COOPSOL
Cooperativa de Economia e Crédito Mútuo dos Empregados do Sebrae Bahia LTDA

Política de Segurança Cibernética e da Informação

Política aprovada pela Diretoria da cooperativa, conforme Resolução 4.893/21 do Banco Central do Brasil, em reunião ordinária realizada em **16/11/2022**.

1. INTRODUÇÃO

A Política de Segurança Cibernética e da Informação da **COOPSOL** é uma declaração formal da cooperativa acerca do seu compromisso com a proteção de Informações Confidenciais e Segurança Cibernética (*cybersecurity*), conforme definição adiante, devendo ser cumprida por todos os integrantes do seu quadro de atividades.

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

O Diretor, Alberto Bispo do Nascimento, é o responsável por esta Política de Segurança Cibernética e da Informação.

2. OBJETIVO

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

Via de regra, nenhuma Informação Confidencial 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 Confidencial, seja sobre a cooperativa, relativa às suas atividades, aos seus cooperados 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 **COOPSOL** são classificados entre: “confidencial”, “público” e “privado”. A Diretoria é responsável por essa classificação. Os dados e as informações devem ser reclassificados sempre que houver mudanças relevantes ou no mínimo anualmente.

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

3. APLICAÇÃO

A efetividade desta Política depende da conscientização de todos os Colaboradores e do esforço constante para que seja feito bom uso das Informações Confidenciais e dos ativos disponibilizados pela cooperativa ao Colaborador.

Esta Política deve ser conhecida e obedecida por todos os Colaboradores que utilizam os recursos de tecnologia disponibilizados pela cooperativa, sendo de responsabilidade individual e coletivo o seu cumprimento.

4. ATRIBUIÇÕES/OBJETIVOS

Esta política tem como objetivo atender a resolução nº 4.893/21 do Banco Central do Brasil e estabelecer os princípios, conceitos, valores e práticas que devem ser adotados na utilização dos recursos que tangem as informações acessadas pelos Diretores, Colaboradores e Prestadores de Serviços da **COOPSOL** na sua atuação e com o mercado.

A **COOPSOL** incorpora em seus valores a certeza de que o exercício de suas atividades e o crescimento de seus negócios devem se basear em princípios éticos, os quais devem ser disseminados por todos os seus colaboradores. Na busca de melhoria contínua do seu desenvolvimento e da satisfação dos cooperados, a **COOPSOL** busca transparência e cumprimento da legislação aplicável às atividades de gestão de recursos de terceiros.

A elaboração desta Política representa o compromisso dos diretores, colaboradores e prestadores de serviços que trabalham na Cooperativa com os valores e as práticas baseadas na integridade, confiança e lealdade. Portanto, a constante busca do crescimento da **COOPSOL** e a defesa dos interesses dos associados estarão sempre relacionadas nas diretrizes aqui expostas.

A área de Controles Internos é responsável pela implementação de um sistema de supervisão que indique que os controles de segurança da informação estão sendo devidamente executados conforme os níveis adotados pela **COOPSOL**. Logo, a área de Controles Internos está apta a constatar eventuais desvios de conduta que possam colocar em risco: Cooperados, Colaboradores e a própria Cooperativa.

5. IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

A Política de Segurança da Informação é uma importante aliada na prevenção e na recuperação de incidentes de segurança, definindo critérios, normas e procedimentos seguros para proteger os ativos da informação e garantir as propriedades básicas de segurança nos sistemas de informação.

Os pilares da segurança da informação nos dão subsídios para proteger as informações da **COOPSOL**. Portanto, quando mencionamos “segurança da informação” entende-se que estamos falando de proteções voltadas às informações impressas, verbais e sistêmicas, bem como nos controles de acesso, vigilância, contingência de desastres naturais, contratações, cláusulas e demais questões que juntas formam uma proteção adequada para qualquer empresa. (ISO 27002 A.5.1.1)

5.1 - O que é Política de Segurança da Informação?

É um conjunto de diretrizes que definem formalmente as regras, os direitos e deveres de todos os colaboradores, visando à proteção adequada dos que compartilham a informação. Ela também define as atribuições de cada um dos profissionais em relação à segurança dos recursos com os quais trabalham, além disso, deve prever o que pode ser feito e o que será considerado inaceitável. (ISO 27002 A.5.1.1)

5.2 - A informação é só o que está nos sistemas?

Entende-se por informação todo e qualquer conteúdo ou dado que tenha valor para a organização ou pessoa. Além do que está armazenado nos computadores, a informação também está impressa em relatórios, documentos, arquivos físicos, ou até mesmo repassada através de conversas nos ambientes interno e externo da Cooperativa.

Por isso, todo cuidado é pouco na hora de imprimir relatórios, jogar papéis no lixo, deixar documentos em cima da mesa, conversar sobre a Cooperativa em locais públicos ou com pessoas estranhas ao nosso meio. (ISO 27002 A.5.1.1)

6. RESPONSABILIDADE NA GESTÃO DA POLÍTICA

6.1 – Alta Administração

a) prover recursos para a implementação, manutenção e melhoria da gestão da segurança da informação;
b) prover comprometimento e apoio à aderência a Política de Segurança Cibernética e da Informação de acordo com os objetivos e estratégias de negócio estabelecidas para organização;
c) fornecer à área responsável pela Segurança da Informação claro direcionamento, apoio, recomendação e apontar restrições sempre que necessário;
d) identificar requisitos legais pertinentes a segurança da informação;
e) garantir a adoção de cláusulas pertinentes à segurança da informação nos contratos estabelecidos com a cooperativa.

