

			GRUPO GTI	TIPO PO	NÚMERO 003
ASSUNTO POLÍTICA DE GESTÃO DE INCIDENTES DE DADOS					
REVISÃO Setembro/2028		DATA DA PUBLICAÇÃO 08/09/2026		VERSÃO 2.0	

1. OBJETIVO

Estabelecer as diretrizes gerais e específicas, os princípios, conceitos e responsabilidades relativos à gestão de incidentes de segurança da informação, com ênfase nos incidentes que afetem dados pessoais, compreendidos como eventos adversos confirmados que violem a confidencialidade, a integridade, a disponibilidade ou a autenticidade de dados pessoais, assegurando tratamento tempestivo e a redução dos impactos aos titulares e ao negócio.

2. ABRANGÊNCIA

Esta Política se aplica a todas as unidades da Prodam-SP e seus colaboradores.

3. TERMOS E DEFINIÇÕES

Para fins desta Política, consideram-se os seguintes termos e definições:

Agentes de Tratamento de Dados Pessoais: São considerados agentes de tratamento de dados pessoais:

- **Controlador:** Pessoa física ou jurídica, de direito público ou privado, a quem compete as decisões referentes ao tratamento de dados pessoais;
- **Operador:** Pessoa física ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do Controlador.

Anonimização: Processos e técnicas por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo.

Agência Nacional de Proteção de Dados (ANPD): autarquia de natureza especial, dotada de autonomia técnica e decisória, responsável por zelar pela proteção de dados pessoais, editar normas e fiscalizar e aplicar as sanções previstas na LGPD, nos termos da Lei nº 15.352/2026.

Colaboradores: todos os empregados de carreira, comissionados, estagiários e aprendizes, contratados ou com qualquer outra forma de vínculo com a Empresa, incluindo colaboradores internos, externos, cedidos e licenciados.

Comitê de Segurança da Informação (CSI): Grupo multidisciplinar, ligado à Presidência da ProdAm-SP, que reúne representantes de diversas áreas da Empresa, indicados pela Diretoria ou pelo Presidente, com o intuito de definir e apoiar estratégias necessárias à implantação e manutenção da Segurança da Informação

Consentimento: Manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada.

CTIR Gov: O Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov) faz parte do Departamento de Segurança de Informação (DSI), do Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

Dado financeiro: dado pessoal relacionado a transações financeiras do titular, inclusive de contratação de serviços e aquisição de produtos.

Dado pessoal: Toda informação relacionada a pessoa natural identificada ou identificável, tal como nome, RG, CPF, e-mail etc. Também são considerados dados pessoais aqueles utilizados para formação do perfil comportamental de determinada pessoa natural.

Dado pessoal afetado: dado pessoal cuja confidencialidade, integridade, disponibilidade ou autenticidade tenha sido comprometida em incidente de segurança.

Dado pessoal sensível: É todo dado pessoal, que possa vir a gerar qualquer tipo de discriminação, sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, referente à saúde ou à vida sexual, genético ou biométrico, quando vinculado a uma pessoa natural.

Dado protegido por sigilo legal, judicial ou profissional: dado pessoal cujo sigilo decorra de norma jurídica, decisão judicial ou do exercício de função, ministério, ofício ou profissão.

Dado de autenticação em sistemas: dado pessoal utilizado como credencial de acesso ou de confirmação de identidade, como contas de login, tokens e senhas.

Encarregado pelo Tratamento de Dados Pessoais (Encarregado de Dados): pessoa indicada por ato formal do agente de tratamento, do qual constem suas formas de atuação e atividades, designada juntamente com seu substituto, para atuar como canal de comunicação entre o Controlador, os titulares e a ANPD, dotada de autonomia técnica, com identidade e informações de contato divulgadas publicamente, de forma clara e objetiva, e sem o exercício de atribuições que configurem conflito de interesse, nos termos da Resolução CD/ANPD nº 18/2024 e do artigo 5º do Decreto Municipal nº 59.767/2020, com a redação dada pelo Decreto Municipal nº 65.117/2026.

Grupo de Resposta a Incidentes (GRI): grupo multidisciplinar composto por técnicos de diversas unidades organizacionais da ProdAm-SP, que atua como ponto central para notificações de incidentes de segurança, provendo a coordenação e o apoio no processo de resposta a incidentes. A indicação de seus membros deve ser feita pelo CSI e aprovada pela Diretoria.

