CEARÁ
GOVERNO DO ESTADO
VICE-GOVERNADORIA

Política de Segurança da Informação, Governança de Dados e Uso de Inteligência Artificial – Assessoria Especial da Vice-Governadoria

Índice

CEARÁ
GOVERNO DO ESTADO
VICE-GOVERNADORIA

Glossário de Termos e Siglas

- **ANPD** — Autoridade Nacional de Proteção de Dados. Órgão da administração pública federal responsável por zelar, implementar e fiscalizar o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD).
- **API** — Application Programming Interface (Interface de Programação de Aplicações). Conjunto de rotinas e padrões que possibilitam a comunicação entre sistemas e aplicações.
- **CFTV** — Circuito Fechado de Televisão. Sistema de monitoramento por vídeo utilizado para segurança patrimonial e controle de acesso.
- **CGE** — Controladoria Geral do Estado. Órgão responsável por atividades de controle interno, auditoria e transparência administrativa.
- **CIDA** — Confidencialidade, Integridade, Disponibilidade e Autenticidade. Conjunto de princípios fundamentais da segurança da informação.
- **CSPD** — Comitê Setorial de Proteção de Dados. Instância institucional responsável por acompanhar e orientar ações relacionadas à proteção e governança de dados.
- **CTIGI** — Coordenadoria de Tecnologia da Informação, Governança e Inovação. Unidade responsável pela gestão da infraestrutura tecnológica, governança digital e segurança da informação no âmbito institucional.
- **DevSecOps** — Development, Security and Operations. Abordagem que integra práticas de desenvolvimento, segurança e operações no ciclo de vida dos sistemas.
- **DPO** — Data Protection Officer (Encarregado de Dados). Agente responsável por atuar como canal de comunicação entre a instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados.
- **Enap** — Escola Nacional de Administração Pública. Instituição responsável pela formação e capacitação de agentes públicos.
- **Git** — Sistema de controle de versão distribuído utilizado para gerenciamento e rastreabilidade de alterações em códigos-fonte e documentos técnicos.
- **IA** — Inteligência Artificial. Conjunto de tecnologias computacionais capazes de executar tarefas que simulam capacidades humanas de análise, aprendizagem ou tomada de decisão.
- **IPS** — Intrusion Prevention System (Sistema de Prevenção de Intrusão). Solução de segurança destinada à identificação e bloqueio de atividades maliciosas em redes e sistemas.
- **ISO 27001** — Norma internacional que estabelece requisitos para implementação de Sistema de Gestão de Segurança da Informação (SGSI).
- **LGPD** — Lei Geral de Proteção de Dados Pessoais (Lei Federal nº 13.709/2018). Norma que dispõe sobre o tratamento de dados pessoais e a proteção dos direitos dos titulares.
- **NIST** — National Institute of Standards and Technology. Instituto responsável por desenvolver padrões e diretrizes técnicas, incluindo referenciais em cibersegurança.
- **OWASP** — Open Web Application Security Project. Projeto internacional que estabelece boas práticas e orientações para segurança em aplicações web.
- **OWASP Top 10** — Documento que lista as dez vulnerabilidades mais críticas em aplicações web, utilizado como referência para desenvolvimento seguro.
- **SQL** — Structured Query Language (Linguagem Estruturada de Consulta). Linguagem utilizada para manipulação e consulta de bancos de dados relacionais.

- **SSL/TLS** — Secure Sockets Layer / Transport Layer Security. Protocolos criptográficos utilizados para garantir a confidencialidade e integridade das comunicações em rede.
- **TI** — Tecnologia da Informação. Área responsável pelo gerenciamento de sistemas, infraestrutura computacional e serviços tecnológicos.
- **TIC** — Tecnologia da Informação e Comunicação. Conjunto de recursos tecnológicos voltados ao armazenamento, processamento e transmissão de informações.
- **WAF** — Web Application Firewall. Firewall especializado na proteção de aplicações web contra ataques e vulnerabilidades conhecidas.
- **XSS** — Cross-Site Scripting. Tipo de vulnerabilidade de segurança que permite a execução indevida de scripts em aplicações web.
- **SPAM** — Sending and Posting Advertisement in Mass (Enviar e Postar Publicidade em Massa).
- **SQL Injection** — É uma vulnerabilidade de segurança onde atacantes inserem comandos SQL maliciosos em campos de entrada de uma aplicação.
- **ISO** — International Organization for Standardization (Organização Internacional de Normalização).
- **FAQs** — Frequently Asked Questions (Perguntas Frequentes).
- **CE** — Ceará.
- **e.g.** — Exempli Gratia (Abreviação em latim que significa "por exemplo").
- **Post-mortem** — Documento ou reunião retrospectiva realizada após um incidente.
- **OpenAI** — Empresa e laboratório de pesquisa de inteligência artificial (IA) estadunidense.

