MANUAL DE TI: PROCEDIMENTO DE GESTÃO DE ACESSOS E SEGURANÇA DA INFORMAÇÃO

PALMAS - TO

2026

63 2111-6350
2111-6356
https://www.palmas.to.gov.br/
previpalmas@palmas.to.gov.br
gabprevipalmas@gmail.com
802 Sul, Avenida NS 02, Alameda 03, APM 15B,
Loteamento Palmas 2a Etapa - Plano Diretor Sul
CEP 77.023-006 – Palmas/TO

SUMÁRIO

1. Objetivo
2. Abrangência
3. Responsabilidades
4. Solicitação de Acesso para Novo Colaborador
5. Análise da Solicitação pela TI
6. Criação do Usuário e Concessão de Acessos
7. Acesso a Sistemas
8. Acesso às Pastas Compartilhadas
9. Conclusão da Configuração
10. Alteração de Setor ou Função
11. Desligamento de Colaborador
12. Segurança da Informação
13. Controle de Equipamentos
14. Gestão de Backup e Retenção de Dados
15. Contingência e Continuidade Operacional
16. Fiscalização e Denúncias

1. OBJETIVO

Estabelecer os procedimentos padrão para a solicitação, criação, alteração, manutenção e revogação de acessos aos recursos de Tecnologia da Informação do PREVIPALMAS.

Este procedimento visa garantir que cada colaborador possua estritamente os acessos necessários para o desempenho de suas atribuições, promovendo a segurança, organização, rastreabilidade e controle das informações e sistemas da instituição.

2. ABRANGÊNCIA

Este procedimento aplica-se a todos os colaboradores, servidores, estagiários, prestadores de serviços e demais usuários que necessitem utilizar os recursos tecnológicos disponibilizados pelo PREVIPALMAS.

São considerados recursos de TI, entre outros:

- Computadores, notebooks e periféricos;
- Rede corporativa e acesso à Internet (cabeada e Wi-Fi);
- E-mail institucional;
- Pastas e compartilhamentos de rede;
- Sistemas de trâmites de processos administrativos;
- Sistemas de processos previdenciários (softwares legados e corporativos);
- Sistemas externos e portais corporativos;
- Conexão remota segura (VPN);
- Serviços e aplicações diversas disponibilizados pela TI.

3. RESPONSABILIDADES

3.1. Responsável pelo Setor Solicitante

- Definir quais acessos o colaborador necessita para exercer suas atividades.
- Solicitar formalmente via e-mail institucional a criação, alteração ou revogação de acessos.

- Informar corretamente os dados cadastrais do usuário e os sistemas/recursos necessários.
- Informar o perfil/nível de acesso necessário para cada aplicação.
- Comunicar prontamente movimentações de pessoal (alterações de setor/função ou desligamentos).

3.2. Setor de Tecnologia da Informação (TI)

- Receber, registrar e analisar as solicitações enviadas.
- Validar as permissões solicitadas conforme os critérios de segurança.
- Criar credenciais, perfis de usuário e configurar os acessos (sistemas, rede, e-mail e pastas compartilhadas).
- Orientar os usuários quanto ao uso adequado dos recursos de TI.
- Garantir o cumprimento do Princípio do Menor Privilégio.
- Garantir o inventário, termo de responsabilidade e reindexação patrimonial na entrega/devolução de equipamentos.
- Atuar na execução de contingências operacionais e rotinas de salvaguarda de cópias de segurança (backups).

4. SOLICITAÇÃO DE ACESSO PARA NOVO COLABORADOR

Sempre que houver a admissão/entrada de um novo colaborador, o responsável pelo setor deverá encaminhar uma solicitação formal à TI via e-mail institucional contendo o formulário de cadastramento preenchido.

4.1. Informações Obrigatórias

Informação	Obrigatoriedade
Nome Completo	Sim
CPF	Sim
Setor de Lotação	Sim
E-mail Institucional	Sim
Sistemas Necessários e Perfis	Sim
Pastas Compartilhadas	Sim
Acesso a VPN	Quando aplicável

5. ANÁLISE DA SOLICITAÇÃO PELA TI

Após o recebimento da solicitação via e-mail, a TI fará a conferência detalhada dos dados enviados:

- **Dados Incompletos:** A solicitação será devolvida ao responsável pelo setor para complementação das informações.
- **Dados Completos:** A TI procederá com a definição de permissões, criação das contas e atribuição de perfis.