Em sua composição deve necessariamente contar com pelo menos um representante das áreas de Segurança da Informação, Infraestrutura, Negócios, Jurídico e Comunicação, além do Encarregado de Dados e eventuais indicações da Diretoria. Os membros deverão exercer a função sem prejuízo das suas atribuições e sem gratificação. O grupo permanece disponível 24x7.

Imprensa: Órgãos e veículos de comunicação em massa, tais como jornais, revistas, rádios, sites, portais e blogs, canais de TV ou TV a cabo, além de redes sociais.

Incidente de segurança da informação: evento adverso confirmado que viole a confidencialidade, a integridade, a disponibilidade ou a autenticidade de ativos de informação da ProdAm-SP ou sob sua custódia, independentemente de envolver dados pessoais.

Incidente de segurança com dados pessoais: espécie de incidente de segurança da informação, caracterizada por evento adverso confirmado relacionado à violação da confidencialidade, da integridade, da disponibilidade ou da autenticidade de dados pessoais, nos termos do artigo 3º da Resolução CD/ANPD nº 15/2024, ao qual se aplicam, além das disposições gerais desta Política, os deveres específicos de avaliação de risco, comunicação e registro previstos nos itens 4.12, 4.13, 5.3 e 5.4.

ITSM: Gerenciamento de Serviços de Tecnologia da Informação – IT Service Management. É uma abordagem estratégica para projetar, fornecer, gerenciar e melhorar a maneira como a tecnologia da informação (TI) é usada em uma organização. O objetivo é garantir que os processos, pessoas e tecnologia corretos estejam em vigor para que a organização possa atender às suas metas de negócios.

Larga escala: incidente que abranja número significativo de titulares, considerados o volume de dados, a duração, a frequência e a extensão geográfica de localização dos titulares.

LOG: processo de registro de eventos relevantes em uma solução computacional. Pode ser relativo a softwares ou hardwares utilizados na solução.

Porta-voz: Interlocutor(a) autorizado(a) a falar institucionalmente em nome da ProdAm-SP.

Pseudonimização: processos e técnicas que reduzem a possibilidade de associar, direta ou indiretamente, o dado ao seu titular. O dado pseudonimizado é considerado dado pessoal para fins de aplicação da LGPD, tendo em vista a possibilidade de sua associação a uma pessoa natural.

Risco ou dano relevante: situação em que o incidente possa afetar significativamente interesses e direitos fundamentais dos titulares, na forma do item 5.3 desta Política.

Servidor NTP (Network Time Protocol): O NTP é um protocolo para sincronização dos relógios dos computadores baseado no protocolo UDP (User Datagram Protocol). É utilizado para sincronização do relógio de um conjunto de computadores e dispositivos em redes de dados com latência variável.

Tratamento (de Dados Pessoais): Toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Ressalta-se que outras operações, além dos exemplos dados acima, podem ser consideradas tratamento de dados pessoais.

WAR ROOM (“Sala de Guerra”): Ambiente reservado para o planejamento de estratégias sobre determinado assunto crítico. Nele se reúnem integrantes de um determinado grupo para focar na solução de problemas.

4. DIRETRIZES

4.1. A ProdAm-SP, bem como seus colaboradores têm o compromisso de zelar pelas informações estratégicas e pessoais de seus colaboradores, clientes e fornecedores.

4.2. Todo colaborador tem obrigação em informar a Empresa em casos de suspeita ou efetivo vazamento de dados, colaborando com evidências para sua investigação.

4.2.1. A omissão, o retardamento injustificado ou a prestação de informação falsa quanto ao dever previsto no item 4.2 sujeita o colaborador às medidas disciplinares previstas no Código de Conduta e Integridade e no regulamento interno de pessoal da ProdAm-SP, sem prejuízo das responsabilidades civil e penal cabíveis, observado o artigo 9º da Lei Federal nº 13.303/2016. Tratando-se de colaborador externo, a inobservância será apurada na forma do respectivo instrumento contratual. A comunicação de boa-fé de suspeita que não venha a se confirmar como incidente não enseja qualquer medida desfavorável ao comunicante.

4.3. Todos os incidentes devem ser registrados, bem como solicitações derivadas do incidente, através de ferramentas corporativas (ITSM). Porém dados sigilosos não devem ser compartilhados, a menos que haja controle de acesso às informações ali postadas, sendo restritas ao Grupo de Resposta a Incidente e ao Encarregado de Dados.

4.4. Para divulgação de informações sobre incidentes de dados, sejam estes pessoais ou não, caberá, exclusivamente, ao Presidente da ProdAm-SP ou ao Encarregado de Dados (em caso de dados pessoais) fornecer informações ao Porta-Voz da Empresa, que é o responsável pela comunicação com a imprensa, conforme estabelece a Política de Porta-Vozes da ProdAm-SP. Nenhum colaborador sem autorização expressa deverá responder qualquer questionamento da imprensa ou de terceiros.

