

GOVERNO DO ESTADO DE GOIÁS
SECRETARIA DE ESTADO DE CIÊNCIA, TECNOLOGIA E INOVAÇÃO

RELATÓRIO DE IMPACTO
À PROTEÇÃO DE DADOS PESSOAIS (RIPD)
Versão Pública

IA CONTRA O CRIME
Sistema Estadual de Videomonitoramento com Inteligência
Artificial

Contrato nº 17/2026/SGG
Versão 1.0

Goiânia, 17 de julho de 2026

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)
Sistema Estadual de Videomonitoramento com Inteligência Artificial
Governo do Estado de Goiás

SUMÁRIO

1- FINALIDADE.....	4
2 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO.....	5
2.1 – Da estrutura tripartite e da responsabilização	5
3 – DESCRIÇÃO DO TRATAMENTO	6
3.1 – Sistemas de Informação Relacionados ao Projeto	6
3.2 – Arquitetura do Tratamento de Dados	6
3.3 – Coleta e Fonte dos Dados	6
3.4 – Processamento.....	6
3.5 – Compartilhamento	7
3.6 – Arquivamento e Destinação	7
3.7 – Escopo	7
3.8 – Contexto	8
3.9 – Finalidade e Vedações.....	8
3.9.1 – Vedações e Desvio de Finalidade	8
4 – ANÁLISE DAS HIPÓTESES LEGAIS E DOS PRINCÍPIOS DA LGPD	9
5 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS.....	10
6 – MEDIDAS PARA TRATAR OS RISCOS (Preventivo).....	12
6.1 – Procedimentos em Caso de Incidente	13
6.2 – Monitoramento de Riscos	13
7- CONCLUSÃO E APROVAÇÕES.....	14
GLOSSÁRIO	15

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)
Sistema Estadual de Videomonitoramento com Inteligência Artificial
Governo do Estado de Goiás

IA CONTRA O CRIME

Sistema Estadual de Videomonitoramento com Inteligência Artificial

Contrato nº 17/2026/SGG

Versão 1.0

Goiânia, 17 de julho de 2026

Histórico de Revisões

Data	Versão	Descrição	Autor
17/07/2026	1.0	Elaboração da primeira versão do relatório.	Equipe Técnica

1- FINALIDADE

O Relatório de Impacto à Proteção de Dados Pessoais (RIPD) tem por finalidade descrever os processos de tratamento de dados pessoais e/ou dados pessoais sensíveis que possam gerar alto risco às liberdades civis e aos direitos fundamentais dos titulares, identificar, analisar e avaliar tais riscos e definir as medidas, salvaguardas e mecanismos de mitigação adotados no âmbito do Sistema Estadual de Videomonitoramento com Inteligência Artificial (Contrato nº 17/2026/SGG).

O projeto ao qual este RIPD se refere integra soluções de inteligência artificial para reconhecimento facial, utilizando câmeras com reconhecimento facial ao vivo (LRF) e leitura automatizada de placas veiculares (LPR) às atividades de videomonitoramento e segurança pública (Projeto). O tratamento abrange dados pessoais e dados pessoais sensíveis — notadamente dados biométricos (imagens faciais), na forma do art. 5º, I e II, da LGPD — e dados de identificação e de natureza criminal.

Nesse contexto, a elaboração deste RIPD decorre dos arts. 5º, XVII, e 38 da LGPD e, conforme orientações da Agência Nacional de Proteção de Dados (ANPD), da necessidade de demonstração documentada de conformidade no tratamento de alto risco envolvendo dados pessoais e dados pessoais sensíveis, em larga escala e com uso de tecnologia emergente no setor público. Este documento atende, ainda, ao princípio da responsabilização e prestação de contas (art. 6º, X da LGPD) e, por tratar-se de agente do Poder Público, ao disposto no art. 32 da LGPD.

