PORTARIA N° 0074/2026

O SUPERINTENDENTE DA SUPERINTENDÊNCIA DE OBRAS PÚBLICAS, no uso de suas atribuições legais nos termos do Parágrafo único do art. 15 da Lei nº 11.966, de 17 de Junho de 1992, combinado com os artigos 2º, 9º e 12º do Decreto nº 34.100 de 8º de junho de 2021, **RESOLVE HOMOLOGAR** a **Política de Segurança da Informação e Comunicação – PoSIC/SOP**, para disseminar e garantir o seu cumprimento, se enquadrando aos termos da Política e cumprindo das normas indicadas no aludido Decreto.

1. INTRODUÇÃO

1.1. A Política de Segurança da Informação e Comunicação da Superintendência de Obras Públicas – SOP, foi definida com base nas diretrizes do **Decreto Estadual nº 34.100**, de 08 de junho de 2021, que ***DISPÕE SOBRE A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO DOS AMBIENTES DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO – TIC DO GOVERNO DO ESTADO DO CEARÁ E SOBRE O COMITÊ GESTOR DE SEGURANÇA DA INFORMAÇÃO DO GOVERNO DO ESTADO DO CEARÁ – CGSI, E DÁ OUTRAS PROVIDÊNCIAS***.

1.2. A presente Política de Segurança da Informação e Comunicação (PoSIC) define os princípios, diretrizes e responsabilidades para a proteção das informações tratadas no âmbito da Superintendência de Obras Públicas - SOP, tendo em vista assegurar a confidencialidade, integridade, disponibilidade e autenticidade das informações e dados, bem como o cumprimento das legislações e normas aplicáveis.

1.3. A PoSIC/SOP visa proteger os ativos informacionais do órgão contra acessos indevidos (qualquer dado, sistema, infraestrutura ou recurso, físico ou digital), uso inadequado, divulgação não autorizada, perda ou destruição, promovendo uma cultura organizacional de segurança e privacidade de dados, em conformidade com a Lei Geral de Proteção de Dados (LGPD) nº 13.709/2018, o citado Decreto Estadual nº 34.100/2021, a Lei Estadual nº 18.699/2023, e as Normas NBR ISO/IEC 27001, 27002 e 27005.

1.4. Estes controles precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados, onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atingidos, com foco na Missão, Visão e Valores estabelecidos no Planejamento Estratégico da SOP. Convém que isto seja feito em conjunto com outros processos de gestão do negócio.

1.5. A informação e os processos de apoio, sistemas e redes de computadores são importantes ativos para os negócios da SOP. Definir, alcançar, manter e melhorar a segurança da informação e comunicação são atividades essenciais para assegurar o bom desempenho, o atendimento aos requisitos legais e a imagem da SOP perante a sociedade, bem como aos demandantes da execução de projetos de construção e de manutenção de obras de edificações e de rodovias.

1.6. As organizações, seus sistemas de informação e redes de computadores são expostos a diversos tipos de ameaças à segurança da informação e comunicação, incluindo fraudes eletrônicas, espionagem, sabotagem, vandalismo, incêndio e inundação. Danos causados por código malicioso e hackers estão se tornando cada vez mais comuns, mais ambiciosos e incrivelmente mais sofisticados.

1.7. Lembremos também que a já citada LGPD traz um entendimento de uma nova cultura de privacidade e proteção de dados no país, o que demanda a conscientização de toda a sociedade acerca da importância dos dados pessoais e os seus reflexos em direitos fundamentais. Nesse sentido, a SOP emitiu e publicou em Diário Oficial do Estado de 03 de fevereiro de 2026, a Portaria nº **0041/2026**, que instituiu o **Comitê Setorial de Proteção de Dados Pessoais** e **Encarregado pelo Tratamento de Dados Pessoais da SOP,** na forma dos Art. 9º e 10º da lei Estadual nº 18.699, de 7 de março de 2024;

1.8. Vale ainda destacar que a PoSIC/SOP denota o cumprimento das recomendações exaradas pelo

Tribunal de Contas do Estado, aferidas por meio do Questionário de Auto Avaliação do Controle Interno – Procedimentos de Controle, da Prestação de Contas Anual, bem como a avaliação da SOP pelo Programa Nacional de Gestão Pública e Desburocratização – GesPública, focado em elevar a qualidade da administração pública por meio de modelos gerenciais de excelência e desburocratização.