4.5. Todo indício ou confirmação de incidentes de dados deverá ser informado à Gerência de Segurança da Informação (GIT). Caso o incidente esteja relacionado ao tratamento de dados pessoais, além da GIT, as informações devem ser encaminhadas prontamente ao Encarregado de Dados. Caberá à GIT a divulgação do incidente à Presidência, e às Diretorias. Em se tratando de dados pessoais esta tarefa será do Encarregado de Dados. A comunicação aos clientes será feita ou pelo Presidente, pelo Encarregado de Dados ou pela Gerência de Comunicação Institucional (GRCI). A comunicação à Imprensa será feita pelo Porta-Voz da Empresa, em conformidade com o que estabelece a Política de Porta-Vozes.

4.6. O Encarregado de Dados é o responsável por contatar e representar a ProdAm-SP junto a Autoridade Nacional de Proteção de Dados (ANPD) no caso de incidentes envolvendo dados pessoais ou quando houver qualquer tipo de comunicação entre a ProdAm-SP e a ANPD.

4.7. O Grupo de Resposta a Incidentes é responsável por informar ao CTIR Gov (quando necessário), com vistas a permitir que sejam dadas soluções integradas para a Administração Pública, bem como a geração de estatísticas.

4.8. A ProdAm-SP, em seu papel de Operadora de dados, informará ao respectivo Controlador sobre qualquer tipo de incidente envolvendo seus dados, mantendo sua transparência com seus clientes, cidadãos e ao mercado.

4.9. Deve ser definido um plano de comunicação de incidentes de dados junto à GRCI e ao Porta-Voz da Empresa, que esteja de acordo com a classificação e o nível de criticidade. Em se tratando de dados pessoais, o Encarregado de Dados será responsável pelo nível de comunicação a ser adotado, apoiado na classificação realizada pelos proprietários dos dados.

4.10. A investigação dos incidentes deverá ser administrada pelo Grupo de Resposta a Incidentes (GRI), apoiado diretamente pelas áreas de infraestrutura, desenvolvimento, jurídico e pelo Encarregado de Dados. Somente os Controladores dos dados são os responsáveis por definir a classificação dos dados, seja quanto a sua natureza pública, seja quanto a dados pessoais e hipótese de tratamento.

4.10.1. A qualificação da ProdAm-SP como Controladora ou Operadora será aferida em relação a cada operação de tratamento afetada pelo incidente, e não de forma genérica. A ProdAm-SP atua como Operadora nos tratamentos executados por conta e ordem dos órgãos e entidades da Administração Municipal, e como Controladora nos tratamentos relativos a seus empregados, candidatos, estagiários, aprendizes, fornecedores, usuários de seus canais próprios e demais atividades administrativas e negociais próprias, hipótese em que lhe incumbem diretamente os deveres dos artigos 37, 48 e 50 da Lei Federal nº 13.709/2018. Verificada a controladoria conjunta, os deveres de comunicação serão exercidos de forma coordenada com o

outro controlador, sem prejuízo da responsabilidade solidária prevista no artigo 42, § 1º, da mesma Lei.

4.10.2. A definição do papel exercido pela Prodam-SP em cada operação afetada compete ao Encarregado de Dados, com apoio da GIT e da GPJ, e será formalizada na avaliação de risco de que trata o item 4.12. Enquanto pendente a qualificação, adotar-se-á a hipótese mais protetiva ao titular para efeito de início da contagem dos prazos regulatórios.

4.11. O Controlador é o responsável pela definição da finalidade, das hipóteses legais de tratamento e pelo prazo do tratamento de dados pessoais.

4.12. Todo incidente que envolva dados pessoais será objeto de avaliação formal de risco, conduzida pela GIT em conjunto com o Encarregado de Dados, da qual constarão a natureza e a categoria dos dados afetados, o número de titulares afetados com discriminação de crianças, adolescentes e idosos, os possíveis impactos aos titulares, as medidas de contenção adotadas e a conclusão fundamentada quanto à existência ou não de risco ou dano relevante. A avaliação será juntada ao registro do incidente.

