(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

RELATÓRIO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS – RIPD 002/2026

PROJETO: IMPLANTAÇÃO DE CONTROLE DE ACESSO POR BIOMETRIA FACIAL NAS CATRACAS

CAMPO	INFORMAÇÃO
Controlador	Câmara Municipal de Vitória da Conquista - BA
Objeto	Sistema eletrônico de controle de acesso às dependências da Câmara Municipal mediante catracas, com possibilidade de autenticação por reconhecimento facial.
Fase	Planejamento da contratação
Versão	1.0
Classificação	Documento integral - uso interno administrativo.
Documentos vinculados	Anexos II-01 a II-15 (Anexo II) e Glossário (Anexo III).

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

Seção 1 - Contexto do produto ou serviço

1.1 Visão geral

A Câmara Municipal de Vitória da Conquista pretende implantar sistema eletrônico de controle de acesso às suas dependências, utilizando catracas dotadas de tecnologia de reconhecimento facial, com os seguintes objetivos:

- organizar o ingresso e a saída de pessoas;
- aprimorar a segurança institucional;
- reduzir riscos relacionados ao uso indevido de credenciais;
- melhorar o controle dos acessos;
- permitir a rastreabilidade dos eventos de entrada e saída;
- auxiliar na proteção de pessoas, instalações, equipamentos e patrimônio.

A utilização da biometria facial deverá ocorrer exclusivamente nos limites estabelecidos neste RIPD. A Câmara deverá disponibilizar mecanismo alternativo de acesso para pessoas que não utilizem a autenticação facial (Anexo II-08), ressalvadas situações concretas em que restrições específicas sejam juridicamente justificadas por requisitos legais ou de segurança.

1.2 Necessidade do RIPD

Este RIPD tem por finalidade descrever os tratamentos de dados pessoais envolvidos no projeto, identificar os riscos aos direitos e liberdades dos titulares, avaliar a necessidade, a adequação e a proporcionalidade do uso da biometria facial e definir as medidas para reduzir esses riscos.

Adicionalmente, o relatório orienta a contratação da solução: estabelece os requisitos que devem constar do Estudo Técnico Preliminar (ETP), do Termo de Referência, do edital e do contrato, e fixa as condições que deverão ser comprovadas antes da entrada em produção do sistema. Serve, ainda, como evidência de prevenção, segurança, transparência e responsabilização da Câmara perante os titulares e a ANPD.

O tratamento é considerado, preventivamente, de elevado risco em razão da combinação dos seguintes elementos:

- utilização de dados biométricos, que são dados pessoais sensíveis;
- emprego de tecnologia de reconhecimento facial;
- tratamento em área acessível ao público;
- decisão automatizada inicial;
- possibilidade de identificação incorreta e de negativa indevida de acesso;
- riscos de discriminação e viés algorítmico;
- riscos decorrentes de incidentes de segurança;
- possibilidade de uso secundário dos dados;

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

- possibilidade de tratamento em larga escala, conforme a quantidade efetiva de titulares cadastrados e a frequência de utilização.

A classificação de risco não significa que o tratamento seja necessariamente ilícito ou inviável, mas impõe maior rigor na demonstração de necessidade, proporcionalidade, segurança, transparência e governança.

1.3 Critérios gerais e específicos de alto risco

CRITÉRIO DO MODELO	PRESENTE?	JUSTIFICATIVA
Larga escala	A confirmar	Depende da quantidade efetiva de titulares cadastrados e da frequência de uso. Estimativa a constar do ETP.
Afetação significativa de interesses e direitos	Sim	Pode haver identificação incorreta, negativa indevida de acesso, discriminação e incidentes com impacto a direitos.
Tecnologia emergente ou inovadora	Sim	Reconhecimento facial para autenticação biométrica.
Vigilância ou controle de zona acessível ao público	Sim	Controle de ingresso e saída nas dependências da Câmara, inclusive de visitantes e cidadãos.
Decisão unicamente automatizada	Não, como decisão definitiva	Há decisão automatizada inicial, mas com intervenção humana obrigatória; não pode haver negativa definitiva exclusivamente algorítmica (Anexo II-07).
Dados sensíveis / crianças / adolescentes / idosos	Sim	Tratamento de biometria (dado sensível) e presença de idosos entre os titulares; vedado o cadastro biométrico de crianças e adolescentes visitantes.

Seção 2 - Tratamento dos dados pessoais

2.1 Descrição dos tratamentos

FINALIDADE	DESCRIÇÃO	TITULARES	DADOS	HIPÓTESE LEGAL PROPOSTA

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

FINALIDADE	DESCRIÇÃO	TITULARES	DADOS	HIPÓTESE LEGAL PROPOSTA
Controle de acesso físico	Permitir ou negar o ingresso conforme regras institucionais.	Vereadores, servidores, estagiários, colaboradores, terceirizados, prestadores, fornecedores, representantes, autoridades, convidados, visitantes e cidadãos.	Nome; documento; CPF quando necessário; vínculo; cargo/função; empresa; autorização; data/hora; entrada/saída; catraca; resultado; falha; intervenção.	Art. 7º, II ou art. 23, caput (execução de competências e atribuições legais), com indicação do Regimento Interno ou ato da Mesa que atribui a gestão da segurança do prédio.
Autenticação biométrica	Confirmar a correspondência entre a pessoa e o cadastro autorizado.	Pessoas que optarem pela biometria.	Imagem facial no cadastro, template, resultado da comparação e informações técnicas necessárias.	Opção A: art. 11, II, "g", c/c art. 23. Opção B: art. 11, I (consentimento). Ver subseção 2.1.1.
Segurança institucional	Proteger pessoas, instalações, equipamentos, documentos e patrimônio.	Categorias acima.	Cadastrais, biométricos e registros estritamente necessários.	Mesma hipótese do controle de acesso e da autenticação.
Rastreabilidade	Registrar eventos mínimos de entrada e saída e permitir auditorias de segurança.	Usuários do sistema.	Data, hora, entrada/saída, catraca, resultado, falha e intervenção.	Art. 7º, II ou art. 23.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

FINALIDADE	DESCRIÇÃO	TITULARES	DADOS	HIPÓTESE LEGAL PROPOSTA
Apuração de incidentes	Usar registros, quando necessário, para apurar incidentes e irregularidades de segurança.	Pessoas relacionadas ao evento.	Registros e dados estritamente necessários.	Art. 7º, II ou VI (exercício regular de direitos em processo), conforme o caso concreto.

