IPREMB
seu futuro, nossa missão

Praça José Lino da Silva, 144
Brasiléia | Betim MG | 32600-308

ipremb.mg.gov.br
31 3595-7828
31 3594-5380

MANUAL DE PROCEDIMENTOS

SEGURANÇA DA INFORMAÇÃO E TECNOLOGIA

OBJETIVO

Estabelecer diretrizes e procedimentos para a gestão da segurança da informação, controle de acessos, operação de sistemas e tratamento de dados no âmbito do IPREMB, garantindo a confidencialidade, integridade e disponibilidade das informações, em conformidade com a Lei Geral de Proteção de Dados (LGPD) e demais legislações aplicáveis.

ABRANGÊNCIA

Este manual aplica-se aos servidores, estagiários, terceirizados, colaboradores do sistema (FAC) e, da SETE (TI da Prefeitura), bem como a todos que utilizam ou tenham acesso aos sistemas e bases de dados do IPREMB.

BASE LEGAL

- Constituição Federal – Princípios da Administração Pública;
- Lei nº 13.709/2018 – Lei Geral de Proteção de Dados (LGPD);
  Lei nº 12.527/2011 – Lei de Acesso à Informação (LAI);
- Lei nº 9.717/1998 – Normas gerais de organização dos RPPS;
- Portaria MPS nº 1.467/2022;
- Normas internas do IPREMB;

DEFINIÇÕES / PALAVRAS-CHAVE

- **Controle de Acesso:** Processo de concessão e revogação de permissões aos sistemas;
- **Dados Pessoais:** Informações relacionadas a pessoa natural identificada ou identificável;
- **Backup:** Cópia de segurança dos dados;
- **Incidente de Segurança:** Evento que compromete a segurança da informação;
- **Logs:** Registros de atividades realizadas nos sistemas;
- **VPN:** Acesso remoto seguro à rede institucional;

RESPONSABILIDADES

1. IPREMB

- Definir políticas de acesso e segurança da informação;
- Nomear o Encarregado de Dados (DPO);

Praça José Lino da Silva, 144
Brasiléia | Betim MG | 32600-308
ipremb.mg.gov.br
31 3595-7828
31 3594-5380

- Monitoramento: Registro e controle de acessos ativos;
- Revisão: Revisão periódica dos acessos (a cada 90 dias);
- Revogação: Bloqueio imediato e recolhimento/adequação de equipamentos pelo setor de TI, quando aplicável;

2. Acessos a Banco de Dados.

- Recebimento da demanda: Identificação da necessidade excepcional;
- Planejamento: Definição do escopo e justificativa;
- Aprovação: Autorização formal da Presidência;
- Execução: Acesso realizado com autenticação segura e registro em logs;
- Acompanhamento Técnico: Setor de TI acompanha a operação para garantir integridade do ambiente e suporte técnico;
- Monitoramento: Acompanhamento pelo responsável designado;
- Encerramento: Registro formal da atividade;
- Arquivamento: Guarda dos logs por período mínimo de 5 anos;

3. Backup e Recuperação de Dados.

- Planejamento: Definição de rotinas de backup;
- Execução: Backup diário incremental e semanal completo (SETE);
- Apoio Técnico: Setor de TI acompanha rotinas e verifica disponibilidade dos sistemas;
- Armazenamento: Guarda em locais seguros e distintos;
- Monitoramento: Verificação periódica da integridade dos backups;
- Teste: Simulação de restauração trimestral;
- Recuperação: Restauração em caso de incidente (prazo máximo de 8 horas);

4. Gestão de Logs e Rastreamento.

- Identificação: Monitoramento contínuo por sistemas e usuários;
- Contenção: Isolamento imediato da ameaça;
- Apoio Técnico: Setor de TI atua na identificação do impacto nos equipamentos e usuários;
- Avaliação: Análise de impacto pelo IPREMB (DPO);

Praça José Lino da Silva, 144
Brasiléia | Betim MG | 32600-308

ipremb.mg.gov.br

31 3595-7828
31 3594-5380

8. **Suporte Técnico e Rotinas Operacionais de TI**

- Recebimento da demanda: Abertura de chamados ou identificação de necessidade;
- Planejamento: Priorização conforme criticidade;
- Execução: Atendimento ao usuário e resolução de problemas;
- Acompanhamento: Monitoramento das rotinas diárias de TI;
- Orientação: Suporte e instrução aos usuários;
- Registro: Controle de atendimentos realizados;
- Melhoria contínua: Identificação de falhas recorrentes e apresentação de soluções.

CONTROLES INTERNOS

- Controle de acessos: Garantia de permissões adequadas;
  Evidências: Logs e registros;
- Controle de manutenção de equipamentos: Registro de todas as intervenções técnicas;
  Evidências: Chamados técnicos e relatórios de manutenção;
- Controle de ativos de TI: Monitoramento de equipamentos e estações de trabalho;
  Evidências: Inventário atualizado;
- Backup de dados: Execução e testes periódicos;
  Evidências: Relatórios de backup;
- Monitoramento de segurança: Acompanhamento contínuo;
  Evidências: Relatórios de incidentes;

INDICADORES

- Número de acessos concedidos/revogados;
- Número de chamados técnicos atendidos;
- Tempo médio de atendimento (SLA);
- Quantidade de manutenções realizadas;
- Tempo de resposta a incidentes;
- Taxa de sucesso na recuperação de backups;