CrediGuaçuí
de braços abertos para você.

POLÍTICA SEGURANÇA CIBERNÉTICA 2022

RESOLUÇÃO DO CMN Nº 4.893/21

Rua Bom Jesus do Livramento, 25 - Centro - Guaçuí-ES - CEP: 29560-000
Tel: (28) 3553-3362 - Telefax: (28) 3553-2194
www.crediguacui.com.br

SUMÁRIO

Rua Bom Jesus do Livramento, 25 - Centro - Guaçuí-ES - CEP - 29560-000
Tel.: (28) 3553-3362 - Telefax (28) 3553-2194
www.crediguacui.com.br

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. OBJETIVO

O objetivo desta política é orientar os colaboradores 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. CONCEITO

Para melhor compreensão da necessidade de se cumprir o descrito na Política de Segurança Cibernética, é necessário conhecer os conceitos que fazem parte desse segmento, onde a informação é extremamente valiosa e passível de riscos que colocam em xeque a continuidade da

cooperativa. Dessa forma, temos os seguintes conceitos para facilitar o entendimento dos colaboradores:

Segurança Cibernética: refere-se a um conjunto de práticas adotadas pelas instituições, que protege a informação armazenada nos computadores, cujo fluxo se dá através de redes de comunicação em nuvem. Essa proteção visa garantir a propriedade da informação quanto a sua confidencialidade, integridade e disponibilidade.

Informação: é a reunião ou conjunto de dados e conhecimentos organizados, que possam constituir referências sobre determinado acontecimento ou processos comunicativos.

Confidencialidade: considera-se que, toda informação deve ser protegida, principalmente se considerado suas características e o grau de sigilo, de forma que exista limitação de acesso e uso apenas às pessoas autorizadas ou a quem é destinada.

Integridade: toda informação deve ser mantida na condição em que foi disponibilizada pelo seu titular, visando protegê-la contra alterações indevidas, intencionais e acidentais.

Disponibilidade: toda informação gerada ou adquirida por um indivíduo ou instituição, deve estar disponível aos seus usuários quando os mesmos necessitarem delas para qualquer finalidade.

Riscos Cibernéticos: são considerados ataques que as informações podem sofrer, oriundos de malware, invasões, fraudes externas, desprotegendo, inclusive, redes e sistemas das organizações, podendo causar danos financeiros, à reputação, e até mesmo colocar em risco a continuidade da instituição.

"MALWARE é um termo amplo que é usado para classificar todo tipo de

software malicioso usado para causar prejuízo, que pode ser até financeiro, danificar sistemas, interceptar dados ou simplesmente irritar o usuário, afetando tanto computadores como celulares e até redes inteiras".

Vírus: software que causa danos à máquina, rede, softwares e banco de dados.

Cavalo de Tróia: aparece dentro de outro software e cria uma porta para a invasão do computador.

Spyware: software malicioso para coletar e monitorar o uso de informações.

Ransomware: software malicioso que bloqueia o acesso a sistemas e bases de dados, solicitando um resgate para que o acesso seja restabelecido.

"ENGENHARIA SOCIAL é uma técnica empregada por criminosos virtuais para induzir usuários desavisados a enviar dados confidenciais, infectar seus computadores com malware ou abrir links para sites infectados".

Pharming: direciona o usuário para um site fraudulento, sem seu conhecimento.

Phishing: links transmitidos por e-mails, simulando ser uma pessoa ou empresa confiável, que envia comunicação eletrônica oficial para obter informações confidenciais.

Vishing: simula ser uma pessoa ou empresa confiável e, por meio de ligações telefônicas, tenta obter informações confidenciais.

Smishing: simula ser uma pessoa ou empresa confiável e, por meio de mensagens de texto, tenta obter informações confidenciais.

Acesso Pessoal: pessoas localizadas em lugares públicos como: bares, cafés e restaurantes, que captam qualquer tipo de informação que possa ser utilizada posteriormente para um ataque.

Fraudes Externas e Invasões: realização de operações por fraudadores, utilizando- se de ataques em contas bancárias, utilizando conhecimentos e ferramentas para detectar e explorar fragilidades específicas em um ambiente tecnológico.