2. APRESENTAÇÃO DA POLÍTICA

2.1. A Superintendência de Obras Públicas (SOP), apresenta sua Política de Segurança da Informação e Comunicação dos Ambientes de TIC, que visa estabelecer princípios, diretrizes e responsabilidades para a Gestão da Segurança da Informação e Proteção de Dados Pessoais, voltadas ao cumprimento do seu papel como responsável pela elaboração de projetos arquitetônicos e complementares, bem como pela supervisão e fiscalização da execução de todas as obras civis públicas de Edificações e de Rodovias, solicitadas pelas diversas Secretarias e Entidades Públicas que não possuem finalidades construtivas, fortalecendo a gestão pública e o desenvolvimento econômico e social.

2.2. A Política de Segurança da Informação e Comunicação da SOP, definida neste documento, alinha-se à diretriz de Governo de "***Rever e aplicar Políticas da Segurança da Informação e Comunicação do Estado***", elaborada no Planejamento Estratégico da Função Tecnologia da Informação do Governo do Estado do Ceará.

2.3. Dessa forma, nesta política passam a figurar **03 (três) elementos principais**:

a) **Princípios**, que são os fundamentos da Política de Segurança da Informação e Comunicação;
b) **Diretrizes**, que são as regras de alto nível que representam os princípios básicos que o Governo do Estado do Ceará resolveu incorporar a sua gestão e servirão como base para que as normas e os procedimentos sejam criados e detalhados; e
c) **Normas e Procedimentos**, que especificam no plano tático os controles que deverão ser implementados para alcançar a estratégia definida nas diretrizes e servir como base para os procedimentos no plano operacional, constantes da Instrução Normativa a ser expedida.

3. OBJETIVO

3.1. Estabelecer princípios e diretrizes gerais para a gestão da segurança da informação e comunicação dos ambientes de TIC da SOP, de maneira a preservar a integridade, confidencialidade e disponibilidade das informações, posteriormente através de Instrução Normativa descrevendo as normas e procedimentos para o manuseio, controle e proteção das informações contra perdas, alterações, divulgações indevidas e acessos não autorizados.

4. ABRANGÊNCIA

4.1. A Política de Segurança da Informação e Comunicação deverá ser aplicada a todas as áreas, instalações, equipamentos, materiais, documentos, pessoas e sistemas de informação existentes na SOP, inclusive em ambientes remotos, em nuvem ou terceirizados, como também às atividades de todos os servidores, colaboradores, consultores externos, estagiários e prestadores de serviço que exercem atividades no âmbito da Superintendência de Obras Públicas – SOP, ou a quem venha a ter acesso a dados ou informações, incumbindo a cada um a responsabilidade e o comprometimento para a sua aplicação.

4.2. **Diretrizes Gerais da Política de Segurança da Informação e Comunicação da SOP**

a) **Diretrizes do Princípio 1 - Alinhamento Estratégico**

- **Conflitos de negócios:** Na existência de conflito entre os controles de segurança e uma necessidade de negócio específica, o novo cenário de controle deve ser analisado pelo **Comitê de Gestão de Segurança da Informação** da SOP, conforme preconiza o Decreto Estadual nº 34.100 que regulamenta a PoSIC/SOP;
- **Gestão de Riscos:** Os ativos, sistemas, processos, produtos e serviços desenvolvidos, adquiridos, implementados ou disponibilizados da SOP devem ser submetidos a um processo

formal de análise, avaliação e tratamento de riscos, visando atingir o grau de segurança adequado para o Governo do Estado;