2.1.1 Análise preliminar da hipótese legal para a biometria

A definição da hipótese legal compete à Procuradoria Jurídica, ouvido o encarregado. Para subsidiar essa decisão, registram-se as duas opções identificadas:

ASPECTO	OPÇÃO A - ART. 11, II, "G", C/C ART. 23	OPÇÃO B - ART. 11, I (CONSENTIMENTO)
Fundamento	Garantia da prevenção à fraude e da segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos do art. 9º.	Manifestação livre, informada, inequívoca, específica e destacada do titular.
Pontos a favor	Adequada à finalidade de autenticação; não depende da vontade do titular para a continuidade do tratamento.	Coerente com a natureza opcional da biometria e com a existência de via alternativa.
Pontos de atenção	Exige demonstração concreta do risco de fraude; a finalidade de segurança do prédio não se confunde integralmente com a "segurança do titular"; cede se prevalecerem direitos fundamentais.	No poder público, a assimetria de poder - especialmente com servidores e terceirizados subordinados - pode comprometer a liberdade do consentimento; exige controle de revogação.
Direitos adicionais	Arts. 18, VI, VIII e IX não se aplicam; a desistência da biometria continua garantida por política institucional (subseção 4.3).	Aplicam-se os arts. 18, VI (eliminação), VIII (informação sobre não consentir) e IX (revogação).

> *O Aviso de Privacidade somente poderá ser publicado depois de definida a hipótese legal de cada tratamento. É possível adotar hipóteses distintas por categoria de titular (por exemplo, servidores e visitantes), desde que registrado.*

2.2 Fluxo do tratamento dos dados pessoais

O fluxo completo, com fluxograma e descrição etapa por etapa, consta do Anexo II-01. Em síntese:

1. informação prévia ao titular por sinalização e aviso;
2. cadastro do titular, quando aplicável, com coleta dos dados mínimos necessários;
3. geração do template biométrico, quando o titular optar pela biometria;
4. armazenamento protegido;
5. tentativa de autenticação na catraca e comparação biométrica;
6. liberação ou bloqueio inicial da catraca;
7. intervenção humana em caso de falha, dúvida ou contestação;
8. registro mínimo do evento;
9. retenção pelo prazo definido;
10. eliminação segura ou anonimização, quando cabível.

A tentativa de autenticação não poderá resultar em tratamento adicional não previsto neste RIPD. Sempre que tecnicamente possível, deverá ser utilizado template protegido, reduzindo-se ao mínimo necessário o armazenamento da imagem facial original.

2.3 Agentes de tratamento e partes interessadas

2.3.1 Controlador

CAMPO	INFORMAÇÃO
Controlador	Câmara Municipal de Vitória da Conquista - Estado da Bahia
CNPJ / endereço / contato	CNPJ: 14.645.717/0001-03 - Rua Coronel Gugé, nº 150, Centro, CEP 45000-510, Vitória da Conquista - BA - Fone (77) 3086-9600 - administracao@camaravc.ba.gov.br
Enquadramento	Controlador singular
Responsabilidades	Determinar finalidades; definir dados; critérios de acesso; retenção; segurança; supervisionar o operador; atender direitos; manter registros; revisar o RIPD; fiscalizar o contrato.
Encarregado	Lucas Fernandes de Melo
Consulta ao encarregado	Participação na elaboração, revisão, implementação e monitoramento.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

2.3.2 Operador(es)

Será operadora a empresa contratada para fornecer, implantar, manter ou operar a solução. A identificação definitiva ocorrerá após a contratação. O operador deverá:

- tratar dados somente conforme instruções documentadas da Câmara;
- não utilizar os dados para finalidade própria, não os comercializar e não os compartilhar sem autorização;
- não utilizar os dados para treinamento de modelos de inteligência artificial;
- manter controles de segurança conforme o Anexo II-04;
- comunicar incidentes à Câmara imediatamente, no prazo máximo de 24 horas da ciência;
- permitir auditorias e cooperar com a Câmara e o encarregado;
- informar suboperadores, localização da infraestrutura e eventual transferência internacional (Anexo II-13);
- eliminar ou devolver os dados ao término do contrato, conforme determinação da Câmara e a legislação.

2.3.3 Outras partes interessadas ou envolvidas

As partes abaixo são consultadas durante a elaboração e a execução do projeto, elas não assinam nem aprovam o RIPD; suas manifestações são registradas na Seção 7.2 e, quando divergentes, expressamente consideradas.

PARTE	ENVOLVIMENTO	RESPONSÁVEL
Unidade responsável pelo projeto	Planejamento e acompanhamento.	Lucas Fernandes de Melo
Tecnologia da Informação	Arquitetura, implantação e suporte.	Lucas Fernandes de Melo
Segurança da Informação	Controles, incidentes e auditorias.	Lucas Fernandes de Melo
Encarregado	Proteção de dados e direitos dos titulares.	Lucas Fernandes de Melo
Procuradoria Jurídica	Hipóteses legais e contratação.	Flavio Farias de Carvalho
Responsável pela contratação	ETP, Termo de Referência, edital e contrato.	Equipe de licitação
Autoridade competente	Decisão sobre a entrada em produção.	Ivan Cordeiro da Silva Filho

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

2.4 Compartilhamento de dados pessoais

Como regra, não haverá compartilhamento dos dados biométricos com terceiros controladores. O operador, atuando por conta e sob instruções da Câmara, é tratado na subseção 2.3.2 e não configura compartilhamento.

Qualquer compartilhamento futuro deverá possuir finalidade específica, fundamento jurídico, limitação aos dados necessários, formalização, registro, análise jurídica e de proteção de dados, observância dos direitos e segurança compatível. Entregas de registros a autoridades somente ocorrerão por ordem judicial ou requisição legal, com registro.

2.5 Transferência internacional de dados pessoais

Antes da contratação, a Câmara exigirá do fornecedor a declaração do Anexo II-13, com localização física dos servidores, países de armazenamento e processamento, suporte estrangeiro, suboperadores estrangeiros, acesso remoto a partir do exterior e mecanismo jurídico de eventual transferência. Será priorizado o armazenamento e processamento no Brasil. Eventual transferência dependerá de análise específica e do atendimento à LGPD (arts. 33 a 36) e à Resolução CD/ANPD nº 19/2024.

2.6 Eliminação de dados pessoais

Os prazos abaixo são detalhados na Política de Retenção e Eliminação (Anexo II-09). Os três primeiros prazos constavam da versão 1.0; os demais são propostas complementares, sinalizadas para validação pela unidade responsável, pela Procuradoria Jurídica e pelo setor de gestão documental.