1. Apresentação

A Assessoria Especial da Vice-Governadoria do Estado do Ceará, no exercício de sua função institucional de articulação, integração e monitoramento de políticas públicas e ações estratégicas demandadas pelo Governo, estabelece a presente política. Este documento é o pilar para a proteção dos ativos institucionais, a garantia da continuidade dos serviços públicos e a promoção de uma gestão ética, transparente e confiável. A Segurança da Informação, a Governança de Dados e o uso responsável da Inteligência Artificial (IA) são reconhecidos como componentes indissociáveis da infraestrutura tecnológica e operacional da Assessoria Especial da Vice-Governadoria.

Este instrumento normativo consolida princípios, diretrizes e práticas mandatórias de Segurança da Informação e Governança de Dados, além de estabelecer parâmetros estratégicos para o uso de Inteligência Artificial, em consonância com as melhores práticas nacionais e internacionais (e.g., ISO 27001, diretrizes do NIST). As diretrizes específicas relativas à IA serão detalhadas em documento complementar — a Política Interna de Uso de Inteligência Artificial —, que será submetida a revisões contínuas para acompanhar a evolução tecnológica, regulatória e as melhores práticas de mercado, especificamente no contexto da Lei Estadual nº 17.611/2021 (CE).

2. Objetivo

Esta política visa alcançar os seguintes objetivos estratégicos e operacionais:

- **Assegurar a Confidencialidade, Integridade, Disponibilidade e Autenticidade (CIDA)** das informações sob responsabilidade da Assessoria Especial da Vice-Governadoria, através da implementação de controles rigorosos e contínuos, alinhados aos princípios da segurança da informação.
- **Promover a Governança de Dados** através da implementação de um *framework* robusto que inclua a classificação, o gerenciamento do ciclo de vida e a gestão adequada de todos os ativos de informação, desde a sua criação até o descarte final, em conformidade com as diretrizes da Lei Federal nº 13.709/2018 (LGPD) e da Lei Estadual nº 18.699/2024 (CE).
- **Definir e atribuir responsabilidades claras** para a proteção, manuseio e uso de dados, informações e sistemas da Assessoria Especial da Vice-Governadoria, garantindo a responsabilização em todos os níveis hierárquicos e operacionais, conforme previsto nas legislações de proteção de dados.
- **Estabelecer princípios gerais para o uso ético, seguro, transparente e auditável da Inteligência Artificial**, assegurando que todas as implementações de IA estejam em estrita conformidade com a legislação aplicável e os direitos fundamentais, em particular a Lei Estadual nº 17.611/2021 (CE).

- **Garantir a conformidade legal e regulatória** com a Lei Geral de Proteção de Dados (LGPD – Lei Federal nº 13.709/2018), a Lei Estadual nº 18.699/2024 (que institui o Sistema Estadual de Proteção de Dados Pessoais) e a Lei Estadual nº 17.611/2021 (que regulamenta o uso de IA no Ceará), além de outras normas e regulamentos pertinentes à Administração Pública Estadual, incluindo a Política de Segurança da Informação e Proteção de Dados Pessoais da ETICE (2024), quando aplicável.

3. Abrangência

As disposições desta política são de cumprimento obrigatório e se aplicam a:

- **Todo o corpo funcional da Assessoria Especial da Vice-Governadoria**, incluindo servidores efetivos, comissionados, colaboradores terceirizados, estagiários, prestadores de serviço, fornecedores e quaisquer terceiros que, porventura, venham a ter acesso a informações, sistemas, serviços ou recursos tecnológicos da Assessoria Especial da Vice-Governadoria, com base nos princípios de responsabilidade e segurança da informação.
- **Todos os dados, informações e sistemas** que estejam sob a responsabilidade institucional da Assessoria Especial da Vice-Governadoria, independentemente do meio de armazenamento ou processamento, abarcando ambientes internos (*on-premises*), ambientes de nuvem (pública, privada ou híbrida) e soluções fornecidas por terceiros, seguindo as diretrizes de segurança da informação e governança de dados.
- **Todas as iniciativas, projetos e sistemas** que envolvam o uso de tecnologias de Inteligência Artificial, desde a fase de concepção até a implementação e desativação, independentemente de sua finalidade, complexidade ou estágio de desenvolvimento, em conformidade com a Lei Estadual nº 17.611/2021 (CE) e a futura Política Interna de Uso de Inteligência Artificial.

4. Princípios

Esta política é fundamentada nos seguintes princípios, que orientam todas as ações e decisões relacionadas à segurança da informação, governança de dados e uso de IA:

4.1. Confidencialidade: Assegurar que o acesso às informações seja restrito apenas a indivíduos, entidades ou processos devidamente autorizados, conforme o princípio do menor privilégio e as boas práticas da ISO 27001.

4.2. Integridade: Proteger as informações contra alterações não autorizadas, acidentais ou intencionais, garantindo sua precisão, completude e consistência ao longo de seu ciclo de vida, em alinhamento com os pilares da segurança da informação.

4.3. Disponibilidade: Garantir que as informações e os sistemas estejam acessíveis e operacionais para usuários autorizados sempre que necessário, de acordo com os requisitos de negócio e serviço, e com a resiliência prevista em planos de continuidade.