2 – IDENTIFICAÇÃO DOS AGENTES DE TRATAMENTO E DO ENCARREGADO

A arquitetura de governança estrutura-se em três agentes, com papéis distintos sob a LGPD:

Papel (LGPD)	Agente / Denominação contratual
Controlador (art. 5º, VI)	Estado de Goiás — doravante CONTRATANTE. Detentora ou representante originária das bases de dados e responsável pelas decisões referentes ao tratamento.
Operador (art. 5º, VII)	GOTech — Goiás Tecnologia — doravante CONTRATADA. Responsável pela custódia e pelo armazenamento dos dados pessoais, pela administração da infraestrutura de servidores e pela gestão e fiscalização do contrato firmado com o PARCEIRO, segundo as instruções da CONTRATANTE.
Suboperador / Parceiro Estratégico	Pax – doravante PARCEIRO. Proprietária da solução tecnológica de processamento, parceira da CONTRATADA nos termos do art. 28, § 3º, II, da Lei nº 13.303/2016, com atuação restrita ao processamento sob demanda nas camadas de aplicação, algoritmos, integrações e geração de alertas, segundo as instruções da CONTRATANTE transmitidas pela CONTRATADA, sem custódia autônoma dos dados pessoais e sem poder decisório sobre as finalidades do tratamento ou as ações policiais.

2.1 – Da estrutura tripartite e da responsabilização

A CONTRATANTE, como Controladora, detém o poder decisório sobre as finalidades e os elementos essenciais do tratamento, incluindo quanto às bases de dados utilizadas, hipóteses de consulta e eventuais comunicações institucionais e com os titulares de dados, eventual comunicação à ANPD e a outras autoridades, atendimento ao exercício de direitos de titulares, exclusão de registros de interesse, regras de acionamento operacional e critérios institucionais de inclusão.

A CONTRATADA atua como Operadora, nos termos do art. 39 da LGPD, em nome da CONTRATANTE e segundo suas instruções documentadas, competindo-lhe a custódia e o armazenamento dos dados pessoais, a administração da infraestrutura tecnológica destinada à sua guarda e a gestão e fiscalização da atuação do PARCEIRO, vedada a determinação de finalidade própria.

O PARCEIRO atua como Suboperador, mediante parceria estratégica com a CONTRATADA nos moldes do art. 28, § 3º, II, da Lei nº 13.303/2016, sendo responsável pela operação da plataforma, pelo processamento algorítmico, pelas integrações, pela geração dos alertas e pelos controles técnicos inseridos na camada de aplicação.

3 – DESCRIÇÃO DO TRATAMENTO

A LGPD (art. 5º, X) considera tratamento toda operação realizada com dados pessoais (coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle, modificação, comunicação, transferência, difusão ou extração). No presente caso, o Projeto tem como finalidade a promoção e o aprimoramento da segurança pública a partir de atividades de videomonitoramento, que incluem, como mencionado, a utilização de soluções de inteligência artificial para reconhecimento facial e LPR.

A descrição a seguir contempla a natureza, o escopo, o contexto e a finalidade do tratamento.

3.1 – Sistemas de Informação Relacionados ao Projeto

Integram o Projeto os seguintes sistemas de informação:

- Plataforma de reconhecimento facial e analítico de vídeo (LFR) de propriedade do PARCEIRO (solução tecnológica).
- Sistema de leitura automatizada de placas (LPR), com geração e cruzamento de alertas de furto/roubo de veículos.
- Bases legadas administradas pela CONTRATANTE, integradas via API (*Application Programming Interface*) ou barramento de serviços para consultas sob demanda
- Infraestrutura de nuvem e *colocation* operada pela CONTRATADA.

3.2 – Arquitetura do Tratamento de Dados

Conforme o art. 31 da LAI, o tratamento de informações pessoais deve ser feito de forma transparente e com respeito à intimidade, vida privada, honra e imagem das pessoas. O Projeto trata dados pessoais e sensíveis (art. 5º, I e II, da LGPD) estruturados em dois pilares: (i) Fontes de Dados operadas pela CONTRATADA e pelo PARCEIRO; e (ii) Bases de Dados da CONTRATANTE, integradas via API para consultas sob demanda.