6.2 – Colaboradores:

a) cumprir fielmente esta Política;
b) buscar orientação do superior hierárquico imediato em caso de dúvidas relacionadas à segurança das Informações Confidenciais;
c) proteger Informações Confidenciais contra acesso, modificação, destruição ou divulgação não autorizadas pela cooperativa;
d) assegurar que os recursos de tecnologia à sua disposição sejam utilizados apenas para as finalidades aprovadas ou não proibidas expressamente 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 Confidenciais;
f) comunicar imediatamente à diretoria sobre qualquer descumprimento ou violação desta Política;
g) utilizar de modo seguro, responsável, moral e ético todos os serviços e sistemas de TI;
h) notificar ao responsável de TI sobre as violações da Política de Segurança Cibernética e da Informação e sobre os incidentes de segurança que venha a tomar conhecimento;
i) manter o sigilo das informações que tenha obtido acesso enquanto Colaborador da cooperativa, mesmo após seu desligamento da empresa.

6.3 – Gestor

a) Apoiar e incentivar o estabelecimento da Política de Segurança Cibernética e da Informação na Cooperativa;
b) garantir que seus subordinados tenham acesso e conhecimento desta Política e demais normas e padrões de segurança da informação;
c) fornecer os recursos financeiros, técnicos e humanos necessários para desenvolver, implantar, manter e aprimorar a segurança das informações da cooperativa;
d) avaliar periodicamente o grau de sigilo e segurança necessários para a proteção das informações sob sua responsabilidade e de sua equipe;
e) designar mais de um responsável para atuação em processos e operações suscetíveis a fraudes e tomando os devidos cuidados para preservar a segregação de funções;
f) acionar as áreas competentes para a aplicação das penalidades, cabíveis aos Colaboradores que violarem a Política de Segurança Cibernética e da Informação e as normas da Cooperativa; e
g) autorizar acessos de seus colaboradores apenas quando forem realmente necessários e segundo os conceitos de *need to know* e *least privilegie*.

6.4 – Área de Infraestrutura

a) orientar e coordenar as ações de segurança da informação, promovendo a execução de acordo com o que foi estabelecido;
b) desenvolver e estabelecer programas de conscientização e divulgação da Política de Segurança Cibernética e da Informação;
c) conduzir o processo de Gestão de Riscos de Segurança da Informação;

d) conduzir a Gestão de Incidentes de Segurança da Informação, incluindo as investigações para determinação de causas e responsáveis, bem como a comunicação dos fatos ocorridos;
e) conduzir os processos de monitoramento e segurança da informação;
f) definir controles para tratamento de riscos, vulnerabilidades, ameaças e não conformidades identificadas pelos processos de SI;
g) propor projetos e iniciativas para melhoria do nível de segurança das informações da COOPSOL;
h) manter atualizada a infraestrutura tecnológica, de acordo com a recomendação de fabricantes de *hardware* e *software*;
i) tratar os riscos e vulnerabilidades identificados em ativos, sistemas ou processos sob sua responsabilidade ou custódia;
j) conduzir a gestão dos acessos a sistemas e informações da COOPSOL;
k) implantar e manter funcionais os controles e padrões de segurança definidos para os ativos de tecnologia;
l) informar imediatamente a alta direção, sobre violações, falhas, anomalias e outras condições que possam colocar em risco as informações e ativos da COOPSOL;
m) controlar alterações em ativos de TI e garantir que estas sejam analisadas criticamente e testadas para que não ocorram impactos adversos na operação da empresa ou em sua segurança;
n) garantir a continuidade dos serviços tecnológicos de forma a atender aos requisitos essenciais do negócio;
o) garantir que todos os ativos críticos de Tecnologia da Informação devem ser instalados em ambientes especializados conhecidos como *Datacenters*. Estes devem conter todas as proteções e contingências necessárias para a sua respectiva proteção.

6.5 – Fornecedores e Parceiros de Negócios

a) cumprir as determinações da Política, Normas e Procedimentos publicados pela COOPSOL;
b) orientar os funcionários da empresa sobre o cumprimento das determinações da Política, Normas e Procedimentos publicados pela COOPSOL; e
c) cumprir com o acordo de confidencialidade.

6.6 – Penalidades

O colaborador que presenciar o descumprimento de alguma das regras acima tem o dever de denunciar tal infração ao responsável pela Infraestrutura. Ademais, o descumprimento das regras e diretrizes impostas neste documento poderá ser considerado falta grave, passível de aplicação de sanções disciplinares.

No caso de prestadores de serviços terceirizados, pode ser solicitada às suas respectivas empresas a troca da equipe alocada na COOPSOL, ou ainda, podem ser aplicadas penalidades a empresa tais como multas, cancelamento do contrato e ações judiciais.