4.4. Transparência: Promover a clareza e a acessibilidade das informações sobre as ações de proteção de dados, governança de dados e uso de IA, especialmente no que tange aos cidadãos e órgãos de controle, em atendimento aos preceitos da LGPD.

4.5. Responsabilidade: Estabelecer que todos os indivíduos e entidades abrangidos por esta política são corresponsáveis pela sua observância e pelo cumprimento das diretrizes nela contidas, com as respectivas responsabilizações em caso de falha, conforme a Lei Complementar Estadual nº 98/2011 (CE) e demais normas.

4.6. Propriedade da Informação: Reiterar que toda informação institucional produzida, tratada ou armazenada no âmbito da Assessoria Especial da Vice-Governadoria é patrimônio informacional do Estado do Ceará, sendo de sua exclusiva propriedade e uso para fins institucionais, respeitado os direitos dos titulares dos dados pessoais.

4.7. Ética e Direitos Fundamentais: O uso de dados e de Inteligência Artificial deve respeitar a dignidade humana, a não discriminação, a privacidade, a liberdade de expressão e a responsabilidade social, evitando vieses e preconceitos. Tal diretriz encontra respaldo nos valores institucionais da Assessoria Especial da Vice-Governadoria, que incluem ética, integridade, inclusão e transparência (Art. 3º, Decreto nº 36.619/2025). Além disso, o Regulamento atribui à Assessoria de Controle Interno e Ouvidoria a responsabilidade de garantir o funcionamento da Comissão Setorial de Ética Pública e do Comitê Setorial de Proteção de Dados (Art. 8º, IX, b), e à Coordenadoria de Tecnologia da Informação, Governança e Inovação a obrigação de assegurar a conformidade dos serviços com a legislação vigente, preservando a segurança, integridade e disponibilidade dos dados (Art. 13, IX e XXVIII).

4.8. Alinhamento Estratégico: Garantir que a gestão da informação e o uso de IA estejam alinhados aos objetivos estratégicos da Assessoria Especial da Vice-Governadoria, contribuindo para a eficiência operacional, a inovação e o fortalecimento da confiança do cidadão nos serviços públicos.

4.9. Garantia da Segurança das Informações: Adotar um conjunto abrangente de medidas de segurança que visem à proteção de dados contra acessos indevidos, perda, destruição ou alteração, focando na resiliência e na recuperação de desastres.

4.10. Conformidade Legal e Regulatória: Assegurar que todas as ações e procedimentos estejam em consonância com as legislações vigentes e os demais regulamentos específicos aplicáveis à Administração Pública Estadual e às melhores práticas.

Dessa forma, a aplicação desses princípios harmoniza-se com a Lei Federal nº 13.709/2018 (LGPD) e a Lei Estadual nº 17.611/2021 (CE).

5. Diretrizes Gerais

As seguintes diretrizes gerais estabelecerão o framework para a implementação das políticas de segurança da informação, governança de dados e uso de inteligência artificial: A Assessoria Especial da Vice-Governadoria implementará e manterá os seguintes controles técnicos e organizacionais:

5.1 Segurança da Informação

- **Controle de Acesso Lógico:** Todo acesso a sistemas, redes e informações deve ser explicitamente autorizado, individualizado, registrado, monitorado e revisado periodicamente, seguindo o princípio do menor privilégio e da necessidade de saber, conforme as recomendações da ISO 27001 e do NIST.
- **Gestão de Incidentes de Segurança:** Deverão ser estabelecidos e formalizados fluxos para a comunicação imediata, registro, análise, resposta, contenção, erradicação e recuperação de incidentes de segurança da informação, com relatórios *post-mortem* e lições aprendidas, alinhado ao NIST Cybersecurity Framework e às exigências da LGPD em relação a notificação de incidentes de segurança.
- **Monitoramento e Auditoria de Acessos:** Registros detalhados de todos os acessos e operações críticas em sistemas e redes deverão ser mantidos e armazenados de forma segura para fins de auditoria, em aderência às normativas de segurança.
- **Segurança em Redes e Sistemas:** Implementação e manutenção contínua de *firewalls* (incluindo *Web Application Firewalls - WAF*), segmentação de redes, sistemas de detecção e prevenção de intrusão (*IPS*), antivírus, e programas de gestão de vulnerabilidades e *patches*, assegurando a atualização constante de sistemas operacionais e aplicações.
- **Segurança Física e Ambiental:** Controle rigoroso de acesso a áreas críticas, como *datacenters*, *racks* de servidores e salas técnicas, através de barreiras físicas (portas de segurança, biometria), sistemas de *CFTV* e monitoramento ambiental (temperatura, umidade, detecção de incêndio), em conformidade com as normas de segurança física da ISO 27001.
- **Confidencialidade Contratual:** Todos os contratos celebrados pela Assessoria Especial da Vice-Governadoria, cujos objetos envolvam o tratamento de informações sensíveis ou estratégicas, deverão conter cláusulas de confidencialidade explícitas e obrigações de conformidade com as normas de segurança da informação por parte de empresas fornecedoras e seus colaboradores, em atendimento às exigências da LGPD e demais legislações aplicáveis.

