cooperáguia

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

Versão: 02/2024

Aprovada em: 27/03/2024

ÍNDICE

1. INTRODUÇÃO

A Política de Segurança da Informação e Segurança Cibernética da COOPERÁGUIA é uma declaração formal da cooperativa acerca do seu compromisso com a proteção de Informações Sigilosas e Segurança Cibernética (cybersecurity), conforme definição adiante, devendo ser cumprida pela Diretoria, Conselho Fiscal, colaboradores e prestadores de serviços.

Seu propósito é estabelecer as diretrizes a serem seguidas no que diz respeito à adoção de procedimentos e mecanismos relacionados à segurança de Informações Sigilosas, bem como cumprir com as determinações contidas na Resolução CMN nº 4.893, de 26 de fevereiro de 2021.

Esse documento tem como responsável o Diretor Responsável pela Política de Segurança Cibernética no UNICAD.

2. OBJETIVO

Esta Política visa proteger as Informações Sigilosas e a propriedade intelectual da COOPERÁGUIA e de seus associados, garantindo a disponibilidade, integridade, confidencialidade, legalidade, autenticidade e auditabilidade das mesmas, bem como aprimorar a segurança cibernética da cooperativa, nos termos da Resolução CMN nº 4.893, de 26 de fevereiro de 2021.

Nenhuma Informação Sigilosa deve ser divulgada, dentro ou fora da cooperativa, a quem não necessite ou não deva ter acesso a tais informações para desempenho de suas atividades profissionais. Qualquer informação, independentemente de ser considerada Informação Sigilosa, seja sobre a cooperativa, relativa às suas atividades, aos seus associados dentre outras, ou obtida em decorrência do desempenho das atividades normais do Colaborador, só poderá ser revelada ou fornecida ao público, à mídia, ou a terceiros de qualquer natureza da maneira e conforme previstos nos documentos internos da cooperativa.

Os dados e as informações da COOPERÁGUIA são classificados entre: “CONFIDENCIAL”, “PÚBLICO” e “ACESSO RESTRITO”. O Diretor Responsável pela Política de Segurança Cibernética no UNICAD é o responsável por essa classificação. Os dados e as informações devem ser reclassificados sempre que necessário.

Na falta de previsão expressa, a revelação ou fornecimento somente poderá ocorrer com o conhecimento e, dependendo do caso, autorização prévia da Diretoria da COOPERÁGUIA.

3. APLICAÇÃO

A efetividade desta Política depende da conscientização da Diretoria, Conselho Fiscal, colaboradores e prestadores de serviços e do esforço constante para que seja feito bom uso das Informações Sigilosas e dos ativos disponibilizados pela cooperativa, e deve ser conhecida e obedecida por todos que utilizam os recursos de tecnologia disponibilizados pela cooperativa, sendo de responsabilidade individual e coletiva o seu cumprimento.

4. RESPONSABILIDADE NA GESTÃO DA POLÍTICA

a) Cumprir fielmente esta Política;
b) Buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança das Informações Sigilosas;
c) Proteger Informações Sigilosas contra acesso, modificação, destruição ou divulgação não

autorizada pela cooperativa;
d) Assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas para as finalidades aprovadas pela cooperativa;
e) Cumprir as leis e normas que regulamentam os aspectos relacionados ao direito autoral e propriedade intelectual no que se refere às Informações Sigilosas;
f) Comunicar imediatamente à Diretoria da COOPERÁGUIA sobre qualquer descumprimento ou violação desta Política.

5. CONCEITOS E PRINCIPIOS

Todas as Informações Sigilosas constituem ativos de valor para a COOPERÁGUIA e, por conseguinte, precisam ser adequadamente protegidas contra ameaças e ações que possam causar danos e prejuízos para a Cooperativa, Associados e Colaboradores.

As Informações Sigilosas podem ser armazenadas e transmitidas de diversas maneiras, como, por exemplo, arquivos eletrônicos, mensagens eletrônicas, sites de Internet, bancos de dados, meio impresso, mídias de áudio e de vídeo, dentre outras. Cada uma dessas maneiras está sujeita a uma ou mais formas de manipulação, alteração, remoção e eliminação do seu conteúdo.