3.3 – Coleta e Fonte dos Dados

A coleta (consumo ou recepção das informações nas bases de destino) abrange dados aptos a identificar o indivíduo. Fontes de coleta: (i) câmeras de videomonitoramento em vias e espaços públicos (captura de imagem facial e de placas); e (ii) bases legadas da CONTRATANTE, integradas via API/barramento e consultadas sob demanda. São tratados: Dados de identificação pessoal; Dados biométricos; Dados de natureza criminal/operacional; Dados de ativos e geolocalização (API LPR).

3.4 – Processamento

O processamento ocorre por integração tecnológica via API, com emprego de inteligência artificial, sob amarras jurídicas severas. O tratamento de dados deve limitar-se ao mínimo necessário, com retorno apenas dos dados essenciais à validação humana. É vedada a criação, alteração, complementação ou correção de dados, bem como o uso para fins alheios

ao projeto. A IA não terá caráter decisório, cabendo ao agente público a validação dos alertas. Métricas e relatórios devem ser minimizados e, sempre que possível, agregados ou pseudonimizados.

O fluxo do tratamento segue a seguinte lógica: captura pela rede de videomonitoramento, processamento algorítmico para identificação de potencial *match*, consulta às bases indicadas pela CONTRATANTE e, caso haja o *match*, retorno com a conclusão.

Os alertas automatizados da tecnologia são insumos técnicos para avaliação humana por agentes públicos, e não decisões automatizadas finais sobre titulares.

3.5 – Compartilhamento

Fundamenta-se no regime especial do art. 4º, III, 'a' e 'd', da LGPD (fins exclusivos de segurança pública e de investigação/repressão de infrações penais), por integração via API e observado o dado mínimo viável, tomando-se o art. 26, *caput* e § 1º, da LGPD como parâmetro material para o uso compartilhado entre entes públicos.

É expressamente vedado o compartilhamento, a cessão a terceiros, a título oneroso ou gratuito, o uso comercial, o uso para treinamento de modelos com finalidade alheia ao Projeto e quaisquer finalidades administrativas não relacionadas às atividades objeto do Contrato nº 17/2026/SGG, salvo instrução formal da CONTRATANTE ou permissivo legal, devidamente fundamentados, documentados e compatíveis com o regime jurídico aplicável.

3.6 – Arquivamento e Destinação

O ciclo de vida obedece à necessidade e à segurança (art. 6º, III e VII), com descarte irreversível ao final do uso:

- Trilhas de auditoria (*logs*): arquivados em ambiente seguro, íntegro e, preferencialmente, imutável por no mínimo 5 (cinco) anos.
- Sanitização das cópias temporárias: ao fim da vigência, exclusão lógica e física de cópias e *caches*, por padrões internacionais (NIST SP 800-88, nível Purge, ou *Cryptographic Erasure*), inviabilizando a recuperação forense.
- Expurgo do Ambiente *Colocation*: deleção irreversível dos “dados crus” ao atingir o 16º dia.
- Formalização: comprovação por Termo de Eliminação de Dados à CONTRATANTE, com inventário das bases, metodologia, *hashes* de verificação e assinatura do responsável técnico e do Encarregado.

3.7 – Escopo

O escopo representa a abrangência e os limites do tratamento. Os dados são sensíveis (biometria facial) e operacionais (situação criminal/ocorrências e alertas de veículos), tratados de forma contínua e sob demanda, conforme a necessidade das operações policiais e de inteligência.

3.8 – Contexto

No âmbito do Projeto, os dados são tratados conforme a expectativa legítima do titular quanto à segurança pública em espaços de acesso público, no contexto de modernização do videomonitoramento com IA. Pela natureza do monitoramento em espaços públicos, o contexto pode englobar incidentalmente grupos vulneráveis; submete-se ao dado mínimo viável e veda a formação de perfis comportamentais.