- **Gestão de Continuidade**: A SOP deve estabelecer um conjunto de estratégias e planos de ação documentados, testados e revisados periodicamente, de maneira a garantir que os seus serviços essenciais sejam devidamente identificados, preservados e entregues, mesmo diante da ocorrência de um desastre até o retorno à situação normal de funcionamento da Instituição;
- **Auditoria e Conformidade:** A prática da Política de Segurança da Informação e Comunicação da SOP, poderá ser auditada por meio do Comitê Gestor de Segurança da Informação do Governo do Estado, de forma a avaliar a conformidade das ações de seus colaboradores em relação ao estabelecido pela PoSIC/SOP e pela legislação aplicável;
- **Monitoramento**: O acesso e utilização de ambientes físicos, bem como o uso dos equipamentos e sistemas tecnológicos da SOP, poderão ser monitorados pelo Comitê Gestor de Segurança da Informação do Governo do Estado, de forma que ações indesejáveis ou não autorizadas sejam detectadas proativamente;
- **Fortalecer o alinhamento estratégico:** A Política de Segurança da Informação e Comunicação dos Ambientes de TIC é agenda estratégica para o Governo do Estado do Ceará, devendo contemplar diretrizes e metas relacionadas ao tema no planejamento estratégico de cada órgão/entidade para fortalecer o alinhamento entre o planejamento de TIC e o planejamento estratégico da SOP, bem como o do Governo do Estado;
- **Objetivos estratégicos mínimos:** O planejamento estratégico da SOP/2025-2028, que será revisado e adaptado ao próximo Plano Plurianual (PPA), deverá conter no mínimo os objetivos estratégicos de: "Assegurar estruturas e práticas de segurança da informação e comunicação" e "Fortalecer o alinhamento entre o planejamento de TIC, as estratégias da SOP e do Governo do Estado";
- **Responsabilidades dos gestores de TIC e de Ativos TIC**: Os gestores de TIC e de ativos de TIC são responsáveis por acompanhar e seguir as Políticas de Segurança da Informação e Comunicação dos Ambientes de TIC do órgão/entidade e do Governo do Estado do Ceará;
- **Responsabilidades da alta gestão:** A alta gestão formada pelos dirigentes máximos é responsável por acompanhar e seguir a PoSIC da SOP, tendo como referência: Prover os recursos necessários à PoSIC; Promover o desenvolvimento de Políticas de Segurança da Informação e Comunicações dos Ambientes de TIC; Estimular a adoção de práticas de governança de segurança da informação e comunicações;
- Implementar práticas de gerenciamento de riscos e continuidade de negócios.

4.3. **Objetivos Estratégicos relacionados às Diretrizes do Princípio 1 - Alinhamento Estratégico:**

a) **Objetivo Estratégico:** Desenvolver e implantar uma Política de Segurança da Informação e Comunicação na SOP.

- **Ações Prioritárias**
- Adotar mecanismos para promover a elaboração, revisão, atualização, divulgação, conscientização e validação dos princípios, diretrizes, normas e procedimentos da Política de Segurança da Informação e Comunicação nos órgãos/entidades estaduais;
- Elaborar plano estratégico de segurança da informação e comunicação para viabilizar todos os recursos necessários para o cumprimento das Políticas de Segurança da Informação e Comunicação;
- Selecionar mecanismos de segurança da informação e comunicação considerando fatores de riscos, tecnologias e custos;
- Criar grupo responsável pela elaboração, implantação, acompanhamento, auditoria e revisão da Política de Segurança da Informação e Comunicação;
- Criar o Comitê de Gestão de Segurança da Informação para coordenar a política de segurança da informação e comunicação da SOP; e
- Estabelecer mecanismos que possibilitem o processo de coleta, recuperação, análise e

correspondência de dados para investigação de questões cíveis, criminais e administrativas, para proteger os usuários e recursos de TIC.

