POLÍTICA DE TECNOLOGIA, SEGURANÇA DA INFORMAÇÃO E BACKUP

Sumário

1. OBJETIVO

Esta política estabelece diretrizes para a Segurança da Informação visando preservar a integridade, confidencialidade e disponibilidade das informações dos associados sob responsabilidade da **Cooperativa de Economia e Crédito Mútuo dos Funcionários Públicos Municipais de Itapira – Credita**, bem como descreve a conduta considerada adequada para o manuseio, controle e proteção das informações contra destruição, perdas, modificação, divulgação indevida e acessos não autorizados, sejam acidentais ou intencionais.

2. ALCANCE

Esta Política é extensiva a todos os colaboradores (funcionários, estagiários e prestadores de serviços) da **Cooperativa de Economia e Crédito Mútuo dos Funcionários Públicos Municipais de Itapira – Credita** que fazem uso de sua infraestrutura de serviços e de seus sistemas informatizados.

3. CONCEITOS/CRITÉRIOS GERAIS

A informação é um ativo que possui grande valor, devendo ser adequadamente utilizada e protegida contra ameaças e riscos.
A informação pode ser manipulada de diversas formas por meio de:

- arquivos eletrônicos;
- mensagens eletrônicas;
- internet;
- banco de dados;
- em meio impresso;
- verbalmente;
- em mídias de áudio e vídeo, etc.

A Cooperativa visando garantir a segurança de suas informações, riscos de falhas, danos e/ou prejuízos que possam comprometer a sua imagem e seus objetivos, implantou políticas e procedimentos de segurança da informação e backup que tem por princípio três aspectos básicos:

- Confidencialidade: somente pessoas devidamente autorizadas pela Cooperativa devem ter acesso à informação;

- Integridade: somente alterações, supressões e adições autorizadas pela Cooperativa devem ser realizadas nos sistemas de informações.

- Disponibilidade: a informação deve estar disponível para os colaboradores autorizados sempre que necessário ou demandado.

Para assegurar os três princípios, a informação deve ser adequadamente gerenciada e protegida contra incidentes, problemas, roubo, fraude, perda não-intencional, acidentes e outras ameaças.

4. DIRETRIZES

Somente atividades lícitas, éticas e autorizadas devem ser realizadas pelos colaboradores, quando da utilização dos recursos de processamento da informação da Cooperativa.
Uma efetiva política de tecnologia, segurança da informação e backup depende da conscientização de todos os envolvidos e do esforço constante para que se faça bom uso da informação e dos recursos de tecnologia existentes na Cooperativa.
Por isso, a política deve ser conhecida e obedecida por todos os colaboradores, estagiários e prestadores de serviços que utilizam recursos da informação de propriedade ou controlados pela Cooperativa, sendo de responsabilidade de cada um o seu fiel cumprimento.

5. RESPONSABILIDADES

5.1. Todos os Colaboradores

- Cumprir rigorosamente a Política de tecnologia, segurança da informação e backup;
- É proibido acessar informação da instituição que não for explicitamente autorizada;
- Responder pela guarda e proteção dos recursos computacionais colocados à sua disposição para o trabalho;
- Relatar prontamente à Gerência Operacional, qualquer fato ou ameaça à segurança dos recursos, tais como quebra da segurança, fragilidade, mau funcionamento, vírus, intercepção de mensagens eletrônicas, acesso indevido ou desnecessário a pastas/diretórios de rede, acesso indevido à Internet e programas instalados sem conhecimento da área operacional e da empresa prestadora de serviços de TI.
- Assegurar que as informações e dados de propriedade da Cooperativa não sejam disponibilizados a terceiros e nem discutidos em ambientes públicos ou em áreas expostas como avião, restaurantes, encontros sociais etc.
- Todo usuário recebe *login* e senha de acesso à rede, internet e e-mail da instituição.

- O *login* e senha de acesso têm caráter pessoal, e é intransferível, cabe ao seu titular total responsabilidade quanto ao seu sigilo.
- A prática de compartilhamento de senhas é terminantemente proibida e o titular que fornecer sua senha a terceiros responderá pelas infrações cometidas, estando sujeito a penalidades previstas pela Cooperativa e pela legislação vigente.
- Caso o usuário desconfie que sua senha não seja mais segura, ou de seu domínio exclusivo, poderá solicitar a Gerência Operacional a alteração desta.
- Nunca abrir ou executar arquivos eletrônicos de origem desconhecida
- Armazenar de forma adequada e protegidas a documentação impressa e arquivos com informações confidenciais.
- As mensagens eletrônicas e seus anexos são de uso exclusivo do remetente e destinatário, podendo conter informações confidenciais e/ou legalmente privilegiadas. Neste caso, não podem ser reproduzidas total ou parcialmente sem o consentimento do autor, sendo que a divulgação não autorizada é proibida.