4.13. A comunicação à ANPD e aos titulares é obrigatória quando o incidente puder acarretar risco ou dano relevante aos titulares, assim caracterizado quando afetar significativamente seus interesses e direitos fundamentais e, cumulativamente, envolver ao menos um dos seguintes elementos: dados pessoais sensíveis; dados de crianças, de adolescentes ou de idosos; dados financeiros; dados de autenticação em sistemas; dados protegidos por sigilo legal, judicial ou profissional; ou dados em larga escala. A ausência de dever de comunicação não dispensa o registro interno do incidente, na forma do item 5.4 desta Política.

4.14. Todos os contratos celebrados com terceiros que envolvam compartilhamento ou tratamento de informações sob responsabilidade da Prodam-SP deverão conter cláusula específica que obrigue a contratada a comunicar formalmente à Prodam-SP, por meio da GIT e do Encarregado de Dados, em até 24 (vinte e quatro) horas contadas da ciência, a ocorrência de qualquer incidente de segurança verificado em sua infraestrutura ou no âmbito da execução contratual, acompanhada dos elementos necessários à instrução da comunicação de que trata o item 5.3.7.1 e das medidas de contenção adotadas, bem como a prestar informações complementares nos prazos que lhe forem assinados e a preservar as evidências na forma do item 5.2.10. A inobservância sujeita a contratada às sanções previstas nos artigos 155 e 156 da Lei Federal nº 14.133/2021 e no respectivo instrumento contratual, sem prejuízo da responsabilização prevista no artigo 42 da Lei Federal nº 13.709/2018.

4.15. O Grupo de Respostas a Incidentes deverá realizar exercícios simulados anuais ou sempre que houver mudanças significativas na infraestrutura.

5. DISPOSIÇÕES GERAIS

5.1. LOG'S – RASTREABILIDADE

5.1.1. O horário de servidores e equipamentos de redes serão sincronizados com uma fonte confiável de tempo (base servidor NTP corporativo) para que não haja disparidades na correlação de eventos, logs e outros dados.

5.1.2. A definição dos logs ´s dentro da infraestrutura, ou nas aplicações, deve ser configurada para que, no mínimo, sejam identificados os autores de modificações em ambientes críticos, principalmente aqueles realizados pelos super usuários/administradores.

5.1.3. Para definição de logs para acesso a informações críticas previstas em regras de negócios (leitura/modificação/etc.), o **Controlador** (ou o proprietário do serviço/aplicação) deverá identificar e definir o tipo de log a ser registrado, bem como sua retenção (tempo de retenção), para que seja também definida a infraestrutura necessária para seu armazenamento e tratamento.

5.1.4. Quando solicitado, as logs serão analisadas pelas áreas gestoras, dentro de suas responsabilidades (ex. Firewall-Segurança, Servidores-Suporte, BD-Suporte, Aplicações-Gerência de negócio/desenvolvimento, switches-Telecomunicações) podendo ser solicitadas pelo Grupo de Resposta a Incidentes ou pela GIT.

5.1.5. Os logs serão retidos pelo prazo mínimo de 1 (um) ano, quanto aos registros de conexão, e de 6 (seis) meses, quanto aos registros de acesso a aplicações, observados os artigos 13 e 15 da Lei Federal nº 12.965/2014. Para os demais logs, notadamente os de ambientes críticos e os relativos a ações de super usuários e administradores referidos no item 5.1.2, o Controlador ou o proprietário do serviço definirá prazo de retenção motivado, proporcional ao risco da operação e compatível com a tabela de temporalidade aplicável, vedada a retenção por prazo indeterminado, nos termos do artigo 6º, incisos III e X, da Lei Federal nº 13.709/2018.

5.1.6. Havendo indício ou confirmação de incidente, os logs pertinentes serão imediatamente preservados de forma íntegra e inalterada, com registro de cadeia de custódia na forma do item 5.2.10, desde a ciência até o encerramento formal do incidente e o decurso dos prazos de eventual apuração administrativa, sancionatória ou judicial, ficando suspensa, quanto a eles, a eliminação ordinária prevista no item 5.1.5. A suspensão será determinada pela GIT ou pelo Encarregado de Dados e registrada no chamado correspondente.

5.2. PROCESSO DE TRATAMENTO DO INCIDENTE

5.2.1. O Encarregado do Dados deverá ser imediatamente acionado quando houver qualquer incidente que envolva dados pessoais, para que tome ciência e possa realizar o acompanhamento das ações, para posterior comunicação para a Diretoria, Presidência, Conselho de Administração, clientes e, se necessário, à ANPD e Titulares dos dados (em caso de risco ou dano relevante aos titulares, conforme item **5.3.4.** desta política).

