

ANEXO SEI Nº 27227235/2025 - SAP.ARC.AUN**ANEXO V - RELATÓRIO DE IMPACTO DE PROTEÇÃO
DE DADOS PESSOAIS****Relatório de Impacto de Proteção de Proteção de Dados Pessoais
Sistema de Videomonitoramento Inteligente com Reconhecimento Facial**

O presente anexo traz explicações a respeito da implementação e utilização do Joinville Sempre Alerta de forma detalhada com o intuito de tranquilizar, esclarecer e informar com relação a segurança, privacidade e utilização da tecnologia para monitoramento que deverá estar disponível na nova plataforma. Entendendo ser necessário demonstrar a utilização das soluções trazidas pelo Joinville Sempre Alerta e o compromisso com a população garantindo o compliance com a legislação vigente e interesse público afastando qualquer dúvida quanto à Implantação e Utilização das solicitações trazidas pelo Joinville Sempre Alerta como parte das políticas públicas de integração, cooperação, interoperabilidade dos serviços Municipais e de Governo Digital.

1. Objetivo do Relatório de Impacto de Proteção de Dados

Este Relatório de Impacto à Proteção de Dados Pessoais (RIPD) tem como objetivo avaliar os riscos decorrentes da implementação de sistema de videomonitoramento inteligente com reconhecimento facial pelo Município de Joinville, identificando medidas necessárias para garantir conformidade com a Lei Geral de Proteção de Dados (LGPD) e proteção dos direitos fundamentais dos cidadãos.

A elaboração deste RIPD justifica-se pela convergência de múltiplos fatores de alto risco previstos na LGPD e Resolução ANPD nº 02/2022, especialmente o tratamento de dados biométricos classificados como dados sensíveis, a utilização de nova tecnologia com inteligência artificial para decisões automatizadas, o tratamento em larga escala abrangendo aproximadamente 664.541 habitantes de Joinville, além da vigilância de zonas públicas com finalidade de segurança pública. Estes elementos caracterizam tratamento massivo de dados pessoais com potencial impacto significativo sobre direitos fundamentais, exigindo avaliação criteriosa dos riscos e medidas de proteção.

2. Identificação dos Agentes de Tratamento e do Encarregado

O Município de Joinville, através da Secretaria de Proteção Civil e Segurança Pública, atuará como Controlador Principal, sendo responsável pelas decisões sobre finalidades e meios de tratamento dos dados pessoais.

A empresa a ser contratada funcionará como Operadora, responsável pelo processamento dos dados pessoais em nome do Município conforme instruções documentadas e cláusulas contratuais específicas.

A função de Encarregado de Tratamento de Dados Pessoais é exercida por Sahmara Liz Botemberger como titular e Rodrigo Ponick como suplente, mantendo canal de comunicação através do e-mail sap.ung.apd@joinville.sc.gov.br e sistema de ouvidoria municipal para atendimento aos direitos dos titulares.

3. Descrição Detalhada do Tratamento**3.1 - Finalidade e Contexto institucional**

A Secretaria de Proteção Civil e Segurança Pública constitui órgão da administração direta municipal responsável por desenvolver políticas de proteção ao cidadão, articulando organismos governamentais para organizar a capacidade de defesa da população em segurança pública e defesa civil. O sistema de videomonitoramento visa apoiar estas atividades através de prevenção, investigação e repressão de ilícitos, utilizando câmeras posicionadas em áreas estratégicas e integradas a softwares de análise com inteligência artificial.

3.2. Fundamentação Legal

O tratamento fundamentar-se-á nos artigos 7º, inciso III, referente à execução de políticas públicas, e 23, sobre segurança pública, ambos da LGPD. Para dados biométricos, aplicar-se-á especificamente o artigo 11, inciso I, alínea 'a', quanto ao cumprimento de obrigação legal pelo controlador. O direito à revisão humana de decisões automatizadas observará rigorosamente o artigo 20 da LGPD, complementado pela jurisprudência do Supremo Tribunal Federal na Ação Direta de Inconstitucionalidade 6.387, que reforça a necessidade de proporcionalidade e justificativa adequada em políticas de monitoramento estatal.

