POLÍTICA DE SEGURANÇA CIBERNÉTICA

COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS SERVIDORES MUNICIPAIS DO SUL FLUMINENSE LTDA.

COOVRE

POLÍTICA DE SEGURANÇA CIBERNÉTICA

PREÂMBULO

Este documento: Política de Segurança Cibernética tem como objetivo atender as determinações do Banco Central do Brasil, que através da Resolução BACEN 4.658/2018, revogada pela Resolução CMN Nº 4.893/2021, que cumprindo decisão do Conselho Monetário Nacional, dispôs sobre A Política de Segurança Cibernética e Sobre os Requisitos para a Contratação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem a serem observados pelas Instituições Financeiras, cujos princípios, conceitos, valores e práticas serão adotados pelos administradores e demais membros estatutários, funcionários e colaboradores em geral da COOVRE, com base em princípios e diretrizes contidos neste documento, buscando assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados pela Cooperativa.

Este documento está dividido nas seguintes seções:

1 – Do Objeto e do Âmbito de Aplicação
2 - Importância da Segurança da Informação
3 - Princípios da Segurança da Informação
4 -Plano de Ação e de Resposta a Incidentes
4.1 –Regras do Uso dos Recursos de Tecnologia
4.2 - Regras para o Uso do Computador
4.3 - Regras para o Uso da Internet
4.4 - Regras para Uso do Correio Eletrônico
4.5 - Regras para Uso do Telefone
4.6 - Linhas Gerais do Comportamento Seguro
5 – Contratação de serviços de Processamento e Armazenamento de Dados em Nuvem.

1 –DO OBJETO E DO ÂMBITO DE APLICAÇÃO

A COOVRE deve implementar e manter Política de Segurança Cibernética, conforme definições em princípios e diretrizes a seguir relacionados, de modo a assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

Essa Política será compatível com os seguintes aspectos:

I. O porte da Cooperativa, que é classificada como "Cooperativa de Capital e Empréstimo" pela Resolução CMN n° 5.051/2022,e classificada como perfil de risco ponderado na forma simplificada, por restrições de diversas operações, que não tem permissão para realizar;

II. A natureza de suas operações, não havendo complexidade dos produtos que pode operar por sua classificação; e,

III. A sensibilidade dos dados e das informações sob responsabilidade da Cooperativa.

A COOVRE não faz parte de nenhum Sistema Cooperativo de Crédito, sendo, portanto, considerada, uma Cooperativa "Solteira" para o Banco Central do Brasil, sendo filiada à Federação Nacional das Cooperativas de Crédito Urbano - FENACRED.

2 – A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

A importância está baseada na proteção preventiva de toda a cadeia de dados confidenciais ou não processados, que são de responsabilidade da Cooperativa, e que são manuseados pelos membros estatutários ou colaboradores da Cooperativa, visando a plena confidencialidade desses dados nas diversas formas que são gerados, com ênfase no armazenamento cibernético.

Essa proteção preventiva requer controles e níveis de acesso às informações; a contínua vigilância e principalmente, sistemas adequados e confiáveis contratados para processamentos e armazenamentos de dados.

3 – PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Conforme está previsto na Resolução CMN Nº 4.893/2021, devem ser previstos diversos aspectos da segurança cibernética e que irão nortear essa política:

I – Objetivos da Segurança Cibernética -assegurar a confidencialidade, a integridade e a disponibilidade dos dados e dos sistemas de informação utilizados.

II –Procedimentos e os controles adotados para reduzir a vulnerabilidade da Cooperativa a incidentes e atender aos objetivos da segurança cibernética - Esses procedimentos requerem controles e níveis de acesso às informações; a contínua vigilância e principalmente, sistemas adequados e confiáveis contratados para processamentos e armazenamentos de dados.

III –Controles específicos, incluindo os voltados para a rastreabilidade da informação, que busquem garantir a segurança das informações sensíveis – Esses procedimentos requerem a utilização de equipamentos e programas confiáveis, com a utilização de programas antivírus adequados e capazes de assegurar a confiabilidade da proteção, aliado a uma manutenção preventiva e constante dessas ferramentas. O armazenamento em nuvem deverá ser adotado como princípio de segurança confiável.