3.9 – Finalidade e Vedações

O fundamento é o regime especial do art. 4º, III, 'a' e 'd', da LGPD (fins exclusivos de segurança pública e de investigação/repressão de infrações penais).

Finalidades por categoria:

- Dados biométricos (imagens faciais): possibilitar a identificação automatizada de indivíduos de interesse para a ação policial, mediante comparação com bases de referência indicadas pela CONTRATANTE.
- Dados de identificação pessoal: permitir a confirmação da identidade do indivíduo após o alerta de *match*, evitando abordagens indevidas por homonímia ou erro de identificação, bem como subsidiar a ação policial com informações qualificadas.
- Dados de natureza criminal/operacional: identificar a existência de mandados de prisão, restrições, registros de interesse ou ocorrências vinculadas ao indivíduo ou veículo, fundamentando a geração de alertas e a tomada de decisão pelos agentes públicos.
- Dados de ativos e geolocalização (LPR): possibilitar o cruzamento de placas veiculares com bases de furtos/roubos e a geração de alertas qualificados, bem como o monitoramento de veículos de interesse à operação policial, mediante registro de placa, data/hora, localização e imagem.
- Trilhas de auditoria: garantir segurança, rastreabilidade e prestação de contas (retenção de 5 anos).

3.9.1 – Vedações e Desvio de Finalidade

- Uso comercial e privado: vedado o uso para finalidades não relacionadas, fins comerciais, compartilhamento com outros clientes ou treinamento com finalidade alheia ao projeto.
- Compartilhamento com terceiros: proibido transferir, ceder ou compartilhar os dados com terceiros, a título oneroso ou gratuito.
- Tratamento discriminatório: vedada a utilização do reconhecimento facial e das bases para fins discriminatórios, ilícitos ou abusivos.

4 – ANÁLISE DAS HIPÓTESES LEGAIS E DOS PRINCÍPIOS DA LGPD

O fundamento por categoria de dado consta do Quadro 1. Por destinar-se a fins exclusivos de segurança pública e de investigação/repressão penal, o tratamento sujeita-se ao regime especial do art. 4º, III, e § 1º, da LGPD — e não às hipóteses autorizativas dos arts. 7º e 11 —, observados o devido processo legal e os princípios do art. 6º:

Quadro 1 – Análise das hipóteses legais e dos princípios da LGPD

Princípio (art. 6º)	Observância no Projeto
Finalidade (I)	O tratamento é realizado para propósito legítimo, específico e explícito de segurança pública; vedado o desvio de finalidade.
Adequação (II)	A implementação do reconhecimento facial e LPR é compatível com a identificação de procurados e o cruzamento de alertas criminais.
Necessidade (III)	O tratamento adota a premissa de limitação ao dado mínimo viável e à finalidade perquirida, incluindo o retorno do <i>match</i> ; minimização de campos exibidos.
Livre acesso (IV)	Os direitos dos titulares são assegurados na forma da legislação específica e dos princípios gerais; canais do Encarregado são disponibilizados aos titulares.
Qualidade dos dados (V)	Há a implementação de regras de atualização, sincronismo, integridade, procedência e validação das bases de referência, bem como monitoramento de falsos positivos, falsos negativos e inconsistências que possam gerar abordagens indevidas.
Transparência (VI)	É adotada transparência proporcional: disponibilização de informações claras sobre agentes, finalidade, categorias de dados e salvaguardas, resguardados sigilo de segurança pública, investigação, segurança da informação e segredos técnicos.
Segurança (VII)	São adotadas salvaguardas tecnológicas que incluem TLS 1.2+, AES-256, MFA, VPN, segregação de funções e <i>datacenter</i> nacional.
Prevenção (VIII)	São adotadas medidas preventivas, incluindo a elaboração deste RIPD, com avaliação prévia de riscos.
Não discriminação (IX)	Há vedação expressa do uso do reconhecimento facial para fins discriminatórios, ilícitos ou abusivos.
Responsabilização e prestação de contas (X)	Há a implementação de medidas para garantir a responsabilização e prestação de contas dos agentes de tratamento envolvidos, incluindo <i>logs</i> imutáveis por 5 anos, auditorias periódicas e Termo de Eliminação de Dados.