TIPO DE DADO	PRAZO / CRITÉRIO	CONSERVAÇÃO EXCEPCIONAL	DESCARTE	SITUAÇÃO
Biometria de visitantes	Até 90 dias após o último acesso	Somente bloqueio por incidente em apuração ou ordem judicial	Eliminação automática e auditável	Definido
Cadastro de visitantes	Até 90 dias após o último acesso	Necessidade legal específica	Eliminação segura	Definido
Registros (logs) de acesso	Até 2 anos	Obrigação legal, processo administrativo, investigação formal, ordem judicial ou incidente em apuração	Eliminação ou anonimização	Definido

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

TIPO DE DADO	PRAZO / CRITÉRIO	CONSERVAÇÃO EXCEPCIONAL	DESCARTE	SITUAÇÃO
Template de vereadores, servidores e colaboradores	Até 30 dias após o fim do vínculo; até 5 dias úteis após desistência da biometria	Nenhuma	Eliminação segura	Definido
Cadastro de servidores e colaboradores no sistema	Até 90 dias após o fim do vínculo	Obrigação legal específica	Eliminação segura	Definido
Imagem facial original do cadastro	Não armazenar; se indispensável, até 24 horas	Nenhuma	Eliminação automática	Definido
Imagem da tentativa de autenticação	Descarte imediato após a comparação	Nenhuma	Descarte automático	Definido
Cópias de segurança (backups)	Ciclo de expiração de até 35 dias	Nenhuma adicional	Expiração automática	Definido
Dados de testes (prova de conceito, homologação, viés)	Até 30 dias após o relatório final	Nenhuma	Eliminação; resultados só agregados	Definido
Registros de contingência em papel	Inserção no sistema em até 5 dias úteis e destruição; máximo 90 dias	Nenhuma	Fragmentação	Definido
Solicitações de titulares	Até 5 anos após a resposta	Processo administrativo ou judicial	Eliminação conforme temporalidade	Definido

A eliminação deverá ser segura, automatizada quando possível, auditável, gerar evidência e abranger cópias e ambientes sob responsabilidade do operador.

2.7 Sistemas de informação relacionados

SISTEMA	HOSPEDAGEM	ESTRUTURANTE?	FUNCIONALIDADES

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

SISTEMA	HOSPEDAGEM	ESTRUTURANTE?	FUNCIONALIDADES
Sistema eletrônico de controle de acesso / biometria facial	Fornecedor externo - a identificar	A confirmar	Cadastro, template, armazenamento, autenticação, comparação, catracas, logs, administração e auditoria.
Infraestrutura de hospedagem	A confirmar (preferência: Brasil ou instalações da Câmara)	A confirmar	Armazenamento, processamento, backup e suporte.

Seção 3 - Análise dos princípios da LGPD

3.1 Finalidade

Controle de acesso, segurança institucional, autenticação, rastreabilidade e apuração de incidentes. São vedados usos incompatíveis, como publicidade, marketing, venda, criação de perfis comportamentais, monitoramento permanente, rastreamento interno sem fundamento, inferência de emoções, classificação racial, étnica ou de gênero, vigilância massiva e treinamento de inteligência artificial.

3.2 Adequação

O tratamento é compatível com as finalidades informadas ao titular; a adequação será reavaliada nas revisões periódicas do RIPD.

3.3 Necessidade

Somente serão tratados dados indispensáveis. São vedados dados sem finalidade, imagens adicionais, dados de comportamento, gênero, raça, emoções, saúde e características não necessárias. A necessidade da própria biometria deve ser demonstrada na análise de alternativas (subseção 3.11).

3.4 Livre acesso

Aviso de Privacidade (Anexo II-11), canal eletrônico, atendimento presencial, contato do encarregado e Formulário de Atendimento aos Direitos (Anexo II-12).

3.5 Qualidade dos dados

Atualização, correção, exclusão de registros incorretos, identificação de inconsistências e correção de erros de vinculação biométrica.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

3.6 Transparência

Sinalização ostensiva antes da área de captação, informando finalidade, uso de biometria, responsável, direitos, canal do encarregado, QR Code do aviso e existência de alternativa.

3.7 Segurança

Medidas técnicas e administrativas descritas na subseção 5.5 e detalhadas nas Especificações Mínimas de Segurança (Anexo II-04).

3.8 Prevenção

Proteção desde o planejamento e em todo o ciclo de vida: privacidade desde a concepção e por padrão, coleta e retenção mínimas e desativação de funções desnecessárias.

3.9 Não discriminação

Testes de desempenho por grupos demográficos e condições de captura (Anexo II-06); suspensão ou não entrada em produção se houver risco discriminatório incompatível.

3.10 Responsabilização e prestação de contas

RIPD, ROPA, instrumentos de contratação, relatórios de testes, auditorias, registros de incidentes, solicitações de titulares e evidências de eliminação constituem as evidências de conformidade.

3.11 Necessidade, adequação e proporcionalidade - alternativas

ALTERNATIVA	IMPACTO À PRIVACIDADE	SEGURANÇA	RISCO	ADEQUAÇÃO
Crachá / credencial	Baixo	Médio (risco de perda / furto)	Médio (Uso por terceiro se clonado ou extraviado)	Alta (Solução tradicional e de baixo custo)
Cartão / QR Code	Baixo	Médio (QR pode ser compartilhado digitalmente)	Médio (Facilidade de repasse de captura de tela)	Alta (Ideal para visitantes e integrações mobile)
Conferência pela recepção	Muito baixo	Baixo (Sujeito a falha humana)	Médio-Alto (Falta de registro automatizado /gargalos)	Média (Recomendado apenas como contingência)

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

ALTERNATIVA	IMPACTO À PRIVACIDADE	SEGURANÇA	RISCO	ADEQUAÇÃO
Biometria facial	Elevado	Elevado (Precisão na identificação inequívoca)	Elevado (Vazamento de dados biométricos/LGPD)	Média-Alta (Excelente segurança, mas exige forte governança jurídica)

A biometria facial não deverá ser adotada exclusivamente por conveniência tecnológica. A decisão deverá considerar benefícios concretos, riscos, alternativas, direitos fundamentais, custos e benefícios, segurança institucional e salvaguardas, com registro no ETP.

Seção 4 - Garantia do exercício dos direitos pelos titulares

A Câmara disponibilizará canal eletrônico e atendimento presencial. As solicitações serão recebidas, registradas, analisadas, respondidas e rastreáveis, conforme o Anexo II-12. A confirmação de existência e o acesso simplificado serão atendidos de imediato; a declaração completa, em até 15 dias (LGPD, art. 19).

4.1 Medidas gerais

- designação formal do encarregado e de seu substituto;
- canal eletrônico e atendimento presencial;
- confirmação de identidade quando necessária;
- procedimentos de recebimento, registro, análise, encaminhamento, atendimento e resposta;
- registro das solicitações e providências;
- fluxos internos entre unidade responsável, encarregado, Procuradoria, TI e Segurança da Informação;
- funcionalidades do sistema para localizar, recuperar, corrigir, bloquear, anonimizar, eliminar ou disponibilizar dados;
- capacitação e revisão periódicas.

