ALECE
ASSEMBLEIA LEGISLATIVA
DO ESTADO DO CEARÁ

ATO NORMATIVO N° 375/2026

INSTITUI A POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (PSI) DA ASSEMBLEIA LEGISLATIVA DO ESTADO DO CEARÁ (ALECE)

A **MESA DIRETORA DA ASSEMBLEIA LEGISLATIVA DO ESTADO DO CEARÁ**, no uso da atribuição que lhe confere o art. 17, XVII, "a", da Resolução n.º 751, de 14 de dezembro de 2022 (REGIMENTO INTERNO),

CONSIDERANDO a necessidade de instituir e manter uma política que norteie toda e qualquer operação com dados, inclusive dados pessoais e dados pessoais sensíveis, no âmbito da Alece, reafirmando o compromisso permanente com a segurança da informação e o respeito aos direitos fundamentais dos titulares de dados;

CONSIDERANDO a necessidade de aderência aos normativos existentes quanto ao acesso e à divulgação da informação, em especial à Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação — LAI), e à Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais — LGPD);

CONSIDERANDO a Política de Privacidade e Proteção de Dados Pessoais da Alece, instituída pela Portaria da Diretoria-Geral nº 800, de 10 de julho de 2024;

CONSIDERANDO a ocorrência de inúmeros incidentes cibernéticos na rede mundial de computadores e a necessidade de processos de trabalho orientados para a boa gestão da segurança da informação;

CONSIDERANDO que a informação, em todo o seu ciclo de vida, constitui um ativo estratégico e, portanto, fundamental para o desempenho das atribuições e atividades inerentes à Alece;

CONSIDERANDO a necessidade de assegurar as propriedades da informação durante todo o seu ciclo de vida;

CONSIDERANDO que toda informação gerada, recebida, mantida, transmitida ou tratada pela Alece pode estar em diferentes meios ou suportes e que é necessário prevenir incidentes, naturais ou não, de origem humana ou tecnológica, que possam comprometer a segurança dessa informação;

CONSIDERANDO a necessidade de estabelecer princípios, objetivos e diretrizes gerais que promovam a gestão integrada e coerente de processos voltados à segurança da informação que sejam periodicamente revistos;

CONSIDERANDO que a segurança é uma qualidade da informação que depende da conscientização de todos os que com ela lidam em qualquer etapa de seu ciclo de vida; e

CONSIDERANDO a necessidade de esclarecer e determinar aos usuários seus direitos e deveres no que se refere à segurança da informação,

RESOLVE:

CAPÍTULO I

DAS DISPOSIÇÕES GERAIS

Seção I

Do Objeto e do Âmbito de Aplicação

Art. 1º Fica instituída a Política de Segurança da Informação (PSI) da Assembleia Legislativa do Estado do Ceará (Alece), que compreende princípios, objetivos e diretrizes **e** define responsabilidades, competências e instrumentos para a gestão da segurança da informação no âmbito da Alece.

Art. 2º A Política de Segurança da Informação (PSI) se aplica a todos os ativos de informação da Alece, incluindo dados, sistemas, aplicativos, dispositivos, redes, serviços e instalações físicas administradas ou utilizadas e a todos os usuários, internos e externos, que tenham acesso a esses ativos, incluindo servidores efetivos, comissionados, temporários, contratados, estagiários, prestadores de serviços, fornecedores, parceiros ou quaisquer outras partes autorizadas a acessar tais ativos.

Seção II

Dos Conceitos

Art. 3º Para os fins de cumprimento da PSI, ficam estabelecidos os seguintes conceitos:

I - Ameaça: qualquer circunstância ou evento com o potencial de causar impacto negativo sobre a segurança da informação;

II - Ativos Críticos: ativos de informação, contratos com fornecedores e relacionamentos com parceiros, infraestrutura física, licenças e certificações e demais equipamentos e processos operacionais imprescindíveis para a prestação dos serviços essenciais da Alece;

III - Ativos de Informação: são todos os recursos, tangíveis ou intangíveis, que produzem, recebem, processam, armazenam, transmitem, protegem ou dão suporte ao conteúdo informacional da Alece e que possuem valor institucional, legal, operacional ou estratégico, incluindo sistemas de informação, aplicações, infraestruturas tecnológicas, meios físicos ou digitais, processos, políticas, procedimentos, pessoas e conhecimentos associados;

IV - Autenticação: processo pelo qual o usuário apresenta sua credencial de acesso a um recurso computacional para que sua identidade seja validada, garantindo que apenas usuários devidamente identificados possam acessar o sistema do qual o recurso computacional faz parte;

V - Autenticidade: propriedade que garante que uma entidade (usuário, dispositivo, aplicação de software ou conjunto de dados) é realmente o que declara ser, assegurando que a identidade ou a origem sejam genuínas e possam ser verificadas de forma confiável;

VI - Autodeterminação Informativa: direito do titular de exercer controle consciente e informado sobre o tratamento de seus dados pessoais, nos limites previstos na lei, sobretudo na Lei Geral de Proteção de Dados Pessoais (LGPD);

VII - Autorização: processo pelo qual um sistema computacional determina quais recursos, ações ou serviços um usuário tem permissão de acessar ou realizar, após a identidade desse usuário ter sido autenticada;