5 – IDENTIFICAÇÃO E AVALIAÇÃO DE RISCOS

Em cumprimento ao art. 5º, XVII, da LGPD, foram identificados e avaliados os principais riscos, considerando-se a probabilidade de ocorrência, o impacto potencial e o nível resultante, bem como os efeitos combinados de múltiplos fatores. O Quadro 2 foi elaborado realizando uma avaliação dos riscos a proteção de dados pessoais do projeto.

Quadro 2 – Riscos Mapeados do projeto

Risco inerente ao tratamento de dados pessoais	
Acesso indevido	Devido a falhas na segregação de funções ou privilégios de acesso excessivos, pode ocorrer o acesso não autorizado por funcionários do PARCEIRO a bases de dados originárias da CONTRATANTE, resultando em quebra de sigilo e potencial vazamento de dados em larga escala.
Exposição de dados pessoais sensíveis	Devido a vulnerabilidades na integração entre ambientes ou uso de protocolos de comunicação inseguros, pode ocorrer o vazamento ou a interceptação de dados biométricos em trânsito, resultando em exposição de dados sensíveis e responsabilização do Estado.
Retenção indevida de dados	Devido a falhas operacionais ou ausência de monitoramento na rotina de expurgo, pode ocorrer a persistência indevida de "dados crus" no Ambiente <i>Colocation</i> além do prazo legal de 15 dias, resultando em aumento desnecessário da superfície de risco e descumprimento do princípio da necessidade
Retenção prolongada de dados pessoais sem necessidade	Devido à ausência de um procedimento formal, adequado e auditável de descarte, pode ocorrer a falha na sanitização ou destruição das bases temporárias ao término da vigência contratual, resultando em manutenção de passivo jurídico e risco contínuo de vazamento para o Estado.
Reidentificação de dados pseudonimizados	Devido a técnicas de cruzamento de dados ou inferência a partir de metadados analíticos insuficientemente protegidos, pode ocorrer a reidentificação de titulares que deveriam estar anonimizados, resultando em quebra de privacidade e uso indevido da informação.
Compartilhar ou distribuir dados pessoais com terceiros sem o consentimento do titular dos dados pessoais	Devido a fragilidades nas barreiras de isolamento lógico do ambiente do parceiro, pode ocorrer a apropriação ou uso de dados do projeto para fins comerciais ou treinamento de modelos de IA de terceiros, resultando em desvio de finalidade e grave quebra de conformidade com a LGPD.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)
Sistema Estadual de Videomonitoramento com Inteligência Artificial
Governo do Estado de Goiás