5.2 Governança de Dados

A governança de dados institucional será orientada pelos seguintes pontos:

- **Classificação da Informação:** Implementação de um sistema de classificação formal das informações (e.g., pública, restrita, confidencial e ultra confidencial), baseado no impacto potencial em caso de divulgação não autorizada, com diretrizes claras para cada nível, alinhado às melhores práticas de gestão da informação.
- **Ciclo de Vida da Informação:** Estabelecimento de controles de segurança em todas as fases do ciclo de vida da informação: criação, coleta, uso, compartilhamento, armazenamento, arquivamento, retenção e descarte seguro, em conformidade com as políticas de retenção de dados e a legislação pertinente, em particular a LGPD e a Lei Estadual nº 18.699/2024 (CE).
- **Comitê Setorial de Proteção de Dados (CSPD):** Criação e manutenção de um Comitê Setorial de Proteção de Dados com atribuições formais para acompanhar a implementação desta política, propor diretrizes para aprimoramento da governança de dados, promovendo a responsabilização e a eficiência no tratamento das informações, em alinhamento com a estrutura prevista na Lei Estadual nº 18.699/2024 (CE).
- **Mapeamento e Inventário de Dados:** Desenvolver e manter um inventário detalhado de todos os dados e sistemas que os tratam, incluindo a finalidade do tratamento, base legal, categorias de dados pessoais e o fluxo da informação, conforme exigido pela **LGPD**.
- **Qualidade de Dados:** Estabelecer processos para garantir a qualidade, precisão e atualização dos dados.
- **Segurança e Proteção de Dados Pessoais:** Implementar mecanismos robustos para a proteção de dados pessoais, desde a anonimização e pseudonimização (sempre que possível) até a criptografia, garantindo o cumprimento integral da LGPD e demais legislações aplicáveis, com base nos princípios de privacidade por design e por *default*.
- **Compartilhamento de Dados:** Regularizar o compartilhamento de dados com órgãos externos, assegurando a formalização de termos de cooperação técnica ou convênios, com cláusulas explícitas sobre segurança, finalidade e responsabilidades, em estrita observância à LGPD e outras normativas de compartilhamento de dados na Administração Pública.

5.3 Uso de Inteligência Artificial

O uso de Inteligência Artificial (IA) pela Assessoria Especial da Vice-Governadoria será orientado pelos princípios de ética, transparência, supervisão humana e conformidade legal, assegurando que todas as práticas estejam alinhadas às normas vigentes de proteção de dados, segurança da informação e governança digital.

5.3.1. Responsabilidade e segurança da informação

- É vedado inserir ou compartilhar dados sensíveis, estratégicos ou internos da organização (tais como documentos oficiais, informações pessoais de servidores, contratos, pareceres, bases de dados institucionais, códigos-fonte proprietários, chaves de API ou credenciais) em ferramentas de IA abertas ou não contratadas oficialmente pelo Governo do Estado.

- Os colaboradores devem adotar postura preventiva e criteriosa quanto ao conteúdo utilizado em interações com IAs, considerando a confidencialidade e o risco de vazamento de informações institucionais.

5.3.2. Uso de ferramentas institucionais e seguras

- Sempre que possível, deverá ser dada preferência ao uso de ferramentas de IA integradas aos pacotes tecnológicos já contratados e homologados pela Vice-Governadoria ou por órgãos centrais do Estado, tais como Microsoft (Copilot), Google (Gemini), OpenAI (via ambientes corporativos) ou soluções internas desenvolvidas sob supervisão da área de TI.

5.3.3. Ética, transparência e supervisão humana

- As decisões e produtos resultantes do uso de IA devem sempre contar com validação humana, sendo o usuário responsável pelo conteúdo gerado e pelos impactos de sua utilização.

- O uso de IA não substitui o julgamento técnico, jurídico ou político dos servidores e colaboradores, devendo ser considerado instrumento de apoio e não de decisão autônoma.

5.3.4. Registro e rastreabilidade

- Sempre que utilizado em processos institucionais, o uso de IA deve ser documentado, mencionando a ferramenta, finalidade é responsável pela revisão humana.

A Assessoria Especial da Vice-Governadoria manterá um Instrumento Normativo Complementar à Política Interna de Uso de Inteligência Artificial — a ser publicado no site institucional — que detalhará as diretrizes técnicas e critérios específicos para adoção, desenvolvimento e uso de sistemas de IA, incluindo:

- Avaliação de Riscos e Impactos Éticos
- Aplicabilidade e Transparência
- Supervisão Humana e Responsabilidade

- Privacidade por Design
- Segurança da Informação e Continuidade Operacional

Essa política será periodicamente revisada pelo CSPD, CTIGI e Assessoria Jurídica, em alinhamento com as orientações da ANPD, CGE e CEPD (Comitê Estadual de Proteção de Dados Pessoais), garantindo sua atualização e conformidade contínua com as melhores práticas nacionais e internacionais.