4.2 Medidas específicas por direito

DIREITO	APLICABILIDADE	MEDIDA
Acesso facilitado às informações - art. 9º	Sim	Aviso, sinalização, canal e encarregado.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

DIREITO	APLICABILIDADE	MEDIDA
Confirmação da existência de tratamento - art. 18, I	Sim	Canal institucional; resposta imediata simplificada.
Acesso aos dados - art. 18, II	Sim	Procedimento do Anexo II-12.
Correção - art. 18, III	Sim	Correção cadastral e de vinculação biométrica.
Anonimização, bloqueio ou eliminação - art. 18, IV	Sim	Avaliação individual e procedimento.
Portabilidade - art. 18, V	A confirmar	Pendente de regulamentação pela ANPD; templates não são portáveis entre sistemas distintos.
Eliminação de dados tratados com consentimento - art. 18, VI	Somente se adotada a Opção B (subseção 2.1.1)	Procedimento específico.
Informação sobre compartilhamentos - art. 18, VII	Sim	Informação pelo canal competente.
Informação sobre a possibilidade de não fornecer consentimento e suas consequências - art. 18, VIII	Somente se adotada a Opção B	O aviso deverá informar que o titular pode não consentir e que a consequência é apenas utilizar a via alternativa, sem prejuízo de acesso.
Revogação do consentimento - art. 18, IX	Somente se adotada a Opção B	Procedimento gratuito e facilitado.
Revisão de decisão automatizada - art. 20	Sim	Revisão humana (Anexo II-07) e informação sobre critérios e procedimentos.

4.3 Alternativa à biometria facial

A Câmara manterá alternativa funcional: identificação convencional, recepção humana, documento quando necessário, credencial ou QR Code, conforme o Procedimento Alternativo de Acesso (Anexo II-08). A recusa não poderá, por si só, resultar em impedimento de acesso a serviço público ou atividade aberta ao cidadão, ressalvadas situações concretas justificadas. A alternativa não

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

poderá ser deliberadamente mais onerosa, constrangedora ou desproporcional. Independentemente da hipótese legal adotada, o titular poderá desistir da biometria a qualquer tempo.

4.4 Crianças e adolescentes

Não será realizado cadastro ou autenticação biométrica facial de crianças e adolescentes visitantes; o acesso ocorrerá por recepção e identificação convencional. Para adolescentes estagiários ou com vínculo institucional específico, deverá haver análise jurídica específica, observado o art. 14 da LGPD. O sistema deverá bloquear tecnicamente o cadastro biométrico de menores nas situações definidas.

Seção 5 - Gestão de riscos

A identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos observarão a metodologia de gestão de riscos. A análise é feita sob a perspectiva do titular dos dados. A matriz completa, com fichas por risco, consta do Anexo II-02.

5.1 Critérios básicos

5.1.1 Impacto

NÍVEL	CRITÉRIO
1 - Muito baixo	Sem desconforto perceptível ou risco a direitos; dados anonimizados ou agregados sem possibilidade de reidentificação.
2 - Baixo	Sem desconforto significativo; dados pseudonimizados ou de difícil identificação.
3 - Médio	Desconforto sem prejuízo financeiro e sem risco relevante; dados identificáveis.
4 - Alto	Restrição relevante, de difícil reversão, ou prejuízo significativo; dados sensíveis ou de pessoas vulneráveis.
5 - Muito alto	Restrição grave ou possivelmente irreversível; potencial dano à vida, integridade ou dignidade; alto volume ou tratamento de alto risco.

5.1.2 Probabilidade

NÍVEL	CRITÉRIO
1 - Muito baixa	Menos de uma ocorrência a cada dois anos.
2 - Baixa	Uma ocorrência a cada dois anos, até uma ocorrência por ano.
3 - Média	Mais de uma ocorrência por ano, até uma ocorrência por semestre.
4 - Alta	Mais de uma ocorrência por semestre, até uma ocorrência por mês.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

NÍVEL	CRITÉRIO
5 - Muito alta	Mais de uma ocorrência por mês.

5.1.3 Estratégia e aceitação

Nível de risco = Impacto × Probabilidade. O **limite de tolerância ao risco** é o nível máximo de risco que a Câmara admite manter sem adotar medidas adicionais, definido pela autoridade competente em alinhamento com a metodologia de gestão de riscos institucionais.

FAIXA	CLASSIFICAÇÃO	TRATAMENTO
1-3	Pequeno	Aceitável, por estar dentro do limite de tolerância ao risco definido pela Câmara.
4-6	Moderado	Aceitável, podendo ser reduzido de forma proporcional.
8-12	Alto	Inaceitável sem controles adequados.
15-25	Crítico	Inaceitável; exige controles imediatos e impede a entrada em produção.

5.2 Identificação, análise e avaliação de riscos

ID	RISCO	P	I	NÍVEL INERENTE	PRINCIPAIS MEDIDAS
R01	Vazamento de biometria	3	5	15 - Crítico	Criptografia, segregação, controle de acesso e testes.
R02	Acesso interno indevido	3	4	12 - Alto	Menor privilégio, MFA e auditoria.
R03	Uso secundário	2	5	10 - Alto	Cláusulas contratuais e bloqueios técnicos.
R04	Falso positivo	3	4	12 - Alto	Revisão humana e testes.
R05	Falso negativo	3	4	12 - Alto	Alternativa humana.
R06	Viés algorítmico	3	5	15 - Crítico	Testes de desempenho e auditoria.
R07	Cadastro indevido de menor	2	5	10 - Alto	Bloqueio de cadastro biométrico.
R08	Retenção excessiva	3	4	12 - Alto	Eliminação automática.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

ID	RISCO	P	I	NÍVEL INERENTE	PRINCIPAIS MEDIDAS
R09	Transferência internacional não identificada	2	5	10 - Alto	Declaração contratual e análise prévia.
R10	Falta de transparência	3	4	12 - Alto	Placas, aviso e canal do encarregado.
R11	Decisão exclusivamente automatizada	3	4	12 - Alto	Intervenção humana.
R12	Compartilhamento indevido	2	5	10 - Alto	Vedação contratual e auditoria.
R13	Ataque cibernético	3	5	15 - Crítico	Segurança em camadas.
R14	Erro de vinculação biométrica	2	5	10 - Alto	Validação e revisão humana.
R15	Indisponibilidade do sistema	3	3	9 - Alto	Plano de contingência.
R16	Utilização para vigilância	2	5	10 - Alto	Limitações técnicas e contratuais.

5.3 Tratamento dos riscos

ID	MEDIDA	EFEITO	RESPOSTA
R01	Cláusulas de segurança, notificação de incidentes em até 24 h, testes prévios e periódicos, monitoramento de acessos e tráfego.	Reduz vulnerabilidades e acelera detecção e contenção.	Mitigar
R02	MFA, menor privilégio, segregação, logs, auditoria e Termo de Responsabilidade (Anexo II-14).	Reduz acessos indevidos e aumenta rastreabilidade.	Mitigar
R03	Vedação de finalidade própria, comercialização, compartilhamento e treinamento de IA; bloqueios técnicos.	Limita reutilização incompatível.	Evitar/Mitigar
R04, R05, R14	Testes de acurácia, falso positivo e falso negativo, condições de captura e intervenção humana (Anexos II-05 e II-07).	Reduz erros e permite correção.	Mitigar

