Controle de Alterações

Data	Tópico - Descrição	Autor	Versão
06/04/2021	Emissão Inicial	Consultoria Externa	V1.0

1. Objetivo

Por meio desta Política de Segurança da Informação ("Política"), se tem o propósito de estabelecer e garantir a segurança dos ativos da informação, prezando pela integridade física, digital e verbal.

A presente Política busca assegurar a gestão da informação para alcançar os resultados desejados, no que se refere à mitigação de riscos, prevenção e redução de efeitos indesejados e contínua melhoria no acesso à informação disponível nos ambientes da **CAPAL**.

Para garantir a segurança desses ativos, a Política, portanto, será pautada nos pilares de: Confidencialidade, Integridade e Disponibilidade.

Assim, a Política será aplicada a todas as unidades de negócios, colaboradores, terceiros, prestadores de serviços e fornecedores que utilizem o ambiente físico e digital, ou que acessem os ativos de informação da **CAPAL**.

2. Glossário

Termo	Definição
Banco de dados	Conjunto estruturado de dados, estabelecido em um ou em vários locais, em suporte eletrônico ou físico.
Controlador	Pessoa natural ou jurídica, de direito público ou privado, a quem competem às decisões referentes ao tratamento de dados pessoais.
Dado Pessoal	Informação relacionada à pessoa natural identificada ou identificável
Dados Sensíveis	Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.
Encarregado (a) pelo Tratamento de Dados Pessoais	Pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD).
Finalidade	Motivo pelo qual o dado pessoal será tratado, ou objetivo que se pretende atingir com o Tratamento dos dados.
Lei Geral de Proteção de Dados Pessoais (LGPD)	A Lei nº 13.709 de 14 de agosto de 2018, também conhecida como Lei Geral de Proteção de Dados Pessoais, ou ainda LGPD, dispõe legalmente sobre o tratamento de dados pessoais no Brasil, tanto por meios digitais, físicos, ios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Operador	Pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Titular	Pessoa natural a quem se referem os dados pessoais que são objeto de tratamento
Titular dos Dados Pessoais	É qualquer pessoa física identificada ou identificável a quem se referem os Dados Pessoais tratados, por exemplo, nossos cooperados e consumidores.
Tratamento	É o manejo, operação, utilização dos Dados Pessoais sob os nossos cuidados, como a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, armazenamento, arquivamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração, entre outros.

3. Escopo e Abrangência

Escopo: Esta política abrange todos os sistemas, equipamentos e informações da Capal, incluindo também seus colaboradores, estagiários, terceirizados, temporários e fornecedores em quaisquer das dependências da Capal, ou locais onde estes se façam presentes, por meio da utilização, do manuseio ou do processamento eletrônico das informações.

Abrangência: Esta política aplica-se a todos os colaboradores da Cooperativa e suas Unidades, independente do cargo ou função; clientes, fornecedores, parceiros e prestadores de serviços da Cooperativa.

4. Política

Por meio desta Política de Segurança da Informação (“Política”), se tem o propósito de estabelecer e garantir a segurança dos ativos da informação, prezando pela integridade física, digital e verbal.

A presente Política busca assegurar a gestão da informação para alcançar os resultados desejados, no que se refere à mitigação de riscos, prevenção e redução de efeitos indesejados e contínua melhoria no acesso à informação disponível nos ambientes da CAPAL.

Para garantir a segurança desses ativos, a Política, portanto, será pautada nos pilares de: Confidencialidade, Integridade e Disponibilidade.

Assim, a Política será aplicada a todas as unidades de negócios, colaboradores, terceiros, prestadores de serviços e fornecedores que utilizem o ambiente físico e digital, ou que acessem os ativos de informação da CAPAL.

5. Princípios de disponibilidade da informação

A Presente Política de Segurança da Informação tem sido formulada com base nos conseguintes princípios:

- Confidencialidade: Busca garantir que a informação esteja acessível apenas aos usuários autorizados pelo acesso, e que esteja, portanto, protegida do conhecimento alheio;
- Integridade: Busca garantir que a informação esteja correta, seja verdadeira e não esteja passível de poder ser alterada, modificada ou ainda danificada.
- Disponibilidade: Busca garantir que a informação esteja disponível, quando necessário e autorizado.