Ataque DDoS e Botnets: ataques que visam negar ou atrasar o acesso aos serviços ou sistemas da instituição; no caso dos Botnets, o ataque vem de inúmeros computadores infectados utilizados para criar e enviar spam ou vírus, ou inundar uma rede com mensagens resultando na negação do serviço.

4. SEGURANÇA CIBERNÉTICA

A Cooperativa, através do Conselho de Administração ou da Diretoria estabelece a Política de Segurança Cibernética, bem como os requisitos para a contratação, avaliação e gestão de serviços de processamento e armazenamento de dados e de computação em nuvem visando total observância e adequação ao exigido na Resolução 4.893/21.

O propósito desta Política é orientar a Cooperativa no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação Cibernética, em conformidade com as disposições constitucionais, legais e regimentais vigentes, a fim de garantir a aplicação dos princípios e diretrizes de proteção das informações e da propriedade intelectual da cooperativa, dos cooperados e envolvidos, além disso, assegurar a proteção dos ativos de informação da Cooperativa contra ameaças, internas ou externas, reduzir a exposição ou danos

decorrentes de falhas de ciber segurança e garantir que os recursos adequados estarão disponíveis, mantendo um processo de segurança efetivo dos negócios.

5. DIRETRIZES CORPORATIVAS

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.

Rua Bom Jesus do Livramento, 25 - Centro - Guaçuí-ES - CEP 29560-000
Tel.: (28) 3553-3362 - Telefax: (28) 3553-2194
www.crediguacui.com.br

- 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.

Conforme a Resolução n° 4.893/21, os serviços de computação em nuvem abrangem a disponibilidade da Cooperativa, sob demanda e de maneira virtual, de ao menos um dos seguintes serviços:

- Processamento de dados, armazenamento de dados, infra estrutura 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.

A Cooperativa é responsável pela Gestão dos serviços contratados incluindo as seguintes atividades:

- Analise 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.

6. 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 instituição.

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.

7. TRATAMENTO DA INFORMAÇÃO

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

8. PROCEDIMENTOS E CONTROLES

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.

9. 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 copias 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.

Rua Bom Jesus do Livramento, 25 - Centro - Guaçuí-ES - CEP: 29560-000
Tel: (28) 3553-3362 - Telefax: (28) 3553-2194
www.crediguacui.com.br

- 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 veículo, 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.

10. GERENCIAMENTO DE INCIDENTES

Tem o objetivo de assegurar que os eventos de segurança de informação sejam tratados de forma efetiva, permitindo o adequado registro, investigação e tomada de ação corretiva em tempo hábil para mitigar o impacto negativo sobre os sistemas de informação da Cooperativa.

Avaliação Inicial:

Avaliar o incidente em conjunto com o Conselho de Administração ou Diretoria para verificar se é provável a sua reincidência ou se é um sintoma de problema crônico, para a tomada de providências e medidas corretivas.

Analisar motivos e consequências imediatas, bem como a gravidade da situação.

Incidente Caracterizado:

Caracterizado o incidente, devem ser tomadas as medidas imediatas, tais como:

- O Diretor responsável pela política de Segurança Cibernética estará avaliando o impacto do incidente nos diversos riscos envolvidos;
- Conforme a relevância (sabotagem, terrorismo, etc) poderá ser registrado um boletim de ocorrência ou queixa crime para as devidas providências;
- Conforme a relevância do incidente comunicar os cooperados que por ventura foram afetados;
- Comunicação tempestiva ao Banco Central do Brasil das ocorrências de incidentes relevantes e das interrupções de serviços relevantes, que configurem uma situação de crise pela Cooperativa.

Recuperação:

Essa fase começa após o incidente ter sido contornado, já tendo sido a contingência acionada e terceiros notificados.

Quaisquer dados que estejam faltando ou que estejam corrompidos, ou problemas identificados por colaboradores internos devem ser comunicados ao Conselho de Administração ou Diretoria.

Retomada:

Tal fase refere-se ao período de transição do retorno ao modo normal de operação e pode incluir a análise de projetos, como voltar a operação normal, reconstrução de eventuais sistemas e eventuais mudanças e medidas de prevenção.