6. CRIAÇÃO DO USUÁRIO E CONCESSÃO DE ACESSOS

Após a validação da solicitação, a TI realizará a criação do perfil do colaborador contemplando:

- Usuário de rede e credenciais de acesso inicial;
- Vinculação a grupos de segurança e permissões de diretório;
- Conta de e-mail institucional;
- Liberação de perfis nos sistemas corporativos;
- Mapeamento de pastas compartilhadas na rede.

Princípio do Menor Privilégio: O usuário receberá exclusivamente as permissões estritamente necessárias para o cumprimento de suas atribuições. Concessões de acessos administrativos ou permissões elevadas exigem justificativa formal e aprovação específica da chefia do setor e da Gerência de TI.

7. ACESSO A SISTEMAS

Para liberação de uso dos sistemas corporativos, o responsável pelo setor deve detalhar a demanda indicando:

- **Sistema:** Nome do sistema solicitado (ex.: SOFTPREV, SPG, Sistema de Processos).
- **Usuário:** Nome do colaborador.
- **Perfil de Acesso:** Consulta, Operacional, Gerencial, Administrativo ou Outro especificando o nível.
- **Justificativa:** Descrição resumida da necessidade do acesso para as rotinas de trabalho.

8. ACESSO ÀS PASTAS COMPARTILHADAS

Para disponibilização de acesso a diretórios e arquivos da rede:

- O responsável pelo setor deve indicar o nome do diretório e o tipo de permissão (ex.: Somente Leitura ou Leitura e Escrita). Exemplo: \\servidor\Financeiro.
- A TI não concederá acesso a diretórios não relacionados à área de atuação do colaborador sem autorização prévia da chefia responsável pela pasta.

9. CONCLUSÃO DA CONFIGURAÇÃO E TESTES

Após a criação e atribuição dos acessos, a TI deverá obrigatoriamente:

1. **Realizar Testes:** Validar o funcionamento das credenciais, login de rede, e-mail e permissões de pastas/sistemas.
2. **Tratamento de Falha no Teste:** Caso ocorra qualquer divergência ou erro durante os testes, a TI deve corrigir a falha antes da liberação final.
3. **Conclusão e Comunicação:** Com os testes validados com sucesso (Teste OK), a TI registrará a conclusão da demanda e responderá ao e-mail do setor solicitante comunicando a liberação dos acessos, fornecendo as orientações iniciais para o usuário.

10. ALTERAÇÃO DE SETOR OU FUNÇÃO

Quando um colaborador for transferido de setor ou mudar de função, o responsável pelo novo setor deverá comunicar a TI por e-mail, informando:

- Nome completo e CPF do colaborador;
- Novo setor e nova função;
- Novos sistemas e pastas compartilhadas necessários;
- Acessos antigos que deverão ser revogados.

Atenção: A transferência de setor implica na reavaliação total dos acessos anteriores. Permissões do setor antigo que não sejam necessárias na nova função serão sumariamente revogadas para evitar o acúmulo indevido de privilégios.

11. DESLIGAMENTO DE COLABORADOR

Em caso de exoneração, rescisão contratual, encerramento de estágio ou término de prestação de serviço, o responsável pelo setor deverá comunicar a TI imediatamente, informando:

- Nome completo e CPF;
- Setor de lotação;

- Data e horário exatos do desligamento.

Ações executadas pela TI:

- Bloqueio imediato da conta de usuário e e-mail institucional;
- Revogação total de permissões a sistemas, pastas e rede corporativa;
- Revogação do acesso VPN e remoção de grupos de comunicação/mensageria;
- Recolhimento, conferência, inventário e reindexação patrimonial dos equipamentos sob responsabilidade do colaborador.

12. SEGURANÇA DA INFORMAÇÃO

12.1. Diretrizes Gerais e Autenticação

- **Responsabilidade dos Ativos:** Toda informação, equipamento e credencial de acesso pertencem ao PREVIPALMAS.
- **Credenciais Individuais:** O acesso aos sistemas é feito por login e senha individuais. As senhas devem ter no mínimo 8 caracteres, mesclando letras maiúsculas, minúsculas, números e caracteres especiais.
- **Uso Pessoal e Intransferível:** É expressamente proibido ao usuário compartilhar sua senha com terceiros. A TI jamais solicitará a senha pessoal do colaborador.