6. EMPRESA PRESTADORA DE SERVIÇOS DE TI

A Cooperativa fechou contrato com empresa especializada no ramo de serviços de TI, que presta suporte técnico e atendimento às demandas diárias da cooperativa. A Mappre – Infraestrutura e Segurança em TI tem sede na cidade de Itapira e conta com profissionais especializados na instalação e manutenção de servidores e estações de trabalho e estão preparados para trabalhar em ambientes críticos e de alta disponibilidade. Dentre os serviços prestados, destacam-se:

- Suporte e atendimento de usuários (via chamado técnico, telefone ou visita "*in loco*");
- Visitas e manutenções preventivas e corretivas,
- Suporte nos assuntos relacionados a melhorias da estrutura de TI,
- Monitoramento de ativos importantes,
- Realização de testes para identificação de vulnerabilidade em sistemas;
- Administração de servidores;
- Administração de rede de computadores;
- Monitoramento e operação do ambiente de produção;
- Controle e execução de batches;
- Gestão de backups;
- Tratamento de incidentes 1º nível (usuário), 2º nível (redes) e 3º nível (projetos de servidores);
- Administração de ferramentas de segurança como firewall e antivírus.

Também são responsabilidades da prestadora de serviços:

- Garantir a integridade da rede da Cooperativa através do uso de *firewalls* e programas antivírus atualizados.
- Instalar softwares de monitoramento.
- Instalar softwares nas estações de trabalho desde que homologados pela Diretoria Executiva da Cooperativa.
- Desinstalar qualquer software considerado nocivo à integridade da rede.
- Orientar os colaboradores sobre os princípios e procedimentos de Segurança da Informação, bem como lhes assegurar treinamento para o uso correto dos recursos, visando evitar falhas e danos ao funcionamento dos sistemas.

7. UTILIZAÇÃO DA INTERNET E CORREIO ELETRÔNICO

7.1. Uso da Internet

Visando o desenvolvimento das atividades profissionais, a Cooperativa disponibilizará acesso à Internet aos seus colaboradores para auxiliar na busca de pesquisa de informações de determinados assuntos de acordo com os interesses da empresa.
Todo acesso à Internet será realizado através da rede corporativa da Cooperativa e será monitorado regularmente, tanto pela Cooperativa quanto pela empresa prestadora de serviços de TI, a fim de preservar a integridade das informações, identificar vulnerabilidades e falhas de segurança, bem como verificar o uso adequado da internet pelos colaboradores.
Os serviços disponibilizados através da Internet poderão ser desativados pela Gerência Operacional ou pela Mappre sem prévio aviso, nos casos que apresentem indícios de tentativa de quebra de segurança ou outras ações que coloquem em risco a imagem e os negócios da instituição.

Não é permitido aos colaboradores:

- Desenvolver negócios particulares;
- Configurar ou alterar as configurações da rede local e dos servidores.
- Comprometer o sigilo das informações;
- Praticar qualquer tipo de hostilidade eletrônica;
- Realizar download de softwares, de jogos, arquivos executáveis, músicas e vídeos;
- Efetuar upload de qualquer software licenciado ou de dados de propriedade da Cooperativa;
- Propagar qualquer tipo de vírus, *worms*, cavalo de tróia ou programas de controle de outros computadores;
- Violar leis e acessar conteúdos incompatíveis com os valores da Cooperativa, tais como: pornografia, incitação à violência, preconceitos em geral e etc.

7.2. Uso de E-mail

O correio eletrônico é um recurso corporativo colocado à disposição dos colaboradores exclusivamente para o desenvolvimento das atividades profissionais.
Toda correspondência enviada por este canal recebe a assinatura da Cooperativa, caracterizando-se como um documento oficial. Seu uso deve seguir os princípios, valores e normas de segurança da instituição.
A concessão de uso de correio eletrônico aos colaboradores deve ser de acordo com os interesses da instituição que poderá a qualquer momento restringir o acesso ao correio eletrônico.
Os colaboradores são responsáveis pelo uso do correio eletrônico de contas sob sua gestão.
O correio eletrônico é corporativo e o domínio é de propriedade única e exclusiva da Cooperativa, ou seja, pertence à instituição e não ao colaborador.
As mensagens que trafegarem pelo correio poderão ser monitoradas e os conteúdos das mensagens poderão ser usados como prova em casos de rescisão de contrato, sendo que isto não caracteriza invasão de privacidade, bem como quebra de sigilo das informações.
Visando preservar a identidade da Cooperativa, as mensagens enviadas pelos colaboradores serão identificadas através de assinatura.
Os colaboradores devem adotar linguagem e postura em concordância com os valores da instituição.