3.3. Dados pessoais tratados

Os dados pessoais a serem tratados abrangerão imagens de videomonitoramento com respectiva data, hora e localização geográfica de captação, além de metadados técnicos necessários ao funcionamento do sistema. Como dados pessoais sensíveis, serão processados templates biométricos faciais e padrões de reconhecimento convertidos em representações matemáticas. Quando houver correspondência positiva, poderão ser associadas informações de identificação como nome, CPF e dados criminais, sempre acompanhadas de logs de sistema e registros de auditoria para fins de rastreabilidade.

3.4. Fluxo Operacional e Técnico

O fluxo operacional iniciar-se-á com a captação em tempo real pelas câmeras nas vias públicas, transmitindo as imagens para sistema central onde algoritmos de inteligência artificial processarão o reconhecimento facial. Alertas serão gerados exclusivamente quando houver correspondência com bases de dados autorizadas, respeitando limite (*threshold*) mínimo de confiabilidade de 90%. Todas as decisões automatizadas passarão obrigatoriamente por validação humana qualificada antes de gerar qualquer consequência jurídica ou operacional.

O armazenamento ocorrerá em servidores localizados exclusivamente no Brasil, com retenção padrão de 15 dias para imagens gerais, prazo a ser estendido apenas nos casos de ordem judicial ou vinculação comprovada a investigações oficiais em andamento. O compartilhamento restringir-se-á a órgãos de segurança pública formalmente autorizados, observando rigorosamente os limites estabelecidos pela Ação Direta de Inconstitucionalidade 6.649 e Arguição de Descumprimento de Preceito Fundamental 695, ambas do Supremo Tribunal Federal.

3.5. Volume e Abrangência

Considerando a população de 664.541 habitantes, o sistema processará aproximadamente 24 (vinte e quatro) horas diárias de captação, com estimativa de processamento de milhares de faces diariamente.

A abrangência poderá estender-se às esferas estadual e federal através de convênios específicos para intercâmbio de dados de segurança pública, sempre precedidos de análise jurídica e autorização expressa.

4. ANÁLISE DE NECESSIDADE E PROPORCIONALIDADE

4.1. Justificativa da Necessidade

O videomonitoramento inteligente apresenta-se como medida necessária ante o cenário atual de segurança pública municipal, permitindo resposta mais eficaz a ocorrências, localização ágil de pessoas desaparecidas e identificação eficiente de foragidos da justiça. A tecnologia otimiza recursos humanos limitados do município e possibilita monitoramento preventivo de áreas identificadas como de maior vulnerabilidade social e criminal.

4.2. Teste de Proporcionalidade

Aplicando-se o teste tríptico da proporcionalidade (adequação, necessidade e proporcionalidade), verifica-se que a medida é adequada ao fim de segurança pública, permitindo identificação mais eficiente de suspeitos e monitoramento preventivo de qualidade superior. Constitui meio menos gravoso disponível quando comparado a alternativas como patrulhamento ostensivo intensivo, significativamente mais custoso, ou videomonitoramento convencional sem inteligência artificial, comprovadamente menos eficaz para os objetivos pretendidos. A proporcionalidade em sentido estrito demonstra que os benefícios concretos de segurança pública justificam a restrição à privacidade, especialmente considerando as robustas salvaguardas implementadas através de revisão humana obrigatória, retenção temporal limitada e transparência ativa com a população.

5. PRINCÍPIOS DE QUALIDADE E MINIMIZAÇÃO

5.1. Minimização dos Dados

O tratamento observará rigorosamente o princípio da minimização, limitando-se ao estritamente necessário para consecução dos objetivos de segurança pública, evitando coleta excessiva ou desnecessária. As câmeras captarão exclusivamente espaços públicos, excluindo propositalmente áreas privadas ou de maior expectativa de privacidade dos cidadãos. Os dados biométricos serão convertidos em templates matemáticos abstratos, impedindo tecnicamente a reconstrução das imagens originais e proporcionando camada adicional de proteção à privacidade.

