PREFEITURA MUNICIPAL DE BARRA MANSA · PROTEÇÃO DE DADOS PESSOAIS

Política de Segurança da Informação e dos Dados

As medidas técnicas e administrativas que protegem os dados — e o papel da Íris como central de segurança da Prefeitura.

Versão 1.0 · vigência a partir de 01/10/2026

1. Objetivo

Esta política estabelece as medidas de segurança, técnicas e administrativas, que a Prefeitura Municipal de Barra Mansa adota para proteger os dados pessoais e as informações públicas contra acessos não autorizados e situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, conforme os arts. 46 a 49 da LGPD. Aplica-se a todos os sistemas integrados à Íris e a todas as pessoas que os acessam.

2. A Íris como central de segurança

A **Íris** (iris.barramansa.rj.gov.br) é a central de segurança e proteção de dados da Prefeitura. Ela reúne, num só lugar:

- **Identidade e acesso:** login central dos sistemas municipais com a conta de rede, criação de contas a partir do cadastro oficial do RH e controle de quem pode acessar o quê;
- **Monitoramento:** painel de disponibilidade e alertas da rede, dos servidores, das aplicações, do e-mail institucional e das rotinas de backup;
- **Inventário de acessos:** registro dos sistemas a que cada servidor tem acesso e revogação no desligamento;
- **Auditoria:** trilha das ações administrativas, dos acessos e das consultas à inteligência artificial;
- **Atendimento ao titular:** canal para pedidos e comunicações sobre dados pessoais, com login gov.br, protocolo e prazo, acompanhados pelo encarregado;
- **Inteligência artificial:** assistente que consolida o monitoramento de toda a infraestrutura e dos sistemas e orienta servidores e cidadãos com base na documentação oficial, respeitando o nível de sigilo de cada documento.

3. Controle de acesso e identidade

- **Conta única e pessoal:** o acesso usa a conta de rede da Prefeitura, validada no Active Directory. Não há senhas locais na Íris e a senha de rede nunca é armazenada nela.
- **Vínculo com o cadastro oficial:** só entra quem tem ficha no RH; a situação funcional decide o que a pessoa pode acessar. Contas genéricas ou compartilhadas são recusadas e contas desativadas no diretório não entram.
- **Perfis de acesso** (servidor, técnico, administrador), verificados no servidor a cada página e a cada operação, com negação por padrão. Toda mudança de perfil, bloqueio ou desbloqueio fica registrada.
- **Proteção contra tentativas repetidas:** limites de tentativas de login por conta e por origem e limites de uso nas operações sensíveis.
- **Primeiro acesso e recuperação de senha:** link de uso único, enviado ao e-mail cadastrado no RH, com validade de até 10 dias; a Íris guarda só a impressão criptográfica do link (SHA-256), nunca o link em si. A senha é gravada diretamente no diretório.
- **Login central (Entrar com a Íris):** padrão OpenID Connect, com fluxo de código de autorização, PKCE obrigatório, tokens assinados (Ed25519) de curta duração (10 minutos) e sem tokens de longa duração. A situação funcional e o aceite do termo são conferidos a cada entrada.
- **Sessões** guardadas no banco de dados, encerradas no bloqueio da conta e com saída de todos os sistemas de uma vez.
- **Acesso de emergência** da TI para quando o diretório estiver fora do ar, com senha protegida por hash forte (scrypt), poucas tentativas permitidas e registro de alerta a cada uso.

4. Proteção dos dados

- **Criptografia em trânsito:** todo acesso é por HTTPS (TLS) com certificado válido; a comunicação com o Active Directory usa LDAPS com certificado da autoridade interna conferido; a ligação entre o servidor da Íris e a rede da Prefeitura passa por túnel cifrado (VPN WireGuard).
- **Proteção de borda:** o domínio fica atrás da rede de proteção da Cloudflare, que filtra tráfego malicioso e ataques de negação de serviço.
- **Minimização e mascaramento:**os registros técnicos ocultam automaticamente senhas, tokens, CPF, e-mails e telefones; o perfil de trabalho mostra dados pessoais como "xxxx"; o conteúdo do chat com a inteligência artificial não é armazenado.
- **Proteção da base de conhecimento:** antes de indexar documentos, um filtro remove senhas, chaves e credenciais; nas respostas, a Íris oculta credenciais e endereços internos; cada

documento tem nível de sigilo (público, interno, restrito, sigiloso) e só aparece para quem pode vê-lo.

- **Integrações autenticadas:** comunicações entre sistemas usam assinatura HMAC-SHA256 com janela de tempo ou chaves de acesso dedicadas; segredos ficam em cofre e em variáveis de ambiente, fora do código-fonte.
- **Validação de entradas** nas operações do sistema e verificação da origem das requisições de login.

5. Infraestrutura, rede e comunicação

[redacted] RESTRITO Trechos tarjados contêm informação cuja divulgação comprometeria a segurança dos sistemas (LGPD, art. 46, e Lei nº 12.527/2011, art. 23): endereços, topologia de rede, localização de cópias de segurança e detalhes de configuração. Ficam à disposição dos órgãos de controle mediante solicitação formal ao encarregado, pelo e-mail lgpd@barramansa.rj.gov.br.

- **Borda e rede interna:** firewall de borda com segmentação em redes virtuais (VLANs), dois links de internet com contingência e unidades remotas ligadas por túneis VPN cifrados ([redacted] TOPOLOGIA). O Wi-Fi institucional separa a rede dos servidores da rede de convidados, que só acessa a internet.
- **Proxy com filtro de conteúdo** autenticado na conta de rede: bloqueia categorias de risco (malware, phishing, jogos de azar, conteúdo impróprio, anonimizadores) e mantém registro de navegação para auditoria.
- **Proteção de borda na nuvem (Cloudflare):** firewall de aplicação (WAF), mitigação de ataques de negação de serviço, bloqueio de robôs e TLS 1.2/1.3 na frente do site, da Íris e dos sistemas próprios.
- **Servidores e contêineres:** portas administrativas fechadas à internet, bloqueio automático de tentativas repetidas de acesso remoto (fail2ban), bancos de dados sem exposição pública ([redacted] ENDEREÇOS).
- **Identidade (Active Directory):** controladores de domínio com comunicação cifrada (LDAPS) e um controlador de contingência em nuvem, com disco cifrado e sem acesso público, para que o login não pare se a rede local cair. A conta de serviço da Íris tem só as permissões delegadas de que precisa.
- **E-mail institucional:** autenticação do domínio com SPF, DKIM (2048 bits) e DMARC em modo de rejeição, antispam, antivírus nas mensagens, bloqueio automático de força bruta, restrição geográfica de acesso e detecção de envio em massa e de contas comprometidas.
- **Estações de trabalho:** padronização por políticas de grupo (atualizações automáticas, Microsoft Defender com regras de redução de superfície de ataque, controle de aplicativos e auditoria

avançada), aplicada em fases.

- **Cofre de senhas:** credenciais administrativas guardadas em cofre criptografado; nenhuma senha é registrada em documentos, notas ou mensagens.

6. Monitoramento e detecção

- Monitoramento contínuo (24 horas) de rede, servidores, links, aplicações, e-mail e backups, com o Zabbix e verificações próprias a cada 5 minutos, painel na Íris e alertas imediatos à equipe de TI;
- Vigilância de segurança: alerta a cada acesso administrativo aos servidores e painéis, portas expostas indevidamente, alterações de configuração do firewall e eventos de login e de grupos privilegiados no diretório;
- A Íris consolida esses sinais e responde à equipe de TI sobre o estado de cada sistema, como parte do seu papel de inteligência artificial do Município.

7. Cópias de segurança (backup)

As cópias de segurança seguem a regra de manter, para cada sistema, uma cópia no próprio servidor e outra fora dele, em armazenamento de nuvem da Prefeitura ([■■■ LOCAL]):

O quê	Frequência	Retenção e cópia externa
Bancos de dados dos sistemas próprios (Íris, Protocolo RH, Central de Veículos, Fábrica de Óculos, GIP e outros)	A cada 6 horas	7 dias no servidor; cópia diária enviada à nuvem
Arquivos enviados aos sistemas (anexos, laudos, fotos)	A cada 6 horas ou diário	Cópia diária na nuvem, sem apagar o histórico
Site institucional	Diário (banco e arquivos)	Cópia diária na nuvem
E-mail institucional	Espelho semanal e sincronização diária	Nuvem; mensagens apagadas são arquivadas com verificação de integridade (tamanho e hash) antes de qualquer exclusão
Servidor de e-mail e Portal da Transparência (configuração, sites e bancos)	Configuração diária; sites e bancos semanal	2 semanas
Diretório (Active Directory)	Periódico	Mídia de instalação do diretório, cifrada, na nuvem

O quê	Frequência	Retenção e cópia externa
Geoprocessamento e servidores em nuvem	Incremental diário, completo semanal e snapshots duas vezes ao dia	Nuvem
Configuração do proxy e do firewall	A cada 6 horas	No servidor e na nuvem

Controle: cada servidor envia à Íris o estado dos seus backups (data, tamanho, envio à nuvem). Backup atrasado (mais de 8 horas), vazio ou não enviado gera alerta imediato à TI, e a Íris guarda o histórico de cada execução. As restaurações são feitas com verificação de integridade (tamanho e hash) para comprovar que a cópia recuperada é idêntica à original.

8. Trilha de auditoria

A Íris registra quem fez, o quê, quando e sobre qual registro: logins, acessos de emergência, importações do RH, criação e alteração de contas, envio de links de acesso, aceites de termo, mudanças de perfil, consultas à inteligência artificial (sem o conteúdo) e operações sobre documentos. A aplicação não altera nem apaga esses registros, que ficam disponíveis à TI, ao encarregado e aos órgãos de controle.

9. Desenvolvimento e operação seguros

- Código-fonte em repositório privado, com revisão por pull request, verificações automáticas (tipagem, lint, testes unitários e de ponta a ponta, simulação de migrações) e auditoria independente das mudanças que mexem em autenticação, autorização e dados;
- Varredura de segredos no histórico do repositório (Gitleaks) e dados reais (como a planilha do RH) mantidos fora do repositório;
- Implantação por contêineres (Docker, Coolify) com imagem construída sem acesso à rede, banco PostgreSQL e cache Redis em rede interna, e promoção para produção só depois de aprovação humana;
- Monitoramento contínuo pelo Zabbix e por verificações próprias, com painel na Íris e acompanhamento da execução dos backups;
- Eliminação automática diária de registros técnicos que já cumpriram a finalidade.

10. Medidas administrativas

- **Termo de responsabilidade** aceito no primeiro acesso, com versão e data registradas (veja a Política de Uso);
- **Mínimo privilégio:** cada pessoa acessa só o necessário para o cargo; o acesso acompanha a situação funcional do RH;
- **Orientação contínua:** a Íris responde dúvidas de segurança e a TI nunca pede senha por nenhum canal;
- **Encarregado designado** e canais públicos de contato (veja Encarregado).

11. Resposta a incidentes

1. **Detecção:** pelo monitoramento, pela trilha de auditoria ou por comunicação de qualquer servidor ou cidadão à TI ou ao encarregado, pelo e-mail lgpd@barramansa.rj.gov.br.
2. **Contenção:** bloqueio de contas e sessões, troca de credenciais e isolamento do sistema afetado.
3. **Avaliação:** o encarregado avalia quais dados e titulares foram afetados e o risco ou dano relevante.
4. **Comunicação:** havendo risco ou dano relevante, comunicação à ANPD e aos titulares em até 3 dias úteis, conforme o art. 48 da LGPD e a Resolução CD/ANPD nº 15/2024.
5. **Registro e melhoria:** o incidente é registrado, com causa, medidas adotadas e lições aprendidas, e os controles são revistos.

12. Melhoria contínua

A segurança é revista continuamente. Estão em andamento, entre outras, as seguintes melhorias:

- segundo fator de autenticação em todas as contas administrativas e de nuvem;
- cifragem das cópias de segurança enviadas à nuvem e solução corporativa de backup;
- testes periódicos e registrados de restauração dos bancos de dados;
- antivírus corporativo com console central de gestão;
- renovação de servidores e estações de trabalho com sistemas legados;
- cabeçalhos de segurança adicionais nas páginas, proteção da trilha de auditoria no próprio banco de dados e varredura automática de dependências e segredos a cada mudança;
- contratos de operador com cláusulas de proteção de dados para todos os fornecedores e tabela de temporalidade dos dados funcionais e dos atendimentos.

O andamento dessas medidas é acompanhado pelo encarregado e revisto junto com este documento.