IV – O registro, a análise da causa e do impacto, bem como o controle dos efeitos de incidentes relevantes para as atividades da instituição – Deve-se estar atento às tentativas de ataques cibernéticos, bem como as apurações em casos de incidentes relevantes ou não, pois qualquer ocorrência demonstrará falhas nas defesas ou prevenções, devendo ser debatidas as ocorrências nos diversos níveis operacionais da Cooperativa, buscando aprimoração dos mecanismos preventivos.

V – As diretrizes para:

a) A elaboração de cenários de incidentes considerados nos testes de continuidade de negócios – Deve-se levar em consideração cenários que possam abalar os negócios, causando interrupções danosas às operações; acesso e roubos de informações confidenciais; acesso e roubos nas contas de depósitos da Cooperativa; destruição de arquivos e bancos de dados; bloqueio de acessos com a liberação mediante resgates criminosos, entre outros.

b) A Definição de procedimentos e de controles voltados à prevenção e ao tratamento de incidentes a serem adotados por empresas prestadoras de serviços a terceiros que manuseiem dados ou informações sensíveis ou que seja relevantes para a condução das atividades operacionais da Cooperativa – Trata-se de uma parte extremamente relevante na política de segurança cibernética, pois a relação cooperativa e as empresas prestadoras desses serviços, deve estar estruturada além da sua capacitação técnica, na confiabilidade recíproca

conquistada em anos de relacionamento. Juridicamente deve estar ancorada em contrato, que seja considerado um ato jurídico perfeito, com cláusulas pétreas e preventivas de segurança, além dos aspectos técnicos sobre os serviços contratados e outros, devendo ser revisto periodicamente para atualizações, aperfeiçoando essa relação com uma segurança jurídica garantidora da prestação dos serviços.

c) A classificação dos dados e das informações quanto a relevância - A Cooperativa como instituição financeira, opera com informações protegidas por sigilo de acordo com a Legislação em vigor (Lei Complementar 105/2001), que relaciona essas operações cuja violação é passível de penalizações. Essas operações elencadas terão tratamento prioritário na classificação de dados na política de segurança cibernética tanto pela relevância, quanto pela penalização imposta por sua violação. O seu manuseio e acesso pelas pessoas que por dever de ofício tem autorização para fazê-lo, deverão ser cientificadas quanto a violações. Outros tipos de dados e informações poderão ter classificação mais abrandada nas atividades da cooperativa.

d) A definição dos parâmetros a serem utilizados na avaliação da relevância dos incidentes – Como está evidenciado no item "c" anterior, os parâmetros levarão em consideração em primeiro lugar, as informações previstas na Lei Complementar 105/2001 e que a cooperativa por sua classificação está autorizada a operar. Atendida essa relevância, as demais informações serão avalizadas por outros critérios, dentro das relevâncias julgadas pertinentes.

VI – Os mecanismos de disseminação da cultura de segurança cibernética na cooperativa, incluindo:

a) A implementação de programas de capacitação e de avaliação periódica de pessoal – Dentro dos programas de treinamento e capacitação dos membros estatutários e colaboradores, a cooperativa incluirá a segurança cibernética como programa de capacitação, bem como a avaliação do pessoal.

b) A prestação de informações a clientes e usuários sobre precaução na utilização de produtos e serviços financeiros –Essa é uma parte sensível no relacionamento cooperativa e seus associados, pois a cooperativa apesar de sua classificação como "capital e empréstimo", centrando suas operações nessas duas modalidades, não pode negligenciar nas orientações e precauções na utilização desses serviços. Os colaboradores serão orientados sempre na prestação dos atendimentos e a informações e orientações no trato desses

serviços, que são protegidos pelo sigilo previstos na Lei Complementar 105/2001.

c) O comprometimento da alta administração com a melhoria contínua dos procedimentos relacionados com a segurança cibernética - A diretoria da cooperativa deverá ter comprometimento prioritário com a segurança cibernética, pois além de ter um diretor responsável indicado pela segurança, deverá buscar estar inteirada no que ocorre na área de segurança cibernética, atuando preventivamente, cobrando informações e providências diuturnas.