b) **Objetivo Estratégico:** Comunicar oficialmente e orientar os usuários na Política de Segurança da Informação e Comunicação dos Ambientes de TIC adotada pela SOP, para garantir a conscientização e a prática.
   - **Ações Prioritárias:**
   - Definir mecanismos para garantir a disseminação da cultura de segurança da informação e comunicação na SOP;
   - Estabelecer medidas para que a política de segurança da informação e Comunicação dos Ambientes de TIC seja cumprida de forma que as diretrizes, normas e procedimentos de segurança sejam aplicados por todos os usuários; e
   - Prover mecanismos de orientação nos procedimentos de segurança e uso correto dos recursos de TIC para todos os usuários.

c) **Diretrizes do Princípio 2 - Diversidade Organizacional**
   - **Alinhamento da política de segurança da informação e comunicação:** A política de segurança da informação e comunicação da SOP deve estar alinhada com a política de segurança da informação e Comunicação dos Ambientes de TIC do Governo do Estado do Ceara;
   - **Natureza e finalidade das atividades:** Deve ser respeitada a natureza e finalidade das atividades de cada órgão/entidade, quanto à elaboração de Políticas, Normas, Procedimentos e controles de segurança corporativa;
   - **Leis e regimentos:** A Política de Segurança da Informação e comunicação deve respeitar as leis e regimentos inerentes à SOP.

4.4. **Objetivos Estratégicos relacionados as Diretrizes do Princípio 2 - Diversidade Organizacional:**

a) **Objetivo Estratégico:** Desenvolver e implementar plano de contingência e respostas a incidentes, considerando a diversidade das atividades das Instituições, respeitando a natureza e finalidade de cada órgão/entidade de forma a assegurar a continuidade do negócio, bem como o seu reestabelecimento em situação de anormalidade.
   - **Ações Prioritárias**
   - Definir os processos e recursos críticos realizando análise de impacto de riscos para elaboração do plano de continuidade do negócio;
   - Estabelecer processos de proteção contra falhas e danos que comprometam as atribuições do Governo do Estado do Ceará;
   - Definir mecanismos formais e periodicamente testados para garantir a continuidade das atividades críticas e o retorno à situação de normalidade; e
   - Definir processo e criar procedimentos para gestão de incidentes.

b) **Diretrizes do Princípio 3 - Garantia da Segurança das Informações**
   - **Responsabilidade e Comprometimento:** Todos os colaboradores da SOP, em qualquer vínculo, função ou nível hierárquico, são responsáveis pela proteção e salvaguarda dos ativos físicos, tecnológicos e informações de que sejam usuários, dos ambientes físicos e computacionais a que tenham acesso, independente das medidas de segurança implementadas;
   - **Segurança das Comunicações:** Garantir a segurança das comunicações entre a SOP e entidades que compõem o Governo do Estado;
   - **Controle de Acessos:** Os acessos aos ambientes físicos e computacionais devem ser controlados, registrados e monitorados, com base na necessidade de conhecer ações desenvolvidas e do privilégio de acesso mínimo para o desempenho das atividades profissionais;
   - **Notificação, Registro e Tratamento de Incidentes:** Todos os colaboradores da SOP, em

qualquer vínculo, função ou nível hierárquico têm a obrigação de reportar imediatamente, por meio dos processos definidos na autarquia, quaisquer incidentes de segurança que tomarem conhecimento, de modo que possam ser registrados, avaliados e tratados;