5.2.1.1. Nos incidentes classificados como de alta criticidade e naqueles que ensejem comunicação à ANPD ou aos titulares, o Encarregado de Dados, em conjunto com a GIT, dará ciência ao Comitê de Auditoria Estatutário e à área responsável pelos controles internos, para acompanhamento e registro, na forma dos artigos 9º e 24 da Lei Federal nº 13.303/2016. A ciência não suspende nem condiciona as providências de contenção e de comunicação previstas nesta Política.

5.2.2. Todo colaborador que tomar conhecimento de indício ou confirmação de incidente que envolva dados pessoais deverá comunicar imediatamente a GIT e o Encarregado de Dados, por meio das ferramentas corporativas, no mesmo dia útil da ciência. O acionamento do Encarregado de Dados é condição para início da contagem dos prazos regulatórios e não pode ser postergado pela investigação técnica em curso.

5.2.2.1. Uma vez acionada a GIT sobre possível incidente de dados, esta procederá à análise preliminar e poderá abrir WAR ROOM e acionar o Grupo de Resposta a Incidentes para análise do evento, incluindo todos os agentes necessários para tratar o incidente.

5.2.2.2. O acionamento do Grupo de Resposta a Incidentes e do Encarregado de Dados é obrigatório, independentemente do estágio da apuração técnica, sempre que houver indício de que o incidente envolva dados pessoais sensíveis, dados de crianças, de adolescentes ou de idosos, dados financeiros, dados de autenticação em sistemas ou dados protegidos por sigilo legal, judicial ou profissional; afete dados pessoais em larga escala; comprometa serviço de missão crítica de órgão ou entidade contratante; ou possa acarretar risco ou dano relevante na forma do item 5.3.4.

5.2.2.3. Havendo dúvida quanto ao enquadramento nas hipóteses do item 5.2.2.2, o acionamento será realizado, cabendo ao Grupo de Resposta a Incidentes deliberar de forma fundamentada sobre o encerramento sumário, com registro no chamado correspondente.

5.2.3. Todos os integrantes do Grupo de Resposta a Incidentes serão acionados pelo NOC, a partir de solicitação feita pela GIT, que, por sua vez, terá todos os contatos e procedimentos necessários para acionamento.

5.2.4. Todas as gerências diretamente envolvidas no incidente deverão verificar a abrangência do incidente e colaborar com evidências para análise.

5.2.5. Todos os integrantes do Grupo de Resposta a Incidentes terão a liberdade de acionar diretamente qualquer área que considere importante na participação para análise/ações de contorno/solução da vulnerabilidade.

5.2.6. O Grupo de Resposta a Incidentes terá o poder de decidir sobre a retirada/suspensão de serviços e/ou sites para conter a vulnerabilidade, inclusive com a possibilidade de bloqueio do serviço de Internet. As ações serão repassadas imediatamente para a Diretoria de Infraestrutura e Tecnologia (DIT) e as demais diretorias dos serviços envolvidos.

5.2.7. O Grupo de Resposta a Incidentes terá o poder de solicitar o isolamento do ambiente afetado para futura análise forense.

5.2.8. O Grupo de Resposta a Incidentes sempre se reportará ao Encarregado de Dados como figura central, tratando-se de incidentes com dados pessoais. O Encarregado de Dados será o responsável pela atualização da Diretoria e da Presidência.

5.2.9. Todas as tratativas poderão ser realizadas remotamente. Em casos de alta criticidade, a GIT ou o Encarregado de Dados poderá solicitar a utilização de uma sala de guerra (WAR ROOM) e atendimento presencial em alguma unidade física específica da Prodam-SP, inicialmente a WAR ROOM será composta pelos integrantes do Grupo de Resposta a Incidentes e aqueles convocados pelo referido grupo.

5.2.10. Durante todas as atividades de tratamento do incidente, é necessário preservar as evidências para análise futura:

- Cadeia de custódia;
- Coleta de imagens forenses;
- Hash dos arquivos;
- Preservação dos logs;

- Isolamento sem alteração das evidências;
- Controle de acesso às evidências.

5.2.11. Após a conclusão de cada incidente, deverá ser realizada reunião de fechamento, contemplando e registrando, no mínimo, as seguintes pautas de discussões:

- Identificação e análise da causa raiz do incidente;
- Identificação das vulnerabilidades exploradas;
- Identificação das falhas de processo;
- Definição das oportunidades de melhorias;
- Elaboração do plano de ação;
- Atualização da documentação;
- Reavaliação dos riscos;
- Revisão dos controles;
- Registro das conclusões da análise do incidente e dos conhecimentos obtidos para fins de melhoria contínua.