6. Diretrizes Específicas

6.1 Acesso À Internet

- A CTIGI monitora e bloqueia automaticamente sites de conteúdo erótico, pedofilia, racismo, drogas e outros que contenham conteúdos contrários às legislações vigentes, utilizando soluções de filtragem de conteúdo e *gateways* de segurança, em estrita conformidade com as políticas internas de uso de recursos tecnológicos e com os princípios de segurança de rede, bem como o NIST Cybersecurity Framework.
- Qualquer necessidade de *download* de programas/softwares deverá ser solicitado à CTIGI por meio de chamado para o e-mail suporteti@vicegov.ce.gov.br, seguindo o processo de homologação e aprovação de *softwares* corporativos, visando manter a integridade e a segurança do ambiente computacional, conforme a Política de Segurança da Informação e Proteção de Dados Pessoais da ETICE (2024).
- O uso da internet é auditado e monitorado constantemente, respeitado os princípios da proporcionalidade, finalidade e transparência e o colaborador poderá vir a prestar contas de seu uso, em conformidade com as diretrizes de privacidade e uso de recursos tecnológicos, e com as normativas de segurança da informação, assegurando a rastreabilidade e a responsabilização.

6.2 Correio Eletrônico

- A CTIGI será responsável pelo gerenciamento, adição, exclusão e adoção de medidas operacionais visando conter a propagação de e-mails suspeitos no ambiente de tecnologia do órgão, incluindo a implementação de filtros *anti-spam*, *anti-malware* e soluções de *sandbox*, em conformidade com as políticas de segurança de e-mail e proteção contra ameaças cibernéticas.
- A qualquer tempo, mediante detecção pelos sistemas e/ou identificação de e-mails suspeitos pela equipe responsável pela administração do sistema de correio eletrônico, procederá com as configurações necessárias objetivando conter eventuais propagações de e-mails suspeitos no órgão, podendo incluir o bloqueio de remetentes, domínios ou anexos específicos, em aderência aos procedimentos de resposta a incidentes de segurança e em conformidade com as diretrizes da ISO 27001.

- O colaborador deverá efetuar abertura de chamado técnico para o e-mail suporteti@vicegov.ce.gov.br, quando houver necessidade de análise de e-mails suspeitos de SPAM pela CTIGI, seguindo os fluxos de comunicação e gestão de incidentes de segurança da informação.
- O colaborador é responsável direto pelas mensagens enviadas por intermédio do seu endereço de correio eletrônico institucional, devendo zelar pela imagem da Assessoria Especial da Vice-Governadoria e observar a legislação vigente, incluindo a Lei Federal nº 13.709/2018 (LGPD) no que tange ao tratamento de dados pessoais em comunicações eletrônicas e a Lei Estadual nº 18.699/2024 (CE).
- É proibido o uso do e-mail institucional para cadastro de *feed* de notícias, sites de compra e venda, redes sociais, faculdade e fornecedores que não sejam relacionados às atividades da Assessoria Especial da Vice-Governadoria, em conformidade com as políticas de uso aceitável de recursos tecnológicos e com o princípio da finalidade.
- Links no corpo do e-mail devem ser clicados apenas quando o remetente for de conhecimento ou confiável, e em caso de dúvida, o colaborador deve contatar a CTIGI antes de prosseguir, aplicando as diretrizes de segurança no uso de correio eletrônico e prevenção de ataques de *phishing* e *malware*.

6.3 Gestão de incidentes

- Os colaboradores da Assessoria Especial da Vice-Governadoria deverão notificar a CTIGI de forma imediata, através dos canais designados (e.g., e-mail suporteti@vicegov.ce.gov.br ou telefone de suporte), caso tenham conhecimento ou suspeita sobre qualquer incidente de segurança da informação, como acesso não autorizado, perda de dados, infecção por *malware* ou comprometimento de sistemas, em conformidade com os procedimentos de comunicação e reporte de incidentes.
- A CTIGI, em conjunto com o DPO (Encarregado de Dados), procederá com a investigação, contenção, erradicação e recuperação do incidente, acionando os planos de resposta a incidentes e comunicando às autoridades competentes e os titulares de dados, quando exigido legalmente pela Lei Federal nº 13.709/2018 (LGPD) e demais normativas, seguindo as diretrizes do NIST Cybersecurity Framework para resposta a incidentes.

6.4 Sistemas

- Os códigos-fontes dos sistemas gerenciados pela Assessoria Especial da Vice-Governadoria deverão estar armazenados em repositórios no Sistema de Controle de Versão definido pela CTIGI (e.g., Git), garantindo a rastreabilidade das alterações e o controle de acesso.
- Todos os sistemas do órgão deverão ter ambientes de desenvolvimento, homologação e produção segregados, com controle de acesso rigoroso e processos formais para a promoção de código entre os ambientes.