Relatório sobre implementação do Plano de Ação e de Resposta a Incidentes:

Será parte integrante do relatório de controles internos e do relatório integrado de gestão de risco da Cooperativa, tendo em vista a complexidade e ao porte da mesma, e deve contemplar, no mínimo, as seguintes informações:

- A efetividade da implementação das ações relativas à implementação da Política de Segurança Cibernética;
- O resumo dos resultados obtidos na implementação das rotinas, dos procedimentos, dos controles e tecnologias a serem utilizados na prevenção e na resposta a incidentes;
- Os incidentes relevantes relacionados com o ambiente cibernético ocorridos no período;

- Os resultados de testes de continuidade de negócios, considerando cenários de indisponibilidade ocasionada por incidentes.

Deverá ser elaborado até 31 de março do ano seguinte ao da data base e aprovado pelo Conselho de Administração em ata de reunião.

11. 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.

12. AVALIAÇÃO DOS SERVIÇOS A SEREM CONTRATADOS

A Cooperativa deve proceder a uma avaliação da relevância dos serviços prestados por empresa com possibilidade de serem contratadas considerando o seguinte:

- Criticidade dos serviços a serem prestados;

- Sensibilidade dos dados e das informações processadas, armazenadas e gerenciadas pela empresa contratada;
- Verificação quanto à adoção, por parte do prestador de serviços quanto a controles que mitiguem efeitos eventuais vulnerabilidade na liberação de novas versões de aplicativos no caso de serem executados através de internet.

13. 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.

14. DOS CONTRATOS

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) A 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.

"Os regimes de resolução são pautados pelo interesse público, pela preservação da estabilidade financeira e pela não interrupção do funcionamento de funções críticas para a economia real".

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

A Cooperativa, tendo em vista a necessidade de agilizar o atendimento de seus cooperados e visando maior segurança e celeridade, fez a contratação do Serviço de Computação em Nuvem.

O contrato foi firmado com a empresa PRODAF INFORMÁTICA que, é a responsável pelos serviços de processamento e armazenamento de dados. Esta, por sua vez, possui contrato regular de Serviços junto a DEDALUS que, é detentora do espaço utilizado pela Cooperativa para armazenar seus dados.

Por sua vez, o espaço objeto do contrato entre a DEDALUS x PRODAF INFORMÁTICA pertence à AMAZON WEB SERVICES.

16. PROCEDIMENTOS E INSTRUÇÕES

Os procedimentos e as instruções encontram-se presentes na Política de Segurança Cibernética, visto que, estes representam as responsabilidades atribuídas à PRODAF INFORMÁTICA, por conta do objeto do contrato de Serviço de Computação em Nuvem.

Assim, é necessário um detalhamento meticuloso das ações, as atividades desenvolvidas e a sua relação com as informações.

Esse nível de detalhamento pressupõe a necessidade de constante revisão e/ou manutenção dessa política, conforme a seguir:

Testes

São realizados testes, sendo estes executados de forma automatizada e por robôs de monitoramento, diariamente.

Acompanhamento

O acompanhamento de carga e desempenho é realizado em tempo real, através de ferramenta automatizada que, no processo de monitoramento do ambiente, pode gerar alerta em caso de pico de uso e recurso de algum servidor.

Administração do Banco de Dados

Toda a parte de administração e verificação do banco de dados é de exclusiva responsabilidade da PRODAF INFORMÁTICA, sendo operacionalizada de forma manual ou automática pelas versões do sistema.

Administração de Contas de Usuários

Os usuários que utilizaram o(s) Sistema(s) da PRODAF INFORMÁTICA serão gerenciados e autorizados pela Cooperativa.

Já o cadastro e criação de usuários para acessar o Cloud pelo GO-Global, serão realizados pela PRODAF INFORMÁTICA mediante solicitação da Cooperativa.

Administração de Ferramentas de Segurança

A administração das ferramentas de segurança como firewalls, IDS/IPS, WAF e BACKUP será de responsabilidade da PRODAF INFORMATICA e da DEDALUS.

Há um monitoramento constante de ocorrências e aplicação de vacinas e regras que visam evitar problemas com ataques.