5.3. COMUNICAÇÃO À ANPD

5.3.1. Toda comunicação de incidentes de dados pessoais à ANPD deve ser realizada pelo **Controlador**. A Prodam-SP, sempre que necessário e como agente de tratamento no papel de **Operador**, dará suporte e apoio ao **Controlador** quanto aos subsídios necessários para comunicação junto à ANPD.

5.3.2. Em caso de incidente de segurança com dados pessoais cujo Controlador seja a Prodam-SP, a comunicação à ANPD será realizada pelo Encarregado de Dados no prazo de 3 (três) dias úteis, contados do conhecimento, pela Prodam-SP, de que o incidente afetou dados pessoais, ressalvada a existência de prazo diverso previsto em legislação específica.

5.3.3. A comunicação será realizada por meio do formulário eletrônico disponibilizado pela ANPD e encaminhada exclusivamente pelo canal indicado em orientação publicada no sítio eletrônico da Autoridade, atualmente o peticionamento eletrônico do Sistema Único de Processo Eletrônico em Rede. A comunicação será firmada pelo Encarregado de Dados e instruída, no mesmo prazo, com documento comprobatório de seu vínculo com a Prodam-SP ou com instrumento de representação, sob pena de a ANPD instaurar procedimento de apuração de incidente de segurança.

5.3.4. Quando o incidente puder acarretar risco ou dano relevante, os titulares serão comunicados pelo Controlador no prazo de 3 (três) dias úteis, contados do conhecimento de que o incidente afetou dados pessoais. A comunicação utilizará linguagem simples e de fácil entendimento e será feita de forma direta e individualizada, pelos meios usualmente utilizados para contato com o titular. Caso a comunicação individualizada seja inviável ou não seja possível identificar os titulares afetados, a divulgação será realizada pelos meios disponíveis, inclusive sítio eletrônico e canais de atendimento, com direta e fácil visualização, pelo período mínimo de 3 (três) meses. A comunicação conterá a natureza e a categoria dos dados afetados, as medidas técnicas e de segurança utilizadas, os riscos e possíveis impactos aos titulares, os motivos de eventual demora, as medidas adotadas ou a adotar para reverter ou mitigar os efeitos, a data do conhecimento do incidente e o contato para obtenção de informações, incluídos os dados do Encarregado de Dados. Recomenda-se a inclusão de orientações aptas a mitigar os efeitos do incidente, considerada boa prática para

os fins do artigo 52, § 1º, inciso IX, da LGPD. O Encarregado de Dados juntará ao processo de comunicação declaração da realização da comunicação aos titulares, com indicação dos meios utilizados, em até 3 (três) dias úteis contados do término do prazo previsto no item 5.3.2.

5.3.5. A GIT, apoiada pelas demais gerências envolvidas, elaborará o relatório de tratamento do incidente, contendo a descrição do evento, a avaliação de risco, as evidências pertinentes e as providências adotadas para reverter ou mitigar seus efeitos, para fins de cumprimento do princípio de responsabilização e prestação de contas e de eventual apresentação à ANPD.

5.3.6. Quando a ProdAm-SP atuar como Operadora, comunicará o incidente ao Encarregado de Dados definido pelo Controlador em até 24 (vinte e quatro) horas da ciência, fornecendo todas as informações necessárias à comunicação à ANPD e aos titulares, conforme item 5.3.8, e prestando apoio na complementação de informações no prazo de 20 (vinte) dias úteis. As obrigações de comunicação entre Controlador e Operador deverão constar de cláusula contratual específica, cabendo ao Encarregado de Dados a manifestação técnica sobre sua redação.

5.3.7. A comunicação do incidente deverá ser realizada o mais breve possível, respeitado o prazo máximo definido no item 5.3.2. A comunicação espontânea e tempestiva, acompanhada da adoção de medidas de contenção e mitigação, demonstra transparência, cooperação e boa-fé, e será considerada na aferição das circunstâncias atenuantes previstas no artigo 52, § 1º, da Lei Federal nº 13.709/2018 e no Regulamento de Dosimetria e Aplicação de Sanções Administrativas, aprovado pela Resolução CD/ANPD nº 4/2023.