- Os sistemas *web* do órgão deverão utilizar um certificado válido SSL/TLS (Secure Sockets Layer/Transport Layer Security) para garantir a criptografia da comunicação e a autenticidade do servidor.
- Os sistemas do órgão deverão ter um padrão para a definição de senhas fortes, implementando políticas de complexidade, periodicidade de troca e bloqueio por tentativas falhas.
- A Assessoria Especial da Vice-Governadoria deverá utilizar um WAF (Web Application Firewall) para proteger suas aplicações *web* de possíveis ataques, como *SQL Injection*, *Cross-Site Scripting* (XSS) e outras vulnerabilidades do *OWASP Top 10*.
- No processo de desenvolvimento de sistemas deverão ser observados padrões de segurança que não ocasionem vulnerabilidades às ferramentas da Assessoria Especial da Vice-Governadoria, através da implementação de práticas de *DevSecOps* e testes de segurança contínuos.

6.5 Utilização de Ativos

- Não são permitidas tentativas de obter acesso não autorizado, tais como tentativas de fraudar autenticação de usuário ou segurança de qualquer servidor, rede, conta ou sistema, o que constitui violação grave desta política e da legislação, incluindo crimes cibernéticos previstos em lei.
- O colaborador deve sempre bloquear o equipamento ao se ausentar (botão Windows + L), a fim de proteger o acesso não autorizado e a exposição de informações sensíveis, aplicando medidas simples, mas eficazes, de segurança para proteger o acesso físico e lógico aos equipamentos.
- Materiais com conteúdo impróprio, como racista, erótico ou preconceituoso, não podem ser acessados, expostos, armazenados ou distribuídos, através de qualquer tipo de ferramenta ou dispositivos que são utilizados na rede da Assessoria Especial da Vice-Governadoria, em conformidade com as políticas de uso aceitável e a legislação sobre conteúdos impróprios.
- Todos os dados relativos à Assessoria Especial da Vice-Governadoria devem ser mantidos no *drive* de rede (compartilhamentos de rede ou plataformas de armazenamento em nuvem institucional), onde existe sistema de *backup* periódico e controle de versão, visando garantir a disponibilidade e a recuperação em caso de perda de dados locais, aplicando as diretrizes de armazenamento seguro e gestão de *backups* em conformidade com a ISO 27001.
- Todos os documentos, vídeos e imagens pessoais não são de responsabilidade da Assessoria Especial da Vice-Governadoria, ou seja, estão sujeitos a exclusão. A estação de trabalho é estritamente para as atividades relacionadas ao trabalho, e qualquer uso indevido pode resultar em sanções, em conformidade com as políticas de uso de recursos tecnológicos e as sanções previstas nesta política.
- O acesso ao Datacenter é exclusivo para a equipe da CTIGI. Em caso da necessidade de acesso de uma outra área ou prestador de serviço, este deve ser acompanhado

por um colaborador autorizado da equipe da CTIGI, com registro formal de acesso e finalidade, aplicando os controles de segurança física e registro de acessos a áreas críticas, em conformidade com as recomendações da ISO 27001.

6.6 Contas, Senhas e Autenticação

- As senhas para os colaboradores deverão conter no mínimo 8 (oito) caracteres, sendo obrigatório o uso de letras, números e caracteres especiais;
- Caso o colaborador suspeite do comprometimento de sua senha, deverá modificá-la imediatamente;
- A senha é individual e intransferível, devendo ser mantida em sigilo. É proibido o seu compartilhamento;
- Contas que ficarem inativas por mais de 90 dias serão bloqueadas;
- O tempo de vida das senhas será de, no máximo, 90 (noventa) dias, quando será forçada a sua troca.

7. Responsabilidades

7.1 Colaboradores, Servidores e Prestadores de Serviço

- Cumprir integralmente todas as normas, diretrizes e procedimentos estabelecidos nesta política e em seus instrumentos complementares.
- Proteger as informações sob sua guarda, zelando pela sua confidencialidade, integridade e disponibilidade, e evitando acessos indevidos, uso inadequado ou divulgação não autorizada.
- Comunicar imediatamente qualquer incidente de segurança da informação ou de proteção de dados (suspeito ou confirmado) à Coordenadoria de Tecnologia da Informação, Governança e Inovação (CTIGI), ao Encarregado de Dados (DPO) ou à sua gestão imediata, utilizando os canais de comunicação designados.
- Responsabilizar-se pessoalmente pelo ativo de Tecnologia da Informação e Comunicação (TIC) sob sua responsabilidade, garantindo sua adequada utilização e proteção contra danos ou uso indevido.
- Responder por toda e qualquer violação de segurança praticada por ação ou omissão, conforme as sanções previstas nesta política e na legislação vigente.
- Utilizar os serviços e recursos tecnológicos da Assessoria Especial da Vice-Governadoria exclusivamente para as necessidades autorizadas e relacionadas às atividades institucionais.
- Proteger sua senha de acesso e quaisquer credenciais de autenticação contra uso indevido, mantendo-as em sigilo absoluto e assumindo a responsabilidade por todas as atividades originadas a partir de sua identificação.

