LGPD - Serviço Distrital de São Luiz do Purunã

	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO	Emissão 14/04/2025	Agente delegado Sérgio Tadeu Pupo
Código P-SI-003		Versão 3.0	

1. INTRODUÇÃO 3

2 - PROPÓSITO 4

3 – DIRETRIZES 5
3.1. OBJETIVO DA GESTÃO 5
3.2 PRESIDÊNCIA E GESTÃO DA SEGURANÇA 5
3.3. Proteção de Recursos 5
3.4. Utilização de Informações e Recursos 5
3.5. Nível de Segurança 5
3.6. Conscientização 5
3.7. Gestão de Ativos 5
3.8. Monitoramento 6
3.9. Gerenciamento das Operações e Comunicações 6
3.10. Desenvolvimento, Manutenção e Produção de Sistemas 6
3.11. Continuidade das Atividades 6
3.12. Terceirização ou Prestação de Serviços 6
3.13. Conformidade – Leis Regente 6
3.14. Administração da Segurança da Informação 6
3.15. Prevenção e Resposta a Incidentes 6
3.16. Gestão de Risco 7
3.17. Propriedade da Informação 7
3.18. Backup 7
3.19. Conformidade – LGPD 7

4 – PAPÉIS E RESPONSABILIDADES 7
4.1.Compete à área de Segurança da Informação 7
4.2.Compete ao Gestor 8
4.3.Compete à área Jurídica do Serviço Distrital de São Luiz do Purunã 9
4.4 Compete ao Encarregado de dados 9

5. SANÇÕES E PUNIÇÕES 10

6.CASOS OMISSOS 10

7.APROVAÇÃO E ATUALIZAÇÃO DA PSI 11

8.GLOSSÁRIO 11

9.GESTÃO DA POLÍTICA 13

1. Introdução

1.1. Atualmente, o alto de número de vazamentos de dados em todos os segmentos da sociedade digital é uma consequência do acesso fácil, que ao mesmo tempo, gera um aumento na complexidade para armazenar tais informações.

Como sabemos, a Segurança da informação é o Pilar principal e apresentamos neste documento orientações, normas, ações e responsabilidades relativas a Proteção da informação.

1.2. As regras aqui estabelecidas serão observadas em todos os seus detalhes por todos os colaboradores e o agente delegado do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ,** bem como por seus prestadores de serviços. Desta forma, quando divulgada e entregue a cópia deste documento, todos os que receberem se comprometem a respeitar todos os tópicos abordados e ficam cientes da repercussão de tais regras no seu dia-a-dia

1.3. São princípios para o Sistema de Gestão de Segurança da Informação a Confidencialidade, a Integridade e a Disponibilidade. Esses dados devem ser preservados, controlados e auditados para garantir que as informações estejam protegidas nas medidas exigidas para sua utilização.

1.4. Esta Política de Segurança da Informação (PSI), aprovada, compreende as diretrizes e normas que servem de base para atender aos princípios fundamentais da Segurança da Informação no **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**.

1.5. A Política de Segurança da Informação tem por princípio a proteção dos dados, informações e conhecimento, classificados como sigilosos, além da preservação dos dados Cartorários.

1.6. Dessa forma, o **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ** estabelece sua Política Geral de Segurança da Informação, como parte integrante do seu sistema de gestão, alinhada às boas práticas e normas internacionalmente aceitas, com o objetivo de garantir níveis adequados de proteção a informações da organização ou sob sua responsabilidade.

1.7. Com o vigor da LGPD, o **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ** designa o Encarregado de Dados – também referido como Data Protection Officer(DPO) que irá Conduzir, Monitorar, Orientar, Assegurar, Organizar e Prestar esclarecimentos referente ao Programa de Conformidade da LGPD no **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, zelando pela sua fiscalização.

2. Propósito

2.1. Constituir diretrizes estratégicas, responsabilidades e competências visando à estruturação da segurança da informação e a conformidade com a LGPD (Lei Geral de Proteção de Dados) juntamente com os Provimentos 74/2018, 149/2023.

