GRUPO	TIPO	NÚMERO
GTI	**PO**	**003**

ASSUNTO		
POLÍTICA DE VAZAMENTOS E INCIDENTES DE DADOS		
REVISÃO	DATA DA PUBLICAÇÃO	VERSÃO
11/04/2023	11/04/2022	1.0

1. OBJETIVO

Estabelecer as diretrizes gerais e específicas a serem adotadas na PRODAM-SP, bem como princípios, conceitos e responsabilidades sobre a gestão de incidentes de segurança da informação focado no possível ou efetivo vazamento de dados, e orientar de forma que estes sejam tratados adequadamente reduzindo ao máximo os impactos para o negócio.

2. ABRANGÊNCIA

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

3. ÁREA RESPONSÁVEL

É de responsabilidade da Gerência de Segurança Operacional de Tecnologia (GIT) em conjunto com o Encarregado de Dados da PRODAM-SP, a elaboração, manutenção e atualização desta política.

4. 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.

Autoridade Nacional de Proteção de Dados (ANPD): Órgão da administração pública federal, dotado de autonomia técnica e decisória, responsável por acompanhar e aplicar as sanções descritas na LGPD. Teve sua estrutura regimental criada por meio do Decreto nº 10.474/2020 de 26/08/2020.

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 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 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.

Encarregado pelo Tratamento de Dados Pessoais (Encarregado de Dados) ou Encarregado de Proteção de Dados ou Data Protection Officer (DPO): É a pessoa física ou jurídica, indicada pelo agente de tratamento que tem como principal atribuição atuar como canal de comunicação entre o **Controlador**, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). No texto desta Política, usaremos o Termo "Encarregado de Dados"

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 (DPO) e eventuais indicações da Diretoria. Os membros deverão exercer a função sem prejuízo das suas atribuições e sem gratificação. (Previsto na GTO_PO_001 - Política de Segurança da Informação)

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.

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.

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.

Procedimento Operacional Padrão (POP): Instrumento normativo utilizado para descrever, de forma detalhada e em linguagem clara e de fácil entendimento, como deve ser executado determinado processo, tarefa ou atividade, a depender da necessidade. Este documento particulariza e demonstra como cada etapa de um processo deve ser desenvolvida, as responsabilidades das áreas, sistemas utilizados, fluxos, prazos e demais informações cabíveis e tem como documentos relacionados os fluxos de processos e a Matriz de Responsabilidades.

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.

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 reservados para o planejamento de estratégias sobre determinado assunto crítico. Nele se reúnem integrantes de um determinado grupo para focar na solução de problemas.

5. DIRETRIZES

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

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

5.3. 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.

5.4. 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. Nenhum colaborador sem autorização expressa deverá responder qualquer questionamento da imprensa ou de terceiros

5.5. Todo indício ou confirmação de incidentes de dados deverá ser informado à Gerência de Segurança Operacional de Tecnologia (GIT). Caso o incidente esteja relacionado ao tratamento de dados pessoais, além da GIT, as informações devem ser encaminhadas prontamente ao Encarregado de Dados. Cabe 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 e aos clientes será feita ou pelo Presidente, pelo Encarregado de Dados ou pela Gerência de Comunicação. A comunicação à Imprensa será feita pelo Porta-Voz da Empresa, em conformidade com o que estabelece a Política de Porta-Vozes.

5.6. 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.

5.7. 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.

5.8. 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.

5.9. Deve ser definido um plano de comunicação de vazamento de dados junto a GPC e o 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.

5.10. A investigação dos vazamentos deverá ser administrada pelo Grupo de Resposta a Incidentes (GRI), apoiado diretamente pelas áreas de infraestrutura, desenvolvimento, jurídico e pelo Encarregado de Dados.

5.11. Somente os **Controladores** dos dados são os responsáveis por definir a classificação dos dados, sejam quanto a sua natureza pública, seja quanto a dados pessoais, com exceção das classificações já expressas em Lei.

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

5.13. Todo vazamento deverá ser identificado quanto ao tipo, quantidade de titulares de dados afetados, quantidade dos dados afetados, consequências concretas e prováveis

5.14. Não será necessário comunicar à ANPD caso não haja qualquer incidente de segurança relacionado a dados pessoais.

6. DISPOSIÇÕES GERAIS

6.1. LOG´S – RASTREABILIDADE

6.1.1. 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.

6.1.2. 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.

6.1.3. 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, para que seja também definida a infraestrutura necessária para seu armazenamento e tratamento.

6.1.4. 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.

6.2. PROCESSO DE TRATAMENTO DO INCIDENTE

6.2.1. 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 6.3.4. desta política).

6.2.2. Uma vez acionada a GIT com um possível incidente de dados, esta, após análise, poderá acionar o Grupo de Resposta a Incidentes para análise do evento.

6.2.3. 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.

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

6.2.5. 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.

6.2.6. 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.

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

6.2.8. 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.

6.2.9. 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.

6.3. COMUNICAÇÃO À ANPD

6.3.1. 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.

6.3.2. Em caso de Incidentes envolvendo dados pessoais, cujo **Controlador** seja a PRODAM-SP, a comunicação será feita pelo Encarregado de Dados à ANPD em até 2 (dois) dias úteis.

6.3.3. A comunicação será feita por meio de formulário específico, disponibilizado pela ANPD em seu sítio[1], sendo peticionado eletronicamente no SEI FEDERAL[2].

6.3.4. Em caso de risco ou dano relevante aos titulares, conforme regulamentação da ANPD, os titulares devem ser avisados pelo **Controlador**.

