Política de Segurança da Informação Aprova

Versão 002 – 06/2026

SEGURANÇA DA INFORMAÇÃO

Objetivos desta Política:

Manter a confidencialidade, integridade e disponibilidade das informações de propriedade ou sob a guarda do Aprova.

Estabelecer medidas para a proteção da infraestrutura que suporta os serviços e atividades de negócio.

Prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético.

Princípios:

As ações relacionadas à SI (Segurança da Informação) no Aprova são norteadas pelos seguintes princípios:

- **Legalidade:** a política de Segurança da Informação levará em consideração as leis, as normas, procedimentos e as políticas administrativas estabelecidas pelo Aprova;
- **Impessoalidade:** a política de Segurança da Informação visará ao interesse público no tratamento das informações, buscando evitar que estas sejam utilizadas para finalidades particulares ou para a obtenção de benefícios pessoais;
- **Moralidade:** a política de Segurança da Informação, deverá observar preceitos éticos e de governança, pautando-se nos ideais de honestidade e justiça;
- **Publicidade:** as diretrizes, normas e procedimentos da política de Segurança da

Informação aqui definidos pelo Aprova, devem ser publicados e amplamente divulgados para o conhecimento dos colaboradores, fornecedores, prestadores de serviços, parceiros, usuários e clientes.

- **Responsabilidade:** a Política de Segurança da Informação deverá ser seguida por toda a equipe do Aprova e conhecida por todos os prestadores de serviços, usuários e clientes, pautando-se por atitudes e comportamentos condizentes com as diretrizes, normas e procedimentos de SI (segurança da informação);
- **Proporcionalidade:** a aplicação da Política de Segurança da Informação, no que abrange o nível, a complexidade e o custo das ações deverá ser adequada ao entendimento administrativo e aos valores dos ativos a serem protegidos.
- **Integridade:** a aplicação da Política de Segurança da Informação deverá ser seguida, para que os dados se mantenham intocados, preservando a originalidade e confiabilidade das informações. O Aprova realiza backup dos dados de seu sistema homônimo durante o período de retenção, todos os procedimentos e sistemas que garantem o acesso à informação durante o período de retenção, tanto no que diz respeito ao portador da informação quanto na legalidade dos formatos, também serão guardados de maneira a proteger as informações contra modificações e eliminação não autorizadas.
- **Disponibilidade:** a aplicação da Política de Segurança da Informação deverá garantir o acesso aos dados sempre que necessário, de maneira fluida, segura e eficiente. Usuários poderão requisitar informações e acesso aos dados através do e-mail dados@aprova.com.br.

Diretrizes gerais:

As informações criadas, armazenadas, manuseadas, transportadas, custodiadas ou descartadas, referentes a utilização da Plataforma Aprova, são patrimônio das Prefeituras e

Órgãos Públicos contratantes, os quais figuram na posição de CONTROLADORES.

1. Informações que recebemos diretamente dos usuários quando realizam o cadastro na plataforma:

- Nome pessoal;
- E-mail;
- Número de telefone;
- Endereço comercial ou residencial;
- CPF;
- Registro de conselho técnico;
- Conteúdo do usuário, por exemplo, informações ou conteúdo que é feito upload no sistema (que podem incluir dados pessoais se forem incluídos dados pessoais em tal arquivo).

2. Informações que recebemos automaticamente quando utilizam nossos serviços (Plataforma Aprova):

- Endereço IP;
- Identificadores de dispositivo;
- Informações do navegador da web;
- Estatísticas de visualização da página;
- Histórico de navegação;
- Informações de uso;
- Cookies;
- Log Data (tempo de acesso, informações de hardware e software).

Quanto às demais informações de trâmite interno, de negócios e operações do Aprova, devem ser utilizadas exclusivamente para desempenho das funções institucionais, estas serão classificadas e manipuladas de acordo com normas e legislação específica em vigor, mantendo a segurança durante todo o ciclo de vida.