VII – As iniciativas para compartilhamento de informações sobre incidentes relevantes mencionados no inciso IV, com outras cooperativas de crédito –Trata-se de uma prática que não é comum, mas que deve ser buscada em função de que diversos incidentes são comuns tendo como origem fontes idênticas e o mesmo "modus operandi". Uma das formas seria através das empresas de informática contratadas, e que prestam serviços a diversas cooperativas e serviriam de elo de compartilhamento de incidentes, e que para tanto, deveriam ser autorizadas a divulgarem incidentes ocorridos para ações preventivas.

CONSIDERAÇÕES COMPLEMENTARES SOBRE OS INCISOS CITADOS ANTERIORMENTE:

Inciso I – Deverá ser contemplada a capacidade da cooperativa para prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, situação esta que está ligada aos operadores do sistema de informática (equipamentos e programas), com sistemas adequados de detecção.

Inciso II – Os procedimentos e controles devem abranger, no mínimo, a autenticação, a criptografia, a prevenção e a detecção de intrusão, a prevenção de vazamento de informações, a realização periódica de testes e varreduras para detecção da vulnerabilidade, a proteção contra programas maliciosos, o estabelecimento de mecanismos de rastreabilidade, os controles de acesso e de segmentação da rede de computadores e a manutenção de cópias de segurança dos dados e das informações, devendo também ser aplicado, no desenvolvimento ou contratação de sistemas de informação seguros, e na adoção de novas tecnologias empregadas na atividade da cooperativa.

Inciso IV – O registro, a análise da causa e o impacto, bem como o controle dos efeitos de incidentes, devem abranger inclusive informações recebidas das empresas de prestação de serviços de informática contratadas.

Inciso V – As diretrizes devem contemplar procedimentos e controles em níveis de complexidade, abrangência e precisão compatíveis com os utilizados pela cooperativa.

4 – PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES.

A Cooperativa estabelecerá Plano de Ação e de Resposta a Incidentes que é parte integrante da Política de Segurança Cibernética.

Este Plano abrangerá o seguinte:

1) Ações a serem desenvolvidas pela Cooperativa para adequar suas estruturas organizacional e operacional aos princípios e às diretrizes de segurança cibernética previstas.

2) As rotinas, os procedimentos, os controles e as tecnologias que serão utilizadas na prevenção e na resposta a incidentes, em conformidade com as diretrizes da política de segurança prevista.

3) A área responsável pelo registro e controle dos efeitos de incidentes relevantes, que estará afeta ao diretor responsável designado pela Política de Segurança Cibernética, a ser informado ao BACEN através do UNICAD.

4.1 – Regras do Uso dos Recursos de Tecnologia

. Os recursos tecnológicos que são de propriedade da cooperativa, são autorizados e disponibilizados exclusivamente para os usuários desempenharem suas funções a serviço da cooperativa.

- A comunicação através dos recursos tecnológicos deve ser formal e profissional dentro da ética, de modo a preservar a imagem institucional da cooperativa.
- Os conteúdos acessados e transmitidos através dos recursos de tecnologia devem ser legais, bem como a utilização de equipamentos e programas, de modo a contribuir para atividades profissionais dentro da ética.
- O uso dos recursos de tecnologia deverá ser submetido a testes periódicos pela Auditoria Interna, com pleno conhecimento e autorização da diretoria da cooperativa, e em conformidade com a Resolução CMN Nº 4.893/2021.
- Cada usuário é responsável pelo uso dos recursos tecnológicos que lhe for confiado e autorizado, que estarão sob sua custódia, garantindo a

conservação, guarda e legalidade dos programas instalados, sendo vedado o uso de programas ilegais nos equipamentos.

- Os recursos de tecnologia da cooperativa disponibilizados para os usuários, não podem ser repassados para terceiros estranhos à cooperativa, salvo em caso de autorização expressa.
- Qualquer anormalidade ou irregularidade nos recursos de tecnologia devem ser comunicados de imediato aos superiores hierárquicos.

