TÍTULO **PROCEDIMENTOS E POLÍTICA PARA USO DE DADOS X SEGURANÇA DA INFORMAÇÃO**		**NÚMERO/REVISÃO** PO – 019 / R - 01
UNIDADE **MATRIZ – T. I**	**ÁREA/SETOR** **T.I – TECNOLOGIA DA INFORMAÇÃO**	**DATA DE APROVAÇÃO** R 00: 15/12/2020 R 01: 22/04/2025

1. OBJETIVOS

Estabelecer procedimentos para a atribuição de níveis de segurança e acesso aos recursos de informática e Internet na cooperativa, com o objetivo de garantir a proteção das informações organizacionais, dos dados dos cooperados, clientes, colaboradores, fornecedores e ativos de TI que são de posse da Coopama.

2. SETOR RESPONSÁVEL

Tecnologia da Informação (T.I)

3. DIRETRIZES

A **Lei Geral de Proteção de Dados Pessoais (LGPD)**, Lei nº 13.709/2018, é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16º do Marco Civil da Internet.

Este POP foi elaborado com o objetivo de orientação e regras relacionadas as definições citadas na referida Lei e o departamento de T.I da cooperativa é responsável pela prática de prevenção e segurança dos dados e informações confiadas a cooperativa, inclusive pelo zelo, cuidados e manutenções dos equipamentos de T.I.

Boas práticas de segurança da informação e de ativos:

- Manter os softwares atualizados;
- Comunicação contra os eventos e incidentes de segurança;
- Ter controle sobre os acessos e uso dos equipamentos;
- Fazer cópias de segurança (Backup`s);
- Investimento em serviços e equipamentos voltados para a segurança;
- Política de segurança e termo de responsabilidade aos usuários;

Elaborado por:	Revisado Por:	*Aprovação Superintendência:*
Renato de Paiva Gonçalves	Lucas Ferreira Chagas Ana Claudia Santiago Brigagão	*Marcelo R. Nogi*

1. Manter os softwares atualizados

São realizadas atualizações periódicas, sempre que necessárias ou disponíveis nos softwares, servidores, computadores e banco de dados.
O departamento de T.I. deve manter os sistemas operacionais originais e atualizados através de sistemas de inventário e política de atualização.
As atualizações de software são importantes porque a maioria dos malwares não tem exatamente como alvo vulnerabilidades de segurança novas e desconhecidas.

2. Comunicação contra os eventos e incidentes de segurança

A comunicação contra os eventos e incidentes de segurança é realizada por meio do GLPI (sistema interno de *service desk* para uso dos colaboradores), onde diante de qualquer acontecimento, necessidade de revisão para proteção dos dados e arquivos são abertos chamados e o mesmo é acompanhado e solucionado dentro do período necessário.

3. Ter controle sobre os acessos

A T.I. deve ter o registro de todos os níveis e controles de acesso. Periodicamente, verificar as funções das pessoas na empresa para definir o acesso a uma funcionalidade específica. Deve ser assegurado o acesso de usuário autorizado aos locais estritamente necessários ao desenvolvimento de suas tarefas.
Os gestores têm autonomia e responsabilidade para solicitar a liberação ou bloqueio de acesso dos usuários de suas respectivas áreas, sendo assim, o departamento de T.I. ou os próprios gestores registram a solicitação por meio do GLPI e assim o realiza.

4. Fazer cópias de segurança (BACKUP's)

O backup ou cópia de segurança é um mecanismo fundamental para assegurar a disponibilidade da informação, caso as bases de dados em que a informação esteja armazenada sejam perdidas ou danificadas. Na cooperativa, os Backup's são realizados diariamente pela TI e sempre que necessário.
O backup realizado no banco de dados é nativo do Oracle e posteriormente utilizado um script que envia para um lugar específico para backups na rede.

5. Investimento em serviços e equipamentos voltados para a segurança

A cooperativa investe em sua infraestrutura tecnológica para proteção de dados por meio de software antivírus e configurações de segurança em servidores, roteadores, switches e sistemas operacionais, contando sempre com o suporte dos respectivos fornecedores. Esse procedimento é importante para que qualquer tentativa de ataque ou invasão seja mitigado e avaliado quanto ao risco do mesmo.

6. Política de segurança e termo de responsabilidade aos usuários:

O departamento de T.I. é responsável por fazer com que a política de segurança aborde a prática real. É necessário manter a política como um conjunto pequeno de definições claras aos quais todos concordam e podem cumprir ao invés de ter uma política muito abrangente que poucos na empresa observem.

Para protocolar a informação compartilhada sobre a Política de Segurança da Informação e dos ativos de T.I. o departamento, juntamente com o RH, utiliza o termo de responsabilidade que segue anexo a esse POP. O Termo de Responsabilidade é atualizado anualmente. Geralmente, o

documento é apresentado, entregue e assinado pelos colaboradores no ato da admissão e sempre que sofre alterações é apresentado novamente.