5.3.7.1. A comunicação à ANPD conterá, no mínimo: a descrição da natureza e da categoria dos dados pessoais afetados; o número de titulares afetados, discriminado, quando aplicável, o número de crianças, de adolescentes e de idosos; as medidas técnicas e de segurança utilizadas para a proteção dos dados, adotadas antes e após o incidente, observados os segredos comercial e industrial; os riscos relacionados ao incidente, com identificação dos possíveis impactos aos titulares; os motivos da demora, caso a comunicação não tenha sido realizada no prazo; as medidas adotadas ou a adotar para reverter ou mitigar os efeitos sobre os titulares; a data da ocorrência do incidente, quando possível determiná-la, e a de seu conhecimento pelo Controlador; os dados do Encarregado de Dados ou de quem represente o Controlador; a identificação do Controlador; a identificação do Operador, quando aplicável; a descrição do incidente, incluída a causa principal, quando identificável; e o total de titulares cujos dados são tratados nas atividades de tratamento afetadas pelo incidente. Cabe ao Controlador solicitar à ANPD, de forma fundamentada, o sigilo das informações protegidas por lei.

5.3.8. Caso não seja possível fornecer todas as informações no prazo do item 5.3.2, a comunicação será realizada com as informações disponíveis e complementada, de maneira fundamentada, no prazo de 20 (vinte) dias úteis contados da data da comunicação. A ANPD poderá, a qualquer tempo, solicitar informações adicionais, inclusive o registro das operações de tratamento dos dados afetados, o Relatório de Impacto à Proteção de Dados Pessoais e o relatório de tratamento do incidente.

5.3.9. Sem prejuízo das comunicações previstas nos itens anteriores, o Encarregado de Dados dará ciência do incidente com dados pessoais ao órgão ou entidade contratante titular do serviço afetado, quando a ProdAm-SP atuar como Operadora, no prazo do item 5.3.6, e à Controladoria Geral do Município, na condição de instância municipal de supervisão do programa de governança em privacidade, nos termos do Decreto Municipal nº 59.767/2020 e alterações vigentes, no prazo do item 5.3.2. As científicações serão registradas no processo do incidente e integrarão o registro de que trata o item 5.4.

5.4. A ProdAm-SP manterá registro de todos os incidentes de segurança com dados pessoais, inclusive daqueles não comunicados à ANPD e aos titulares, contendo, no mínimo: a data de conhecimento do incidente; a descrição geral das circunstâncias em que ocorreu; a natureza e a categoria dos dados afetados; o número de titulares afetados; a avaliação do risco e os possíveis danos aos titulares; as medidas de correção e mitigação adotadas; a forma e o conteúdo da comunicação, quando realizada; e os motivos da ausência de comunicação, quando for o caso. O registro será mantido pelo prazo mínimo de 5 (cinco) anos, contado da data do registro, observadas as regras aplicáveis aos documentos de guarda permanente previstas na tabela de temporalidade aplicável. A guarda e a atualização do registro são de responsabilidade do Encarregado de Dados, com apoio da GIT.

5.5. Recebida determinação da ANPD para adoção de medidas preventivas, de medidas de reversão ou mitigação, ou de ampla divulgação do incidente em meios de comunicação, o Encarregado de Dados dará ciência imediata à Presidência e à Diretoria e coordenará seu cumprimento com a GIT, a Gerência Jurídico-Consultiva e de Governança Corporativa (GPJ) e a GRCl. A ampla divulgação determinada pela Autoridade não se confunde com a sanção de publicização prevista no artigo 52, inciso IV, da LGPD, e a comunicação à imprensa observará a Política de Porta-Vozes.

6. DETALHAMENTO DOS PROCESSOS

Para detalhamento dos processos envolvidos nesta Política será elaborado o Fluxo de Atividade de Processo (FAP).

7. RESPONSABILIDADES E COMPETÊNCIAS

7.1. ENCARREGADO DE DADOS

- a) Caberá ao Encarregado de Dados, a responsabilidade pelo canal de comunicação entre a Empresa e a ANPD, bem como contatar os demais Encarregados de Dados eleitos pelos Controladores.
- b) O Encarregado de Dados, logo após sua nomeação, deverá proceder com o cadastro no sistema SEI FEDERAL, no Protocolo Central da Presidência da República

7.2. GRUPO DE RESPOSTA A INCIDENTES (GRI)

- a) Atuar como ponto central para notificações de incidentes de segurança, provendo a coordenação e o apoio no processo de resposta a incidentes.
- b) Gerar relatório final contendo informações mínimas de:
 - Identificação;
 - Registro;
 - Classificação;
 - Contenção;
 - Preservação das evidências;
 - Erradicação;
 - Recuperação
 - Conhecimentos obtidos para fins de melhoria contínua;
 - Encerramento.

