Políticas de Segurança

- Proteção de dados de clientes (coleta mínima e consentimento explícito).
- Armazenamento seguro dos dados em bancos criptografados.
- Acesso restrito a informações via autenticação multifatorial (exemplo - verificação em duas etapas.
- Atualizações OTA para coleiras e dispositivos.
- Criptografia ponta a ponta (TLS/SSL) na comunicação.
- Controle de autenticação para ações críticas em dispositivos.
- Gestão de incidentes com detecção rápida e resposta imediata.
- Política de senhas fortes e troca periódica.
- Treinamento e conscientização de colaboradores.
- Comunicação transparente sobre incidentes em até 72 horas.