A adoção de políticas e procedimentos que visem garantir a segurança de Informações Sigilosas deve ser prioridade constante da cooperativa, reduzindo-se os riscos de falhas, os danos e prejuízos que possam comprometer a sua imagem e objetivos. Assim, por princípio, a guarda e segurança das Informações Sigilosas devem abranger três aspectos básicos, destacados a seguir:

a) **acesso**: somente pessoas devidamente autorizadas pela cooperativa devem ter acesso às Informações Sigilosas;

b) **integridade**: somente alterações, supressões e adições autorizadas pela cooperativa devem ser realizadas às Informações Sigilosas; e

c) **disponibilidade**: as Informações Sigilosas devem estar disponíveis para os Colaboradores autorizados sempre que necessário ou for demandado.

Para assegurar os 3 (três) aspectos acima, as Informações Sigilosas devem ser adequadamente gerenciadas e protegidas contra furto, fraude, espionagem, perda não intencional, acidentes e outras ameaças.

Em cumprimento à Resolução nº 4.893/21, a cooperativa possui 4 (quatro) pilares principais no seu programa de segurança cibernética:

a) Identificação e avaliação de riscos (risk assessment);
b) Ações de prevenção e proteção;
c) Monitoramento e testes;
d) Plano de resposta.

A implantação e monitoramento da capacidade da cooperativa atender a estes pilares deverão ser feito pela Diretoria da COOPERÁGUIA. Também a fim de atingir os objetivos dispostos acima, todos que se aplicam a essa política terão suas próprias responsabilidades.

A cooperativa deverá ter uma abordagem holística em relação à segurança cibernética, sendo obrigação pela Diretoria da COOPERÁGUIA promover conscientização para que os Colaboradores saibam as suas respectivas funções na proteção de Informações Sigilosas, para que possam agir de maneira apropriada frente às situações que requeiram respostas.

6. MODELO ADOTADO

A COOPERÁGUIA optou por manter a Diretoria de Tecnologia de Inovação (DTI) do Grupo Águia Branca à segurança das informações, segurança cibernética, contingência e outros assuntos relacionados com tecnologia da informação, inclusive para a realização de tarefas (e.g. instalações, substituições, configurações), verificações e manutenções periódicas.

Assim sendo, para implementação e monitoramento contínuo da presente Política, a COOPERÁGUIA conta com o suporte e assessoria da Diretoria de Tecnologia e Inovação (DTI) do Grupo Águia Branca.

7. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

7.1. Identificação e Avaliação de Riscos (Risk Assesssment):

A COOPERÁGUIA juntamente com a Diretoria de Tecnologia e Inovação (DTI) deverá identificar e avaliar os principais riscos cibernéticos aos quais está exposta e adotará medidas para tratar os riscos identificados.

Em seu Código de Segurança Cibernética, 2ª edição, página 5, publicada em 06/12/2017, a ANBIMA – Associação Brasileira das Entidades dos Mercados Financeiros e de Capitais definiu que os ataques mais comuns de criminosos cibernéticos (cybercriminals) são os seguintes:

a) Malware (e.g. vírus, cavalo de troia, spyware e ransomware);
b) Engenharia Social;
c) Pharming;
d) Phishing scam;
e) Vishing;
f) Smishing;
g) Acesso pessoal;
h) Ataques de DDoS e botnets; e
i) Invasões (advanced persistente threats).

7.2. Ações de Prevenção e Proteção:

A COOPERÁGUIA juntamente com a Diretoria de Tecnologia e Inovação (DTI) adota regras para concessão de senhas de acesso a dispositivos corporativos, sistemas e rede, em função da relevância para acesso. A COOPERÁGUIA trabalha com o princípio de que concessão de acesso deve somente ocorrer se os recursos acessados forem relevantes ao usuário.

Os eventos de login e alteração de senhas são auditáveis e rastreáveis, e o acesso remoto a arquivos e sistemas internos ou na nuvem têm controles adequados.