4.2 Regras do Uso do Computador

- O (s) computador (es) disponibilizado(s) para o usuário é de propriedade da cooperativa, é deve(m) ser utilizado(s) com zelo e os cuidados necessários para assegurar seu(s) pleno (s) funcionamento dentro da vida útil estimada de uso(s).
- O computador é uma ferramenta tecnológica disponibilizada para o usuário, que tem como objetivo facilitar o desempenho de suas atividades profissionais, com o pressuposto do usuário possuir capacitação técnica para utilizar a ferramenta.
- A utilização do(s) equipamento(s) poderá implicar e/ou exigir a utilização de senha específica e login de acesso, bem como limites de acesso, de modo a que se possa identificar a qualquer tempo o usuário na realização de tarefas, pois a senha e o login serão a assinatura digital do usuário.
  A cooperativa pode a qualquer tempo suspender, limitar e/ou proibir o acesso de usuário, em casos supervenientes que justifiquem,
- É vedada a cessão de senha pelo usuário, sendo de sua inteira responsabilidade tal ocorrência, pois a mesma é pessoal e intransferível.
- Será exigido que num prazo de 180 dias as senhas sejam trocadas, podendo ocorrer a qualquer momento pelo usuário ou superior hierárquico.
- Os programas básicos, operacionais e aplicativos instalados no(s) computador(res) são de responsabilidade da cooperativa, cabendo ao usuário a sua correta utilização, desde que esteja capacitado para tal, e em caso de necessidades, deverá encaminhar solicitação a superior hierárquico de novas configurações.
- O usuário tem a responsabilidade de cuidar adequadamente do(s) equipamento(s) que utiliza, sendo considerado o custodiante desses

recursos, garantindo a sua integridade física, seu funcionamento, bem como solicitação de manutenção.

- Bloqueios de acesso podem ser implantados como formas preventivas de incidentes, devendo o usuário estar sempre atento a atualizações de programas de proteção antivírus; tentativas de ataques; programas maliciosos e outras situações que possam redundar em incidentes, devendo estar também sempre atento a realizar cópias de segurança de programas e arquivos, se for de sua responsabilidade, evitando negligências como não realizar cópias nos períodos determinados; armazenar em locais seguros, mesmo que faça arquivamento de dados em nuvem; não deixar cópias de segurança acopladas a equipamentos, pois em caso de ataques as perdas custarão caro.
- O usuário deve estar ciente que a instalação ou utilização de programas não autorizados, constitui crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19.02.1998, sujeitando os infratores a pena de detenção e multa. A cooperativa não se responsabiliza por qualquer ação individual que esteja em desacordo com a lei mencionada, sendo considerada sua prática uma ameaça à segurança da informação, e será tratada com aplicação de ações disciplinares.

4.3 - Regras do Uso da Internet

- O usuário é responsável por todo acesso realizado com sua autenticação.
- Não é permitido ao usuário acessar endereços na Internet que possam violar direitos de autor; marcas; licenças de programas ou patentes existentes registradas; conteúdo pornográfico, relacionado a sexo, exploração infantil ou ao crime de pedofilia; contenham informações que não colaborem ou prejudiquem para o alcance dos objetivos da Cooperativa; defendam atividades ilegais; menosprezem, depreciem ou incitem o preconceito a determinadas classes como sexo, raça, orientação sexual, religião, nacionalidade, local de nascimento ou deficiência física.
- O usuário deve garantir que está cumprindo a legislação em relação ao direito autoral, licença de uso e patentes existentes, e que o uso do material foi autorizado pelo gestor de sua área.

- O uso de serviços tais como mensagens instantâneas; uso de serviço de rádio, TV, download de vídeos, filmes, músicas, e correio eletrônico particular, poderão ser tolerados suas utilizações pelo usuário, desde que não se confunda e nem prejudiquem os trabalhos da Cooperativa, situação que poderá não ser permitida e até proibida.