2.2. Promover ações necessárias à implementação e à manutenção da segurança da informação;

2.3. Orientar quanto à adoção de controles e processos para atendimento dos requisitos para Segurança da Informação;

2.4. Prevenir possíveis causas de incidentes e responsabilidade legal do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**;

2.5. Combater atos acidentais ou intencionais de destruição, modificação, apropriação ou divulgação indevida de informações, de modo a preservar os ativos de informação e a imagem do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**;

2.6. Esta PSI se aplica a todos os responsáveis, prestadores de serviço, colaboradores e usuários externos que fazem uso dos ativos de informação e de processamento no ambiente do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**;

2.7. Estabelecer as competências e atribuições dos responsáveis envolvidos nesta política;

2.8. Tornar a segurança da informação como um dos elementos fundamentais no planejamento estratégico do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, conforme seus princípios básicos:

- Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.
- Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.
- Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes, sempre que necessário.

3. Diretrizes

3.1. O objetivo da gestão de Segurança da Informação do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ** é garantir a gestão sistemática e efetiva de todos os aspectos relacionados à segurança da informação, provendo suporte às operações críticas do negócio e minimizando riscos identificados e seus eventuais impactos.

3.2. O agente delegado está comprometido com uma gestão efetiva de Segurança da Informação. Desta forma, adota todas medidas cabíveis para garantir que esta política seja adequadamente comunicada, entendida e seguida. Revisões periódicas serão realizadas para garantir sua contínua pertinência e adequação às necessidades do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**.

3.3. **Proteção de Recursos**

3.3.1. Proteger os recursos de Tecnologia da Informação e Comunicações, as informações e sistemas contra a modificação, destruição, acesso ou divulgação não autorizada, garantindo sua confidencialidade, integridade e disponibilidade

3.4. **Utilização de Informações e Recursos**

3.4.1. Assegurar que informações e recursos tecnológicos sejam tornados disponíveis para Órgãos integrados com o **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ** e devidamente autorizados, e que sejam utilizados apenas para finalidades lícitas, éticas e administrativamente aprovadas.

3.5. **Nível de Segurança**

3.5.1. Garantir que na criação de novos serviços, a seleção de mecanismos de segurança e a aquisição de bens e contratação de serviços, levem em consideração o balanceamento de aspectos tais como: riscos, tecnologia, austeridade no gasto, qualidade, velocidade e impacto no negócio, possuindo sistema de proteção redundante para fazer detecção de intrusos.

3.6. **Conscientização**

3.6.1. Tomar medidas para que Órgãos integrados com acesso às informações, ambientes e recursos tecnológicos do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, sejam devidamente conscientizados quanto à Segurança da Informação, face às suas responsabilidades e atuação.

3.7. **Gestão de Ativos**

3.7.1. Assegurar a análise periódica dos ativos da informação (bases de dados e arquivos, contratos e acordos, documentação de sistemas, informações sobre pesquisa, manuais, material de treinamento, procedimentos de suporte ou operação, planos de continuidade de negócios, procedimentos de recuperação, trilhas de auditoria e informações armazenadas) de forma que estejam devidamente inventariados, protegidos, tenham um usuário responsável e tenham mapeadas suas vulnerabilidades e ameaças de segurança.

3.8. **Monitoramento**

3.8.1. Garantir o monitoramento do tráfego de informações efetuado em ambientes e recursos de Tecnologia de Informação e Comunicações, rastreando e identificando possíveis ocorrências de eventos críticos, no estrito interesse da administração do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, obedecendo a legislação aplicável.

3.9. **Gerenciamento das Operações e Comunicações**

3.9.1. Garantir a operação segura e corrente dos recursos do processamento da informação por intermédio da implementação de controles internos de segurança considerando as pessoas, procedimentos, ambientes e tecnologia.

3.10. **Desenvolvimento, Manutenção e Produção de Sistemas**

3.10.1. Assegurar que o desenvolvimento, manutenção, aquisição e adaptação de produtos de mercado e sistemas internos e/ou externos, sejam providos dos requisitos de Segurança necessários para garantir informações confiáveis, íntegras e oportunas.

3.11. **Continuidade das Atividades**

3.11.1. Garantir a continuidade das atividades do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, reduzindo a um período aceitável e factível, a interrupção causada por desastres ou falhas de segurança, por intermédio da combinação de ações de administração de crises, prevenção e recuperação dos serviços.