Outro ponto importante é que, ao incluir novos equipamentos e sistemas em produção, a COOPERÁGUIA juntamente com a Diretoria de Tecnologia e Inovação (DTI) deverá garantir que sejam feitas configurações seguras de seus recursos. Devem ser feitos testes em ambiente de homologação e de prova de conceito antes do envio à produção.

A COOPERÁGUIA através da DTI conta com recursos anti-malware tais como:

- Firewall, para proteção de rede e de intrusos;
- Antivírus, para proteção de estações de trabalhos;
- IPS, para detecção e proteção de intrusos; e
- Proxy, para encapsulamento da rede interna.

Da mesma maneira a DTI monitora o acesso a websites e restringe a execução de softwares e/ou aplicações não autorizadas.

A COOPERÁGUIA através da Diretoria de Tecnologia e Inovação (DTI) realiza, também, backup das informações e dos diversos ativos da instituição, conforme as disposições do presente documento e do Plano de Continuidade do Negócio.

Todo incidente da informação é registrado e mantido através de backup por 10 anos pela Diretoria de Tecnologia e Inovação (DTI).

A Diretoria de Tecnologia e Inovação (DTI) é responsável por responder a incidentes.

A Diretoria da COOPERÁGUIA é responsável por coordenar o compartilhamento de informações sobre incidentes com demais instituições financeiras e o Banco Central do Brasil.

7.3. Monitoramento e Testes:

Os sistemas, serviços, dados, informações (incluindo as Informações Sigilosas) disponíveis na COOPERÁGUIA ou por esta disponibilizados para serem usados pelos Colaboradores não devem ser interpretados como sendo de uso pessoal. Todos os Colaboradores devem ter ciência de que o uso está sujeito a monitoramento periódico, inclusive em equipamentos pessoais acessados durante o expediente da COOPERÁGUIA, fazendo uso da sua rede ou não, sem frequência determinada ou aviso prévio. Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware) pela DTI.

Os registros obtidos e o conteúdo dos arquivos poderão ser utilizados com o propósito de determinar o cumprimento do disposto nesta Política, e nos demais documentos internos da COOPERÁGUIA e, conforme o caso, servir como evidência em processos administrativos, arbitrais e/ou judiciais.

A COOPERÁGUIA possui através da PRODAF um roteiro de testes indicando as ações de proteção implementadas para garantir seu bom funcionamento e efetividade. Da mesma maneira deve diligenciar de modo a manter inventários atualizados de hardware e software, bem como sistemas operacionais.

Periodicamente, a COOPERÁGUIA através da PRODAF realiza testes de segurança no ***SYSCOOP32*** e ***SYSCOOPWEB***, executando, mas não se limitando, os seguintes procedimentos:

a) Análise periódica de vulnerabilidade com reteste caso sejam detectadas vulnerabilidades;
b) *Pentest* a cada dois anos com reteste caso sejam detectadas vulnerabilidades;
c) Análise de vulnerabilidades em todos os sistemas pertencentes à COOPERÁGUIA, incluindo programas adquiridos;
d) Todos os testes de vulnerabilidades devem ser executados, exceto testes de stress (DoS e DDOS);

É de responsabilidade da PRODAF:

- Executar a análise de vulnerabilidades; e
- Corrigir as vulnerabilidades detectadas.

A PRODAF deve realizar correções de vulnerabilidades detectadas nos serviços prestados.

A DTI monitora a disponibilidade dos serviços prestados (serviços de rede, e-mail, telefonia, etc.) através do sistema "Nagios", e a PRODAF através do sistema "Dynatrace".

Caberá à PRODAF a elaboração de relatório contendo o resultado das análises de vulnerabilidades e dos *Pentests* após a realização dos mesmos, o qual será apresentado à Diretoria da COOPERÁGUIA.

Sem prejuízo dos testes realizados na forma mencionada acima, a COOPERÁGUIA através da PRODAF realizará simulações de ataques e respostas da cooperativa que seriam possíveis nestes casos. As simulações deverão prever as ferramentas mais usadas pelos criminosos cibernéticos, revelando as principais vulnerabilidades dos sistemas da COOPERÁGUIA, o que permitirá efetuar as correções devidas a tempo de evitar ou mitigar um ataque real.