7.3. GERÊNCIA DE SEGURANÇA DA INFORMAÇÃO (GIT)

- a) Recepcionar as informações e verificar os indícios sobre possíveis incidentes de dados, informando à GRI e ao Encarregado de Dados, conforme o caso.
- b) Apoiar no atendimento de todas as diretrizes demandadas pelo Encarregado de Dados e GRI, provendo suporte técnico e informações para auxílio de suas atividades.

7.4. DEMAIS GERÊNCIAS DA PRODAM

Apoiar o Encarregado de Dados e o GRI no atendimento de todas as demandas e solicitações relacionadas às suas atividades.

8. VIGÊNCIA E ATUALIZAÇÃO

Esta Política terá vigência indeterminada e será revisada e atualizada com periodicidade máxima de 2 (dois) anos, ou em prazo inferior, nas hipóteses de alteração de legislação ou regulamentação, ou de mudança do direcionamento estratégico da empresa.

9. LEGISLAÇÕES E DOCUMENTOS RELACIONADOS

9.1. LEGISLAÇÕES/NORMATIVOS EXTERNOS

Lei Federal nº 13.709/2018, de 14/08/2018

Dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Decreto nº 10.474/2020 de 26/08/2020

Aprova a Estrutura Regimental e o Quadro Demonstrativo dos Cargos em Comissão e das Funções de Confiança da Autoridade Nacional de Proteção de Dados e remaneja e transforma cargos em comissão e funções de confiança.

Decreto Municipal nº 59.767 de 15/09/2020

Regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) - no âmbito da Administração Municipal direta e indireta.

Decreto Municipal nº 65.117 de 23/04/2026

Introduz alterações no Decreto nº 59.767, de 15 de setembro de 2020, que regulamenta a aplicação da Lei Federal nº 13.709, de 14 de agosto de 2018 – Lei de Proteção de Dados Pessoais (LGPD) – no âmbito da Administração Municipal Direta e Indireta.

Resolução CD/ANPD nº 1, de 28 de outubro de 2021

Aprova o Regulamento do Processo de Fiscalização e do Processo Administrativo Sancionador.

Resolução CD/ANPD nº 4, de 24 de fevereiro de 2023

Aprova o Regulamento de Dosimetria e Aplicação de Sanções Administrativas

Resolução CD/ANPD nº 15, de 24 de abril de 2024

Aprova o Regulamento de Comunicação de Incidente de Segurança.

Resolução CD/ANPD nº 18, de 16 de julho de 2024

Aprova o Regulamento sobre a atuação do encarregado pelo tratamento de dados pessoais.

9.2. NORMATIVOS INTERNOS

Política de Privacidade e Proteção de Dados Pessoais

Política de Segurança da Informação

Política de Divulgação de Informações Relevantes

Política de Porta Vozes

Cartilha LGPD

10. DOCUMENTOS INCORPORADOS E REVOGADOS

Esta Política revoga e substitui o seguinte documento normativo e demais disposições em contrário:

- GTI-PO-003 Política de Vazamentos e Incidentes de Dados, versão 1.1, publicada em 02/05/2024.

11. DISPOSIÇÕES FINAIS

Situações não previstas e as dúvidas a respeito desta Política deverão ser analisadas pela GIT e pelo Encarregado de Dados e submetidas à aprovação da Diretoria.

12. REVISÕES E APROVAÇÕES

Responsabilidade	Área
Elaboração e Atualização	Gerência de Compliance e Gestão de Riscos (GPR) + Gerência de Segurança da Informação (GIT) + Encarregado de Dados
Revisão	Gerência Jurídica-Consultiva e de Governança Corporativa (GPJ)
Aprovação	Diretoria Executiva
Vigência	Esta Política entrará em vigor a partir da data de sua publicação, revogadas as disposições em contrário

Esta política foi aprovada pela Diretoria Executiva da ProdAm-SP, na 2434ª Reunião de Diretoria ocorrida no dia 04/09/2026, conforme informações constantes no processo SEI nº 7010.2026/0009098-4

HISTÓRICO DE VERSÕES E ALTERAÇÕES

Versão	Data	Alteração	Origem da Alteração
1.0	11/04/2022	Primeira versão	Primeira versão
1.1	02/05/2024	Atualização dos nomes e siglas das Unidades Organizacionais	De acordo com a(s) IN-E 010/2024, IN-E 011/2024 e IN-E 020/2024 conforme autoriza IN-D 005/2022.
2.0	08/09/2026	Alteração do nome da Política e de seu objetivo; revisão das diretrizes, das disposições gerais e das responsabilidades e competências.	Revisão Periódica