4.4 - Regras do Uso do Correio Eletrônico:

- A cooperativa disponibiliza endereços de seu correio eletrônico para utilização dos usuários, no desempenho de suas funções profissionais, que pode ser o geral da cooperativa coovre@uol.com.br, como também específico para o usuário, desde que simplifique e agilize os trabalhos a realizar.
- No caso de endereço eletrônico individual para usuário, este é intransferível e pertence à cooperativa, sendo o mesmo enquanto permanecer o vínculo com a Cooperativa.
- Em caso de necessidade por qualquer que seja o motivo justificado e aprovado, poderá haver alteração no endereço individual
- O usuário que utiliza o endereço individual do correio eletrônico da cooperativa, é responsável por todo o acesso, conteúdo de mensagens e uso relativo ao seu e-mail, podendo enviar mensagens necessárias ao seu desempenho profissional e a sua atuação na cooperativa.
- Não é permitido criar, copiar ou encaminhar mensagens ou imagens que contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza; façam parte de correntes de mensagens, independentemente de serem legais ou ilegais.
- O usuário deve estar ciente que o correio eletrônico da cooperativa deve ser utilizado para os serviços da instituição em todos os seus aspectos formais e profissionais, devendo abster-se de uso particular ou em benefício de terceiros não autorizados, salvo se previamente autorizado.
- O uso indevido do correio eletrônico da cooperativa será passível de sanções disciplinares, principalmente por tratar-se de uma forma de comunicação sensível para a imagem da cooperativa como instituição financeira, não devendo ser exposta de maneira inadequada por essa poderosa ferramenta de comunicação, até por causa das implicações

legais dessas mensagens, sendo até utilizadas como provas em juízo em casos de contendas.

4.5 – Regras do Uso do Telefone

- A cooperativa disponibiliza telefone(s) fixo(s) para utilização dos membros estatutários e usuários colaboradores, para atendimento ao quadro social e ao público m geral.
- O telefone como meio de comunicação, é parte fundamental da segurança da informação da cooperativa.
- Sua utilização fundamental é ser um canal de comunicação entre a cooperativa e seus associados, sendo prioritário o seu funcionamento nessa tarefa.
- O usuário colaborador deve saber que esse tipo de comunicação alavanca as atividades da cooperativa, e por isso deve ser utilizado de forma ética e profissional no trato com sua clientela, e que são os seus associados.
- Os atendimentos devem ser formais e objetivos aos usuários clientes, fornecedores e ao público em geral, de modo a fique evidenciado um padrão de atendimento que será uma das marcas da cooperativa para esse público.
- O usuário colaborador deve ser breve e objetivo, sendo que nos casos em que não consiga dar o atendimento adequado, deve dirigir ao superior hierárquico sua solução.
- O usuário colaborador pode receber e fazer chamadas particulares, mas sempre com brevidade e objetividade, de modo que a(s) linha(s) estejam prontamente liberadas o mais rápido possível para atendimento do público usuário.
- O uso racional das linhas telefônicas pressupõe economia no custo mensal com telefone, devendo ser buscado e implementado por todos.
- O usuário colaborador deverá estar sempre atento em evitar prestar informações confidenciais no telefone ao quadro social, uma vez que pode não ser a pessoa do outro lado da linha, a não ser que pela prática, tenha a plena certeza que se trata do associado certo e que busca informações, principalmente as confidenciais. Via de regra, as informações confidenciais devem ser prestadas presencialmente, ou

através de sistemas confiáveis. Nunca é demais lembrar que o vazamento de informações confidenciais, são passíveis de punições por força da Lei Complementar 105/2001.

4.6 – Linhas Gerais do Comportamento Seguro

- O usuário colaborador deve saber que o acesso à cooperativa é vedado para aqueles que não são membros estatutários e usuários colaboradores e/ou prestadores de serviços. O acesso quando ocorrer para quem é vedado, deve ser sob expressa autorização e de forma limitada. Os dados confidenciais não podem ser acessados de maneira alguma para quem não é permitido. O atendimento ao quadro social e ao público em geral, deve ser de forma destacada, e de preferência, sem acesso ao local de trabalho da equipe.
- O usuário colaborador deve ter sempre o devido cuidado no ambiente externo da cooperativa, evitando falar informações restritas e confidenciais, como também em portar "laptops ou pendrives" com informações confidenciais.
- O usuário colaborador deve ter o devido cuidado com o lixo de informações confidenciais. Deve-se procurar utilizar fragmentadoras de papéis para o correto descarte desses documentos.
- O usuário colaborador deve ter o devido e imprescindível cuidado com suas senhas e logins de acesso aos equipamentos, pois eles são suas assinaturas digitais, e a sua violação pode gerar enormes prejuízos à cooperativa, e punições serão inevitáveis, que poderão ser no mínimo por negligência.
- O usuário colaborador deverá adotar um comportamento seguro quanto a não compartilhar e nem divulgar sua senha a terceiros; não transportar informações confidenciais sem o conhecimento e/ou a devida autorização; não discutir assuntos confidenciais em ambiente público; abrir e-mails com mensagens de origem desconhecida ou suspeita; armazenar e proteger adequadamente documentos impressos e arquivos eletrônicos com informações confidenciais, e por fim, seguir corretamente a política de segurança cibernética para uso da Internet e correio eletrônico, ou outras formas de comunicação, como aplicativos WhatsApp; Facebook; Instagram e outros, caso sejam utilizados pela cooperativa.