5.2. Exatidão e Atualização

Para garantir exatidão e atualização contínua, o sistema implementará controles rigorosos de qualidade para assegurar precisão dos algoritmos, incluindo testes periódicos de acurácia e detecção proativa de vieses discriminatórios. As bases de dados utilizadas para comparação serão mantidas constantemente atualizadas e submetidas a auditorias regulares para prevenir falsos positivos e garantir efetividade operacional sem prejuízo aos direitos dos cidadãos.

6. ANÁLISE DETALHADA DE RISCOS

6.1. Matriz de Riscos

A análise de riscos identifica como principais ameaças o vazamento de dados biométricos, classificado como risco médio devido à baixa probabilidade mas alto impacto potencial, mitigado através de criptografia robusta e rigorosos controles de acesso.

Os falsos positivos em reconhecimento facial constituem risco alto pela probabilidade média mas impacto elevado, exigindo limite (*threshold*) mínimo de 90% e validação humana obrigatória como medidas de contenção.

A discriminação algorítmica representa risco alto considerando tanto probabilidade média quanto impacto significativo, demandando testes regulares de viés e calibração periódica dos algoritmos.

O acesso não autorizado configura risco médio, com baixa probabilidade mas alto impacto, controlado através de autenticação multifator e manutenção de logs detalhados.

O uso indevido por operadores apresenta risco baixo devido à baixa probabilidade e impacto médio, mitigado através de treinamento específico e termos rigorosos de confidencialidade.

Os ataques cibernéticos constituem risco alto pela probabilidade média e impacto potencialmente devastador, exigindo monitoramento contínuo 24 (vinte e quatro) horas e sistemas robustos de backup seguro.

Para grupos vulneráveis, crianças e adolescentes enfrentam risco específico de identificação inadequada devido a mudanças faciais durante o desenvolvimento, demandando exclusão das bases de comparação, exceto em casos de desaparecimento com expressa autorização judicial.

Idosos podem enfrentar dificuldades de reconhecimento devido a alterações faciais naturais, requerendo ajustes específicos nos algoritmos e revisão manual reforçada.

Os cenários de falha incluem falha total do sistema, contingenciada através de videomonitoramento tradicional sem prejuízo das operações de segurança, e comprometimento das bases de dados, exigindo isolamento imediato dos sistemas, investigação forense especializada e comunicação tempestiva à ANPD conforme Resolução CD/ANPD nº 15/2024.

| RISCO | PROBABILIDADE | IMPACTO | NÍVEL | MITIGAÇÃO PRINCIPAL |
|------------------------------------|---------------|---------|-------|--|
| Vazamento de dados biométricos | Baixa | Alto | Médio | Criptografia, controles de acesso |
| Falsos positivos em reconhecimento | Média | Alto | Alto | Threshold 90%, validação humana |
| Discriminação algorítmica | Média | Alto | Alto | Testes de viés, calibração periódica |
| Acesso não autorizado | Baixa | Alto | Médio | Autenticação multifator, logs |
| Uso indevido por operadores | Baixa | Médio | Baixo | Treinamento, termos de confidencialidade |
| Ataques cibernéticos | Média | Alto | Alto | Monitoramento 24/7, backup seguro |

7. MEDIDAS DE PROTEÇÃO E MITIGAÇÃO

As medidas técnicas de segurança da informação abrangem criptografia para dados em repouso e transmissão, autenticação multifator obrigatória, controles de acesso estruturados por perfis funcionais, monitoramento ininterrupto 24 (vinte e quatro) horas por dia e backup criptografado com testes regulares de recuperação. A proteção algorítmica implementa limite (*threshold*) mínimo de 90% para geração de alertas, descarte automático de reconhecimentos com baixa confiabilidade, testes regulares de viés e acurácia, além de validação humana obrigatória para todas as decisões de impacto.