Plano de Contingência

Como todo o ambiente PRODAF INFORMÁTICA cloud é virtualizado, a qualquer momento, sendo necessário, podem-se levar os snasphot dos servidores para qualquer datacenter da AMAZON no mundo, de forma a subir um novo ambiente de uso dos sistemas.

Para acesso às informações, basta o colaborador na Cooperativa autorizada, conectar-se a qualquer rede de internet, em qualquer lugar do mundo.

"Snapshot é o registro do estado de um sistema, aplicação ou arquivos em determinado ponto no tempo".

Ocorrência de Incidente

As verificações são realizadas por meio de pentests, que tem ocorrido de acordo com demanda dos clientes e com certa frequência.

O tempo de restabelecimento por um eventual ataque, uma vez ocorrendo, dependerá do tipo de ataque, visto que, eventualmente, pode ser resolvido em poucos minutos ou, havendo situações mais complexas, demandará a abertura de uma janela maior para correção. No pior dos cenários, o retorno de snapshot pode ocorrer no máximo em 02 (duas) horas.

"Pentest é uma forma de detectar e explorar vulnerabilidades existentes nos sistemas, ou seja, simular ataques de hackers".

Registro de Incidentes

Considerando a responsabilidade da PRODAF INFORMÁTICA na administração do banco de dados e das ferramentas de segurança da Cooperativa, torna-se necessário a comunicação ao Diretor Responsável pela Política de qualquer incidente relevante, sendo este formalizado através de relatório e/ou declaração contendo o registro dos incidentes verificados em testes, ou os que efetivamente ocorreram.

17. ESTRUTURA DE GERENCIAMENTO

Embora a responsabilidade pela administração do banco de dados, bem como das ferramentas utilizadas para garantir a segurança desses dados, seja de responsabilidade da PRODAF INFORMÁTICA, a Cooperativa deve garantir, como parte interessada, e se respaldar do atendimento da Política de Segurança Cibernética por parte daquela, através de relatórios e/ou declarações emitidos por conta da verificação dos controles de Segurança Cibernética, cuja periodicidade poderá ser semestral ou anual.

Esse gerenciamento dos procedimentos e controles tem o objetivo de assegurar que os procedimentos operacionais de segurança sejam desenvolvidos, implementados e modificados de acordo com objetivas e diretrizes estabelecidas na Política de Segurança Cibernética da Cooperativa.

Nesse sentido, a estrutura de gerenciamento deve prever o atendimento de padrão mínimo para conhecimento do Conselho de Administração ou Diretoria da Cooperativa.

18. GESTÃO DE ACESSO ÀS INFORMAÇÕES

O acesso e cadastro de usuários para acessar o Cloud pela GO-Global, será realizado pela PRODAF INFORMÁTICA mediante solicitação da Cooperativa. Nesse sentido, caberá a esta a verificação do controle de acessos, por conta do monitoramento efetivado, que devem ser revistos periodicamente como forma de manter as restrições e/ou permissões autorizadas pela Cooperativa.

Rua Bom Jesus do Livramento, 25 - Centro - Guaçuí-ES - CEP: 29560-000
Tel.: (28) 3553-3362 - Telefax: (28) 3553-2194
www.crediguacui.com.br

Considerando os serviços contratados de processamento e armazenamento em nuvem, torna-se prudente a apresentação de relatórios que demonstrem o efetivo monitoramento, aplicação de testes, tratamentos e resposta aos incidentes, quando de sua ocorrência, com vistas a minimizar o risco de falhas, favorecendo uma administração segura e transparente para ambas as partes. Esse relatório deve ser apresentado ao Conselho de Administração ou Diretoria da Cooperativa semestral ou anual.

Segurança Física e Lógica

Caberá à PRODAF INFORMÁTICA orientar se as condições e configurações das máquinas utilizadas pela Cooperativa, atendem aos propósitos estabelecidos para o bom desempenho e gerenciamento do serviço em nuvem.

No que tange ao seu quadro de colaboradores, a PRODAF INFORMÁTICA deve mantê-los atualizados e em constante treinamento, com vista a acompanhar as novidades acerca da Segurança da Informação e Cibernética.

Continuidade de Negócio

A estrutura de gerenciamento, em linhas gerais, visa garantir que a Política está sendo cumprida, com vistas a minimizar a ocorrência de fatores que coloquem em risco as atividades da Cooperativa, e conseqüentemente expondo-a a risco de descontinuidade.