7. CONCEITOS E PRINCIPIOS

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

As Informações Confidenciais 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 a garantir a segurança de Informações Confidenciais 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 Confidenciais devem abranger três aspectos básicos, destacados a seguir:

a) **acesso**: somente pessoas devidamente autorizadas pela cooperativa devem ter acesso às Informações Confidenciais;
b) **integridade**: somente alterações, supressões e adições autorizadas pela cooperativa devem ser realizadas às Informações Confidenciais;
c) **disponibilidade**: as Informações Confidenciais devem estar disponíveis para os Colaboradores autorizados sempre que necessário ou for demandado; e
d) **confidencialidade**: Proteção da informação compartilhada contra acessos não autorizados. Ameaça à segurança acontece quando há uma quebra de sigilo de uma determinada informação, permitindo que sejam expostas voluntária ou involuntariamente, dados restritos e que deveriam ser acessíveis apenas por um determinado grupo de usuários.

Para assegurar os 04 (quatro) aspectos acima, as Informações Confidenciais 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; e
d) plano de resposta.

A implantação e monitoramento da capacidade da cooperativa que atender a estes pilares deverá ser feito pelo Diretor responsável. Também a fim de atingir os objetivos dispostos acima, cada setor da cooperativa terá suas próprias responsabilidades.

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

8. REGRAS DE USO DE TECNOLOGIA

a) Os meios que permitem o acesso à informação são autorizados e disponibilizados exclusivamente para o usuário desempenhar suas funções na COOPSOL ou para outras situações formalmente permitidas. (ISO A.6.1.3)
b) Quando o usuário se comunicar através dos recursos de tecnologia da COOPSOL, a linguagem falada ou escrita deve ser profissional, de modo que não comprometa a imagem da Cooperativa. (ISO A.7.1.3)
c) Os conteúdos acessados e transmitidos através dos recursos de tecnologia da COOPSOL devem ser legais, de acordo com o Código de Ética, e devem contribuir para as atividades profissionais do usuário. (ISO A.15.1.5)
d) O uso dos recursos de tecnologia da COOPSOL pode ser examinado, auditado ou verificado pela empresa, mediante autorização expressa da Diretoria, sempre respeitando a legislação vigente. (ISO A.10.10.1)
e) Cada usuário é responsável pelo uso dos recursos que lhe foram fisicamente entregues, e estão sob sua custódia, garantindo a conservação, guarda e legalidade dos programas (*softwares*) instalados (ISO A.6.1.3)
f) Os recursos de tecnologia da COOPSOL, disponibilizados para os usuários, não podem ser repassados para outra pessoa interna ou externa à organização. (ISO A.6.1.3)
g) Ao identificar qualquer irregularidade no recurso de tecnologia o usuário deve comunicar imediatamente à área de Controles Internos. (ISO A.13.1.1)

9. REGRAS DE USO DO COMPUTADOR

I. Propriedade do Computador

O recurso computador disponibilizado para o usuário é de propriedade da COOPSOL.

II. Disponibilização e uso

O recurso computador disponibilizado para o usuário pela COOPSOL tem por objetivo o desempenho das atividades profissionais desse usuário na Cooperativa. É necessário que o gestor do usuário o autorize a usar o computador. Deve ser feita uma solicitação à área de Suporte de TI, que autorizará tecnicamente e fará a liberação mediante a disponibilização de recursos.

Todos os equipamentos, *softwares* e permissões de acessos devem ser testados, homologados e autorizados pela Diretoria para o uso na COOPSOL. Além disso, a Cooperativa pode a qualquer momento retirar ou substituir o computador disponibilizado para o usuário.

Cada computador tem o seu gestor, que é responsável por esse equipamento. O controle das máquinas é de responsabilidade da Diretoria da Cooperativa.

A identificação do usuário ao computador é feita através de *login* e senha disponibilizado pela empresa responsável pela TI, portanto ela é sua assinatura eletrônica. Os usuários que não possuem perfil de administrador deverão ter senha de tamanho variável, possuindo no mínimo 6 (seis) caracteres alfanuméricos, utilizando caracteres especiais (@ # $ %) e variação entre caixa-alta e caixa-baixa (maiúsculo e minúsculo) sempre que possível.

Já os usuários que possuem perfil de administrador ou acesso privilegiado deverão utilizar uma senha de no mínimo 8 (oito) caracteres, alfanumérica, utilizando caracteres especiais (@ # $ %) e variação de caixa-alta e caixa-baixa (maiúsculo e minúsculo) obrigatoriamente.

É de responsabilidade de cada usuário a memorização de sua própria senha, bem como a proteção e a guarda dos dispositivos de identificação que lhe forem designados.

As senhas não devem ser anotadas ou armazenadas em arquivos eletrônicos (*Word, Excel*, etc.), compreensíveis por linguagem humana (não criptografadas); não devem ser baseadas em informações pessoais, como próprio nome, nome de familiares, data de nascimento, endereço, placa de veículo, nome da empresa, nome do departamento; e não devem ser constituídas de combinações óbvias de teclado, como “abcdefgh”, “87654321”, entre outras.