As medidas organizacionais estabelecem governança através de Comitê Gestor incluindo representantes da SEPROT, Procuradoria-Geral, Controladoria-Geral e Encarregado de Tratamento de Dados Pessoais, com reuniões regulares para análise de casos críticos e deliberações sobre o sistema. A capacitação envolve treinamento obrigatório sobre LGPD, uso responsável de inteligência artificial e procedimentos operacionais para todos os envolvidos, complementado por reciclagem semestral e atualizações conforme evolução normativa.

O regime de auditoria compreende auditorias internas regulares conduzidas pela própria administração, auditoria externa anual por empresa especializada independente, revisão semestral obrigatória deste

RIPD e monitoramento contínuo de conformidade através de indicadores específicos de desempenho e aderência às normas de proteção de dados.

8. DIREITOS DOS TITULARES E TRANSPARÊNCIA

Os cidadãos podem exercer seus direitos através da Ouvidoria do Município (<https://www.joinville.sc.gov.br/servicos/registrar-pedido-de-informacao-sobre-dados-pessoais/>)

Os direitos aplicáveis incluem confirmação da existência de tratamento, acesso aos dados pessoais quando não comprometer investigações em andamento, correção de inexatidões identificadas e oposição ao tratamento nos casos legalmente previstos.

A transparência ativa se dará com a implementação de sinalização em todas as áreas monitoradas através de placas informativas, campanhas educativas de esclarecimento sobre o funcionamento do sistema, relatórios sobre os resultados da Plataforma, e política de privacidade específica disponível em canais oficiais.

9. GOVERNANÇA E CONTROLE SOCIAL

A estrutura de governança centra-se no Comitê Gestor composto inicialmente por profissionais técnicos da área de segurança pública do Município, acompanhados de representantes da Procuradoria-Geral, Controladoria-Geral e Encarregado de Tratamento de Dados Pessoais do Município, com a atribuição de analisar incidentes, vieses algorítmicos e casos de reconhecimento equivocado.

A accountability e prestação de contas estruturam-se através de documentação completa de todas as operações conforme artigo 37 da LGPD, incluindo registro detalhado de acessos realizados, decisões automatizadas executadas, compartilhamentos efetivados e incidentes identificados. Os indicadores de monitoramento contemplam taxa de falsos positivos e negativos, tempo médio de resposta a solicitações de titulares, número e gravidade de incidentes de segurança e efetividade mensurável das medidas de segurança pública implementadas.

A Plataforma e Programa Smartville deve passar regularmente por revisões, sendo analisado todos os impactos, eficiência e alinhamento, com as expectativas prévias sendo todo o processo documentado, incluindo todos os ajustes de processos e procedimentos realizados. Qualquer variação de resultado positivo ou negativo será possível corrigir, como qualquer intercorrência, que incline o programa em direção diferente da definida como referência. Sendo um processo de melhoria constante dos sistemas que compõem a Plataforma, assim como tudo que compõem o Programa Smartville, com metodologias de gestão, em todos os aspectos do programa.

10. GESTÃO DE INCIDENTES

Os procedimentos de resposta a incidentes iniciam-se com detecção através de monitoramento automatizado com alertas em tempo real, canais estruturados para reportes internos e externos, além de análise proativa e sistemática de logs de segurança. A resposta efetiva exige acionamento do plano específico de resposta a incidentes tão logo identificado o incidente, isolamento imediato de sistemas potencialmente comprometidos, preservação cuidadosa de evidências para investigação e comunicação tempestiva às autoridades competentes.

A comunicação de incidentes observa rigorosamente a obrigatoriedade de notificação à ANPD em até 24 (vinte e quatro) horas para incidentes classificados como de alto risco conforme Resolução CD/ANPD nº 15/2024, comunicação aos titulares afetados quando aplicável e exigida, além de transparência adequada sobre medidas adotadas para contenção e correção das falhas identificadas.