Não é permitido aos colaboradores:

- Configurar e/ou manter configuradas contas de correio eletrônico de servidores externos, isto é, diferentes da adotada oficialmente pela Cooperativa.
- Utilizar o correio eletrônico para fins ilegais, propagandas comerciais, políticas, partidárias, religiosas, correntes, boatos e *spam*.

O usuário deve remover do Correio Eletrônico as mensagens que não são mais úteis para o desenvolvimento de suas atividades. A impressão de e-mails contendo informações sensíveis ao negócio não deve permanecer em impressoras públicas / compartilhadas.

A identificação de contas de e-mail deve seguir os padrões estabelecidos pela Cooperativa em formato pré-definido e padronizado.

8. GESTÃO DE ACESSO A SISTEMAS DE INFORMAÇÕES

Todo acesso às informações e aos ambientes lógicos da Cooperativa devem ser controlados de forma a garantir acesso apenas às pessoas autorizadas pelo respectivo proprietário da informação ou responsável por sua guarda e preservação.
O controle de acesso deve ser documentado e formalizado, contemplando os seguintes itens:

- Pedido formal da Gerência Operacional de concessão e cancelamento de autorização de acesso do usuário aos sistemas de informação feito via sistema de atendimento (Mantis) da Prodaf e acesso a rede interna via chamado da Mappre (prestador de serviços de TI);
- Verificação se o nível de acesso concedido é apropriado ao perfil do colaborador;
- Remoção imediata de autorizações dadas aos colaboradores afastados ou desligados da Cooperativa ou que tenham mudado de função, se for o caso.

A solicitação de criação de contas de acesso aos sistemas deve ser centralizada e executada pela Gerência Operacional, bem como também a sua remoção e bloqueio, quando necessário.

É de responsabilidade do usuário a correta utilização de *logins* e senhas, sendo estes pessoais e intransferíveis, bem como adotar as políticas de segurança da informação da Cooperativa.

8.1. Permissões e Acessos (Rede Interna e SYSCOOP32-Prodaf)

Os perfis de permissão de acesso aos sistemas e diretórios serão individuais para cada colaborador.

Para evitar conflitos de interesse, os colaboradores terão acesso apenas aos serviços e sistemas relacionados ao Cargo/Função que exerçam.

Em caso de exceção ou necessidade extra de serviços, deverá ser solicitada à Gerência Operacional a autorização para acesso aos módulos e recursos necessários.

9. BACKUP

O Backup é a forma com a qual a Cooperativa garante que todas as informações do seu sistema (SYSCOOP32) e todos os seus arquivos de uso interno estejam seguros e resguardados em casos de perdas significativas.

9.1. Onde é gravado o Backup

- O armazenamento dos arquivos é feito em nuvem, no aplicativo Mappre Box, e toda a responsabilidade de manutenção e verificações periódicas está a cargo da

Mappre – Infraestrutura e Segurança em TI. O backup em nuvem é restaurado e testado pela Mappre 1 (uma) vez por mês. Para maior segurança a Cooperativa possui também um HD externo, da marca Samsung, com capacidade para 1 TB (um terabyte), para armazenamento dos arquivos.

- Quanto aos arquivos utilizados pela Cooperativa, todos os funcionários são orientados a salvar todo e qualquer arquivo de uso interno no servidor, que é de onde parte as informações para os backups diários.
- Os Backups do sistema SYSCOOP32 ficam armazenados no banco de dados chamado Sybase, da Amazon, empresa responsável por gerenciar o Cloud da Prodaf. Quando necessário sua restauração deve ser solicitada via sistema de atendimento da Prodaf (Mantis).

9.2. Arquivos Backupeados

- São backupeados todas as informações contidas no sistema SYSCOOP32 e TODOS os arquivos utilizados pela Cooperativa para controles internos, como planilhas e documentos.