Falhas de segurança de acesso	Devido a compartilhamento de senhas ou falhas no controle de acesso à rede, pode ocorrer o acesso ao sistema por meio de VPN por usuário não homologado, potencial acesso indevido por pessoas não autorizadas.
Falhas de auditoria de sistema	Devido a falhas na configuração de auditoria do sistema, interrupção dos serviços de monitoramento ou geração de logs incompletos (sem campos essenciais como identificação funcional ou justificativa), pode ocorrer a incapacidade de rastrear ações de usuários ou de produzir prova eletrônica íntegra, resultando em impunidade em caso de abuso de poder, desvio de finalidade ou falha na prestação de contas do Estado.
Indisponibilidade de serviços	Devido a falhas de infraestrutura, software ou conectividade nas bases de dados da CONTRATANTE, pode ocorrer a indisponibilidade ou falha na integração do serviço, resultando em prejuízo à continuidade das operações de segurança pública.
Acesso não autorizado	Devido a falta de justificativa detalhada e motivada nas consultas, pode ocorrer o uso do sistema para rastreamento contínuo ou perfilamento da rotina de cidadãos sem restrição criminal, resultando em violação de direitos fundamentais e risco de ações por abuso de poder.
Informação insuficiente sobre a finalidade do tratamento	Devido à baixa qualidade de imagem ou limitações do algoritmo, pode ocorrer a geração sistêmica de um alerta de "match" incorreto (falso positivo), resultando em poluição da análise e sobrecarga para o operador humano.
Informação insuficiente sobre a finalidade do tratamento	Devido a falha na validação humana ou excesso de confiança na tecnologia, pode ocorrer a realização de uma abordagem policial indevida baseada em um falso positivo, resultando em constrangimento ilegal de cidadãos inocentes e danos à imagem da instituição.
Acesso não autorizado	Devido a APIs mal configuradas ou falhas nos controles de segregação de dados, pode ocorrer o compartilhamento ou a cessão de dados trafegados a terceiros não autorizados, resultando em quebra de sigilo e violação direta da LGPD.

6 – MEDIDAS PARA TRATAR OS RISCOS (Preventivo)

São obrigatórias as seguintes medidas de salvaguarda, com gerenciamento contínuo e auditável pelos gestores do contrato:

Quadro 3 – Medidas para tratar os riscos de forma preventiva

Controle / Medida(s) adotada(s)
Segregação de funções (SoD); acesso do PARCEIRO apenas a resultados de consultas; autenticação gerenciada pela CONTRATADA; VPN sob privilégio mínimo.
Criptografia em trânsito (TLS 1.2+) em toda a integração; criptografia em repouso (AES-256).
Expurgo automático e irreversível dos “dados crus” no 16º dia; monitoramento da rotina de deleção.
Padrões NIST SP 800-88 (Purge) ou <i>Cryptographic Erasure</i> ; entrega do Termo de Eliminação de Dados em até 10 dias após o fim do tratamento.
Minimização, agregação ou pseudonimização de dados analíticos, conforme aplicável; vedação de saída de dado pessoal identificável do Ambiente de Dados Pessoais.
Vedação contratual expressa de uso comercial, administrativo não relacionado e de treinamento de IA com finalidade alheia ao projeto; auditoria contínua.
MFA obrigatório; bloqueio de requisições fora da VPN homologada; revisão periódica de credenciais.
Trilhas de auditoria em camadas, <i>logs</i> imutáveis (IP, usuário, data/hora, justificativa) retidos por no mínimo 5 anos.
Protocolo de contingência: suporte técnico da CONTRATADA e consulta manual aos sistemas da CONTRATANTE, garantindo continuidade.
Processamento de latitude/longitude restrito ao cruzamento de alertas criminais (furto/roubo); vedado o monitoramento contínuo, a análise de rotina de deslocamento ou o perfilamento de cidadãos sem restrição, salvo instrução específica e documentada da CONTRATANTE dentro das finalidades legais aplicáveis.
Submissão rígida ao dado mínimo viável; vedação de perfis comportamentais; registro da justificativa da ação; e registro de falsos positivos, falsos negativos e alertas descartados para aperfeiçoamento da governança. A solução do PARCEIRO deve fornecer exclusivamente alertas acompanhados de grau de similaridade, sem caráter decisório ou vinculante; <i>Fine tuning</i> do limiar de similaridade; Monitoramento de acurácia.
Validação humana obrigatória, exclusivamente por agente público, do <i>match</i> antes de qualquer abordagem. A decisão de agir (ou não agir) baseada no alerta é de responsabilidade do agente e deve ser registrada em sistema, vinculando a ação ao seu número de identificação funcional e a um procedimento ou ordem de serviço, garantindo uma trilha de auditoria completa da decisão humana; Treinamento.
Vedação absoluta de cessão/compartilhamento a terceiros; termo de confidencialidade assinado por todos os agentes com acesso.