3. Informações coletadas internamente pelo Aprova:

- Nome completo;
- Data de nascimento;
- Número e imagem da Carteira de Identidade (RG);
- Número e imagem do Cadastro de Pessoas Físicas (CPF);
- Número e imagem do Título de Eleitor;
- Número e imagem do Certificado de Reservista;
- Número e imagem da Carteira Nacional de Habilitação (CNH);
- Número e Imagem do cartão de vale transporte (quando utilizado pelo empregado);
- Número e imagem do Programa de Integração Social (PIS);
- CTPS física e/ou digital;
- Fotografia 3×4;
- Imagem da Certidão de Casamento ou Declaração de União Estável; ● Imagem do Diploma de nível de instrução ou escolaridade;
- Endereço completo;
- Números de telefone, WhatsApp e endereços de e-mail;
- Banco, agência e número de contas bancárias;

- Nome de usuário e senha específicos para uso dos serviços do Aprova e de sistemas terceirizados.
- Comunicação, verbal e escrita, mantida entre o Titular e o Controlador;
- Exames e atestados médicos, especialmente admissionais, periódicos, incluídos de retorno por afastamento superior a 30 dias em caso de doença, acidente ou parto, de mudança de função, demissionais e ainda aqueles que atestem doença ou acidente.

Além disso, recebemos informações sobre usuários, colaboradores e terceiros de alguns de nossos provedores que auxiliam o Aprova com serviços de marketing ou promocionais relacionados à forma como você interage com nosso site, produto, serviços, anúncios ou comunicações. Essas informações que receberemos dependerão das políticas e das configurações de sua conta com o serviço de terceiros (ex: Facebook, Instagram).

Declaração de comprometimento:

Os Gestores do Aprova estão comprometidos e apoiam os princípios estabelecidos nesta PSI de proteção de seus recursos tangíveis e intangíveis de acordo com as necessidades de negócio e em conformidade com o ambiente legal, primando pela confidencialidade, integridade, disponibilidade, autenticidade e legalidade das informações.

Aplicações da PSI:

As diretrizes aqui estabelecidas deverão ser seguidas por todos os colaboradores, bem como os prestadores de serviço quando atuando em nome do Aprova, e se aplicam à informação em qualquer meio ou suporte.

Esta política dá ciência a cada colaborador de que os ambientes, sistemas,

computadores e redes da empresa poderão ser monitorados e gravados, com prévia informação, conforme previsto nas leis brasileiras.

É também obrigação de cada colaborador manter-se atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do seu gestor sempre que não estiver absolutamente seguro quanto à aquisição, uso e/ou descarte de informações.

Do uso de recursos de TI:

Os recursos de tecnologia da informação vinculados ao Aprova colocados à disposição dos colaboradores para uso como ferramenta de trabalho, devem ser utilizados em atividades primordialmente relacionadas ao trabalho desempenhado por estes.

É vedado o uso de recursos computacionais para armazenar ou transmitir conteúdo ilegal, difamatório, invasivo à privacidade, obsceno ou injurioso.

O uso dos recursos computacionais por colaboradores do Aprova estão sujeitos à monitoração, desde que respeitados os princípios constitucionais e legais aplicáveis à matéria.

Os equipamentos, ferramentas e sistemas são concedidos aos colaboradores com todos os controles necessários para cumprir os requisitos de segurança estabelecidos por esta PSI.

Atribuir cada conta ou dispositivo de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, sendo que:

- Os usuários (logins) individuais de colaboradores são de responsabilidade dos próprios colaboradores.
- Os usuários (logins) de terceiros serão de responsabilidade do gestor da área contratante (Prefeituras e Órgãos Públicos).

Segregar as funções administrativas, operacionais e educacionais a fim de restringir ao mínimo necessário os poderes de cada indivíduo e eliminar a existência de pessoas que possam excluir os logs e trilhas de auditoria das suas próprias ações.

Administrar, proteger e testar as cópias de segurança dos programas e dados relacionados aos processos críticos e relevantes para o Aprova, os quais são realizados em diferentes máquinas para evitar a perda de dados. Implantar controles que gerem registros auditáveis para retirada e transporte de mídias das informações custodiadas pela TI, nos ambientes totalmente controlados por ela.

O gestor da informação deve ser previamente informado sobre o fim do prazo de retenção, conforme estabelecido na Política de Retenção e Descarte de Dados, para que tenha a alternativa de realizar a manutenção da informação.

Sempre que necessário, conforme a classificação dos dados e informações, além do meio de armazenamento, as técnicas criptográficas deverão ser usadas para garantir sua proteção e confidencialidade.

Ressalta-se a importância das configurações de segurança, a fim de que os colaboradores do Aprova não desativem ou ignorem, inclusive quanto a restrições de acesso de determinados tipos de sites (ex: sites contendo conteúdos explícito ou ilegal).