9.3. Periodicidade

- O backup do sistema SYSCOOP32 é feito **diariamente**, às 21h00min e enviado no mesmo instante para o servidor de backup (Sybase).
- Na nuvem, toda e qualquer modificação nos arquivos utilizados no dia a dia são salvos automaticamente no aplicativo Mappre Box que faz um backup a cada 3 horas. O backup no HD externo é feito todo dia útil, às 11:30hrs e tem duração de 3 horas, com término às 14:30hrs. Fica a cargo dos colaboradores plugar o HD externo no servidor para a realização do backup.

9.4. Tempo de retenção

- O servidor do sistema SYSCOOP32 armazena o backup dos últimos **90 dias**. Os arquivos e documentos internos armazenados em nuvem ficarão disponíveis por **7 dias,** os arquivos armazenados no HD externo ficarão disponíveis por **tempo indeterminado**.

9.5. Guarda

- O HD externo, onde ficam salvos todas as informações da Cooperativa, é confiado a um funcionário que o levará para casa com a responsabilidade de preservar sua integridade e trazê-lo todos os dias para que novas informações sejam adicionadas.

O armazenamento do backup dos arquivos é de inteira responsabilidade de todos os funcionários da entidade, pois ele é um dos instrumentos que garante a continuidade e qualidade dos serviços prestados pela Cooperativa.

10. PROGRAMAS E FERRAMENTAS DE SEGURANÇA À INFORMAÇÃO

A Cooperativa possui em seus computadores e em seu Servidor software antivírus pago com licença de uso para 3 anos, o Kaspersky, instalado para prevenir, detectar e eliminar vírus dos computadores.

A Cooperativa também dispõe de um firewall no Servidor, chamado Pf Sense, programado para controlar os acessos a internet, como páginas maliciosas, e qual conteúdo poderá trafegar pela rede, bem como as conexões que serão aceitas ou negadas. O firewall impede também possíveis tentativas de invasão por hackers. O monitoramento desta ferramenta, bem como as manutenções preventivas ficam à cargo da Mappre – Infraestrutura e Segurança em TI.

Para não perder nenhum trabalho e para evitar que alguma informação se corrompa em caso de falta de energia elétrica, as estações de trabalho estão equipadas de Nobreaks que são capazes de fornecer energia por até 20 minutos e o Servidor está equipado com um Nobreak que fornece energia por até 1 hora.

11. CONTROLES DE ACESSOS EXTERNOS

Quanto aos acessos remotos realizados, quando há necessidade de manutenção preventiva ou algum tipo de suporte, são feitos pela Mappre ou pela Prodaf via software "team viewer", cujo acesso só é liberado mediante a liberação da senha e ID do programa.

Por questões de segurança, nenhum outro tipo de prestador de serviços tem a autorização para fazer acessos remotos nos computadores da Cooperativa, sendo que todos os funcionários têm o conhecimento desta regra interna.

12. MONITORAMENTO E CONTROLE DA SEGURANÇA DA INFORMAÇÃO

Os sistemas, informações e serviços utilizados pelos colaboradores são de exclusiva propriedade da **Cooperativa de Economia e Crédito Mútuo dos Funcionários Públicos Municipais de Itapira – Credita** e não devem ser utilizados para uso pessoal.

Todos os colaboradores devem ter ciência de que o uso das informações e dos sistemas de informação da Cooperativa podem ser monitorados, e que os registros

assim obtidos poderão ser utilizados para detecção de violações das normas internas e, conforme o caso, bem como servir como prova em processos administrativos e/ou legais.

13. APROVAÇÃO, DIVULGAÇÃO E REVISÃO DA POLÍTICA

Esta Política de Tecnologia, Segurança da Informação e Backup está aprovada pela Diretoria Executiva, será publicada no site da Instituição e divulgada para todos os colaboradores e partes externas relevantes para o necessário cumprimento.

Para assegurar a sua contínua pertinência, adequação e eficácia esta Política será revisada criteriosamente em periodicidade anual ou quando mudanças significativas exigirem.

14. BASE REGULATÓRIA

Resolução CMN nº 4.606 de 19 de outubro de 2017

Resolução CMN nº 4.557 de 23 de fevereiro de 2017

Resolução CMN nº 4.658 de 26 de Abril de 2018

Luciano Donisete Couto
Diretor responsável pelo Gerenciamento Contínuo de Riscos

Nicodemus de Arimatéia Pereira
Diretor Presidente

Wilson Antonio Golfetto
Diretor Operacional