3.12. **Terceirização ou Prestação de Serviços**

3.12.1. Manter nível de segurança da informação adequado, quanto aos aspectos desta política, naquilo que se refere a responsabilidade pelos procedimentos, sistemas e recursos, terceirizados no todo ou em parte, promovendo auditorias periódicas, buscando o cumprimento dos requisitos de segurança da informação.

3.13. **Conformidade – Leis Regente**

3.13.1. Garantir o cumprimento das leis, regulamentos e normas que regem as atividades do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, de forma a obter máxima aderência aos instrumentos legais e normativos, garantindo o êxito nas exigências regulamentadores.

3.14. **Administração da Segurança da Informação**

3.14.1. Assegurar que a administração da segurança da informação do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, seja feita pelo agente delegado ou por seus prepostos legalmente autorizados, por intermédio de área específica, com responsabilidades de estabelecer, implementar, manter e coordenar a elaboração e revisão da Política de Segurança da Informação, bem como avaliar e analisar assuntos a ela pertinentes.

3.15. **Prevenção e Resposta a Incidentes**

3.15.1. Assegurar que medidas preventivas sejam tomadas com o objetivo de diminuir o risco de ocorrência de fraudes e/ou incidentes que comprometam a segurança da informação, devendo existir canal de comunicação adequado para esse fim.

3.16. **Gestão de Risco**

3.16.1. Fundamentar-se em atividades coordenadas para direcionar e controlar no que se refere aos riscos (risco deve ser entendido como perigo ou possibilidade de perigo, ou seja, a possibilidade de perda ou exposição à perda). Deve ser avaliado como uma combinação da probabilidade de um evento e a sua consequência, portanto, um compromisso entre a probabilidade de um evento e o seu impacto.

3.17. **Propriedade da Informação**

3.17.1. Garantir que toda informação armazenada e em trânsito por meio de tecnologia, procedimentos e ambientes é de sua propriedade, e será usada apenas por usuários devidamente autorizados para fins profissionais, no estrito interesse da Associação.

3.18. **Backup**

3.18.1. Os backups devem ser realizados por sistemas de agendamento. Além dos backups normalmente realizados no servidor, deverá ser feito backup adicional mantido em dispositivo externo com as informações codificadas (criptografadas) em ambiente seguro para armazenagem fora do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, nos termos do disposto no provimento nº 74/2018 do CNJ. A rotina implementada de backup deve estar formalmente documentada para consultas e auditorias.

3.19. **Conformidade – LGPD**

3.19.1. Garantir o cumprimento em seu Programa de Conformidade da LGPD, de forma a obter máxima aderência aos instrumentos legais e normativos, garantindo que os requisitos de segurança sejam cumpridos.

4. Papéis e Responsabilidades

4.1. Compete à área de Segurança da Informação:

4.1.1. Propor controles e melhorias relacionados ao tema de segurança da informação;

4.1.2. Definir e documentar as políticas e procedimentos relacionados à operacionalização da segurança da informação;

4.1.3. Monitorar e analisar os alertas e informações relacionados à segurança das informações;

4.1.4. Apoiar a avaliação e a adequação de controles específicos de segurança da informação para novos sistemas ou serviços;

4.1.5. Testar a eficácia dos controles utilizados e informar aos gestores os riscos residuais;

4.1.6. Disseminar a cultura de Segurança junto às demais áreas da Instituição;

4.1.7. Participar dos projetos em que a área estiver envolvida, acompanhando e sugerindo questões relacionadas ao tema da área;

4.1.8. Proteger as informações contra acessos indevidos e divulgação não autorizada.

4.1.9. Zelar para que os recursos tecnológicos sejam utilizados de forma eficaz, dentro das finalidades e de Conhecimento do Gestor.

4.1.10. Não compartilhar ou divulgar credenciais de acesso ou equipamentos, sem a autorização explícita.

4.1.11. Cumprir as regras estabelecidas na PSI, normas e procedimentos de segurança da informação, bem como as demais leis, regulamentos e normas aplicáveis.