A presente Política deve ser interpretada em conformidade com os demais documentos adotados pela CAPAL, seja através dos Avisos e Políticas que versem sobre a Proteção de Dados, normas de conduta e informações internas, também junto à legislação vigente.

O acesso ao documento desta Política, bem como as atualizações disponíveis podem ser consultadas por meio da via digital, através da Intranet, rede local ou fisicamente junto ao Comitê de Privacidade e Proteção de Dados.

6. Diretrizes de uso, desempenho e segurança da informação

As informações sejam elas físicas ou digitais, tanto em ambiente virtual, por meio dos Sistemas utilizados pela **CAPAL**, bem como no meio físico, são de sua exclusiva e intransferível propriedade. Desse modo, a manipulação desses dados seja de qualquer modo, pelos Usuários, representa apenas a detenção e não a posse ou propriedade desses ativos.

Bem como as informações sejam essas de cooperados, colaboradores, terceiros, empresas parceiras e/ou concorrentes, todas elas devem ser tratadas de forma ética, sigilosa e pautadas pelos princípios anteriormente elencados.

Aos Usuários, são estabelecidos os direitos e deveres de apoiar e fiscalizar o cumprimento da presente Política, reportando quaisquer intervenientes à área de Tecnologia da Informação pelo descumprimento, risco ou incidente de Segurança da Informação e das diretrizes e Princípios que norteiam essa Política.

- **Aos Colaboradores**

Prezando pela ética e confidencialidade e a segurança da informação, todo colaborador deve se abster de discutir assuntos confidenciais que envolvam a rotina e informações da **CAPAL** e das operações que envolvam seus trabalhos, principalmente, mas não se restringindo aos ambientes públicos e/ou compartilhados, tais como restaurantes, encontros sociais, transportes coletivos, encontros familiares, etc., sem juízo de proferir informações e comentários, opiniões ou fomentar debates sobre essas informações em blogs, redes sociais, grupos de aplicativos de conversa, entre outros.

Dentro e fora das dependências físicas da **CAPAL**, colaboradores e terceirizados deverão sempre se pautar pela ética e sigilo profissionais, sendo vedado quaisquer compartilhamentos de informações profissionais, tais como informações da operação, dados de cooperados, dados de clientes, dados de colaboradores, remuneração e valores, pautas de reuniões, etc., para finalidades que não se relacionem com a atividade profissional de competência e cargo do funcionário.

Ademais, todas as questões relativas a senhas, usuários, acesso e/ou credenciais tais como logins, senhas, Ids, tokens, etc., são de uso pessoal e intransferíveis, sendo obrigação do colaborador manter seu sigilo de acordo com a Política de Senhas adotada pela **CAPAL**.

Cabe ressaltar que os Logs de dados são documentados e armazenados no sistema interno da **CAPAL** por período determinado. Assim, todas as operações oferecidas pela **CAPAL**, sejam em seus serviços, produtos, atendimento ao cooperado, suporte, entre outros, deverão observar regras em relação aos ativos de informação e à privacidade, respeitando os princípios anteriormente elencados, as diretrizes vigentes e as políticas adotadas pela cooperativa.

7. Diretrizes de uso dos ativos da informação

Aos ativos de tecnologia da informação, tais como dispositivos móveis, rede de Internet e softwares serão pautados pela utilização exclusiva para fins relacionados à atividade profissional do Usuário, sendo vedado o uso particular, salvo exceções expressamente autorizadas.

Os ativos de tecnologia da informação da **CAPAL** serão descartados de acordo com a **Norma de Descarte**, seguindo o princípio de que cada tipo de ativo deverá ser destruído de modo a impossibilitar sua recuperação por pessoas não autorizadas.