Após 03 (três) tentativas de acesso, a conta do usuário será bloqueada. Para o desbloqueio é necessário que o usuário entre em contato com o responsável pelo TI.

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.

A periodicidade máxima para troca das senhas é 90 (noventa) dias, não podendo ser repetidas as 03 (três) últimas senhas. Os sistemas críticos e sensíveis para a instituição e os *logins* com privilégios administrativos devem exigir a troca de senhas a cada 30 dias. Os sistemas devem forçar a troca das senhas dentro desse prazo máximo.

Todos os acessos devem ser imediatamente bloqueados quando se tornarem desnecessários.

Portanto, assim que algum usuário for demitido ou solicitar demissão, deverá imediatamente comunicar tal fato ao responsável pela Tecnologia da Informação, a fim de que essa providência seja tomada. A mesma conduta se aplica aos usuários cujo contrato ou prestação de serviços tenha se encerrado, bem como aos usuários de testes e outras situações similares.

III. Programas utilizados no computador

Os programas aplicativos, programas básicos, como sistema operacional e ferramentas, e componentes físicos são implantados e configurados pela área de suporte. É desabilitado aos usuários implantar novos programas ou alterar configurações sem a permissão formalizada da Gerência. Como também é desabilitado ao usuário implantar ou alterar componentes físicos no computador.

IV. Responsabilidade do usuário

Cuidar adequadamente do equipamento, pois o usuário é o custodiante deste recurso. Garantir a sua integridade física e o seu perfeito funcionamento, seguindo as regras e orientações fornecidas pela área de Suporte de TI.

V. Outras proteções

É implantada a proteção de tela no computador e/ou proteção de ausência (após um tempo de inatividade, o computador bloqueia o sistema, exigindo senha para ser usado novamente). Como também é implantado o "*log-off*" automático por inatividade durante o período de 24 (vinte e quatro) horas.

VI. Termo de Compromisso

Para ter acesso à informação da COOPSOL, o usuário deverá assinar (manual ou eletronicamente) um termo de compromisso. Os casos de exceção serão definidos pela Diretoria.

O Controle Interno da COOPSOL alerta todos os usuários que a instalação ou utilização de *software* não autorizados constitui em crime contra a propriedade intelectual, de acordo com a Lei 9.609 de 19/02/1998, sujeitando os infratores à pena de detenção e multa. A COOPSOL não se responsabiliza por qualquer ação individual que esteja em desacordo com a Lei mencionada acima. Todas as práticas que representem ameaça à segurança da informação serão tratadas com a aplicação de ações disciplinares.

10. REGRAS DE USO DE *INTERNET*

a. Responsabilidade e forma de uso

O usuário é responsável por todo acesso realizado com a sua autenticação. Sendo assim, todas as regras visam basicamente o desenvolvimento de um comportamento eminentemente ético e profissional do uso da *internet*. Embora a conexão direta e permanente da rede corporativa da instituição com a *internet* ofereça um grande potencial de benefícios, ela abre a porta para riscos significativos para os ativos de informação.

Qualquer informação que é acessada, transmitida, recebida ou produzida na *internet* está sujeita a divulgação e auditoria. Portanto, a COOPSOL, em total conformidade legal, reserva-se ao direito de monitorar e registrar todos os acessos a ela.

Os equipamentos de tecnologia e serviços fornecidos para o acesso à *internet* são de propriedade da instituição, que pode analisar e, se necessário, bloquear qualquer arquivo, *site*, correio eletrônico, domínio ou aplicação armazenados na rede/*internet*, estejam eles em disco local, na estação ou em áreas privadas da rede, visando assegurar o cumprimento de sua Política de Segurança Cibernética e da Informação.

A COOPSOL, ao monitorar a rede interna, pretende garantir a integridade dos dados e programas. Dessa forma, toda tentativa de alteração dos parâmetros de segurança, por qualquer colaborador, sem o devido credenciamento e a autorização para tal, será julgada inadequada e os riscos relacionados serão informados ao colaborador e a Diretoria.

O uso de qualquer recurso para atividades ilícitas poderá acarretar ações administrativas e as penalidades decorrentes de processos civil e criminal, sendo que nesses casos a instituição cooperará ativamente com as autoridades competentes.

A *internet* disponibilizada pela instituição aos seus colaboradores, independentemente de sua relação contratual, pode ser utilizada para fins pessoais, desde que não prejudique o andamento dos trabalhos.

Como é do interesse da COOPSOL que seus colaboradores estejam bem informados, o uso de *sites* de notícias ou de serviços, por exemplo, é aceitável, desde que não comprometa a banda da rede em horários estritamente comerciais, não perturbe o bom andamento dos trabalhos, nem implique conflitos de interesse com os seus objetivos de negócio.

Apenas os colaboradores autorizados pela instituição poderão copiar, captar, imprimir ou enviar imagens da tela para terceiros, devendo atender à norma interna de

uso de imagens, à Lei de Direitos Autorais, à proteção da imagem garantida pela Constituição Federal e demais dispositivos legais.