5 – CONTRATAÇÃO DE SERVIÇOS DE PROCESSAMENTO E ARMAZENAMENTO DE DADOS E DE COMPUTAÇÃO EM NUVEM.

A Resolução BACEN 4.893/2021, prevê que as instituições financeiras devem assegurar que suas políticas estratégicas e estruturas para gerenciamento de riscos de segurança cibernética, devem levar em consideração os critérios de decisão quanto à terceirização na contratação de serviços relevantes de processamento e armazenamento de dados e de computação em nuvem, tanto no país e/ou no exterior.

Previamente à contratação desses serviços, devem ser adotados procedimentos que:

I – A adoção de práticas de governança corporativa e de gestão proporcionais à relevância do serviço a ser contratado e aos riscos a que estejam expostas.

II – A verificação da capacidade do potencial prestador de serviços de assegurar o cumprimento da legislação e da regulamentação em vigor; o acesso da cooperativa aos dados e às informações a serem processados ou armazenados pelo prestador de serviços; a confidencialidade, a integridade, a disponibilidade e a recuperação dos dados e das informações processados ou armazenados pelo prestador de serviços; sua aderência a certificações exigidas; o acesso da cooperativa aos relatórios gerados pelas auditorias independente do prestador de serviços, relativos aos procedimentos e aos controles utilizados na prestação dos serviços a serem contratados; o provimento de informações e de recursos de gestão adequados no monitoramento dos serviços a serem prestados; identificação e segregação dos dados dos clientes da cooperativa por meio de controles físicos ou lógicos e a qualidade dos controles de acesso voltados à proteção dos dados e das informações.

OPÇÃO I – A Cooperativa tem contrato de Prestação de Serviços de Processamento e Armazenamento de Dados e de Computação em Nuvem com a Empresa: Prodaf Informática; CNPJ 02.915.447/0001-16; com sede na Avenida Waldemar Mees, 43, sala 302, Centro, Marechal Floriano, ES CEP 29255-000.

Esta Política de Segurança Cibernética foi aprovada em Reunião da Diretoria da Cooperativa de Economia e Crédito Mútuo dos Servidores Municipais do Sul Fluminense Ltda. – COOVRE, em 29/07/21, revisada e aprovada pela diretoria em 27/02/2025, devendo ser divulgada para todos os membros estatutários; aos usuários colaboradores, e bem com ao quadro social.

Volta Redonda, 27 de fevereiro de 2025.

Maurício Cezar Pinho
Diretor Presidente

Paulo Roberto Souza de Oliveira
Diretor Financeiro

Carlos Roberto Nunes da Cunha
Diretor Administrativo

Ivanil de Souza
Conselheiro

RELATÓRIO ANUAL SOBRE A IMPLEMENTAÇÃO DO PLANO DE AÇÃO E DE RESPOSTA A INCIDENTES INERENTES À POLIÍTICA DE SEGURANÇA CIBERNÉTICA DA COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS SRVIDORES MUNICIPAIS DO SUL FLUMINENSE LTDA.

O Diretor Responsável pela Política de Segurança Cibernética e pela Execução do Plano de Ação e de Resposta a Incidentes da Cooperativa de Economia e Crédito Mútuo dos Servidores Municipais do Sul Fluminense Ltda., apresenta à Diretoria da Cooperativa, o RELATÓRIO ANUAL sobre a implementação do Plano de Ação e de Resposta a Incidentes referente ao exercício de 202..... – Data-Base ...../202....., inerente a Política de Segurança Cibernética da Cooperativa vigente, conforme a seguir:

Tendo em vista que não houve ocorrências a registrar de incidentes cibernéticos no exercício de 202....., apresentamos as seguintes considerações nos tópicos do Relatório Anual.