6.3.5. A GIT apoiada por todas as demais gerências envolvidas no incidente elaborará documentação com a avaliação interna do incidente, medidas tomadas e análise de risco, para fins de cumprimento do princípio de responsabilização e prestação de contas.

6.3.6. Quando se tratar de incidente de dados pessoais, a PRODAM-SP, como agente de tratamento no papel de **Operador**, deverá comunicar ao Encarregado de Dados definido pelo **Controlador**, em até 24 (vinte e quatro) horas.

6.3.7. A comunicação à ANPD só será necessária quando o incidente de dados constitua um risco relevante para os direitos e liberdades do titular dos dados.

6.3.8. A comunicação do vazamento deverá ser realizada o mais breve possível, respeitando o prazo máximo definido no item 6.3.2. Nesse sentido, a realização da comunicação demonstrará transparência e boa-fé e será considerada em eventual fiscalização.

6.3.9. A comunicação a ANPD deve conter as seguintes informações:

I. Identificação e dados de contato de:

- Entidade ou pessoa responsável pelo tratamento.
- Encarregado de Dados ou outra pessoa de contato.
- Indicação se a notificação é completa ou parcial. Em caso de comunicação parcial, indicar que se trata de uma comunicação preliminar ou de uma comunicação complementar.

II. Informações sobre o incidente de segurança com dados pessoais:

- Data e hora da detecção.
- Data e hora do incidente e sua duração.
- Circunstâncias em que ocorreu a violação de segurança de dados pessoais, por exemplo, perda, roubo, cópia, vazamento, dentre outros.
- Descrição dos dados pessoais e informações afetadas, como natureza e conteúdo dos dados pessoais, categoria e quantidade de dados e de titulares afetados
- Resumo do incidente de segurança com dados pessoais, com indicação da localização física e meio de armazenamento.
- Possíveis consequências e efeitos negativos sobre os titulares dos dados afetados.
- Medidas de segurança, técnicas e administrativas preventivas tomadas pelo controlador de acordo com a LGPD.

[1] https://www.gov.br/anpd/pt-br/assuntos/atual-formulario-de-comunicacao-de-incidentes-de-seguranca-com-dados-pessoais_01-03-2021-4.docx

[2] https://sei-pr.presidencia.gov.br/sei/controlador_externo.php?acao=usuario_externo_logar&acao_origem=usuario_externo_gerar_senha&id_orgao_acesso_externo=0

- Resumo das medidas implementadas até o momento para controlar os possíveis danos.
- Possíveis problemas de natureza transfronteiriça.
- Outras informações úteis às pessoas afetadas para proteger seus dados ou prevenir possíveis danos.

6.3.10. Caso não seja possível fornecer todas as informações no prazo definido, será realizada uma comunicação preliminar, no prazo de 2 (dois) dias úteis à ANPD, informando que informações adicionais serão fornecidas posteriormente.

7. DETALHAMENTO DOS PROCESSOS

Para detalhamento dos processos envolvidos nesta Política será publicado seu respectivo Procedimento Operacional Padrão (POP).

8. RESPONSABILIDADES E COMPETÊNCIAS

8.1. ENCARREGADO DE DADOS

- Cabe 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.
- O Encarregado de Dados, logo após sua nomeação, deve proceder com o cadastro no sistema SEI FEDERAL, no Protocolo Central da Presidência da República

8.2. GRUPO DE RESPOSTA A INCIDENTES (GRI)

- Cabe ao GRI atuar como ponto central para notificações de incidentes de segurança, provendo a coordenação e o apoio no processo de resposta a incidentes.

8.3. GERÊNCIA DE SEGURANÇA OPERACIONAL DE TECNOLOGIA (GIT)

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

8.4. DEMAIS GERÊNCIAS DA PRODAM

- Apoiar o Encarregado de Dados e ao GRI em todas as solicitações, em apoio a suas atividades.

9. APROVAÇÃO

Esta Política deverá ser aprovada pela Diretoria Executiva em Reunião de Diretoria.

10. VIGÊNCIA E ATUALIZAÇÃO

Esta Política será válida pelo período de até 1 (um) ano, devendo ser atualizada neste período ou em prazo inferior, nas hipóteses de alteração da legislação ou regulamentação, ou no caso de mudança do direcionamento estratégico da Empresa.

11. LEGISLAÇÕES E DOCUMENTOS RELACIONADOS

11.1. LEGISLAÇÕES EXTERNAS

- Lei nº 13.709/2018, de 14/08/2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) 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.

11.2. NORMATIVOS INTERNOS

- GTI_PO_002 - Política de Privacidade e Proteção de Dados Pessoais
- GTI_PO_001 – Política de Segurança da Informação
- P004 – Política de Divulgação de Informações Relevantes
- GCO_PO_007 – Política de Porta-Vozes
- Cartilha LGPD Prodam 2020.

12. 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.

13. REVISÕES E APROVAÇÕES

Responsabilidade	**Área**
Elaboração e Atualização	Gerência de Segurança Operacional de Tecnologia (GIT) e Encarregado de Dados
Revisão	Gerência de Conformidade (GJO) e Diretoria Jurídica e de Governança Corporativa (DJU)
Aprovação	Diretoria Executiva

Esta política foi aprovada pela Diretoria Executiva da PRODAM-SP, na 2097ª Reunião de Diretoria ocorrida no dia 08/04/2022, conforme respectiva Ata, anexa ao processo SEI nº 7010.2022/0003170-0

HISTÓRICO DE VERSÕES E ALTERAÇÕES

Versão	Data	Alteração	Origem da Alteração
1.0	11/04/2022	Primeira versão da Política	Primeira versão da Política