4.1.12. Estar atualizado em relação a esta PSI e aos procedimentos e normas relacionadas, buscando orientação do Gestor sempre que estiver com dúvidas;

4.1.13. Não criar, adquirir ou realizar uso de softwares não homologados ou não autorizados pelo Gestor;

4.1.14. Realizar as cópias de segurança do ambiente tecnológico;

4.1.15. Configurar os equipamentos, ferramentas e sistemas como todos os controles necessários para cumprir os requerimentos de segurança estabelecidos nesta PSI e normas adicionais;

4.1.16. Planejar, implantar, fornecer e monitorar a capacidade de armazenamento, processamento e transmissão, necessárias para ambiente computacional;

4.2. **Compete ao Gestor do Serviço Distrital de São Luiz do Purunã**

4.2.1. Aprovar juntamente com o agente delegado e revisar periodicamente a PSI;

4.2.2. Determinar as diretrizes da Serventia;

4.2.3. Apresentação de assuntos relevantes ao agende delegado, quando cabível;

4.2.4. Reforçar junto à equipe de Segurança da Informação, o cumprimento das diretrizes desta PSI, bem como servir como replicador das boas práticas e controles.

4.2.5. Propor ajustes e ferramentas à área de Segurança da Informação que auxilie nos processos de negócio da área;

4.2.6. Informar, à área de Segurança da Informação, sobre o encerramento de contratos em que os prestadores de serviços possuam qualquer tipo de acesso físico ou lógico às informações;

4.2.7. Contribuir nos processos de revisão periódica de acessos ou em outras situações em que forem acionados pela área de Segurança da Informação.

4.3. **Compete à área Jurídica do Serviço Distrital de São Luiz do Purunã**

4.3.1. Requerer a inserção de cláusulas que obriguem o cumprimento desta PSI, LGPD e demais leis, regulamentos e normas aplicáveis aos prestadores de serviços, cujos contratos tenham sua análise requerida ao departamento, assegurando que as informações sejam utilizadas apenas para sua finalidade dentro do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ** e preservando sua confidencialidade.

4.4. **Compete ao Encarregado de dados**

4.4.1. Elaborar as Políticas de Segurança em conformidade com a LGPD;

4.4.2. Conduzir o Programa de Conformidade da LGPD no **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, zelando pela sua fiscalização;

4.4.3. Monitorar o cumprimento das legislações de proteção de dados pessoais aplicáveis, de acordo com as políticas do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ;**

4.4.4. Orientar os destinatários desta Política quanto ao regime de privacidade e proteção de dados pessoais do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**;

4.4.5. Assegurar que as regras e orientações relativas à proteção de dados sejam informadas e incorporadas nas rotinas e práticas do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**;

4.4.6. Organizar treinamentos sobre proteção de dados pessoais no **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**;

4.4.7. Prestar esclarecimentos, oferecer informações e apresentar relatórios sobre as operações de tratamento de dados pessoais e seus impactos para as autoridades públicas competentes (e.g. Corregedoria do Estado, Ministério Público, Autoridade Nacional de Proteção de Dados Pessoais, etc.);

4.4.8. Responder às solicitações e reclamações de titulares de dados pessoais cujos dados tenham sido objeto de tratamento por uma unidade do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**.

4.4.9. Auxiliar em auditorias ou qualquer outra medida de avaliação e monitoramento envolvendo proteção de dados;

4.4.10. Auxiliar em auditorias ou qualquer outra medida de avaliação e monitoramento envolvendo proteção de dados;

5. Sanções e Punições

5.1. Na hipótese de violação desta PSI ou das normas de segurança da informação, o Gestor determinará as sanções administrativas que serão aplicadas ao infrator, sendo que:

5.1.1. Para os colaboradores, pode acarretar na aplicação de advertência e/ou suspensão ou desligamento formal conforme previsto na Matriz de Penalidades;

5.1.2. Para os prestadores de serviços, pode acarretar na aplicação rescisória imediata do respectivo contrato estabelecido violado.

5.2. A aplicação de sanções e punições será realizada conforme a análise do Gestor de Segurança da Informação, devendo-se considerar a gravidade da infração, efeito alcançado, recorrência e as hipóteses previstas pelas devidas Leis, podendo, no uso do poder, disciplinar que lhe é atribuído, aplicar a pena que entender cabível quando tipificada a falta grave, conforme termo descrito no item 5.1.