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

ID	MEDIDA	EFEITO	RESPOSTA
R06	Avaliação de viés por grupos e condições (Anexo II-06) e suspensão se o risco for incompatível.	Reduz discriminação e falhas sistemáticas.	Mitigar
R07	Bloqueio técnico do cadastro de menores visitantes.	Impede cadastramento indevido.	Evitar
R08	Prazos definidos, eliminação automática, auditoria e evidências (Anexo II-09).	Reduz retenção excessiva.	Mitigar
R09	Declaração de infraestrutura, países, suporte e suboperadores; análise prévia (Anexo II-13).	Evita transferência não identificada.	Evitar/Mitigar
R10	Sinalização, aviso, QR Code e canais.	Aumenta a transparência.	Mitigar
R11	Revisão humana e procedimento alternativo.	Evita negativa definitiva exclusivamente algorítmica.	Mitigar
R12	Vedação contratual, autorização e auditoria.	Reduz compartilhamentos não autorizados.	Evitar/Mitigar
R13	Criptografia, gestão de vulnerabilidades, backup isolado e plano de resposta (Anexo II-10).	Reduz probabilidade e impacto de ataques.	Mitigar
R15	Plano de contingência e acesso alternativo.	Mantém a continuidade.	Mitigar
R16	Limitações técnicas e contratuais e vedação de vigilância.	Evita expansão para monitoramento não previsto.	Evitar

5.4 Riscos residuais acima do nível de aceitação

Risco residual é o risco que permanece depois de aplicadas as medidas de tratamento. Na fase de planejamento, ele ainda não pode ser medido, pois depende do fornecedor escolhido, da hospedagem, dos suboperadores, dos testes e da efetiva implementação dos controles.

Por isso, a tabela abaixo permanece em branco nesta versão. Os níveis residuais serão apurados no Relatório de Validação para Entrada em Produção (Anexo II-15) e registrados aqui, com atualização deste RIPD, antes do início da operação. Nenhum risco com nível residual Crítico poderá ser aceito.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

ID	NÍVEL RESIDUAL	JUSTIFICATIVA DA EXCEÇÃO	APROVADOR

5.5 Segurança da informação

Medidas mínimas, detalhadas no Anexo II-04:

- criptografia em trânsito e em repouso;
- controle de acesso baseado em função e princípio do menor privilégio;
- autenticação multifator para administradores e acesso remoto;
- segregação de ambientes e segregação lógica da base biométrica;
- logs administrativos protegidos e monitoramento;
- backups protegidos, com cópia isolada;
- gestão de vulnerabilidades, atualizações e testes periódicos, inclusive teste de intrusão antes da produção;
- plano de resposta a incidentes;
- eliminação segura;
- controles contra extração ou cópia indevida e detecção de atividades anômalas, quando disponível.

5.6 Reconhecimento facial e riscos algorítmicos

A avaliação não deverá usar apenas taxa genérica de "acerto". Devem ser consideradas acurácia, falso positivo, falso negativo, iluminação, posição da face, distância da câmera, qualidade da imagem, oclusões, condições de captura, diversidade da base de testes e limitações conhecidas, conforme os Anexos II-05 e II-06.

Como referência para a definição dos critérios de aceitação, propõem-se as seguintes metas técnicas:

MÉTRICA	META PROPOSTA	PROTOCOLO
Taxa de falso positivo (FMR/FPIR)	≤ 0,1%	Anexo II-05
Taxa de falso negativo (FNMR/FNIR)	≤ 2%	Anexo II-05
Diferença de desempenho entre grupos demográficos	Razão máxima de 1,5 vez entre o grupo com mais erros e o grupo com menos erros	Anexo II-06

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

> *As metas acima são propostas técnicas, e não exigências legais. Deverão ser deliberadas pela unidade responsável e pela STI e fixadas no edital antes da licitação, não podendo ser flexibilizadas depois de conhecidos os resultados dos testes.*

O fornecedor deverá apresentar documentação do algoritmo, metodologia de treinamento e validação quando pertinente, métricas, condições de teste, limitações, resultados em diferentes condições, evidências de avaliação de viés e mecanismo de atualização. Alteração significativa do algoritmo deverá ser comunicada com antecedência mínima de 30 dias e poderá exigir nova avaliação técnica, novos testes e atualização deste RIPD.

5.7 Decisão automatizada e intervenção humana

A autenticação poderá produzir decisão automatizada inicial, que não será definitiva em caso de falha, dúvida, contestação, baixa qualidade, erro de vinculação ou inconsistência cadastral. Nesses casos, conforme o Anexo II-07:

- a catraca indicará a ocorrência de forma discreta;
- o titular será encaminhado à recepção;
- agente humano realizará a conferência e decidirá conforme as regras institucionais;
- o evento será registrado somente na medida necessária;
- será evitado qualquer constrangimento público.

5.8 Incidentes de segurança

O tratamento de incidentes seguirá o Plano de Resposta a Incidentes (Anexo II-10), com as seguintes regras principais:

COMUNICAÇÃO	PRAZO	FUNDAMENTO
Do operador à Câmara e ao encarregado	Imediatamente, no máximo em 24 horas da ciência	Obrigação contratual proposta
À ANPD, quando houver risco ou dano relevante aos titulares	3 dias úteis a partir da ciência de que dados pessoais foram afetados; complementação em até 20 dias úteis	LGPD, art. 48; Resolução CD/ANPD nº 15/2024
Aos titulares afetados	3 dias úteis a partir da ciência	Resolução CD/ANPD nº 15/2024

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

COMUNICAÇÃO	PRAZO	FUNDAMENTO
CERT.br / CTIR Gov	Assim que possível	Notificação voluntária: a obrigatoriedade dos canais federais (CTIR Gov, CISC gov.br) alcança a administração pública federal, não a Câmara Municipal
Autoridade policial	Quando houver indício de crime	Legislação penal

Incidentes que envolvam dados biométricos serão presumidos como de risco relevante, salvo demonstração técnica em contrário. As etapas incluem identificação, contenção, preservação de evidências, avaliação de impacto, comunicações, recuperação, correção de vulnerabilidades, registro e atualização da análise de riscos. A comunicação de incidente à ANPD é gatilho obrigatório de revisão deste RIPD.

5.9 Privacidade desde a concepção e por padrão

- menor quantidade de dados, menor prazo de retenção e menor número de pessoas com acesso;
- armazenamento protegido e coleta mínima;
- desativação de funções desnecessárias;
- ausência de classificação comportamental e de vigilância não prevista.

O fornecedor não poderá habilitar funcionalidades adicionais sem autorização formal da Câmara e nova avaliação de proteção de dados.

5.10 Requisitos obrigatórios para o Termo de Referência

Os requisitos estão consolidados, com forma de comprovação, no Checklist do Anexo II-03, e incluem: limitação às finalidades; proibição de uso secundário, comercialização, compartilhamento não autorizado e treinamento de IA; tratamento conforme instruções da Câmara; criptografia, MFA, segregação, logs, auditoria, backup e resposta a incidentes; template protegido e não armazenamento da imagem original quando desnecessária; irreversibilidade do template quando tecnicamente viável; documentação e métricas do algoritmo com critérios de aceitação fixados no edital; intervenção humana; bloqueio de biometria de menores visitantes; informações para o aviso e para o atendimento de direitos; declaração de hospedagem, suboperadores e transferência internacional; direito de auditoria; e eliminação ao término do contrato.