12.2. Compartilhamento de Contas

É proibida a utilização de contas genéricas ou compartilhadas por múltiplos usuários. Cada colaborador deve possuir identificação própria para garantir a auditabilidade e rastreabilidade das ações executadas nos sistemas.

12.3. Uso Adequado da Infraestrutura de TI

- **E-mail e Internet:** O correio eletrônico e a navegação na internet são para uso estritamente institucional. É proibido o uso de e-mail pessoal para fins de trabalho, o download de arquivos não autorizados ou acesso a sites impróprios.
- **Rede Wi-Fi:** A rede sem fio corporativa é disponibilizada exclusivamente para equipamentos onde não há possibilidade do uso de rede cabeada ou mediante prévia autorização da TI para visitantes/dispositivos específicos.

- **Estações de Trabalho:** É proibida a instalação de softwares não licenciados ou não homologados, o consumo de alimentos/bebidas próximo aos equipamentos e a retirada de ativos sem formulário prévio de autorização.

13. CONTROLE DE EQUIPAMENTOS

A concessão e a distribuição de equipamentos tecnológicos (computadores, notebooks e periféricos) aos colaboradores do PREVIPALMAS têm como objetivo garantir uma infraestrutura adequada, segura e eficiente para o desempenho das atividades institucionais.

- **Vinculação e Uso:** Cada computador é associado diretamente à conta de rede e ao perfil do usuário para assegurar o controle do patrimônio, a auditoria de acessos e a segurança da informação. Os equipamentos são de uso estritamente profissional.
- **Manutenção:** Cabe ao Setor de TI a preparação, instalação de softwares homologados, manutenção preventiva/corretiva e atualizados.

14. GESTÃO DE BACKUP E RETENÇÃO DE DADOS

Para assegurar a integridade e disponibilidade das informações institucionais, a TI adota políticas de redundância e salvaguarda contínua:

- **Redundância:** Utilização de servidores locais distintos e cópias externas em nuvem para proteção contra perda de dados, falhas físicas ou ciberataques.
- **Sistema SOFTPREV:** Backups diários executados à meia-noite (00:00h) em servidor físico dedicado, mantidos em ambiente seguro com retenção de até 5 anos (em conformidade com a LGPD e normas arquivísticas previdenciárias).
- **Sistema SPG:** Backups automatizados diários às 23:59h com retenção de 7 dias armazenados em nuvem.

15. CONTINGÊNCIA E CONTINUIDADE OPERACIONAL

Estabelece procedimentos de resposta imediata a incidentes tecnológicos (falhas de hardware, indisponibilidade de internet, telefonia ou servidores) para mitigar paralisações nos serviços previdenciários e administrativos do PREVIPALMAS.

15.1. Procedimentos de Restauração

- **Falha em Servidores de Arquivos ou Hospedagem:** Notificação imediata dos setores afetados com previsão de retorno, alocação de hardware reserva, restauração das cópias de segurança (backups) e testes de integridade/autenticação antes da liberação.
- **Falha de Conectividade e Links de Internet:** Verificação dos equipamentos locais de rede (modems, roteadores, nobreaks), acionamento imediato da prestadora do serviço/operadora e disponibilização de canais alternativos de comunicação.

15.2. Notificação de Incidentes

O PREVIPALMAS adota transparência nas comunicações durante indisponibilidades. Em caso de incidentes graves, os usuários internos e públicos externos serão notificados sobre o status e previsão de normalização por meio de e-mail institucional, mensagens de texto via WhatsApp, contato telefônico ou publicação no portal institucional.

16. FISCALIZAÇÃO E DENÚNCIAS

- **Monitoramento:** Todos os ambientes, computadores, e-mails e conexões da rede do PREVIPALMAS estão sujeitos a monitoramento contínuo para fins de auditoria e segurança.
- **Canais de Denúncia:** Notificações de incidentes, violações de segurança ou uso indevido de recursos devem ser encaminhadas à Ouvidoria do PREVIPALMAS ou à Gerência de TI pelos canais oficiais.