6.1 – Procedimentos em Caso de Incidente

Caso as medidas preventivas falhem e ocorra incidente de segurança no âmbito do tratamento de dados pessoais do Projeto (acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão dos dados pessoais), as seguintes medidas serão adotadas:

- Isolamento: suspender credenciais e isolar tecnicamente os sistemas afetados imediatamente.
- Comunicação interna: a CONTRATADA e/ou o PARCEIRO notifica o Encarregado da CONTRATANTE em prazo não superior a 24 horas da ciência.
- Comunicação à ANPD e aos titulares: a CONTRATANTE, como Controladora, avalia e, quando aplicável, realiza a comunicação à ANPD e aos titulares afetados, observados o art. 48 da LGPD, a regulamentação aplicável, o risco ou dano relevante aos titulares e eventuais restrições justificadas por segurança pública ou investigação.
- Relatório de incidente: entrega de Relatório Circunstanciado de Incidente, sem demora injustificada, pela parte que identificou o incidente.

6.2 – Monitoramento de Riscos

Considerando a natureza crítica dos dados tratados (biometria e segurança pública), o apetite a risco da Secretaria para este projeto é classificado como baixo. Por esta razão, absolutamente todos os riscos identificados estarão sujeitos a um regime de monitoramento rigoroso e contínuo, garantindo que as ações de controle permaneçam eficazes ao longo de todo o ciclo de vida do tratamento, observando as seguintes premissas operacionais:

- Acompanhamento de Riscos Altos e Extremos: Os riscos que, mesmo após a aplicação dos controles inerentes, mantiverem potencial de impacto severo (Níveis Alto e Extremo), deverão ser acompanhados constantemente. A CONTRATADA deverá fornecer à CONTRATANTE painéis de controle em tempo real (dashboards) e configurar alertas automatizados (avisos) para desvios de padrão, tentativas de intrusão ou falhas operacionais críticas.
- Alimentação do Sistema IRIS (CGE-GO): Em estrito cumprimento às normas de compliance do Estado, a consolidação do monitoramento será registrada no Sistema IRIS (Inteligência de Riscos e Integridade no Setor Público).
- Periodicidade e Responsabilidade: A atualização no Sistema IRIS ocorrerá com frequência quadrimestral. Esta tarefa será de responsabilidade do gestor de riscos do contrato ou servidor formalmente designado por ele.
- Base de Evidências: A alimentação quadrimestral do sistema não será baseada em percepções subjetivas, mas fundamentada em dados concretos: o gestor reportará os incidentes de segurança efetivamente verificados no período e as respectivas ações de correção realizadas, utilizando os KPIs (Indicadores-Chave de Desempenho) estabelecidos para o projeto.

7- CONCLUSÃO E APROVAÇÕES

O Projeto apresenta nível de risco elevado, em razão da natureza sensível dos dados (biometria facial) e da complexidade da integração entre entes públicos e privados. Não obstante, a arquitetura proposta – que mantém o armazenamento sob controle direto da CONTRATADA, em território nacional, e limita o PARCEIRO ao fornecimento da solução e ao processamento sob demanda, com segregação de funções – oferece salvaguardas adequadas à mitigação dos riscos identificados.

ENCARREGADO DE DADOS (DPO) — CONTRATANTE

Encarregado pelo Tratamento de Dados Pessoais - SECTI

AUTORIDADE DA CONTRATANTE

Secretário de Estado de Ciência, Tecnologia e Inovação

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)
Sistema Estadual de Videomonitoramento com Inteligência Artificial
Governo do Estado de Goiás