É proibida a divulgação e/ou o compartilhamento indevido de informações da área administrativa em listas de discussão, *sites* ou comunidades de relacionamento, salas de bate-papo ou *chat*, comunicadores instantâneos ou qualquer outra tecnologia correlata que venha surgir na *internet*.

Os colaboradores com acesso à *internet* poderão fazer o *download* (baixa) somente de programas ligados diretamente às suas atividades e deverão providenciar o que for necessário para regularizar a licença e o registro desses programas, desde que autorizados pela Diretoria.

O uso, a instalação, a cópia ou a distribuição não autorizada de *softwares* que tenham direitos autorais, marca registrada ou patente na *internet* são expressamente proibidos. Qualquer *software* não autorizado baixado será excluído.

Os colaboradores não poderão em hipótese alguma utilizar os recursos da COOPSOL para fazer o *download* ou distribuição de *software* ou dados pirateados, atividade considerada delituosa de acordo com a legislação nacional.

O *download* e a utilização de programas de entretenimento, jogos ou músicas (em qualquer formato) poderão ser realizados por usuários que tenham atividades profissionais relacionadas a essas categorias.

Como regra geral, materiais de cunho sexual não poderão ser expostos, armazenados, distribuídos, editados, impressos ou gravados por meio de qualquer recurso.

Colaboradores com acesso à *internet* não poderão efetuar *upload* (subida) de qualquer *software* licenciado para COOPSOL ou de dados de sua propriedade aos seus parceiros e clientes, sem expressa autorização do responsável pelo *software* ou pelos dados.

Os colaboradores não poderão utilizar os recursos da COOPSOL para deliberadamente propagar qualquer tipo de vírus, *worm*, cavalo de troia, *spam*, assédio, perturbação ou programas de controle de outros computadores.

O acesso a *softwares peer-to-peer (Kazaa, BitTorrent e afins)* não serão permitidos. Já os serviços de *streaming* (rádios *on-line*, canais de *broadcast* e afins) serão permitidos de acordo com a necessidade e autorização da Diretoria.

Não é permitido acesso a sites de *proxy*. 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 pela Diretoria.

b. Uso de serviços de mensagem instantânea

Serviços de comunicação instantânea (*WhatsApp, Telegram, Facebook Messenger* e afins) serão disponibilizados apenas aos usuários indicados pela Diretoria e poderão ser bloqueados de acordo com a necessidade da Diretoria.

c. Bloqueio de endereços de *Internet*

Periodicamente a área de infraestrutura revisará e bloqueará o acesso para os endereços da *Internet* que não estejam alinhados com esta Política e com o Código de Ética da Cooperativa.

11. REGRAS DO USO DO CORREIO ELETRÔNICO (*E-MAIL*)

a. Endereço eletrônico do usuário

A COOPSOL disponibiliza endereços de correio eletrônico do domínio do Sebrae BA para utilização do usuário no desempenho de suas funções profissionais. (ex: setor@trc.sebraeba.com.br)

O endereço eletrônico disponibilizado para o usuário é individual e intransferível, sendo assim o endereço eletrônico cedido para o usuário deve ser o mesmo durante todo o seu período de vínculo com a COOPSOL. Se houver necessidade de troca de endereço, a alteração deverá ser autorizada pela Diretoria e registrada para possibilitar uma posterior verificação de autoria.

b. Criação, manutenção e exclusão do endereço de correio eletrônico

A utilização desse endereço de correio eletrônico pelo usuário necessita ser autorizado pela Diretoria. A liberação do endereço de correio eletrônico será feita pela Diretoria de maneira controlada e segura com o objetivo de garantir que apenas o usuário tenha possibilidade de utilizar o referido endereço.

Quando acontecer desligamento de usuário, a Cooperativa deverá comunicar a área de Suporte de TI e bloquear os usuários das redes.

c. Acesso à distância

O usuário pode acessar o seu endereço eletrônico cedido pela COOPSOL mesmo quando estiver fora do ambiente da empresa, através do serviço de correio eletrônico via *internet* (*web mail*).

d. Propriedades do endereço

O endereço de correio eletrônico disponibilizado para o usuário e as mensagens associadas a esse endereço são de propriedade da COOPSOL. Em situações autorizadas pela Diretoria, as mensagens do correio eletrônico de um usuário poderão ser acessadas pela COOPSOL ou por pessoas por ela indicada. Não deve ser mantida, portanto, expectativa de privacidade pessoal.

e. Responsabilidades e forma de uso

O usuário que utiliza um endereço de correio eletrônico é responsável por todo acesso, conteúdo de mensagens e uso relativos ao seu *e-mail*, pode enviar mensagens necessárias para o seu desempenho profissional na Cooperativa. É proibido criar, copiar ou encaminhar mensagens ou imagens que:

i. Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;
ii. Façam parte de correntes de mensagens, independentemente de serem legais ou ilegais;
iii. Repassem programadas ou mensagens de alerta sobre qualquer assunto. Havendo situações em que o usuário ache benéfico divulgar o assunto para a Cooperativa, a sugestão deve ser encaminhada para a Diretoria, que definirá a sua publicação ou não;
iv. Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, local de nascimento ou deficiência física;
v. Possuam informação pornográfica, obscena ou imprópria para um ambiente profissional;
vi. Sejam susceptíveis de causar qualquer tipo de prejuízo a terceiros;
vii. Defendam ou possibilitem a realização de atividades ilegais;
viii. Possam prejudicar a imagem da COOPSOL; e
ix. Sejam incoerentes com o nosso Código de Ética.