5.11 Obrigações contratuais do operador

Além das obrigações da subseção 2.3.2, o contrato deverá prever: confidencialidade; acesso por função; logs administrativos; criptografia; segregação lógica; comunicação de incidentes em até 24

horas; auditoria; cooperação com a Câmara e o encarregado; identificação de suboperadores; comunicação prévia (mínimo de 30 dias) de alteração de hospedagem, suboperador ou algoritmo; fornecimento de evidências técnicas; auxílio no atendimento dos direitos; eliminação e certificado ao término; e sanções específicas por descumprimento, com base na Lei nº 14.133/2021, sem prejuízo da responsabilidade prevista nos arts. 42 a 45 da LGPD.

Os agentes públicos que descumprirem as regras deste RIPD e de seus anexos estarão sujeitos ao regime disciplinar previsto no Regime Jurídico Único dos Servidores Públicos do Município de Vitória da Conquista, Lei 1786/2011 e suas alterações posteriores.

5.12 Monitoramento e indicadores

Serão monitorados, periodicamente, pelo responsável pelo STI e encarregado: número de titulares cadastrados; número de autenticações; falhas; taxas de falso positivo e falso negativo; intervenções humanas; reclamações; solicitações de titulares; incidentes; tentativas de acesso administrativo; eliminações e cumprimento dos prazos de retenção; cadastros de menores bloqueados; auditorias; alterações no algoritmo e na infraestrutura; indisponibilidade; erros de vinculação; resultados de avaliações de viés; e compartilhamentos.

5.13 Governança e documentação

A Câmara manterá, no processo administrativo do projeto: RIPD, ROPA, ETP, Termo de Referência, edital, contrato, parecer jurídico, manifestação do encarregado, documentação técnica e de segurança, evidências de testes, resultados de acurácia, falso positivo, falso negativo e viés, auditorias, incidentes, solicitações, eliminações e revisões periódicas.

Os documentos complementares do Anexo II seguem o formato do Guia para Elaboração de Políticas, Normas e Procedimentos do PPSI 2.0, conforme sua natureza: a Política de Retenção e Eliminação (II-09) é redigida em artigos, como norma; o Procedimento de Intervenção Humana (II-07) e o Procedimento Alternativo de Acesso (II-08) seguem o modelo de procedimento operacional padrão, com passos numerados, tabela de responsáveis e exceções.

Seção 6 - Histórico de atualizações

Este RIPD é um documento vivo e deverá ser revisado diante de fatos novos, alterações relevantes, novos riscos ou novas orientações e regulamentações da ANPD.

DATA	VERSÃO	ATUALIZAÇÃO	RESPONSÁVEL
15/09/2026	1.0	Elaboração do RIPD de origem.	Lucas Fernandes de Melo

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

6.1 Quando o RIPD deve ser revisado

A revisão é obrigatória nos seguintes momentos:

- **Antes da contratação:** para incorporar as definições do ETP e da hipótese legal.
- **Após a escolha do fornecedor:** para registrar operador, hospedagem, suboperadores e características do algoritmo.
- **Antes da entrada em produção:** isto é, antes de o sistema começar a funcionar de fato com pessoas reais, após a fase de testes. Nessa revisão, os resultados do Relatório de Validação (Anexo II-15) - testes, riscos residuais e pendências - são incorporados ao RIPD, que é então submetido à aprovação do controlador.
- **Durante a operação:** sempre que houver alteração relevante de sistema, finalidade, hipótese legal, hospedagem, algoritmo ou fluxo; após incidente relevante ou comunicação de incidente à ANPD; diante de novos riscos; e, no mínimo, uma vez por ano.

Seção 7 - Aprovação

7.1 Aprovação pelo controlador

RESPONSÁVEL	NOME	CARGO / FUNÇÃO	ASSINATURA	DATA
Representante do controlador	Ivan Cordeiro da Silva Filho	Presidente da Câmara Municipal		

7.2 Registro de manifestações das partes interessadas

As partes abaixo assinam exclusivamente suas próprias manifestações, sem que isso implique aprovação, validação ou corresponsabilidade pelo conteúdo final do RIPD. Manifestações divergentes devem ser anexadas e expressamente endereçadas pelo controlador.

PARTE INTERESSADA	NOME	REFERÊNCIA DA MANIFESTAÇÃO	ASSINATURA	DATA
Encarregado	Lucas Fernandes de Melo	RIPD/ROPA		
Procuradoria Jurídica	Flavio Farias de Carvalho	Parecer Jurídico		

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

PARTE INTERESSADA	NOME	REFERÊNCIA DA MANIFESTAÇÃO	ASSINATURA	DATA
Responsável pela contratação	Ivan Cordeiro da Silva Filho	Termo de referência / edital / adjudicação e homologação / Contrato		

Conclusão

A implantação de sistema de controle de acesso por biometria facial nas catracas da Câmara Municipal de Vitória da Conquista pode ser considerada tecnicamente possível, desde que permaneça estritamente vinculada às finalidades de controle de acesso e segurança institucional e que sejam implementadas as salvaguardas previstas neste RIPD.

A utilização de reconhecimento facial envolve dados biométricos sensíveis e riscos de segurança, identificação incorreta, falso positivo e falso negativo, discriminação, viés, transparência, retenção, uso secundário e decisões automatizadas.

Permanecem pendentes, nesta fase, a definição da hipótese legal de cada tratamento, a validação dos prazos complementares de retenção e a fixação dos critérios de aceitação dos testes no edital.

A entrada em produção fica condicionada à demonstração documentada de necessidade, adequação, proporcionalidade, fundamento jurídico, segurança, acurácia, controle de erros, avaliação de viés, transparência, alternativa efetiva, intervenção humana, retenção limitada, eliminação segura, governança e capacidade de atendimento aos direitos.

O presente RIPD é favorável à continuidade do planejamento e da contratação, desde que as condições e salvaguardas sejam incorporadas aos instrumentos de contratação e efetivamente implementadas.

Aprovação

Declaro que analisei este relatório e aprovo as medidas de proteção e aceito os riscos que continuam, nos termos descritos.

_____

IVAN CORDEIRO DA SILVA FILHO

Presidente da Câmara Municipal de Vitória da Conquista

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

Anexo I - Condições para implantação

As condições abaixo são essenciais: o descumprimento de qualquer uma impede a entrada em produção até sua regularização. A verificação é feita no Relatório de Validação (Anexo II-15).