O backup de todas as informações armazenadas nos servidores será realizado na forma descrita no Plano de Contingência e Continuidade de Negócios da cooperativa, com vistas a evitar a perda de informações, e viabilizando sua recuperação em situações de contingência.

As rotinas de backup são periodicamente monitoradas.

7.4. Plano de Resposta:

Havendo indícios ou de suspeita fundamentada, a DTI e PRODAF realizarão os procedimentos necessários nos serviços prestados pelas mesmas de modo a identificar o evento ocorrido.

Os procedimentos a serem aplicados poderão variar de acordo com a natureza e o tipo do evento.

Na hipótese de vazamento de Informações Sigilosas ou outra falha de segurança, inclusive em decorrência da ação de criminosos cibernéticos, as providências pertinentes deverão ser iniciadas de modo a sanar ou mitigar os efeitos no menor prazo possível.

Em caso de necessidade, poderá ser contratada empresa especializada para combater ao evento identificado.

Caso o evento tenha sido causado por algum Colaborador, deverá ser avaliada a sua culpabilidade nos termos do Código de Ética e Conduta.

Eventos que envolvam a segurança das Informações Sigilosas ou que sejam decorrentes de quebra de segurança cibernética deverão ser formalizados em relatório para deliberação pela Diretoria da COOPERÁGUIA. Tanto o evento, quanto as medidas corretivas adotadas e a deliberação da Diretoria da COOPERÁGUIA, ainda que sumariamente, deverão constar no Relatório de Controles Internos.

A Diretoria de Tecnologia e Inovação e PRODAF serão responsáveis pelo registro e controle dos efeitos de incidentes nos serviços prestados pelas mesmas.

Os procedimentos de segurança (resposta a incidentes, cenários de incidentes e tecnologias) devem ser testados periodicamente.

O plano de ação e de resposta a incidentes deverá ser revisado sempre que necessário.

8. DIRETRIZES DE SEGURANÇA DA INFORMAÇÃO

8.1. Adoção de Comportamento Seguro:

Independentemente do meio e/ou da forma em que se encontrem, as Informações Sigilosas podem ser encontradas na sede da COOPERÁGUIA e fazem parte do ambiente de trabalho de todos os Colaboradores. Portanto, é fundamental para a proteção delas que os Colaboradores adotem comportamento seguro e consistente.

Na COOPERÁGUIA, o processo relacionado à cultura de segurança cibernética compreende os seguintes procedimentos:

a) Programa de conscientização realizado anualmente;
b) A Diretoria da COOPERÁGUIA é responsável por implementar e manter o programa de conscientização;
c) Novos colaboradores devem ser treinados sobre a Política de Segurança Cibernética;
d) Associados da COOPERÁGUIA são informados sobre precaução no uso de seus serviços através dos canais de comunicação e atendimento utilizados pela Cooperativa;
e) A Diretoria da COOPERÁGUIA é responsável por compartilhar alterações nos procedimentos de segurança da informação da COOPERÁGUIA através de e-mail para colaboradores e através do site da cooperativa para os associados.

O uso do e-mail corporativo é exclusivo para assuntos relacionados aos negócios conduzidos pela COOPERÁGUIA. Desde que não haja abusos, o eventual uso do e-mail para assuntos particulares é tolerado. É terminantemente proibido o envio de mensagens e arquivos anexos que possam causar constrangimento a terceiros, bem como conteúdo político ou outro que possa colocar a COOPERÁGUIA em risco.

A COOPERÁGUIA se reserva o direito de monitorar o uso dos dados, informações, serviços, sistemas e demais recursos de tecnologia disponibilizados aos seus Colaboradores, e que os registros e o conteúdo dos arquivos assim obtidos poderão ser utilizados para detecção de violações aos documentos internos da cooperativa e conforme o caso, servir como evidência em processos administrativos, arbitrais ou judiciais.

A Diretoria da COOPERÁGUIA implantará as medidas necessárias para realizar o monitoramento, bem como para estabelecer as permissões de acesso aos documentos e arquivos da COOPERÁGUIA. Nesse sentido, o monitoramento poderá ser realizado pela DTI mediante:

a) Gravação em vídeo do ambiente da cooperativa;
b) Registro de mensagens de e-mail;
c) Registro de acesso à Internet;
d) Registro de acesso à rede interna;
e) Registro de acesso a documentos e arquivos.