- Utilizar somente programas/softwares legalizados, licenciados e analisados tecnicamente pela CTIGI, sendo expressamente proibido o uso, instalação ou distribuição de *software* não licenciado, pirata ou não autorizado.
- Utilizar os serviços de forma otimizada e compartilhada, evitando desperdícios de recursos computacionais, tais como o uso inadequado do tempo de rede, do acesso à Internet, dos recursos de impressão e do espaço em disco.
- Manter-se atualizado sobre as diretrizes e procedimentos de segurança da informação e proteção de dados através da participação em treinamentos e do acesso aos materiais de capacitação fornecidos.

7.2 Coordenadoria de Tecnologia da Informação, Governança e Inovação (CTIGI)

- Implementar, manter e monitorar os controles técnicos de segurança (como firewall, antivírus, auditoria de acessos, soluções de backup, monitoramento de rede e prevenção de intrusão), assegurando a confidencialidade, integridade e disponibilidade dos dados institucionais; apoiar a implementação de diretrizes de classificação da informação e do ciclo de vida dos dados; propor e manter a integridade e a segurança dos bancos de dados sob responsabilidade da Assessoria Especial da Vice-Governadoria.
- Mapear processos de segurança e de gestão de TI, identificando riscos e propondo melhorias; coordenar a gestão de vulnerabilidades, a resposta a incidentes e a implementação de planos de continuidade de negócios e recuperação de desastres; manter atualizado o planejamento estratégico de TI da Assessoria Especial da Vice-Governadoria, alinhado às diretrizes estaduais e aos objetivos institucionais.
- Apoiar, sempre que necessário, o Comitê Setorial de Proteção de Dados (CSPD) e o Encarregado de Dados (DPO) no desempenho de suas atribuições, fornecendo suporte técnico, administrativo e operacional para a adequada implementação das práticas de governança de dados e de proteção de dados pessoais.

8. Capacitação e Cultura Institucional

A Assessoria Especial da Vice-Governadoria do Estado do Ceará reconhece que a efetividade desta política e a conformidade com as normas de segurança da informação, governança de dados e uso de Inteligência Artificial dependem criticamente da capacitação contínua e da promoção de uma cultura institucional sólida.

8.1 Objetivos

- Sensibilizar e conscientizar todos os colaboradores sobre a importância da Lei Geral de Proteção de Dados (LGPD), da Lei Estadual nº 18.699/2024 (que institui o Sistema

Estadual de Proteção de Dados Pessoais) e da Lei Estadual nº 17.611/2021 (que regulamenta o uso de IA no Ceará), destacando seus impactos nas atividades cotidianas e na responsabilidade individual e coletiva.

- Promover uma cultura organizacional pautada pela responsabilidade, segurança, ética digital e privacidade por design e por *default*, incentivando a adoção de práticas seguras no manuseio de informações e no uso de tecnologias.
- Capacitar tecnicamente os profissionais que operam, desenvolvem ou supervisionam sistemas de informação, tratam dados institucionais e implementam soluções de Inteligência Artificial, dotando-os do conhecimento e das habilidades necessárias para desempenhar suas funções em conformidade com as melhores práticas de segurança e governança.

8.2 Público-Alvo

Todos os colaboradores da Assessoria Especial da Vice-Governadoria, incluindo servidores efetivos, comissionados, colaboradores terceirizados, estagiários e prestadores de serviço, com diferentes níveis de profundidade e granularidade de conteúdo conforme suas funções e o grau de acesso a informações sensíveis.

8.3 Estratégias de Capacitação

- Participação em workshops temáticos aprofundados sobre proteção de dados, cibersegurança avançada e ética digital em IA. Tais formações deverão se alinhar às melhores práticas de mercado, como as preconizadas pelo NIST (National Institute of Standards and Technology) e a ISO 27001, além de abordar cenários de risco e o fiel cumprimento da Lei Federal nº 13.709/2018 (LGPD), da Lei Estadual nº 18.699/2024 (CE) e da Lei Estadual nº 17.611/2021 (CE).
- Participação em eventos e treinamentos técnicos e de gestão promovidos por instituições de referência como CGE, Etice, Enap e parceiros estratégicos especializados em segurança da informação e governança de dados. A participação deverá ser certificada, e o conhecimento adquirido deverá ser replicado internamente, fomentando a disseminação de boas práticas.
- Produção e disseminação contínua de materiais internos de orientação com linguagem técnica e operacional (e.g., cartilhas detalhadas, vídeos tutoriais interativos, guias práticos, FAQs estruturados) que detalhem procedimentos específicos para manuseio de dados, uso de sistemas, identificação de ameaças e resposta a incidentes de segurança.
- Inclusão preferível de módulos específicos de segurança da informação, governança de dados e uso ético de IA em programas de integração de novos colaboradores, com incentivo à avaliação de compreensão e à assinatura de termo de responsabilidade, em conformidade com as diretrizes da Política de Segurança da Informação e Proteção de Dados Pessoais da ETICE (2024), quando aplicável.