GLOSSÁRIO

Termo	Definição
AES-256	Padrão de criptografia avançada de 256 bits, utilizado para proteger dados em repouso.
ANPD	Agência Nacional de Proteção de Dados. Órgão responsável por fiscalizar e regular a aplicação da LGPD no Brasil.
API (<i>Application Programming Interface</i>)	Interface que permite a comunicação e a troca de dados entre diferentes sistemas de informação.
Controlador	Agente de tratamento (no âmbito deste relatório, o Estado de Goiás) a quem competem as decisões referentes ao tratamento de dados pessoais.
Dado Mínimo Viável	Princípio normativo que orienta a coleta, o acesso e o processamento limitados apenas aos dados estritamente necessários para atingir uma finalidade legal específica.
Dados Biométricos	Dados pessoais sensíveis referentes a características físicas ou comportamentais de uma pessoa natural, como imagens faciais.
DPO (<i>Data Protection Officer</i> / Encarregado)	Profissional responsável por atuar como canal de comunicação entre o controlador, os titulares dos dados e a ANPD.
Expurgo	Eliminação definitiva e irreversível de dados, caracterizada pela exclusão dos “dados crus” após o prazo de retenção estipulado.
Falso Positivo	Ocorrência em que o sistema de inteligência artificial identifica incorretamente uma correspondência (“match”), gerando um alerta sobre indivíduo não correspondente à base de referência.
KPI (<i>Key Performance Indicator</i> / Indicador-Chave de Desempenho)	Métrica quantificável utilizada para medir e monitorar a eficácia de processos operacionais e controles de riscos.
LAI	Lei de Acesso à Informação (Lei nº 12.527/2011).
LGPD	Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018). Diploma legal brasileiro que dispõe sobre o tratamento de dados pessoais.
LPR (<i>License Plate Recognition</i>)	Tecnologia de leitura automatizada de placas veiculares, utilizada para a identificação automática de veículos.
Match	Correspondência positiva encontrada por um sistema algorítmico, como a identificação de similaridade de um rosto ou de uma placa com registros presentes em uma base de dados.
MFA (<i>Multi-Factor Authentication</i> / Autenticação Multifator)	Controle de segurança da informação que exige mais de um método de verificação de identidade para conceder acesso a um sistema.
Operador	Agente de tratamento (no âmbito deste relatório, a GOTEch) que realiza o tratamento de dados pessoais em nome e segundo as instruções do controlador.

Relatório de Impacto à Proteção de Dados Pessoais (RIPD)
Sistema Estadual de Videomonitoramento com Inteligência Artificial
Governo do Estado de Goiás

RIPD (Relatório de Impacto à Proteção de Dados Pessoais)	Documentação que contém a descrição dos processos de tratamento de dados pessoais que podem gerar alto risco à garantia dos princípios gerais, bem como medidas, salvaguardas e mecanismos de mitigação.
Sanitização	Processo de exclusão segura de dados, tanto em âmbito lógico quanto físico, realizado de modo a impossibilitar a sua recuperação por técnicas forenses.
SGG	Secretaria-Geral de Governo.
SoD (<i>Segregation of Duties</i> / Segregação de Funções)	Controle de segurança estruturado para mitigar riscos de acessos indevidos e abusos, distribuindo tarefas e privilégios sistêmicos.
Suboperador (Parceiro Estratégico)	Agente (no âmbito deste relatório, a empresa detentora da solução tecnológica) contratado pelo operador para auxiliar na execução do processamento de dados, estritamente sob as diretrizes do controlador.
TLS (<i>Transport Layer Security</i>)	Protocolo de segurança de redes responsável por garantir a criptografia e a integridade de dados durante a sua transmissão (dados em trânsito).
Tratamento de Alto Risco	Operações de tratamento de dados que, por sua natureza, escala ou pelo uso de tecnologias emergentes (ex. inteligência artificial), apresentam potencial de afetar significativamente os interesses e direitos fundamentais dos titulares.
VPN (Virtual Private Network / Rede Privada Virtual)	Protocolo de conexão segura que provê o tráfego de dados de modo protegido e o acesso remoto a ambientes de rede restritos.