É proibido reproduzir qualquer material recebido pelo correio eletrônico ou outro meio, que possa infringir direitos de autor, marca, licença de uso de programas ou patentes existentes, sem que haja autorização expressa do autor do trabalho e da organização.

O usuário deve estar ciente que uma mensagem de correio eletrônico da COOPSOL é um documento formal e, portanto, possui as mesmas responsabilidades de um documento convencional em papel timbrado da entidade. Exceto quando especificamente autorizado para tal, é proibido emitir opinião pessoal, colocando-a em nome da COOPSOL. Devendo sempre observar se o endereço do destinatário corresponde realmente ao destinatário desejado. Deve ser diligente em relação:

i. Aos usuários que receberão a mensagem (Destinatário/to, copiado/Cc e Copiado Oculto/Bcc);
ii. Ao nível de sigilo da informação contida na mensagem;
iii. Aos anexos da mensagem, enviando os arquivos apenas quando for imprescindível e garantindo a confidencialidade dos mesmos;
iv. Ao uso da opção encaminhar (*Forward*), verificando se é necessária a manutenção das diversas mensagens anteriores que estão encadeadas.

O usuário deverá deixar mensagem de ausência quando for passar um período maior do que 48 horas sem acessar seu correio eletrônico. Essa mensagem deve indicar o período de ausência e o endereço do substituto e para quem deve ser enviada a mensagem.

12. REGRAS DO USO DO TELEFONE

a. Número do telefone do usuário

A COOPSOL disponibiliza telefones para utilização do usuário no desempenho de suas funções profissionais. Se houver necessidade de troca de telefone, a alteração deverá ser autorizada pela Diretoria e registrada para possibilitar uma posterior verificação de autoria.

b. Propriedades do número do telefone

O telefone disponibilizado para o usuário e as conversas associadas a esse número são de propriedade da COOPSOL.

c. Responsabilidade e forma de uso

O usuário que utiliza um telefone:

i. É responsável por todo conteúdo da conversa;
ii. Pode utilizar o telefone para o seu desempenho profissional na empresa;
iii. É proibido utilizar o telefone para conversas que:

- Contenham declarações difamatórias ou linguagem ofensiva de qualquer natureza;

- Menosprezem, depreciem ou incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade, naturalidade ou deficiência física;
- Possuam informações pornográfica, obscena ou imprópria para um ambiente profissional;
- Defendam ou possibilitem a realização de atividades ilegais;
- Possam prejudicar a imagem da COOPSOL;
- Sejam incoerentes com o nosso Código de Ética.

13. MONITORAMENTO E AUDITORIA DO AMBIENTE

Para garantir as regras mencionadas nesta Política, bem como de sua versão educacional, a COOPSOL poderá:

i. Implantar sistemas de monitoramento nas estações de trabalho, servidores, correio eletrônico, conexões com a *internet*, dispositivos móveis ou *wireless* e outros componentes da rede – a informação gerada por esses sistemas poderá ser usada para identificar usuários e respectivos acessos efetuados, bem como material manipulado;
ii. Tornar públicas as informações obtidas pelos sistemas de monitoramento e auditoria, no caso de exigência judicial, solicitação e determinação da Diretoria;
iii. Realizar, a qualquer tempo, inspeção física nas máquinas de sua propriedade;
iv. Instalar sistemas de proteção, preventivos e detectáveis, para garantir a segurança das informações e dos perímetros de acesso.

14. CÓPIAS DE SEGURANÇA *(BACKUP)*

Para que seja possível uma gestão segura, efetiva, confiável, administrável e passível de auditoria:

a) A cópia de segurança é feita de forma centralizada no ambiente dos equipamentos e servidores corporativos, sob a responsabilidade da área de Suporte de TI ou empresa fornecedora do serviço;
b) A área de Suporte de TI ou a empresa fornecedora, fornecerá o serviço de recuperação, a partir dos arquivos de cópia de segurança, cumprindo parâmetros de nível de serviço previamente estabelecido.

Todos os *backups* devem ser automatizados por sistemas de agendamento automatizado para que sejam preferencialmente executados fora do horário comercial, nas chamadas "janelas de *backup*" – períodos em que não há nenhum ou pouco acesso de usuários ou processos automatizados aos sistemas de informática.

A gestão dos sistemas de *backup* deverá realizar pesquisas frequentes para identificar atualizações de correção, novas versões do produto, ciclo de vida (quando o *software* não terá mais garantia do fabricante), sugestões de melhorias, entre outros.

O tempo de vida e uso das mídias de *backup* deve ser monitorado e controlado pelos responsáveis, com o objetivo de excluir mídias que possam apresentar riscos de gravação ou de restauração decorrentes do uso prolongado, além do prazo recomendado pelo fabricante.

Os *backups* imprescindíveis, críticos, para o bom funcionamento dos negócios, exigem uma regra de retenção especial, seguindo as determinações fiscais e legais existentes no país.