Esse monitoramento poderá ser realizado automaticamente (software e/ou hardware), pela Diretoria de Tecnologia e Inovação (DTI).

Apenas Diretoria de Tecnologia e Inovação (DTI) poderá acessar os arquivos contendo as gravações e registros do monitoramento realizado, bem como, mediante autorização prévia da Diretoria da COOPERÁGUIA poderá contratar prestadores de serviços externos para realizar o monitoramento.

O acesso será realizado aleatoriamente, de maneira inopinada e sem periodicidade definida. Os documentos, dados e informações encaminhadas pelos prestadores de serviços serão para uso exclusivo da Diretoria da COOPERÁGUIA.

Sempre que necessário será lavrado termo de monitoramento e acesso aos arquivos contendo registros e gravações.

8.2. Gestão de Acesso a Sistemas de Informação e a Outros Ambientes Lógicos:

O uso das Informações Sigilosas e dos recursos de tecnologia disponibilizados pela COOPERÁGUIA é monitorado, e os registros decorrentes do uso poderão ser utilizados para verificação e evidência da adequação das regras desta Política, e demais regras internas da cooperativa, através de monitoramento a ser efetuado pela Diretoria de Tecnologia e Inovação (DTI).

Todo acesso às Informações Sigilosas, aos ambientes lógicos e à sede da COOPERÁGUIA deve ser controlado, de forma a garantir permissão apenas às pessoas expressamente autorizadas pela Diretoria da COOPERÁGUIA.

O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

a) Pedido formal de concessão e cancelamento de autorização de acesso do usuário aos sistemas;
b) Utilização de identificador do Colaborador (ID de Colaborador) individualizado, de forma a assegurar a responsabilidade de cada Colaborador por suas ações e omissões;
c) Verificação se o nível de acesso concedido é apropriado ao perfil do Colaborador e se é consistente com a Política de Segregação das Atividades;
d) Remoção imediata de autorizações dadas aos Colaboradores afastados ou desligados da COOPERÁGUIA, ou que tenham mudado de função, se for o caso; e
e) Revisão periódica das autorizações concedidas.

8.3. Utilização da Internet:

O uso da Internet deve restringir-se às atividades relacionadas aos negócios e serviços da COOPERÁGUIA, e para a obtenção de informações e dados necessários ao desempenho dos trabalhos.

8.4. Sites na Internet

O acesso a sites externos na Internet é monitorado. Os arquivos contendo os registros das tentativas de acesso e dos acessos são armazenados nos servidores da Diretoria de Tecnologia e Inovação.

Adicionalmente, o Diretor Responsável pela Política de Segurança Cibernética no UNICAD poderá ser informado sobre acessos e tentativas de acesso a determinados sites.

8.5. Ramais Telefônicos:

O ramal telefônico utilizado pela OUVIDORIA da COOPERÁGUIA é gravado, e o conteúdo das conversas é armazenado em arquivos no servidor da DTI. Conforme já esclarecido anteriormente, a Diretoria da COOPERÁGUIA possui livre acesso às gravações com o propósito de verificação de conteúdo.

Ao término da verificação, a Diretoria da COOPERÁGUIA emitirá termo de monitoramento, conforme Anexo I, informando o arquivo acessado, a data do acesso e se foram identificados indícios que possam indicar eventual infração ao disposto nesta Política, e nos demais documentos internos da cooperativa.

8.6. Telefones Celulares:

Os Colaboradores deverão evitar utilizar telefones celulares durante o horário de expediente enquanto estiverem na sede da COOPERÁGUIA. Os aparelhos deverão ser mantidos no modo "silencioso" e somente poderão ser atendidas ligações pessoais de reconhecida importância para a cooperativa.

8.7. Mensagens Instantâneas:

A comunicação por mensagens instantâneas de texto e voz pela Internet para assuntos particulares deve ser evitada durante o horário de expediente, enquanto os Colaboradores estiverem na sede da COOPERÁGUIA, mas não está proibida. Em caso de necessidade, os Colaboradores devem permitir o acesso a todas as mensagens instantâneas com o propósito de avaliar eventuais infrações ao disposto nos documentos internos.