I – SOBRE A EFETIVIDADE DS IMPLEMENTAÇÃO DAS AÇÕES DESENVOLVIDAS PARA ADEQUAÇÃO DA ESTRUTURA ORGANIZACIONAL E OPERACIONAL AOS PRINCÍPIOS E ÀS DIRETRIZES DA POLÍTICA DE SEGURANÇA CIBERNÉTICA.

Consideramos que a implementação das ações de adequação da estrutura organizacional e operacional das diretrizes da Política de Segurança Cibernética implantadas na cooperativa, estão em conformidade com o previsto.

Os sistemas contratados de Serviços de Implementação e Manutenção de Sistema Informatizado para Controle de Gestão Administrativa, Financeira e Contábil, com a empresa Prodaf Informática funcionaram a contento no decorrer do exercício de 202....., sem ocorrências de incidentes a registrar de

incidentes, pelo que consideramos que os fundamentos de segurança estão aptos e operantes, por propiciarem o pleno funcionamento da cooperativa sem interrupções nos serviços.

Da mesma forma, os serviços de contratação de armazenamento de dados em novem funcionaram a contento, com a geração de cópias de segurança de backup e os seus armazenamentos em nuvem asseguraram uma garantia à continuidade dos negócios.

II- DOS RESULTADOS OBTIDOS NA IMPLEMENTAÇÃO DAS ROTINAS, DOS PROCEDIMENTOS, DOS CONTROLES E DAS TECNOLOGIAS UTILIZADAS NA PREVENÇÃO E NA RESPOSTA A INCIDENTES OCORRIDOS NO PERÍODO

Atestamos que os resultados obtidos na implementação das rotinas dos procedimentos, controles e das tecnologias utilizadas, deram maior segurança na prevenção de incidentes que pudessem afetar a continuidade dos negócios ou causar prejuízos na atividade da cooperativa.

III – RELATO DOS INCIDENTES RELEVANTES OCORRIDOS NO AMBIETE CIBERNÉTICO NO PERÍODO.

Atestamos que não houve incidentes relevantes a relatar no exercício de 202... no ambiente cibernético, dando a tranquilidade necessária para a continuidade dos negócios dentro de um ambiente previsível e confiável.

IV- RESULTADOS DOS TESTES DE CONTINUIDADE DE NEGÓCIOS CONSIDERANDO CENÁRIOS DE INDISPONIBILIDADE OCASIONADA POR INCIDENTES.

Conforme está previsto em contratos, temos assegurado a continuidade dos negócios em casos de incidentes cibernéticos, pela rápida recuperação de dados e sistemas armazenados em nuvem, com a substituição imediata de servidor próprio afetado por servidor virtual da empresa contratada, bem com a sua assistência técnica, o que nos dá uma certa tranquilidade nesse aspecto, de poder contar com uma rápida resposta a incidentes.

Conclusão

Isto posto senhores diretores, submeto à consideração dessa diretoria, o Relatório Anual do exercício de 202....., do Plano de Ação e de Resposta a Incidentes da Política de Segurança Cibernética da COOP.....

Volta Redonda, ...

Carlos Roberto Nunes da Cunha

Diretor Responsável pela Política de **Segurança Cibernética**

COOPERATIVA DE ECONOMIA E CRÉDITO MÚTUO DOS SERVIDORES MUNICIPAIS DO SUL FLUMINENSE LTDA. – COOVRE

CHECKLIST DE SEGURANÇA CIBERNÉTICA

DATA: ...../...../.....

1. ORIENTAÇÃO A TODOS OS COLABORADORES SOBRE A UTILIZAÇÃO DOS COMPUTADORES, INTERNET E E-MAILS

☐ Diponibilizar Política de Segurança Cibernética da COOVRE para todos os colaboradores, que contempla o uso seguro de computadores, internet e e-mails.

☐ Promover a realização de cursos voltados para o tema.

☐ Reforçar periodicamente as boas práticas de como evitar o uso indevido de e-mails e o acesso a sites não seguros.