Em relação aos colaboradores do Aprova a importância das configurações de segurança, a fim de que eles não as desativem ou ignorem, inclusive quanto a restrições de acesso de determinados tipos de sites.

Backup e restauração de arquivos:

O Aprova realiza backup dos dados durante o período de retenção, todos os procedimentos e sistemas que garantem o acesso à informação durante o período de retenção, tanto no que diz respeito ao portador da informação quanto na legalidade dos

formatos, também serão guardados de maneira a proteger as informações contra perdas como resultado de futuras mudanças tecnológicas.

A restauração de arquivos armazenados na Plataforma Aprova só será possível em dados que foram gerados backup's anteriormente, conforme rotina automatizada.

Restauração de arquivos terá um prazo máximo de 30 dias corridos para os backups diários, não sendo possível recuperar arquivos mais antigos que esse período, com exceção das cópias mensais de backups a nível histórico.

É de responsabilidade de cada colaborador o armazenamento de arquivos inerentes ao desempenho de suas atividades para garantir o backup dos mesmos e retenção de mensagens pelo período indicado na Política de Retenção e Descarte de Dados.

É dever do colaborador, a manutenção no diretório que tem acesso, mantendo organizado, evitando acúmulo de arquivos e duplicadas.

Haverá limpeza periódica dos arquivos armazenados no Canal de Comunicação Interna (Slack Technologies), para que não haja acúmulo desnecessário de arquivos e de recursos computacionais, bem como para que dados não sejam armazenados incorretamente.

Recomendações de Segurança para Colaboradores e Terceiros:

- No tocante a utilização de senhas de acessos, os usuários deverão cumprir o contido na Política de Senhas do Aprova.
- Evitar acessar sites e aplicativos em dispositivos (computadores, celulares e tablets) de terceiros, públicos ou não confiáveis. O mesmo vale para redes Wi-Fi públicas;
- Manter seus dispositivos com os sistemas operacionais e aplicativos atualizados;
- Procurar instalar uma solução de antivírus no seu computador e a mantenha

atualizada;

● Evitar abrir e-mails cujo remetente ou conteúdo sejam desconhecidos;

● Não clicar em links disponibilizados em e-mails ou em mensagens SMS suspeitas e/ou desconhecidas;

● Não realizar o download ou execute arquivos anexos em e-mails suspeitos; ● Evitar emprestar seu celular para pessoas desconhecidas;

● Manter sempre pelo menos uma cópia de segurança (backup) de dados importantes.

Nossa responsabilidade:

A LGPD promoveu uma série de mudanças no tratamento dos dados pessoais, dentre elas, estão as definições acerca das obrigações dos controladores/operadores de dados pessoais. De forma a seguir em conformidade com estes preceitos, o Aprova têm a responsabilidade em manter todos os dados seguros, coletando somente os que realmente forem necessários para a prestação dos serviços, garantindo que sejam tratados e compartilhados de acordo com os limites e hipóteses informados aos titulares.

O Aprova objetiva a transparência e a conformidade com todas as diretrizes e orientações mais modernas e seguras aplicáveis aos processos de tratamento de dados, para que isto ocorra a informação e disponibilidade para contato se fazem indispensáveis, desta forma, disponibilizamos diversos canais para contato direto com a equipe do Aprova.

Canais de Comunicação:

A equipe do Aprova segue aberta e disposta para auxiliar em qualquer dúvida ou indagação sobre a proteção de dados, possibilitando a garantia e exercício dos direitos reservados aos titulares. Entre em contato conosco através de nosso site

https://prefeituras.movidesk.com/kb/ e de nosso e-mail Suporte@aprova.com.br.

Alterações:

A equipe do Aprova reserva o direito de corrigir, alterar ou atualizar esta Política periodicamente, sem aviso prévio, ficando a critério do usuário verificá-la sempre que acessar o website ou Plataforma.

Para colaboradores do Aprova, haverá publicação no canal de Comunicação Interna (Slack) mencionando a ocorrência de alterações nesta PSI.

Eventuais correções, alterações desta Política entrarão em vigor imediatamente após a publicação.

Informações do Aprova, que poderá figurar como operador ou controlador, dependendo da situação:

Aprova Digital, inscrito no CNPJ/MF sob o n° 24.757.040/0001-40, Razão Social "APROVA DIGITAL S/A" com sede em Cascavel/Paraná, na Rua Afonso Pena, 1876 - 4º Andar, Centro, CEP 85812- 101.