Na situação de erro de *backup* e/ou *restore* é necessário que ele seja feito logo no primeiro horário disponível, assim que o responsável tenha identificado e solucionado o problema.

Testes de restauração (*restore*) de *backup* devem ser executados por seus responsáveis, nos termos dos procedimentos específicos, aproximadamente a cada 30 ou 60 dias, de acordo com a criticidade do *backup.*

Por se tratar de uma simulação, o executor deve restaurar os arquivos em local diferente do original, para que assim não sobreponha os arquivos válidos.

15. CLASSIFICAÇÃO DA INFORMAÇÃO

É de responsabilidade da Diretoria estabelecer critérios relativos ao nível de confidencialidade da informação (relatórios e/ou mídias) gerada por sua área de acordo com a tabela abaixo:

a) **Pública** - É toda informação que pode ser acessada por usuários da organização, clientes, fornecedores, prestadores de serviços e público em geral.
b) **Interna** - É toda informação que só pode ser acessada por funcionários da organização. São informações que possuem um grau de confidencialidade que pode comprometer a imagem da organização.
c) **Confidencial** - É toda informação que pode ser acessada por usuários da organização e por parceiros da organização. A divulgação não autorizada dessa informação pode causar impacto (financeiro, de imagem ou operacional) ao negócio da organização ou ao negócio do parceiro.
d) **Restrita** - É toda informação que pode ser acessada somente por usuários da organização explicitamente indicado pelo nome ou por área a que pertence. A divulgação não autorizada dessa informação pode causar sérios danos ao negócio e/ou comprometer a estratégia de negócio da organização.

16. REDE SEM FIO *(WIFI):*

O acesso à rede *Wi-Fi* da COOPSOL somente será permitido aos funcionários, terceirizados e cooperados devidamente cadastrados.

O cooperado e terceirizado que desejar usufruir desta tecnologia, deverá solicitar as informações necessárias de acesso aos funcionários da COOPERATIVA, o usuário estará ciente e de acordo com as normas abaixo:

a) Não fazer passar por outra pessoa ou dissimular sua identidade quando utilizar os recursos computacionais;
b) Responsabilizar-se pela sua identidade eletrônica, senha, credenciais de autenticação, autorização ou outro dispositivo de segurança;
c) Responder pelo mau uso dos recursos computacionais em quaisquer circunstâncias;
d) Responder por atos que violem as regras de uso dos recursos computacionais, estando, portanto, sujeito às penalidades legais;
e) O cooperado ou terceirizado deve manter seus computadores pessoais com *softwares* de *drivers* e antivírus atualizados.

Por tratar de uma rede sem fio particular fornecida apenas para os funcionários, cooperados e terceirizados, o acesso à *internet* é monitorado e terá restrições de acesso. Se necessário, o cooperado e/ou terceirizado deve procurar a COOPERATIVA para maiores esclarecimentos.

17. LINHAS GERAIS DE COMPORTAMENTO

No ambiente externo, é melhor ficar atento

Falar sobre informações restritas ou segredos profissionais em um lugar público ou por telefone merecem cuidado especial. Frequentemente, as pessoas são o elo mais fraco na segurança da informação de uma Cooperativa.

Quando seu equipamento viajar com você, evite deixá-lo por muito tempo sozinho em uma sala ou mesa da Cooperativa. Qualquer *pendrive* ou conexão de rede pode conter dados valiosos.

Cuidado com o lixo que você produz

O lixo pode ser uma fonte de informações para pessoas mal intencionadas. Destrua os documentos que contenham informações sensíveis, pessoais ou da COOPSOL antes de descartá-los. Se o papel que vai ser jogado no lixo contém informações que não devem ser lidas por estranhos, rasgue-o antes de jogá-lo fora.

Cuidado com senhas e acessos no sistema

Cada tarefa desenvolvida na COOPSOL precisa ter um responsável. A única forma de saber o responsável por cada atividade é através da identificação do usuário. Tudo que é feito com a sua identificação (assinatura ou senha) é de sua responsabilidade. Portanto, cuidado com seus dados, seja na rede ou nos sistemas, pois sua identificação serve para garantir que você é realmente quem está usando esse acesso. Se uma outra pessoa tem acesso a sua senha, ela poderá utilizá-la para se passar por você, porém, a responsabilidade por tudo que ela fizer será sua.

Alguns exemplos de ações que podem ser atribuídas a você, são:

a) Liberação de ações indevidas;
b) *E-mails* com informações inadequadas; e
c) Acesso a páginas da *internet* proibidas.

Compartilhar sua senha é como assinar um cheque em branco. É permitido apenas a utilização de senhas fortes, isto é, com mais de 8 (oito) caracteres, combinando numéricos e alfanuméricos, maiúsculas e minúsculas e não utilize datas comemorativas, sobrenomes, nome do cônjuge, nome dos filhos, placas de carro etc. Não escreva a senha em local público ou de fácil acesso.