- **Treinamento e Conscientização:** Todos os colaboradores devem conhecer a Política de Segurança da Informação e Comunicação da SOP e serem orientados regularmente por meio de campanhas de conscientização e treinamentos, de acordo com suas funções, garantindo assim maior efetividade e eficácia das ações de segurança da Informação e comunicação;
- **Revisão e análise crítica:** Os conjuntos de documentos que compõem a PoSIC/SOP devem passar por revisões e análises críticas periódicas em no máximo 4 (quatro) anos, ou sempre que ocorrer fato ou evento relevante que motive sua revisão antecipada;
- **Proteção Física:** Toda proteção física deve ser compatível com o risco identificado.
- **Ameaças Externas:** Deve ser estabelecida também a proteção contra ameaças externas e do meio ambiente, como proteção contra incêndios e enchentes ou outras formas de desastres naturais;
- **Cópias de Segurança:** Gerar no mínimo cópias de segurança dos dados classificados como críticos e sua respectiva restauração em tempo aceitável, a fim de não prejudicar o bom andamento das atividades da SOP com uso preferencial do ambiente de nuvem.
- **Suporte jurídico:** A implantação de uma Política de Segurança da Informação e Comunicação deve contar com suporte jurídico ou de profissionais qualificados sobre os aspectos legais e seus requisitos.

4.5. **Objetivos Estratégicos relacionados às Diretrizes do Princípio 3 - Garantia da Segurança das Informações:**

a) **Objetivo Estratégico:** Definir procedimentos de rotina para a execução de cópias de segurança e disponibilização dos recursos de reserva.

b) **Ações Prioritárias**

- Implantar rotina de backup (cópias), armazenamento, testes de integridade e recuperação de dados (restore) preferencialmente utilizando o ambiente de nuvem;
- Implantar normas e responsabilidades sobre o controle das mídias de software.

c) **Objetivo Estratégico:** Garantir de forma segura o acesso e manuseio das informações no âmbito da SOP.

d) **Ações Prioritárias**

- Definir normas e procedimentos de acesso a dados, informações e conhecimentos por pessoas da SOP, por outros órgãos/entidades e terceiros.

e) **Objetivo Estratégico:** Assegurar que os sistemas de informações em operação e em implantação, possuam documentação suficiente para garantir sua manutenção, instalação e utilização.

f) **Ações Prioritárias**

- Definir e implantar metodologias de desenvolvimento de sistemas implementando requisitos de segurança;
- Implantar a cultura de documentação de sistemas de processamento como manuais técnicos e operacionais, e
- Definir procedimentos para controle de liberação de ativos de TIC.

g) **Objetivo Estratégico:** Garantir que apenas pessoas autorizadas tenham acesso a funcionalidades e informações dos sistemas de processamento.

h) **Ações Prioritárias**

- Manter controle de acesso a todos os sistemas utilizando identificação de uso pessoal e intransferível e com validade estabelecida, que permita de maneira clara o seu reconhecimento;
- Prever trilhas de auditoria nos sistemas de processamento críticos, e
- Definir controles para que usuários tenham acesso apenas aos recursos necessários e imprescindíveis ao desenvolvimento do seu trabalho.

i) **Diretrizes do Princípio 4 - Propriedade da informação**

- **Uso de Correio:** Assegurar que o uso do Correio Eletrônico institucional seja disciplinado, ficando claro para os usuários o conceito de não privacidade no seu uso, sendo utilizado preferencialmente serviços em nuvem;
- **Uso da internet:** Assegurar que o acesso à Internet, provido pelo Governo do Estado, seja disciplinado, ficando claro para os usuários o conceito de não privacidade no seu uso;
- **Proprietários e Ativos de TIC:** Os ativos de TIC devem ser identificados, assim como seus respectivos colaboradores responsáveis, devendo ser atribuída a responsabilidade pela manutenção da sua segurança. A emissão dos Termos de Responsabilidade é de competência da área de Gestão Patrimonial de Bens Móveis;
- **Informações sensíveis:** Funcionários com acesso a informações sensíveis devem ser adequadamente analisados antes da liberação de acesso.

j) **Direitos de Acesso:** Deve ser prevista também uma forma de retirar direitos de acesso e de devolução de ativos, caso o vínculo empregatício do colaborador (funcionário, terceirizado ou comissionado) seja encerrado. A administração dos Direitos de Acesso deve ser preferencialmente sistematizada e gerida pela área de Gestão de Pessoas.

k) **Informações Críticas:** O processamento de informações críticas ou sensíveis deve ser mantido em áreas seguras, com controle de acesso apropriado, preferencialmente em ambiente de nuvem.