- ☐ aprovação deste RIPD pelo controlador;
- ☐ conclusão da análise jurídica;
- ☐ manifestação do encarregado;
- ☐ definição da hipótese legal de cada tratamento;
- ☐ demonstração documentada da necessidade e proporcionalidade;
- ☐ avaliação das alternativas menos invasivas;
- ☐ inclusão das exigências no Termo de Referência;
- ☐ fixação, no edital, dos critérios de aceitação de acurácia e viés;
- ☐ inclusão das exigências no contrato;
- ☐ validação dos prazos de retenção;
- ☐ definição do local de hospedagem;
- ☐ identificação do operador e dos suboperadores;
- ☐ contrato com cláusulas de proteção de dados;
- ☐ testes de segurança;
- ☐ testes de acurácia, falso positivo e falso negativo;
- ☐ avaliação de viés;
- ☐ validação das condições de captura;
- ☐ sinalização física;
- ☐ aviso de privacidade publicado após definição da hipótese legal;
- ☐ canal para titulares;
- ☐ procedimento alternativo de acesso;
- ☐ bloqueio de biometria de menores;
- ☐ treinamento da recepção;
- ☐ teste de intervenção humana;
- ☐ teste de eliminação automática;
- ☐ plano de resposta a incidentes;

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

- ☐ indicadores;
- ☐ validação da infraestrutura;
- ☐ avaliação de transferência internacional;
- ☐ documentação dos testes;
- ☐ registro dos riscos residuais (subseção 5.4);
- ☐ aprovação formal da entrada em produção.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

Anexo II - Documentos complementares

CÓDIGO	DOCUMENTO	NATUREZA / FORMATO
II-01	Fluxograma do tratamento de dados	Documento técnico
II-02	Matriz detalhada de riscos	Documento técnico
II-03	Checklist de requisitos do Termo de Referência	Instrumento de verificação
II-04	Especificações mínimas de segurança	Especificação técnica
II-05	Protocolo de testes de acurácia, falso positivo e falso negativo	Protocolo técnico
II-06	Protocolo de avaliação de viés algorítmico	Protocolo técnico
II-07	Procedimento de intervenção humana	Procedimento operacional padrão
II-08	Procedimento alternativo de acesso	Procedimento operacional padrão
II-09	Política de retenção e eliminação	Norma (em artigos)
II-10	Plano de resposta a incidentes	Plano
II-11	Aviso de privacidade	Documento público
II-12	Formulário de atendimento aos direitos	Formulário
II-13	Declaração do fornecedor sobre hospedagem, suboperadores e transferência internacional	Declaração (modelo)
II-14	Termo de responsabilidade e confidencialidade	Termo (modelo)
II-15	Relatório de validação para entrada em produção	Relatório

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

Anexo III - Glossário

Termos técnicos e jurídicos utilizados neste RIPD e em seus anexos, em ordem alfabética.

TERMO	SIGNIFICADO
Adequação	Princípio da LGPD segundo o qual o tratamento deve ser compatível com as finalidades informadas ao titular.
AES-256	Padrão de criptografia simétrica com chave de 256 bits, amplamente utilizado para proteger dados armazenados.
Agentes de tratamento	O controlador e o operador (LGPD, art. 5º, IX).
Algoritmo	Conjunto de instruções computacionais que, no reconhecimento facial, extrai características do rosto e calcula a semelhança entre imagens.
Anonimização	Uso de meios técnicos razoáveis pelos quais o dado perde a possibilidade de associação, direta ou indireta, a uma pessoa (LGPD, art. 5º, XI).
ANPD	Agência Nacional de Proteção de Dados, órgão responsável por zelar, implementar e fiscalizar o cumprimento da LGPD.
Ataque de apresentação	Tentativa de enganar o sistema biométrico apresentando à câmera uma foto, vídeo, máscara ou outro artefato no lugar do rosto verdadeiro.
Auditoria	Verificação independente e documentada de que controles, contratos e procedimentos estão sendo cumpridos.
Autenticação	Processo de confirmar que uma pessoa é quem afirma ser, comparando uma característica apresentada com o cadastro autorizado.
Autenticação multifator (MFA)	Exigência de dois ou mais fatores independentes para acessar um sistema, como senha e código enviado ao celular.
Autoridade competente	Agente com poder decisório para autorizar a entrada em produção, aceitar riscos residuais e determinar suspensões.
Backup (cópia de segurança)	Cópia dos dados mantida para recuperação em caso de perda, falha ou ataque.
Base legal (hipótese legal)	Fundamento previsto nos arts. 7º ou 11 da LGPD que autoriza o tratamento de dados pessoais.
Biometria facial	Uso de características mensuráveis do rosto para identificar ou autenticar uma pessoa.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

TERMO	SIGNIFICADO
Bloqueio	Suspensão temporária de qualquer operação de tratamento, com guarda do dado (LGPD, art. 5º, XIII).
Catraca	Equipamento de controle físico de passagem que libera ou impede a entrada e a saída de pessoas.
CERT.br	Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil, mantido pelo NIC.br, que recebe notificações de incidentes de qualquer organização.
Comparação biométrica	Etapa em que o sistema confronta o template gerado na catraca com os templates cadastrados e calcula um escore de semelhança.
Consentimento	Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento para finalidade determinada; para dados sensíveis, deve ser específica e destacada (LGPD, arts. 5º, XII, e 11, I).
Contenção	Fase da resposta a incidentes em que se isola o problema para impedir que ele se espalhe ou cause mais danos.
Controlador	Pessoa a quem competem as decisões sobre o tratamento de dados pessoais; neste caso, a Câmara Municipal (LGPD, art. 5º, VI).
Criptografia	Técnica que transforma dados em formato ilegível para quem não possui a chave, protegendo-os em trânsito e em repouso.
CTIR Gov	Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo, vinculado ao GSI/PR, de notificação obrigatória para a administração pública federal.
Dado pessoal	Informação relacionada a pessoa natural identificada ou identificável (LGPD, art. 5º, I).
Dado pessoal sensível	Dado sobre origem racial ou étnica, convicção religiosa, opinião política, saúde, vida sexual, dado genético ou biométrico, entre outros (LGPD, art. 5º, II).
Decisão automatizada	Decisão tomada por sistema computacional sem participação humana; o titular pode pedir sua revisão (LGPD, art. 20).
Edital	Instrumento que torna pública a licitação e fixa suas regras, inclusive critérios de aceitação da solução.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