☐ Instruir sobre o uso adequado de senhas (complexidade, mudança periódica e nunca compartilhar).

☐ Relembrar sobre a proibição de instalar softwares não autorizados nos computadores da cooperativa.

Considerações:_____

_____

2. VERIFICAÇÃO DE COMPUTADORES NÃO AUTORIZADOS OU SOFTWARES NÃO LICENCIADOS

☐ Verificar se todos os computadores estão devidamente autorizados e configurados conforme a Política de Segurança Cibernética da COOVRE.

☐ Verificação quanto a instalação de softwares não licenciados ou não autorizados.

☐ Verificar licenciamento de todos os softwares utilizados pela cooperativa.

☐ Atualizar regularmente a lista de softwares licenciados e os requisitos de conformidade.

Considerações: _____

_____

3. MANTER OS SISTEMAS OPERACIONAIS E SOFTWARES DE APLICAÇÃO SEMPRE ATUALIZADOS, INSTALANDO AS ATUALIZAÇÕES SEMPRE QUE FOREM DISPONIBILIZADAS

☐ Ativar atualizações automáticas para sistemas operacionais e softwares licenciados essenciais.

☐ Verificar a disponibilidade de novas atualizações e aplicar atualizações de segurança.

☐ Verificar compatibilidade de novos patches de segurança com sistemas existentes.

Considerações: _____

_____

4. MONITORAR DIARIAMENTE AS ROTINAS DE BACKUP, EXECUTANDO TESTES REGULARES DE RESTAURAÇÃO DOS DADOS

☐ Verificar se o backup diário está sendo realizado.

☐ Armazenar backups em locais seguros, preferencialmente com redundância (ex.: backup na nuvem e em mídia física).

☐ Monitorar alertas de falhas no backup e garantir que as falhas sejam corrigidas imediatamente.

Considerações: _____

_____

5. REALIZAR, PERIODICAMENTE TESTES DE INVASÃO EXTERNA E PHISHING, COM O APOIO DA EMPRESA DE TI CONTRATADA

☐ Planejar e executar testes de invasão sempre que houver mudanças significativas na infraestrutura.

☐ Simular ataques de phishing para avaliar a conscientização dos colaboradores e a eficácia dos controles de segurança.

☐ Fornecer feedback e treinamento adicional para os colaboradores identificados como alvos em tentativas de phishing.

Considerações: _____

_____

6. REALIZAR ANÁLISES DE VULNERABILIDADES NA ESTRUTURA TECNOLÓGICA PERIODICAMENTE OU SEMPRE QUE HOUVER MUDANÇA SIGNIFICATIVA EM TAL ESTRUTURA, COM O APOIO DA EMPRESA DE TI CONTRATADA

☐ Realizar uma análise de vulnerabilidades em toda a infraestrutura tecnológica, pelo menos uma vez por trimestre.

☐ Priorizar correções de vulnerabilidades com maior impacto potencial.

☐ Garantir que qualquer mudança significativa na infraestrutura (ex.: nova implementação de sistemas, novos dispositivos, atualizações importantes) seja seguida de uma análise de vulnerabilidade.

☐ Documentar todos os resultados das análises e as ações corretivas realizadas.

Considerações: _____

_____

7. TESTAR O PLANO DE AÇÃO E DE RESPOSTA À INCIDENTES, SIMULANDO OS CENÁRIOS COM O APOIO DA EMPRESA DE TI CONTRATADA

- [ ] Revisar e atualizar o plano de resposta a incidentes sempre que houver mudanças significativas na estrutura ou por forças normativas.

- [ ] Realizar simulações de incidentes de segurança, como ataques cibernéticos ou violações de dados, ao menos uma vez por ano.

- [ ] Avaliar a eficácia da resposta a incidentes com base nos resultados dos testes.

- [ ] Documentar os aprendizados e ajustar o plano de resposta conforme necessário.

- [ ] Garantir que todos os membros da equipe saibam qual é o procedimento a seguir em caso de incidente real.

Considerações: _____

_____

Este checklist abrange práticas e atividades essenciais para garantir a segurança e a conformidade tecnológica dentro da COOVRE, sendo aprovada a sua adoção a partir de 27/02/2025.