5.3. Para o caso de violações que impliquem em atividades ilegais, ou que possam incorrer em dano ao **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**, o infrator será responsabilizado pelos prejuízos, cabendo aplicação das medidas judiciais pertinentes.

6. Casos Omissos

6.1. Os casos omissos serão avaliados pelo Gestor ou Encarregado de Dados para posterior deliberação.

As diretrizes estabelecidas nesta política e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação da área de Segurança da Informação da [NOMESERVENTIA], adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção às informações.

7. Aprovação e atualização da PSI

7.1. Os controles de segurança da informação devem ser planejados, aplicados, implementados e, periodicamente, avaliados de acordo com os objetivos e os riscos.

7.2. Alteração da PSI realizada conforme as seguintes regras.

7.2.1. Ordinariamente a cada 1 ano.

7.2.2. Extraordinariamente sempre que identificada a necessidade.

8. Glossário

8.1. **Ameaça**: ameaça pode ser considerada um agente externo ao ativo de informação, pois, se aproveita de suas vulnerabilidades para quebrar os princípios básicos da informação – a confidencialidade, integridade ou disponibilidade, que pode vir a prejudicar o **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**.

As ameaças podem ser naturais: são aquelas que se originam de fenômenos da natureza; involuntárias: são as que resultam de ações desprovidas de intenção para causar algum dano, e intencionais: são aquelas deliberadas, que objetivam causar danos, tais como *hacker*.

8.2. **Integridade:** Corresponde à preservação da precisão, consistência e confiabilidade das informações e Sistemas ao longo dos processos ou de seu ciclo de vida, fazendo com que circulem ou sejam armazenados do mesmo modo como foram criados, sem que haja interferência externa para corrompê-los, comprometê-los ou danificá-los.

8.3. **Disponibilidade:** Está relacionada ao tempo e acessibilidade que se tem aos dados e Sistemas, ou seja, se eles podem ser consultados a qualquer momento.

8.4. **Confidencialidade:** Relacionado com a privacidade dos dados. Esse conceito se relaciona às ações tomadas para assegurar que informações confidenciais e críticas não sejam roubadas do Sistema por meio de *ciberataques*, espionagem, entre outras práticas. Além disso, a confidencialidade está relacionada ao princípio do "menor privilégio" ou hierarquização, que estabelece acesso apenas a poucas pessoas, no caso, dados para os Órgãos integrados que tenha autorização, conforme a necessidade de conhecimento e o nível de responsabilidade por ele instituído.

Sendo assim, é um princípio com forte política de classificação e cujas seguintes características conferem maior suporte:
Identificação;
Autenticação;
Autorização;
Controles de acesso;
Privacidade;

8.5. **Ativo de informação:** Patrimônio intangível, constituído por suas informações de qualquer natureza, incluindo de caráter estratégico, técnico, administrativo, financeiro, bem como quaisquer informações criadas ou adquiridas por meio de integrações, aquisição via recebimento de atos, o **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ** em formato, físico ou digitalizado, armazenada, trafegada ou transitando pela infraestrutura computacional ou

por infraestrutura externa contratada pela organização, além dos documentos em suporte físico, ou mídia eletrônica transitados dentro e fora de sua estrutura física.

8.6. **Controle:** Medida de segurança adotada para o tratamento de um risco específico.

8.7. **Gestor da Informação:** Usuário da informação que ocupe cargo específico, ao qual foi atribuída responsabilidade sob um ou mais ativos de informação criados, adquiridos, manipulados ou colocados sob a responsabilidade de sua área de atuação.

8.8. **Incidente de segurança da informação:** Um evento ou conjunto de eventos indesejados de segurança da informação que tem possibilidade significativa de afetar as operações ou ameaçar as informações do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ.**

8.9. **Risco de segurança da informação:** Efeito da incerteza sobre os objetivos de segurança da informação do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ.**

8.10. **RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Risco)**

8.11. **Segurança da informação:** A preservação das propriedades de confidencialidade, integridade e disponibilidade das informações do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ**.