Adote um comportamento seguro

a) Não compartilhe nem divulgue sua senha a terceiros;
b) Não transporte informações confidenciais da COOPSOL em qualquer meio (CD, DVD, *pendrive*, papel, etc) sem as devidas autorizações e proteções;
c) Assuntos confidenciais de trabalho não devem ser discutidos em ambientes públicos ou em áreas expostas (aviões, restaurantes, encontro sociais, etc);
d) Não abra mensagens de origem desconhecida;
e) Armazene e proteja adequadamente documentos impressos e arquivos eletrônicos que contém informações confidenciais;
f) Siga corretamente a Política para uso de *internet* e correio eletrônico estabelecida pela COOPSOL.

18. GESTÃO DE MUDANÇAS

A área de Suporte de TI é responsável por participar, documentar, homologar e implementar toda e qualquer alteração seja de acesso, *hardware* e *software* ou que tenha impacto direto no desenvolvimento do negócio ou operacional da COOPSOL. As solicitações devem ser encaminhadas da Diretoria para a área de Suporte de TI, e tais demandas devem ser registradas em sistemas para acompanhamento histórico.

19. PROGRAMA DE DISSEMINAÇÃO DA CULTURA DE SEGURANÇA CIBERNÉTICA

Capacitação e Avaliação Periódica de Pessoal

A COOPSOL deverá promover continuamente a capacitação, reciclagem e o aperfeiçoamento de todos os usuários da cooperativa, por meio de programas de divulgação, sensibilização, conscientização e capacitação em segurança da informação e comunicações, com o propósito de criar uma cultura de segurança dentro da cooperativa.

Informações aos Cooperados Sobre Precauções no Uso de Produtos e Serviços da Cooperativa.

Criação de documentos que sirvam de modelos para o uso seguro dos produtos e serviços da cooperativa, esses modelos devem conter o conteúdo exato do ofertado e caso necessário deverá ser atualizado de acordo com as alterações dos produtos e serviços e deverá ser repassado para os cooperados.

Comprometimento da Diretoria com Melhoria Contínua dos Processos de Segurança da Informação.

Propor as metodologias e os processos específicos para a segurança da informação, como avaliação de risco e sistema de classificação da informação e apoiar iniciativas que visem à segurança dos ativos de informação da COOPSOL.

Publicar e promover as versões desta Política e as Normas de Segurança da Informação e conscientizar os colaboradores em relação à relevância da segurança da informação para o negócio, mediante campanhas, palestras, treinamentos e outros meios.

Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços.

20. PROCEDIMENTOS DE SEGURANÇA CIBERNÉTICA

Em conformidade com o artigo 15º da Resolução nº 4.893/21, a cooperativa deverá realizar a comunicação ao Banco Central do Brasil da contratação de serviços relevantes de processamento, armazenamento de dados e de computação em nuvem, até 10 (dez) dias após a contratação dos serviços.

21. ENDEREÇO ELETRÔNICO

Em cumprimento ao art. 4º, da Resolução nº 4.893/21, a presente Política está disponível no endereço eletrônico da **COOPSOL**: https://coopsol.coop.br/politicas-e-manuais/**.** Eventuais comunicações para o Diretor responsável devem ser enviadas através dos seguintes canais: atendimento presencial ou coopsol@trc.sebraeba.com.br.

22. REVISÕES E ATUALIZAÇÕES

De acordo com o art. 10, da Resolução nº 4.893/21, esta Política será revisada ao menos uma vez a cada ano. Não obstante as revisões estipuladas, poderá ser alterada sem aviso prévio e sem periodicidade definida em razão de circunstâncias que demandem tal providência.

Quando da atualização, todos serão informados sobre a entrada em vigor de nova versão deste documento e a disponibilizará na página da **COOPSOL** na *internet*, conforme indicado acima.

23. VIGÊNCIA

Esta Política passa a vigorar na data de sua aprovação. Conforme art. 9º, da Resolução nº 4.893/21, compete a Diretoria aprovar esta Política, devendo este ato ser evidenciado em ata de reunião do referido órgão estatutário.

Esta Política foi aprovada em Reunião Ordinária da Diretoria realizada em 16/11/2022 e segue assinada por todos os presentes.

Salvador/BA, 16 de novembro de 2022.

ALBERTO BISPO DO NASCIMENTO:37076884534
Assinado de forma digital por ALBERTO BISPO DO NASCIMENTO:37076884534
Dados: 2022.11.24 08:29:48 -03'00'

Alberto Bispo do Nascimento

Diretor Presidente

FERNANDO EDMAR DE OLIVEIRA SILVA:01338483536
Assinado de forma digital por FERNANDO EDMAR DE OLIVEIRA SILVA:01338483536
Dados: 2022.11.24 11:55:04 -03'00'

Fernando Edmar de Oliveira Silva

Diretor Operacional

RENATO LISBOA DA SILVEIRA:38055783500
Assinado de forma digital por RENATO LISBOA DA SILVEIRA:38055783500
Dados: 2022.11.24 11:14:55 -03'00'

Renato Lisboa da Silveira

Diretor

Valdirene Carvalho de Pádua
Assinado de forma digital por Valdirene Carvalho de Pádua
Dados: 2022.11.24 10:50:40 -03'00'

Valdirene Carvalho de Pádua

Diretora Administrativo e Financeiro