8.8. Utilização e Conexão de Equipamentos:

Somente é permitido o uso de equipamentos homologados e devidamente contratados pela COOPERÁGUIA.

A utilização de equipamentos pessoais por terceiros nas instalações da COOPERÁGUIA e a conexão destes na rede interna e à Internet requer autorização prévia e expressa a Diretoria da COOPERÁGUIA. Os Colaboradores estão autorizados a conectar seus telefones celulares e computadores pessoais diretamente à rede interna e à Internet, desde que utilizem suas credenciais de acesso.

A conexão de dispositivos móveis de armazenamento (e.g. USB Drive) somente poderá ser realizada mediante autorização prévia e expressa da Diretoria da COOPERÁGUIA.

8.9. Acesso de Terceiros:

O acesso de terceiros aos arquivos e sistemas da COOPERÁGUIA será possível, na forma definida pelo o Diretor Responsável pela Política de Segurança Cibernética no UNICAD, mas deve sempre ser precedido da assinatura de um contrato de confidencialidade que estabeleça penalidade no caso de infração. Ademais, o terceiro deverá garantir à cooperativa, ainda que contratualmente, de que possui os controles necessários à boa guarda e proteção das informações aos quais terá acesso.

9. ENDEREÇO ELETRÔNICO

A presente Política está disponível no endereço eletrônico da COOPERÁGUIA: **http://cooperaguia.coop.br/** Eventuais comunicações para o Diretor Responsável pela Política de

Segurança Cibernética no UNICAD devem ser enviadas para: **cooperaguia@cooperaguia.coop.br**.

10. REVISÕES E ATUALIZAÇÕES

Esta Política será revisada ao menos uma vez a cada ano. Não obstante as revisões estipuladas poderão ser alteradas sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

A Diretoria da COOPERÁGUIA informará aos Colaboradores sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da COOPERÁGUIA na Internet, conforme indicado acima.

11. VIGÊNCIA

Compete ao Diretor Responsável pela Política de Segurança Cibernética no UNICAD aprovar esta Política, devendo este ato ser evidenciado em ata de reunião do referido órgão estatutário.

12. 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.

13. 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.

14. 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.

A comunicação deverá ser realizada até dez dias após a contratação dos serviços, e ter 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.

15. 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".

16. 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.

17. 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.

18. 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.

19. 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.

Proteção do Ambiente

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, para 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 consequentemente 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.

20. 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.

Esta política, aprovada pela Diretoria da COOPERÁGUIA na reunião de 27/03/2024 deverá ser revisada no mínimo a cada dois anos, ou, por alteração normativa, recomendação de órgãos fiscalizadores, melhorias identificadas pela administração da cooperativa.

Cariacica, ES, 27 de março de 2024.

DocuSigned by:
52F9D89D07084C4...

Gilberto Vieira da Silva
Diretor Presidente

DocuSigned by:
Andreia Gabriel
4C86C77F9C5C4C5...

Andreia Gabriel Bastos Ferreira
Diretora Administrativa

DocuSigned by:
Ciro Ferreira da Rocha
899F24CCBAC1440...

Ciro Ferreira da Rocha
Diretor Comercial

DocuSigned by:
Hudson Vieira
A98FDEBBD74D41C...

Hudson Vieira da Silva
Diretor Operacional

21. ANEXO I - TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES E DE SEGURANÇA CIBERNÉTICA

ANEXO I

TERMO DE ADESÃO À POLÍTICA DE SEGURANÇA DAS INFORMAÇÕES E DE SEGURANÇA CIBERNÉTICA

Eu, _____, inscrito no CPF/MF sob o nº _____ , declaro que li e estou plenamente de acordo com as disposições da Política de Segurança das Informações e de Segurança Cibernética aprovados pela COOPERÁGUIA em ..... Comprometo-me a cumprir com os termos dispostos na mesma, preservando a confidencialidade das informações as quais terei acesso.

Local e data

_____
Assinatura
Nome: