PREFEITURA MUNICIPAL DE BARRA MANSA · PROTEÇÃO DE DADOS PESSOAIS

Política de Uso da Íris e dos Sistemas

Regras de uso da Íris e dos sistemas municipais: conta pessoal, uso aceitável e responsabilidades.

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

Esta política define as regras de uso da **Íris** (iris.barramansa.rj.gov.br) — o sistema de atendimento, monitoramento e central de segurança da Prefeitura Municipal de Barra Mansa — e dos sistemas municipais que usam a conta de rede da Prefeitura, como o login central da Íris para o Protocolo RH. Aplica-se a servidores efetivos, comissionados, contratados, estagiários e prestadores de serviço com acesso aos sistemas.

1. Conta de acesso

- O acesso usa a **conta de rede** da Prefeitura (a mesma do computador), com a senha validada pelo Active Directory. A Íris não guarda a senha de rede.
- A entrada aceita o usuário de rede, o CPF ou o e-mail cadastrado no RH. O primeiro acesso e a recuperação de senha são feitos em "Não consigo entrar": o link de uso único vai para o e-mail pessoal cadastrado no RH e expira.
- A Íris e a equipe de TI **nunca pedem senha** por chat, telefone, e-mail ou mensagem. Pedido desse tipo deve ser tratado como tentativa de fraude e informado à TI.
- O acesso acompanha a situação funcional do cadastro oficial do RH. Quando todos os vínculos terminam, a pessoa perde os serviços internos de TI e mantém só o necessário para ser atendida pelo RH, com a conta de rede numa unidade isolada, sem internet e sem pastas da secretaria.

2. Uso aceitável

- Usar os sistemas apenas para as atividades do cargo e no interesse público;
- Consultar somente os dados necessários ao serviço — "só para olhar" também é uso indevido;
- Não inserir no chat da Íris senhas, dados bancários, dados de saúde nem dados pessoais de terceiros que não sejam necessários ao atendimento;
- Não tentar burlar controles de acesso, testar vulnerabilidades ou usar a conta de outra pessoa;
- Manter o cadastro verdadeiro e atualizado e bloquear o computador ao se ausentar;
- Comunicar imediatamente à TI qualquer suspeita de incidente: senha exposta, e-mail suspeito, perda de equipamento ou acesso indevido.

3. Inteligência artificial

- A Íris responde **com base na documentação oficial** da Prefeitura e cita a fonte. Quando não sabe, diz que não sabe — e a dúvida vira fila de curadoria da TI.
- As respostas são **apoio ao trabalho**: não substituem norma, parecer jurídico nem decisão da autoridade competente.
- Os documentos passam por filtro que remove credenciais e dados sensíveis antes de serem indexados, e cada pessoa só recebe respostas compatíveis com o seu perfil de acesso.

4. Termo de responsabilidade e proteção de dados

Ao definir a senha pela primeira vez, o servidor declara ciência do termo abaixo (versão 1). A data, a hora e a versão do aceite ficam registradas.

O acesso é pessoal e intransferível. O acesso aos sistemas da Prefeitura Municipal de Barra Mansa é **pessoal e intransferível**. Sua senha é sua assinatura: tudo o que for feito com o seu usuário é de sua responsabilidade, inclusive por quem você tenha deixado usá-lo. Compartilhar credenciais é falta funcional.

Uso exclusivo para as atividades do cargo. Os sistemas devem ser usados **exclusivamente para as atividades do seu cargo**. Consultar dados sem necessidade de serviço, copiar ou divulgar informações, alterar registros indevidamente ou usar os sistemas para interesse particular é uso indevido de recurso público — ainda que "só para olhar".

Dados pessoais são protegidos por lei. Os dados tratados nos sistemas incluem **dados pessoais de cidadãos e servidores**, protegidos pela Lei Geral de Proteção de Dados (Lei nº 13.709/2018). O acesso, o uso e o compartilhamento indevidos desses dados sujeitam o agente público a responsabilização, sem prejuízo das sanções previstas na própria LGPD.

O descumprimento tem consequência. O descumprimento deste termo pode resultar em **responsabilização administrativa, civil e penal**: processo disciplinar na forma do estatuto dos servidores, dever de reparar danos causados, e enquadramento nos crimes de inserção de dados falsos, modificação não autorizada de sistema de informações e violação de sigilo funcional (arts. 313-A, 313-B e 325 do Código Penal).

A Íris está de olho. Cada login, consulta e alteração feita com o seu usuário é registrada em trilha de auditoria imutável — com data, hora, usuário e origem do acesso — e os sistemas são monitorados 24 horas por dia. Desvios de uso são detectados e comunicados à Coordenadoria de Tecnologia da Informação e à Controladoria Geral do Município.

5. Monitoramento e auditoria

O uso dos sistemas é registrado em trilha de auditoria (quem, o quê, quando e de onde), para a segurança da informação pública e para a apuração de responsabilidades. Os registros técnicos ocultam dados pessoais e só são consultados por pessoas autorizadas.

6. Documentos relacionados

- Política de Privacidade
- Política de Segurança da Informação e dos Dados
- Encarregado pelo Tratamento de Dados Pessoais