l) **Acessibilidade, Disponibilidade e Integridade**: Garantir a acessibilidade, disponibilidade e integridade das informações para o acesso público.

m) **Interoperabilidade:** Viabilizar a interoperabilidade e acessibilidade entre os órgãos e entidades que compõem o Governo do Estado.

n) **Certificação Digital:** Incentivar e apoiar o estudo e implantação de soluções de segurança e certificação digital, observando o cumprimento de requisitos de segurança mínimos e a interoperabilidade entre a SOP e os órgãos e entidades que compõem o Governo do Estado, sendo essas soluções baseadas preferencialmente em código aberto quando aplicável.

4.6. **Objetivos Estratégicos relacionados às Diretrizes do Princípio 4 - Propriedade da informação:**

a) **Objetivo Estratégico:** Estabelecer que as condições e termos de licenciamento de softwares e direitos de propriedade intelectual devam ser respeitados.

b) **Ações Prioritárias**

- Definir normas para instalação de softwares com objetivo de combater o uso de cópia ilegal;
- Garantir o controle das licenças de softwares utilizados pela SOP;
- Adotar procedimentos para que a instalação e uso de softwares e sistemas computacionais, devam ser homologados e autorizados pela SOP/GETEC, e
- Definir mecanismos para cessão de softwares e sistemas computacionais no âmbito do Governo do Estado do Ceará.

c) **Objetivo Estratégico:** Adotar critérios relacionados ao uso de ativos de TIC na SOP.

d) **Ações Prioritárias**

- Manter os ativos de TIC críticos em áreas seguras e adequadas, protegidos contra perigos ambientais e com implantação de controles de acesso, preferencialmente utilizando o ambiente de nuvem;
- Inventariar os ativos, classificando-os quanto à importância, prioridade e nível de proteção;
- Proteger os ativos de TIC de possível roubo e modificação, definindo controles e monitoramentos de forma a minimizar a perda ou dano;
- Adotar controles de acesso físico e lógico para uso de ativos no âmbito da SOP, alinhados às competências da gestão patrimonial de bens móveis;
- Estabelecer processos de aquisição de bens e serviços baseados em preceitos legais;
- Aprimorar e/ou definir critérios de seleção, movimentação ou desligamento de pessoal que impactam na segurança da informação e comunicação, e
- Implementar mecanismos de registro de históricos dos ativos de TI, garantindo a sua

rastreabilidade.

e) **Objetivo Estratégico:** Estabelecer responsabilidades e requisitos básicos de utilização da Internet e correio eletrônico no âmbito da SOP.

f) **Ações Prioritárias**
- Elaborar plano de comunicação para conscientização de que o uso da internet e correio eletrônico não é um direito e sim uma concessão;
- Disseminar o conceito de não privacidade do uso da Internet e correio eletrônico.

g) **Objetivo Estratégico:** Assegurar que todos os usuários ao utilizarem esses serviços deverão fazê-los no estrito interesse da SOP, mantendo uma conduta profissional, especialmente em se tratando da utilização de bem público.

h) **Ações Prioritárias**
- Implantar mecanismos de autenticação e monitoramento, que determinem a titularidade de todos os acessos à Internet e correio eletrônico, e
- Criar mecanismos de controle da demanda e da disponibilidade, garantindo a qualidade do serviço.

4.7. **Diretrizes do Princípio 5 - Alinhamento com os aspectos legais**

a) **Conformidade Legal – Aderência às leis:** Assegurar que a SOP cumpra e façam cumprir as leis que vigoram no país, em especial as leis de combate à pedofilia, preconceito racial, o Estatuto da Criança e do Adolescente, pirataria de software e do direito autoral, de proteção a grupos historicamente vulnerabilizados, com foco em direitos humanos e proteção social;

b) **Conformidade Legal - A gestão da segurança da informação e comunicação:** Deve atender aos requisitos legais dos órgãos regulatórios de segurança da informação e comunicação do Governo Municipal, Estadual e Federal, assim como, às normas ABNT de segurança da informação, aplicáveis ao negócio da instituição.