- **O E-mail**

Ao e-mail corporativo, qual seja, (@**CAPAL**.coop.br), é permitido somente o uso para fins legítimos e relacionados ao desempenho de suas funções laborais, sendo expressamente vedado:

- Enviar mensagens de e-mail usando o endereço de seu departamento, nome de usuário de outra pessoa ou e-mail que não esteja autorizado;
- Enviar mensagens de e-mail não solicitadas divulgando informações a terceiros sem autorização ou ainda para múltiplos destinatários, exceto se relacionadas a uso legítimo da instituição;
- Falsificar ou adulterar o conteúdo de mensagens de e-mails ou ainda o endereço do remetente, fazendo-se passar por outra pessoa;
- Acessar sem autorização os e-mails de outro usuário;
- Reproduzir, transmitir ou divulgar mensagens que contenham qualquer ato ou orientação que conflitem com os interesses da CAPAL;
- Nem mesmo reproduzir e/ou encaminhar mensagens que contenham ameaças eletrônicas, tais como: vírus, spam e demais malwares;
- Acessar arquivos com código executável (.exe, .com, .bat, .pif, .js, .vbs, .hta, .src, .cpl, .reg, .dll, .inf) ou qualquer outra extensão que apresente riscos à segurança dos equipamentos ou Tecnologias da Informação da CAPAL.

Ademais, fica expressamente proibido realizar quaisquer ações as mensagens de e-mail que:

- Visem obter acesso não autorizado a outro computador, servidor ou rede;
- Visem interromper um serviço, servidores ou rede de computadores por meio de qualquer método ilícito ou não autorizado;
- Visem burlar qualquer sistema de segurança;
- Visem monitorar secretamente, assediar ou ameaçar outro Usuário;
- Visem acessar informações confidenciais sem explícita autorização do proprietário;
- Incluam material protegido por direitos autorais sem a permissão do detentor dos direitos.

- **A Internet**

Os colaboradores devem adequadamente utilizar a Internet, respeitando as diretrizes e princípios anteriormente mencionados, além de no tráfego online estar consciente das questões de direitos autorais, das regras de licenciamento de softwares, dos direitos de propriedade intelectual, direitos de posse, propriedade e uso, além do respeito e observância à privacidade e proteção de suas informações e das informações de colaboradores, cooperados, terceiros e toda a comunidade que possua dados juntos à **CAPAL**.

O uso da Internet deve ser pautado pelo bom senso quanto aos sites acessados, tempo de utilização e páginas que não criem riscos desnecessários para a **CAPAL**.

Ademais, o acesso à Internet, por meio da rede corporativa, deve ser efetuado somente por equipamentos autorizados pelo setor de Tecnologia da Informação (TI).

Não é permitido o uso de programas ou páginas de bate-papo (chat) de qualquer natureza, exceto para desempenho de sua atividade profissional.

Veda-se a divulgação, compartilhamento de informações de quaisquer gêneros, tais como confidenciais ou restritas, tanto nas ferramentas de comunicação internas, e mais gravemente ainda nas redes sociais de quaisquer gêneros e/ou sites ou qualquer tecnologia via internet.

Não é permitido acessar, armazenar, divulgar e repassar qualquer material ilícito ligado à pornografia, pedofilia, jogos, racismo, homofobia, religião, bitcoins, mp3 e vídeos, entre outros.

Não é permitido burlar os controles de internet, usando software ou outros métodos.

Não é permitido utilizar programas para download/upload de arquivos como Peer-to-Peer de qualquer natureza, exceto para desempenho de sua atividade profissional.

Reitera-se que, as solicitações de liberação de sites que sejam úteis às tarefas diárias deverão ser feitas via chamado para análise e liberação do setor TI.

8. Gestão de acessos e identidade

Tanto o acesso físico e digital aos ativos de informação da **CAPAL** devem se pautar devidamente pela necessidade, com acesso restrito aos usuários com autorização formal e que necessitem do acesso para o desempenho de suas atividades;

Assim como a observância dos requisitos acima, reitera-se que a **CAPAL** tem adotado que cada colaborador deve possuir seu usuário e senha, sendo intransferível, de modo que não haja compartilhamento dessas informações pelos titulares.

O acesso será gerido pelo Departamento de Tecnologia da Informação, em conjunto com o Departamento de Recursos Humanos, demais gestores nos termos da **Norma de Acessos**.