IMPORTANTE: Os gestores e coordenadores devem orientar e exigir dos colaboradores que as medidas preventivas citadas no termo de responsabilidade sejam rigorosamente seguidas.

Realização de Backup's:

Backup/Restore

Backup realizado diariamente de forma automática;

1. **Realizar uma ou mais cópias de segurança para os seguintes dados, no mínimo:**
   - Configurações de equipamentos de rede (roteadores, switches, etc);
   - Compartilhamento de arquivos da rede;
   - Dados realmente importantes. A análise da importância dos dados deve ser feita no contexto das atividades de negócio do departamento, visto que o mesmo dado pode ter importâncias diferentes para setores, e suas conclusões devem estar refletidas na política de backup;
2. **Realizar o backup com foco nos dados ou arquivos corporativos e não nos arquivos pessoais dos usuários;**
   - Dados ou arquivos corporativos são aqueles utilizados, ou que impactam, nas atividades dos departamentos. Para esta classificação, o setor deverá adotar a supremacia da essência sobre a forma. Desta forma, arquivos alegados como pessoais devem ser considerados como corporativos se eles impactarem nas atividades do departamento.
3. Não realizar o backup de arquivos que possam conter códigos maliciosos nem de arquivos que possam ter sido modificados/substituídos por agentes externos não autorizados. Exceção feita a backups realizados especificamente para propósitos de segurança da informação, que podem ser executados apenas por colaborador formalmente capacitado em Segurança da Informação e designado pelo gerente de T.I.
4. Considerar as disponibilidades técnicas, físicas, orçamentárias e de pessoal para a elaboração e atualização da política de backup;
5. Copiar para o Servidor de Arquivos local e na nuvem;
6. Documentar data e hora da cópia;
7. Manter cópia de Backup salva por no mínimo 15 dias (os arquivos armazenados em rede ficarão armazenados por no mínimo 30 dias);
8. Realizar Restore do backup para verificar integridade das informações.

Backup e formatação de estação de trabalho

Realizado de acordo com a necessidade e por meio de solicitações para os técnicos e analista de sistema, ou feito de forma automática pelo OneDrive da Microsoft.

- O(a) interessado(a) faz a solicitação junto ao sistema GLPI;

- O(a) interessado(a) deverá previamente realizar o backup dos seus arquivos pessoais. O TI não se responsabiliza pela perda dos mesmos;
- O TI recebe a solicitação, analisa e processa o pedido;
- Após a máquina formatada é realizada a transferência dos arquivos de volta para a estação de trabalho.
- A estação de trabalho é restaurada e devolvida ao usuário;
- Todas as estações já estão configuradas para realizarem a sincronização automática com a nuvem, via OneDrive da Microsoft.

Bloqueio e desbloqueio de sites

Os bloqueios/desbloqueios são realizados pelo analista de sistema mediante solicitação dos Coordenadores, Supervisores e Gerentes.

- O coordenador, supervisor ou gerente faz a solicitação junto ao TI através do GLPI;
- O TI faz a análise do site em questão;
- Caso proceda o pedido o TI efetua o bloqueio/desbloqueio.

Manutenções preventivas

Manutenções preventivas são realizadas periodicamente com o objetivo de prevenção de problemas técnicos como vírus e outras infecções, conforme disponibilidade dos fornecedores.

Além das manutenções preventivas, os usuários podem solicitar reparos quando necessário, conforme processo descrito abaixo:

- O usuário interessado faz a solicitação junto ao TI através do sistema GLPI informando com o máximo de detalhes o problema;
- O TI analisa o pedido classificando-o conforme sua prioridade;
- O TI verifica a causa do problema;
- O problema é resolvido.

Obs.: em HIPÓTESE ALGUMA, a TI solucionará problemas de computadores pessoais;

Política e Termo de responsabilidade para uso de recursos de informática

Eu, XXXXXXXXX, CPF número: XXX.ZZZ.YYY-GG, RG número 33.444.555-00, com contrato de trabalho estabelecido com Cooperativa Agrária de Machado, declaro que tenho conhecimento das condições de uso das ferramentas de informática disponibilizadas para o meu trabalho, nos termos das regras expostas no presente documento, com as quais concordo e comprometo-me seguir integralmente.

Machado XX/XX/20XX.

_____

(Assinatura)

CONDIÇÕES DE USO DE INTERNET E RECURSOS DE INFORMÁTICA

1. Todos os equipamentos de informática, programas, vias ou condições de acesso à internet, inclusive correio eletrônico, são de propriedade da Cooperativa Agrária de Machado e são colocados à disposição dos COLABORADORES apenas e tão somente como ferramentas de trabalho e para uso no desempenho de suas atividades profissionais, sendo vedado o seu uso nas seguintes condições:

a) durante os períodos de afastamento (licença-maternidade, férias, afastamento previdenciário etc.), no qual, será suspenso o acesso ao sistema, VPN, uso de e-mail, internet em todas as ferramentas de informática, para segurança dos dados da cooperativa e legislações;

b) para fins de ordem pessoal sem expressa autorização do superior imediato responsável;