O aprendizado organizacional garante que cada incidente gera relatório específico de lições aprendidas, com implementação efetiva de melhorias preventivas e revisão criteriosa dos procedimentos de segurança existentes. O Comitê Gestor avalia de forma regular todos os incidentes ocorridos para identificar padrões recorrentes e oportunidades concretas de melhoria sistêmica.

11. REVISÃO E ATUALIZAÇÃO

O cronograma de revisões estabelece atualização semestral obrigatória deste RIPD considerando novos riscos identificados na operação, mudanças tecnológicas implementadas, alterações no marco normativo aplicável e incorporação de lições aprendidas durante a implementação e operação do sistema.

Revisões extraordinárias ocorrem sempre que houver mudanças significativas no sistema operacional, promulgação de nova legislação aplicável, ocorrência de incidentes graves classificados como de alto impacto ou recomendações específicas emanadas de órgãos de controle interno ou externo.

Os indicadores de efetividade permitem monitoramento contínuo da efetividade das medidas de proteção através de indicadores quantitativos como número de incidentes registrados, tempo médio de resposta a solicitações e taxa de conformidade com procedimentos, complementados por indicadores qualitativos incluindo nível de satisfação dos titulares consultados, grau de confiança social no sistema e efetividade mensurável para consecução dos objetivos de segurança pública.

12. CONCLUSÃO E RECOMENDAÇÕES

A implementação do sistema de videomonitoramento inteligente com reconhecimento facial em Joinville apresenta riscos significativos, mas gerenciáveis à proteção de dados pessoais dos cidadãos. As medidas propostas, incluindo cláusulas contratuais robustas, Comitê Gestor com funcionamento regular, auditorias periódicas sistemáticas, transparência ativa com a população e observância rigorosa de todos os dispositivos da LGPD, constituem framework juridicamente adequado e tecnicamente viável para equilibrar as necessidades legítimas de segurança pública com a proteção efetiva dos direitos fundamentais dos cidadãos.

As recomendações prioritárias incluem implementação integral de todas as medidas de segurança identificadas antes do início efetivo das operações, capacitação específica e continuada de todas as equipes direta ou indiretamente envolvidas, estabelecimento formal do Comitê Gestor com funcionamento regular e documentado, realização de projeto piloto com acompanhamento intensivo durante os primeiros meses e desenvolvimento detalhado de procedimentos de resposta a incidentes com treinamento prático das equipes.

O presente relatório tem caráter dinâmico e deverá ser atualizado periodicamente, sempre que houver mudanças relevantes na tecnologia utilizada, nos fluxos de tratamento de dados ou no marco regulatório aplicável.

Joinville, 02 de setembro de 2025

Responsável: Sahmara Liz Botemberger

Encarregada de Tratamento de Dados Pessoais do Município de Joinville

Próxima Revisão: Versão Final do Termo de Referência



Documento assinado eletronicamente por **Evelin Fernanda Vargas, Coordenador(a)**, em 06/11/2025, às 16:48, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº 8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.



Documento assinado eletronicamente por **Paulo Rogerio Rigo, Secretário (a)**, em 06/11/2025, às 16:57, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº 8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.



Documento assinado eletronicamente por **Paulo Isaias Stremel de Almeida, Gerente**, em 07/11/2025, às 09:03, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº 8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.



Documento assinado eletronicamente por **Rodolfo Lauro Weinert, Diretor (a) Executivo (a)**, em 07/11/2025, às 13:15, conforme a Medida Provisória nº 2.200-2, de 24/08/2001, Decreto Federal nº 8.539, de 08/10/2015 e o Decreto Municipal nº 21.863, de 30/01/2014.



A autenticidade do documento pode ser conferida no site <https://portalsei.joinville.sc.gov.br/> informando o código verificador **27227235** e o código CRC **BECA0535**.

Av. Hermann August Lepper, 10 - Bairro Saguazu - CEP 89221-005 - Joinville - SC - www.joinville.sc.gov.br