9. Gestão de riscos, incidentes e segurança da informação

Riscos, Incidentes e Segurança da informação devem ser permanentemente analisados e monitorados de acordo com a **Norma de Gestão de Incidentes** e com as melhores normas técnicas disponíveis no mercado, tais como ISOs da família 27000, ITIL, COBIT e outras.

Cabe destacar que os incidentes de Segurança da Informação serão analisados, classificados, tratados, registrados e reportados ao solicitante e ao gestor do processo ou sistema impactado.

Todo incidente de Segurança da Informação deve ser usado como base para a implementação de novos ou modificação de controles existentes.

Destaca-se que os ativos de informação estratégicos que suportam os negócios da CAPAL devem ser mantidos em backup dedicado e exclusivo.

10. Conscientização, orientações e treinamentos

O Comitê deve promover programas periódicos para a conscientização de toda a organização quanto à segurança das informações corporativas. De modo que serão organizados treinamentos, campanhas de conscientização, palestras, workshops, entre outros;

Os eventos sobre segurança da informação são obrigatórios para todos os colaboradores, terceiros e demais partes interessadas e poderão ser utilizados como critérios para aplicação de penalidades e avaliação de metas.

11. Monitoramento, violações e penalidades pelo descumprimento da segurança da informação

- **Do Monitoramento**

Pelo monitoramento da informação, entende-se que o uso dos ativos de informações e dos sistemas de informação podem ser monitorados, podendo a **CAPAL** utilizar a informação gerada por esses sistemas para identificar usuários e respectivos acessos efetuados, bem como material manipulado.

Ademais, a **CAPAL** poderá realizar, sem aviso prévio, a qualquer tempo a inspeção física ou auditoria nos ativos de informação nas máquinas de sua propriedade.

- **Da violação da política**

Qualquer violação a esta Política, suas normas e princípios correlatos serão analisadas enquanto incidentes da Segurança da Informação, cabendo análise pelo Comitê.

Caberá ao Comitê à apuração interna do ocorrido, juntamente com o responsável pela área ou superior imediato do colaborador responsável direta ou indiretamente (incluindo-se omissões ou tentativas) pela infração, sem prejuízo da ação em conjunto com a área de Recursos Humanos, Jurídica e Diretoria da CAPAL.

As violações, ainda que por omissão ou mera tentativa não consumada, a esta Política e toda e qualquer diretriz ou norma publicada, sem prejuízo das demais sanções de natureza civil, criminal e trabalhista, poderão ensejar as seguintes penalidades: advertência verbal, advertência por escrito, suspensão não remunerada e a demissão por justa causa.

A aplicação de sanções e punições deverá considerar a gravidade da infração, o tempo de remediação, efeitos alcançados, reincidência e as hipóteses previstas no artigo 482 da Consolidação das Leis do Trabalho, podendo o Comitê, no uso de seu poder disciplinar aqui estabelecido, aplicar a pena cabível com o aval da Diretoria da Cooperativa.

Além das sanções, entendendo o Comitê por necessário e viável, aplicará ao colaborador a medida educativa da realização de cursos, workshops, treinamentos, etc., que se façam necessários.

Ao colaborador ou prestador de serviço envolvido na violação à Política e/ou respectivas diretrizes ou normas será assegurado tratamento justo, correto e confidencial, de modo que qualquer medida tomada deverá ser proporcional e aplicada de acordo com o Código de Conduta, contrato de trabalho ou prestação de serviços, a presente Política e normas e legislação vigente.

No caso de terceiros contratados ou prestadores de serviço, o Comitê analisará a ocorrência e deliberará sobre a efetivação das sanções e punições conforme condições contratuais.

As violações que impliquem em atividades ilegais, ou que possam incorrer em riscos aos titulares de dados pessoais, ou dano à CAPAL, ensejará a responsabilização pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

12. Medidas disciplinares

O não cumprimento das normas aqui previstas, independentemente de seu cargo e função, ensejará medidas administrativas como a advertência, sem prejuízo de outras sanções mais graves, uma vez que são entendidas por essas políticas como obrigatórias aos membros da CAPAL.