TERMO	SIGNIFICADO
Eliminação	Exclusão definitiva de dado ou conjunto de dados, abrangendo todas as cópias (LGPD, art. 5º, XIV).
Encarregado	Pessoa indicada pelo controlador para atuar como canal de comunicação com os titulares e a ANPD (LGPD, art. 5º, VIII).
Entrada em produção	Momento em que o sistema deixa a fase de testes e passa a funcionar de fato, com pessoas reais e dados reais.
Escore	Número calculado pelo algoritmo que expressa o grau de semelhança entre dois rostos.
ETP - Estudo Técnico Preliminar	Documento da fase de planejamento da contratação que demonstra a necessidade, as alternativas e a solução mais adequada (Lei nº 14.133/2021, art. 18).
Exfiltração	Retirada não autorizada de dados de um sistema por um atacante ou agente interno.
Falso negativo	Erro em que o sistema não reconhece uma pessoa que está cadastrada e autorizada.
Falso positivo	Erro em que o sistema reconhece uma pessoa como se fosse outra pessoa cadastrada, ou reconhece como autorizado quem não está.
Firmware	Software interno que controla o funcionamento de um equipamento, como os terminais das catracas.
FMR / FPIR	Taxas técnicas de falso positivo: FMR (False Match Rate) na verificação 1:1; FPIR (False Positive Identification Rate) na identificação 1:N.
FNMR / FNIR	Taxas técnicas de falso negativo: FNMR (False Non-Match Rate) na verificação 1:1; FNIR (False Negative Identification Rate) na identificação 1:N.
Homologação	Fase de testes da solução instalada, em condições reais, antes da entrada em produção.
Identificação 1:N	Modo em que o rosto é comparado com todos os cadastros da base para descobrir quem é a pessoa.
Incidente de segurança	Evento adverso confirmado que comprometa a confidencialidade, integridade, disponibilidade ou autenticidade de dados pessoais.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

TERMO	SIGNIFICADO
Intervenção humana	Atuação de um agente da Câmara para conferir, revisar e decidir situações em que a decisão automatizada falhou ou foi contestada.
Larga escala	Tratamento que abrange número significativo de titulares, volume relevante de dados, longa duração ou ampla extensão geográfica.
LGPD	Lei Geral de Proteção de Dados Pessoais - Lei nº 13.709, de 14 de agosto de 2018.
Limiar (threshold)	Valor mínimo de escore a partir do qual o sistema considera que dois rostos pertencem à mesma pessoa; limiares mais altos reduzem falsos positivos e aumentam falsos negativos.
Limite de tolerância ao risco	Nível máximo de risco que a Câmara admite manter sem adotar medidas adicionais, definido pela autoridade competente em alinhamento com a gestão de riscos institucional. Substitui, neste RIPD, a expressão "apetite institucional".
Log (registro)	Anotação automática de um evento no sistema, como uma passagem pela catraca ou uma ação de um administrador.
Menor privilégio	Princípio segundo o qual cada usuário recebe apenas as permissões estritamente necessárias à sua função.
Minimização / necessidade	Princípio da LGPD que limita o tratamento ao mínimo necessário para a finalidade.
NIST FRTE	Programa de avaliação independente de algoritmos de reconhecimento facial do National Institute of Standards and Technology (EUA), antigo FRVT.
Nível de risco	Resultado da multiplicação entre o impacto e a probabilidade de um risco.
Oclusão	Obstrução parcial do rosto por óculos, máscara, boné, cabelo ou adereços, que pode prejudicar o reconhecimento.
Operador	Pessoa que realiza o tratamento em nome do controlador; neste caso, a empresa contratada (LGPD, art. 5º, VII).
Pentest (teste de intrusão)	Simulação controlada de ataque para encontrar vulnerabilidades antes que sejam exploradas.
Portabilidade	Direito de transferir dados a outro fornecedor, mediante requisição, conforme regulamentação da ANPD (LGPD, art. 18, V).

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

TERMO	SIGNIFICADO
Privacidade desde a concepção e por padrão (privacy by design / by default)	Incorporação da proteção de dados desde o planejamento do sistema e configuração inicial na opção mais protetiva ao titular.
Prova de conceito (POC)	Demonstração prática da solução, antes da contratação, para verificar se atende aos requisitos.
Prova de vida (liveness)	Recurso que verifica se há uma pessoa real diante da câmera, detectando ataques de apresentação.
Pseudonimização	Tratamento pelo qual o dado perde a associação direta a uma pessoa, salvo pelo uso de informação adicional mantida separadamente (LGPD, art. 13, § 4º).
QR Code	Código gráfico bidimensional lido por câmera de celular ou leitor, usado para acessar o aviso ou como credencial temporária.
Ransomware	Programa malicioso que sequestra dados, geralmente por criptografia, exigindo pagamento para liberá-los.
Rastreabilidade	Capacidade de reconstruir quem fez o quê, quando e onde, a partir dos registros.
RBAC - controle de acesso baseado em função	Modelo em que as permissões são atribuídas a perfis (recepção, supervisor, administrador) e não a pessoas individualmente.
Recuperação	Fase da resposta a incidentes em que sistemas e dados são restaurados com segurança.
Retenção	Período durante o qual os dados são mantidos antes da eliminação.
RIPD	Relatório de Impacto à Proteção de Dados Pessoais: documentação do controlador que descreve os tratamentos que podem gerar riscos aos titulares e as medidas de mitigação (LGPD, art. 5º, XVII).
Risco inerente	Nível de risco antes da aplicação das medidas de tratamento.
Risco residual	Nível de risco que permanece após a aplicação das medidas de tratamento.
ROPA	Registro das Operações de Tratamento de Dados Pessoais (inventário), exigido pelo art. 37 da LGPD.

(77) 3086-9600
RUA CORONEL GUGÉ - 150,
BAIRRO CENTRO, CEP 45000-510
VITÓRIA DA CONQUISTA - BA

TERMO	SIGNIFICADO
Segregação de ambientes	Separação entre ambientes de produção, homologação e desenvolvimento, para evitar que testes afetem dados reais.
Segregação lógica	Separação, por meios de software e rede, entre a base biométrica e outros sistemas ou clientes.
SLA (acordo de nível de serviço)	Compromisso contratual de prazos de atendimento e disponibilidade.
Suboperador	Empresa contratada pelo operador que também trata os dados, como provedor de nuvem ou suporte técnico.
Template biométrico	Representação numérica das características do rosto, gerada pelo algoritmo e usada nas comparações; não é a foto.
Termo de Referência	Documento que descreve o objeto a ser contratado, requisitos, obrigações e critérios de aceitação (Lei nº 14.133/2021, art. 6º, XXIII).
Titular	Pessoa natural a quem se referem os dados pessoais (LGPD, art. 5º, V).
TLS	Protocolo criptográfico que protege a comunicação entre sistemas pela rede (dados em trânsito).
Transferência internacional	Envio ou acesso de dados pessoais a partir de país estrangeiro ou organismo internacional (LGPD, arts. 33 a 36; Resolução CD/ANPD nº 19/2024).
Tratamento	Toda operação realizada com dados pessoais, como coleta, armazenamento, uso, compartilhamento e eliminação (LGPD, art. 5º, X).
Uso secundário	Utilização de dados para finalidade diferente daquela para a qual foram coletados.
Verificação 1:1	Modo em que o rosto é comparado apenas com o cadastro da pessoa que se apresenta (por exemplo, após aproximar um cartão).
Viés algorítmico	Diferença sistemática de desempenho do algoritmo entre grupos de pessoas (por cor de pele, sexo, idade), que pode gerar discriminação.
VLAN	Rede lógica separada dentro da rede física, usada para isolar os equipamentos do sistema.
Vulnerabilidade	Fragilidade em sistema, equipamento ou processo que pode ser explorada por uma ameaça.