8.12. **Vulnerabilidade:** A *NBR ISO/IEC 27002:2005* define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Vulnerabilidade são as fraquezas presentes nos ativos, que podem ser exploradas, seja ela intencionalmente ou não, resultando assim na quebra de um ou mais princípios da segurança da informação. Ao terem sido identificadas as vulnerabilidades ou os pontos fracos, será possível dimensionar os riscos aos quais o ambiente está exposto e assim definir medidas de segurança apropriadas para sua correção.

8.13. **Backup:** Significa Cópia de Segurança, para indicar a existência de cópia de um ou mais arquivos guardados em diferentes dispositivos de armazenamento. Se, por qualquer motivo, houver perda dos arquivos originais, a cópia de segurança armazenada pode ser restaurada para repor os dados perdidos.

8.14. **Lei Geral de Proteção de Dados ("LGPD"):** Diploma normativo (Lei nº 13.709, de 14 de agosto de 2018) que dispõe sobre o tratamento de dados pessoais em meios digitais ou físicos realizados por pessoa natural ou por pessoa jurídica, de direito público ou privado, tendo como objetivo defender os titulares de dados pessoais e ao mesmo tempo permitir o uso dos dados para finalidades diversas, equilibrando interesses e harmonizando a proteção da pessoa humana com o desenvolvimento tecnológico e econômico.

8.15. **Proteção redundante:** Manter sistemas duplicados ou triplicados para garantir a disponibilidade de processos e equipamentos críticos.

8.16. **Autoridade Nacional de Proteção de Dados("ANPD"):** Órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da LGPD em todo território nacional. A ANPD foi instituída pela LGPD como órgão da administração pública federal com autonomia técnica, integrante da Presidência da República, definido a sua natureza como transitória e passível de transformação pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.

8.17. **Dados Pessoal**: Qualquer informação relacionada a pessoa natural, direta ou indiretamente, identificada ou identificável, seja em meio digital ou físico.

8.18. **Dados Pessoal Sensível**: Categoria especial de dados pessoais referentes a origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de carácter religioso, filosófico ou político, referentes à saúde ou à vida sexual, dados genéticos ou biométricos relativos a pessoa natural.

8.19. **Titular do Dado**: Pessoa natural a quem se referem os dados pessoais, tais como antigos, presentes ou potenciais clientes, colaboradores, contratados, parceiros comerciais e terceiros.

8.20. **Tratamento:** Toda operação realizada com dados pessoais, como as que se referem: a coleta, produção, classificação, utilização, acesso, reprodução, transmissão, 6 distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência ou extração.

8.21. **Anonimização**: Processo por meio do qual o dado perde a possibilidade de associação, direta ou indireta, a um indivíduo, considerados os meios técnicos razoáveis e disponíveis no momento do tratamento.

8.22. **Privacidade**: é o direito à reserva de informações pessoais e da própria vida pessoal, pode ser também entendida como a vontade de controlar a exposição e a disponibilidade de informações acerca de si mesmo, o que é chamado de regulação dos limites: a quantidade de controle que um indivíduo exerce sobre a entrada e saída de declarações de si mesmo e a quantidade de contato que se tem com outras pessoas. Esse processo tem implicações diretas no tipo de relação que o indivíduo exerce com e sobre outras pessoas em sua vida.

9. Gestão da Política

9.1. A Política Geral de Segurança da Informação foi elaborada pelo agente delegado do **SERVIÇO DISTRITAL DE SÃO LUIZ DO PURUNÃ** e entra em vigor na data de 14/04/202.

Documento	Política de Segurança da Informação
Tipo de Instrumento Normativo	Política
Categoria do Assunto	Controle e Conformidade
Versão	3
Identificação	[IDENTIFICAÇÃO-PSI.14.4.202]
Elaborada por	Gustavo Felipe Pruche
Posição do elaborador	Encarregado de Dados - DPO

gov.br Documento assinado digitalmente
SERGIO TADEU PUPO
Data: 14/04/2025 11:43:29-0300
Verifique em https://validar.iti.gov.br

Sérgio Tadeu Pupo
Oficial e Tabelião

gov.br Documento assinado digitalmente
GUSTAVO FELIPE PRUCHE
Data: 14/04/2025 11:40:14-0300
Verifique em https://validar.iti.gov.br

Gustavo Felipe Pruche
Encarregado de Dados