

- **Adoção de práticas de Governança Corporativa e de Gestão proporcionais a relevância dos serviços que estão sendo contratados e aos riscos que estão expostos, como por exemplo:**

  - ✓ Se mantém Política de Segurança da Informação;
  - ✓ Se possui Plano de Continuidade Operacional;
  - ✓ Se as mudanças ou alterações de serviços ou sistemas são registradas e autorizadas quando de sua implantação em produção (Gestão de Mudanças);
  - ✓ Se mantém Gestão de Incidentes.

- **Verificação da capacidade do potencial Prestador de Serviços de forma a assegurar os seguintes requisitos:**

  - ✓ Cumprimento da legislação e da regulamentação em vigor;
  - ✓ Permissão de acesso da Cooperativa aos dados e as informações a serem processadas ou armazenadas pelo Prestador de Serviços;

- ✓ Confidencialidade, Integridade, disponibilidade e recuperação dos dados e das Informações processadas ou armazenadas pelo Prestador de Serviços;
- ✓ Aderência a certificações que a Cooperativa possa exigir para a prestação do serviço a ser contratado;
- ✓ Acesso da Cooperativa aos relatórios elaborados por empresa de Auditoria especializada independente contratada pelo Prestador de Serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços contratados;
- ✓ Provimento de informações e de recursos de Gestão adequados ao monitoramento dos serviços a serem prestados;
- ✓ Identificação e segregação dos dados dos clientes da Cooperativa por meio de controles físicos e lógicos;
- ✓ Qualidade dos controles de acesso voltados à proteção dos dados e das informações dos cooperados.

Os contratos firmados entre a Cooperativa e as empresas prestadoras de serviços relevantes de processamento, armazenamento de dados e computação em nuvem devem prever:

a) 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, quando houver;
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;
d) A obrigatoriedade, em caso de extinção do contrato, de:

- ✓ Transferência dos dados ao novo prestador de serviços ou à Cooperativa;
- ✓ Exclusão dos dados pela empresa contratada substituída após a transferência dos dados e a confirmação da integridade e da disponibilidade dos dados recebidos.

e) O acesso da Cooperativa à:

- ✓ Informações fornecidas pela empresa contratada visando o cumprimento dos itens previstos nos itens a,b e c acima;
- ✓ Informações relativas às Certificações exigidas pela Cooperativa e aos relatórios de auditoria especializada contratada pelo prestador de serviços;
- ✓ Informações e recursos de Gestão adequados ao monitoramento dos serviços prestados.

f) A obrigação da empresa contratada de notificar a cooperativa sobre a subcontratação de serviços relevantes para a Instituição;
g) Permissão de acesso do Banco Central às seguintes informações:

- ✓ Contratos e acordos firmados para a prestação de serviços;
- ✓ Documentação e informações referentes aos serviços prestados;

- ✓ Os dados armazenados;
- ✓ As informações sobre processamentos;
- ✓ As cópias de segurança dos dados e das informações;
- ✓ Códigos de acesso aos dados e as informações.

h) A adoção de medidas pela Cooperativa em decorrência de determinação do Banco Central;

i) A obrigatoriedade da empresa contratada de manter a cooperativa permanentemente informada sobre eventuais limitações que possam afetar a prestação dos serviços ou o cumprimento da legislação e regulamentação em vigor;

j) O contrato deve também prever, para o caso de decretação de regime de resolução da Cooperativa pelo Banco Central:

- ✓ A obrigação da empresa contratada para a prestação de serviços concederem pleno e irrestrito acesso do responsável pelo regime de resolução aos contratos, aos acordos, a documentação e as informações referentes aos serviços prestados, aos dados armazenados e as informações sobre seus processos, as cópias de segurança dos dados e das informações, bem como aos códigos de acesso que esteja em poder da empresa contratada;
- ✓ A obrigação de notificação prévia do responsável pelo regime de resolução sobre a intenção da empresa contratada interromper a prestação de serviços, com pelo menos 30 (trinta) dias de antecedência da data prevista para a interrupção, observando que:
  - ➢ A empresa contratada obriga-se a aceitar eventual pedido de prazo adicional de 30 (trinta) dias para a interrupção do serviço, realizado pelo responsável pelo regime da resolução;
  - ➢ A notificação prévia deve ocorrer também na situação em que a interrupção for motivada por inadimplência da cooperativa.

8. COMUNICAÇÃO AO BANCO CENTRAL

A Cooperativa deverá informar previamente ao Banco Central a contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem.

Essa comunicação deve ser realizada 60 dias antes da contratação dos serviços e deve conter as seguintes informações:

- ✓ Denominação da empresa a ser contratada;
- ✓ Os serviços relevantes a serem contratados;
- ✓ 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, nos casos de contratação no exterior.

As alterações contratuais que impliquem modificações nas informações contratuais devem ser comunicadas ao Banco Central no mínimo 60 dias antes da alteração contratual.

A contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, a ser realizada pela Cooperativa quando houver, deve observar os seguintes requisitos:

- ✓ A existência de convênio para troca de informações entre o Banco Central do Brasil e as autoridades supervisoras dos países onde os serviços poderão ser prestados;
- ✓ Assegurar que a prestação dos serviços não cause prejuízo ao seu regular funcionamento nem embaraço a atuação do Banco Central do Brasil;
- ✓ Definir, previamente à contratação, os países e as regiões em cada país onde os serviços poderão ser prestados e os dados poderão ser armazenados, processados e gerenciados; e
- ✓ Prever alternativas para a continuidade dos negócios, no caso de impossibilidade de manutenção ou extinção do contrato de prestação de serviços.

No caso de inexistência de convênio citado nos itens anteriores a cooperativa deverá solicitar autorização do Banco Central para a contratação, observando o prazo e as informações já mencionadas.

A Cooperativa deve assegurar que a legislação e a regulamentação nos países e nas regiões em cada país onde os serviços poderão ser prestados não restringem nem impedem o acesso das instituições contratantes e do Banco Central do Brasil e às informações.

9. MECANISMOS DE ACOMPANHAMENTO E DE CONTROLE

Os mecanismos de acompanhamento e de controle visam assegurar:

- A implementação das suas disposições;
- O monitoramento do seu cumprimento, inclusive por meio de métricas e indicadores adequados;
- A avaliação da sua efetividade;
- A identificação e a correção de eventuais deficiências.

Junto ao relatório de controles internos, emitido anualmente, será avaliada a implementação dessa política, o monitoramento de seu cumprimento, a avaliação de sua efetividade e a identificação de possíveis melhorias e correções.

Os mecanismos de que trata o caput devem ser submetidos a testes periódicos pela auditoria interna.

10. CONSIDERAÇÕES FINAIS

Esta política entrará em vigor na data da sua aprovação pela Diretoria e será revisada anualmente ou quando houver mudanças regulamentares que demandem atualizações internas ou alteração de produtos e serviços internos que dementem readequação das análises e ações.