c) para a transmissão, o acesso ou a reprodução de material de conteúdo sexualmente ofensivo, agressivo, difamatório, discriminatório ou que seja proibido por lei ou não recomendado pelo costume ou pela moral média, inclusive o acesso a redes de relacionamentos, fóruns, blogs, correios eletrônicos ou qualquer forma similar que promova a discriminação de raça, origem, idade, estado civil, sexo, filiação política ou religiosa, inaptidão ou preferência sexual e pedofilia;

d) para atividades ilegais ou que interfiram no trabalho alheio;

e) para obter acesso não autorizado a qualquer outro computador, rede, banco de dados ou informações armazenadas eletronicamente;

f) para reproduzir, instalar, alterar, copiar, distribuir programas de computador (softwares), conteúdos literários, fonográficos e/ou audiovisuais entre outros, protegidos por direitos autorais, sem a expressa autorização do autor;

g) para o envio de mensagens eletrônicas de conteúdo abusivo, obsceno, difamatório, correntes, propagandas, angariação de fundos ou qualquer material que possa violar a legislação vigente, regulamentos internos ou código de ética e conduta Cooperativa Agrária de Machado.

h) para a transferência de arquivos da Cooperativa Agrária de Machado para sites, repositórios e qualquer outra forma de tecnologia de armazenamento de dados físico, lógico ou virtual, de origem desconhecida pela cooperativa, sem expressa autorização do superior imediato responsável;

i) cadastrar o e-mail profissional em listas de discussão, redes de relacionamento, fóruns e/ou formas similares de comunicação, bem como a manifestação de opinião em nome da Cooperativa Agrária de Machado, sem expressa autorização do superior imediato responsável;

j) para uso, cópia, instalação ou transmissão de quaisquer programas de computador (softwares) não autorizados previamente pela área de suporte da Cooperativa Agrária de Machado, ainda que tais programas sejam de legítima propriedade do COLABORADOR;

k) desinstalação de programas (softwares), a alteração de configuração de equipamentos ou a desabilitação de quaisquer mecanismos de controle ou verificação que estejam instalados nos recursos que forem colocados à sua disposição para o exercício de suas atividades profissionais, sem prévia autorização da área de suporte;

l) abertura dos equipamentos de informática, bem como a remoção ou alteração de quaisquer partes de tais equipamentos, sem a devida autorização da área de suporte da Cooperativa Agrária de Machado

m) divulgação de sua senha pessoal de acesso aos equipamentos de informática, programas, vias e condições de acesso à internet, a terceiros e a outros colaboradores;

n) divulgação fora e dentro do âmbito profissional, de fatos ou informações de qualquer natureza, a que os COLABORADORES tenham acesso em decorrência de suas atribuições, salvo por meio judicial ou com o pedido e expressa autorização do superior imediato responsável;

2. A Cooperativa Agrária de Machado é proprietária de todas as mensagens e dos conteúdos dos acessos feitos com o uso das ferramentas por ele fornecidas;

3. A Cooperativa Agrária de Machado tem o pleno direito de monitorar, interceptar, copiar, transmitir ou eliminar as comunicações eletrônicas e os acessos à internet feitos por meio das ferramentas ora mencionados, salvo os acessos relacionados à internet banking e webmail pessoal, sem qualquer aviso prévio e sem que isto implique qualquer forma de violação da privacidade, intimidade ou imagem do COLABORADOR envolvido;

4. Os COLABORADORES devem atender integral e prontamente a todas as orientações e diretivas emanadas pelo Cooperativa Agrária de Machado e que tenham relação com o uso de equipamentos de informática, programas, vias ou condições de acesso à internet;

5. Os COLABORADORES devem empenhar-se no sentido de manter em boas condições todos os equipamentos de informática, programas, vias e condições de acesso à internet que lhes sejam fornecidos para o desempenho de suas atividades profissionais, devendo reportar de imediato ao Cooperativa Agrária de Machado a qualquer tipo de problema técnico ou ocorrência anormal;

6. É de responsabilidade do COLABORADOR manter as informações sigilosas e/ou confidenciais em áreas seguras (de acesso exclusivo do colaborador mediante login e senha), desta forma, evitando acesso indevido por parte de outros usuários não autorizados.

7. Os COLABORADORES serão trabalhista, civil e penalmente responsáveis pelo uso indevido das ferramentas ora mencionadas, pela não obediência às presentes regras e por quaisquer prejuízos que estes comportamentos possam causar a Cooperativa Agrária de Machado ou a terceiros;

8. A Cooperativa Agrária de Machado poderá alterar as presentes regras, no todo ou em parte, sempre que houver tal necessidade, sem prévio aviso.

9. Notebooks, Pen-Drivers e HD-Externos particulares para serem usados dentro da rede da cooperativa abrangida neste documento, precisam ser autorizados pelos Gerentes da Área e pelo pessoal de TI. Equipamentos de terceiros devem ser levados ao suporte para serem verificadas atualização do antivírus e existência de vírus.