9. Sanções

O descumprimento das diretrizes estabelecidas nesta Política poderá ensejar a apuração de responsabilidade funcional, administrativa, civil ou penal, conforme o caso, nos termos da legislação vigente e do regime jurídico aplicável a cada vínculo funcional.

A aplicação de eventuais penalidades observará o devido processo legal, assegurados o contraditório e a ampla defesa, no termo da Lei nº 9.826/74 e das demais normas aplicáveis.

As sanções decorrentes do descumprimento, observarão o regime jurídico aplicável a cada vínculo funcional, nos termos da legislação estadual vigente, não constituindo este Regimento inovação no rol de penalidades administrativas, limitando-se a estabelecer diretrizes internas de conduta e conformidade institucional.

10. Disposições Finais

- Esta política, de caráter mandatório, deve ser amplamente divulgada por todos os canais de comunicação oficiais da Assessoria Especial da Vice-Governadoria, garantindo o acesso e a ciência de todos os servidores, colaboradores e prestadores de serviços. A assinatura de termo de ciência e conformidade será obrigatória para todos, formalizando o compromisso com as diretrizes aqui estabelecidas.
- A Assessoria Especial da Vice-Governadoria compromete-se a alocar e otimizar os recursos financeiros, tecnológicos e humanos necessários para a plena implementação, manutenção e aprimoramento contínuo das diretrizes aqui estabelecidas, em conformidade com as prioridades orçamentárias e estratégicas.
- Os casos omissos e as eventuais dúvidas quanto à aplicação da Política devem ser encaminhados à Coordenadoria de Tecnologia da Informação, Governança e Inovação.
- Questões específicas e detalhadas sobre o uso, desenvolvimento e regulamentação de sistemas de Inteligência Artificial serão abordadas e regulamentadas em instrumento normativo complementar específico — a Política Interna de Uso de Inteligência Artificial —, que será submetida a revisões mais frequentes para acompanhar a rápida evolução tecnológica e regulatória do tema, mantendo a conformidade com a Lei Estadual nº 17.611/2021 (CE).
- Este documento possui natureza normativa interna, vinculando todos os colaboradores, servidores e prestadores de serviço no âmbito da Assessoria Especial da Vice-Governadoria.

11. Revisão da Política

- Esta política será submetida a um processo de revisão formal e obrigatório, no mínimo a cada dois anos (24 meses), ou sempre que houver a promulgação de novas leis,

regulamentos ou normas técnicas aplicáveis (e.g., atualizações da LGPD, da Lei Estadual nº 18.699/2024 (CE), da Lei Estadual nº 17.611/2021 (CE), ou diretrizes da Portaria MJSP nº 961/2025), mudanças significativas nos processos internos, na estrutura organizacional ou nas tecnologias de informação e comunicação utilizadas pela Assessoria Especial da Vice-Governadoria.

- O processo de revisão será conduzido de forma colaborativa pela Coordenadoria de Tecnologia da Informação, Governança e Inovação (CTIGI), com o suporte técnico e estratégico do Comitê Setorial de Proteção de Dados (CSPD) e do Encarregado de Dados (DPO).
- Todas as versões atualizadas do documento deverão ser formalmente publicadas nos canais oficiais da Assessoria Especial da Vice-Governadoria.

12. Referências Normativas Utilizadas

As seguintes normas, leis e documentos foram utilizados para embasar a elaboração da presente política:

- Lei Federal nº 13.709/2018 (LGPD) – Dispõe sobre o tratamento de dados pessoais e protege os direitos dos titulares.
- Lei Estadual nº 18.699/2024 (CE) – Institui o Sistema Estadual de Proteção de Dados Pessoais.
- Lei Estadual nº 17.611/2021 (CE) – Regulamenta o uso de Inteligência Artificial no Ceará.
- Política de Segurança da Informação e Proteção de Dados Pessoais da ETICE (2024) – Norma que pode ser referenciada por outros órgãos estaduais enquanto não houver política própria.
- Portaria MJSP nº 961/2025 – Estabelece diretrizes sobre uso de soluções de tecnologia da informação aplicadas às atividades de investigação criminal e inteligência de segurança pública.
- OWASP Top 10 – Documento que descreve as 10 vulnerabilidades de segurança mais críticas em aplicações web.
- NIST (National Institute of Standards and Technology) – Instituto americano que desenvolve padrões e diretrizes em segurança da informação.
- ISO 27001 – Norma internacional para sistemas de gestão de segurança da informação.
- Lei Complementar Estadual nº 98/2011 (CE) – Dispõe sobre o regime jurídico dos servidores públicos civis do Estado do Ceará, das autarquias e das fundações públicas estaduais.
- Lei Estadual nº 9.826/74 – Dispõe sobre o Estatuto dos Funcionários Públicos Civis do Estado