Nesse sentido, para evitar a descontinuidade do negócio, torna-se necessário proceder com a análise dos incidentes, de forma que estes

correspondam a um nível crítico ou aceitável, e verificar se estão em consonância com as medidas corretivas a serem adotadas.

19. COMUNICAÇÃO AO CONSELHO DE ADMINISTRAÇÃO OU DIRETORIA

Tendo em vista a complexidade que envolve o cumprimento da Política de Segurança Cibernética, e a dificuldade da Cooperativa em validar ou não a efetivação dos procedimentos, é imperioso manter o Diretor Responsável pela política informado sobre indícios de irregularidades verificados quando do cumprimento das determinações dessa política.

Assim, caberá à PRODAF INFORMÁTICA realizar a comunicação de possíveis indícios quando de sua ocorrência, de forma semestral ou anual, quando encaminhar relatório demonstrando as verificações realizadas sob a ótica da gestão de acessos, proteção de ambientes, segurança física e lógica e continuidade do negócio.

20. DOCUMENTOS DISPONÍVEIS AO BANCO CENTRAL

Os seguintes documentos devem ficar à disposição do Banco Central do Brasil pelo prazo mínimo de 5 (cinco) anos, base regulatória Resolução Bacen n° 4.893 de 26/02/2021.

- Política de Segurança Cibernética;
- Ata de Reunião do Conselho de Administração ou Diretoria implementando / aprovando a Política de Segurança Cibernética e suas revisões;

- Documento relativo ao Plano de Ação e de Resposta a Incidentes relatórios a implementação da Política de Segurança Cibernética;
- Relatório anual de Controles Internos e Gerenciamento de Risco no qual devem contemplar o item sobre a implementação do Plano de Ação e de Resposta a Incidentes;
- Documentação sobre os procedimentos relativos à contratação de serviços de processamento e armazenamento de dados e de computação em nuvem;
- Documentação sobre os serviços relevantes de processamento, armazenamento de dados e de computação em nuvem prestados no exterior, "**caso isso ocorra**";
- Contratos de prestação de serviços relevantes de processamento, armazenamento de dados e computação em nuvem;
- Dados, registros e informações relativas aos mecanismos de acompanhamento e de controles com vistas a assegurar a implementação e a efetividade da Política de Segurança Cibernética, 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.

21. ABRANGÊNCIA, APROVAÇÃO, DIVULGAÇÃO, E REVISÃO DA POLÍTICA

O conteúdo desta Política aplica-se a todos os colaboradores e prestadores de serviços relevantes da Cooperativa no âmbito de suas atividades, atribuições e responsabilidades.

Aprovada pelo Conselho de Administração ou Diretoria a qual está comprometida com a melhoria contínua do disposto nesse documento.

Publicada no site da Cooperativa e divulgada a todos os colaboradores, empresas contratadas de serviços cibernéticos, clientes e partes externas relevantes, para o necessário cumprimento.

É obrigação de todo colaborador conhecer e praticar às disposições desta Política e assegurar que, quando necessário, prestadores de serviços sejam informados sobre as regras estabelecidas.

22. CONSIDERAÇÕES FINAIS

Esta política será revisada anualmente ou quando mudanças significativas ocorrerem, assegurando a sua contínua pertinência, adequação e eficácia e aprovada pelo Conselho de Administração ou Diretoria em Ata de Reunião mensal.

Esta política de segurança cibernética foi revisada no segundo semestre de 2021 e aprovado em reunião do Conselho de Administração realizada em 18/11/2021.

Renato Caiado Casotti
Diretor Presidente

Jorge Guedes da Silva
Diretor Administrativo

Gilson Costa de Oliveira
Diretor Financeiro

Agenor Luiz Ferraz Thomé
Conselheiro

Alcenir Tadeu de Paula
Conselheiro

Christiany Fitaroni P. de Azevedo
Conselheira

Rua Bom Jesus do Livramento, 25 - Centro - Guaçuí-ES - CEP.: 29560-000
Tel.: (28) 3553-3362 - Telefax: (28) 3553-2194
www.crediguacui.com.br