c) **Conformidade Legal - Cumprimento do decreto estadual vigente:** Devem ser adotadas medidas para o cumprimento do decreto estadual vigente, que estabelece a Política de Segurança da Informação e Comunicação dos Ambientes de TIC para o Governo do Estado do Ceará.

d) **Conformidade Legal -** Aderência às normas técnicas e boas práticas: Deve-se buscar aderência às normas técnicas e boas práticas que regem a Gestão da Segurança da Informação e Comunicação. Serão consideradas as legislações específicas aplicadas à SOP.

e) **Classificação e Tratamento da Informação:** Todas as informações e os respectivos recursos tecnológicos que as suportam devem ser classificados de acordo com seu grau de sigilo e receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida. A Classificação de Informação como sigilosa ou reservada será definida pelo Comitê Setorial de Proteção de Dados Pessoais e do Encarregado pelo Tratamento de Dados Pessoais da SOP.

f) **Acesso às informações de TIC:** O acesso às informações de TIC deverá ser fornecido mediante pedido formal, e seu andamento deverá estar em conformidade com a Lei de Acesso à Informação (LAI).

g) **Pedidos de acesso a informações de TIC:** Não serão atendidos pedidos de acesso a informações de TIC classificadas como sigilosas, excetuando-se os casos em que a legislação prevê.

h) **As informações classificadas como sigilosas:** As informações classificadas como sigilosas para o acesso do cidadão, podem ser fornecidas em casos de auditoria (§ 1º, inciso II, art. 3°, da Lei n° 13.325, de 14.07.03).

i) Especificações técnicas de sistemas informatizados: As informações referentes a especificações técnicas de sistemas informatizados, diretórios de rede, servidores, bancos de dados e redes (por ex.: casos de uso, código-fonte, diagramas de banco de dados, dicionário de dados etc) são classificadas como sigilosas independente do órgão ou entidade que produza ou possua a sua guarda. (§ 1º, inciso V, art. 1°, da Portaria CGAI nº 01/2016).

j) **Referências Legais:**
- Lei de Acessibilidade, Lei nº 13.146, de 2015;

- Lei de Acesso a Informação (LAI), Lei nº 12.527, de 2011;
- Marco Civil da Internet, Lei nº 12.965, de 2014, e Decreto nº 8.771, de 2016;
- Lei Antipirataria, Lei nº 9.609, de 1998;
- Lei de Pornografia Infantil, Lei nº 8.069, de 1990;
- Lei de Crimes Cibernéticos, Leis nº 12.735, de 2012, e 12.737, de 2012;
- Lei Geral de Proteção de Dados do Brasil (LGPD), Lei nº 13.709, de 2018;
- Lei Estadual nº 18.699/2024, que estabelece o Modelo de Governança da Proteção de Dados Pessoais no âmbito do Poder Executivo Estadual;
- Norma ABNT NBR ISO/IEC 27001:2022/2024 – Tecnologia da Informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação;
- Norma ABNT NBR ISO/IEC 27005:2023 – Tecnologia da Informação – Técnicas de segurança – Gestão de Riscos de Segurança da Informação;
- NIST Cybersecurity Framework (CSF) – Referência para detecção, proteção, resposta e recuperação de incidentes cibernéticos.

4.8. **Objetivos Estratégicos relacionados às Diretrizes do Princípio 5 - Alinhamento com os aspectos legais:**

a) **Objetivo Estratégico:** Fortalecer metodologia de classificação de informações e conhecimentos no âmbito da SOP.

b) **Ações Prioritárias**

- Desenvolver processo de classificação da informação para definir níveis e critérios adequados; e
- Estabelecer normas, padrões e procedimentos relacionados à produção, tramitação, transporte, manuseio, custódia, armazenamento, conservação, eliminação e cessão de documentos no âmbito da SOP.