VIII - Ciclo de vida dos dados ou da informação: conjunto de etapas pelas quais os dados ou informações são produzidos, recebidos, coletados, registrados, classificados, tratados, armazenados, acessados, utilizados, compartilhados, preservados e avaliados, observados os critérios de acesso, sigilo, transparência e proteção da informação previstos na Lei de Acesso à Informação, bem como os prazos de guarda, destinação e eliminação definidos na Tabela de Temporalidade da Alece, no âmbito de suas atribuições, sistemas, processos e atividades institucionais;

IX - Confidencialidade: propriedade que assegura que dados, informações ou documentos sejam acessados, utilizados ou divulgados apenas por pessoas, unidades ou sistemas devidamente autorizados, observados o grau de sigilo ou de acesso atribuído por autoridade competente, a legislação aplicável e as normas institucionais da Alece;

X - Conformidade: propriedade que garante o cumprimento das legislações, normas e procedimentos relacionados à segurança da informação, privacidade e proteção a dados pessoais;

XI - Conteúdo Informacional: qualquer informação ou dado registrado, produzido, recebido, adquirido, coletado ou mantido pela Alece no exercício de suas atribuições institucionais, independentemente do formato, suporte ou meio de armazenamento, incluindo documentos, registros, bases de dados e demais informações sob sua custódia;

XII - Controle: conjunto de medidas, mecanismos ou salvaguardas adotadas para prevenir, reduzir, mitigar ou aceitar riscos, compreendendo o Manual de Gerenciamento de Riscos da Alece, políticas, normas, procedimentos, diretrizes, práticas, processos ou estruturas organizacionais de natureza administrativa, técnica, operacional, de gestão ou legal, aplicáveis aos ativos de informação e às atividades da Alece;

XIII - Controle de acesso: conjunto de políticas, procedimentos, mecanismos e recursos técnicos ou administrativos destinados a autorizar, restringir, monitorar ou negar o acesso de pessoas, sistemas ou processos aos ativos de informação da Alece, de acordo com critérios de autenticação, autorização, necessidade de acesso e segregação de funções;

XIV - Credencial de acesso: qualquer informação, meio ou mecanismo utilizado para que os controles de acesso identifiquem, autentiquem e autorizem um usuário, sistema ou entidade a acessar recurso ou ativo de informação protegido, podendo incluir, entre outros: identificador de usuário e senha; crachás ou cartões de acesso (com ou sem identificação visual); dispositivos de autenticação física ou digital (tokens, chaves criptográficas, cartões virtuais); e métodos biométricos, como impressão digital, reconhecimento facial, palmar ou de íris;

XV - Custodiante da informação: pessoa, unidade ou órgão responsável por implementar, operar e manter os controles de segurança da informação, assegurando a proteção do conteúdo informacional sob sua guarda, em conformidade com as políticas, normas e procedimentos estabelecidos pela Alece;

XVI - Dado pessoal: qualquer informação relacionada a pessoa natural identificada ou identificável;

XVII - Dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;

XVIII - Disponibilidade: propriedade que assegura que dados, informações ou serviços estejam acessíveis por usuários, sistemas ou processos devidamente autorizados, sempre que necessário ao desempenho das atividades institucionais;

XIX - Gestor de ativo de informação: titular de cada um dos órgãos da Alece responsável pela gestão, uso e operação dos ativos de informação sob sua competência, incluindo a definição de requisitos de segurança, níveis de acesso e prioridades no tratamento e gerenciamento de riscos;

XX - Incidente de segurança da informação: evento ou conjunto de eventos não planejados ou indesejados, confirmados ou sob suspeita, que resultem ou possam resultar na violação das propriedades da informação, no comprometimento de ativos de informação ou na interrupção de qualquer dos serviços institucionais;

XXI - Informação: conjunto de dados, registros, textos, imagens, áudios, documentos, sistemas ou outras formas de representação dotadas de significado em determinado contexto, independentemente do meio, formato, suporte ou forma de veiculação;

XXII - Integridade: propriedade que assegura que a informação permaneça completa, íntegra e fidedigna, protegida contra alterações, destruições ou perdas não autorizadas ou não registradas, em qualquer fase de seu ciclo de vida;

XXIII - Não repúdio: propriedade que assegura a impossibilidade de negar a autoria, a realização ou a participação em uma ação, transação ou operação previamente executada, envolvendo ativos de informação, mediante o uso de mecanismos técnicos e administrativos adequados;

XXIV - Plano de continuidade de negócios (PCN): conjunto de estratégias e planos de ação preventivos contendo a documentação dos procedimentos e das informações necessários à manutenção dos ativos de informação críticos e à continuidade de suas atividades em local alternativo previamente definido, em casos de incidente, até que a situação seja normalizada;

XXV - Plano de recuperação de desastres (PRD): conjunto de estratégias e planos de ação contendo a documentação dos procedimentos e das informações necessários a restaurar sistemas de TI e infraestruturas tecnológicas após um desastre (como incêndios, enchentes, falhas de hardware, ataques cibernéticos etc.), garantindo que os sistemas de TI possam ser recuperados e estejam operacionais dentro de um prazo aceitável após um desastre;

XXVI - Privacidade da informação: refere-se ao conjunto de direitos dos titulares e deveres institucionais no tratamento de dados pessoais ou dados pessoais sensíveis, abrangendo as atividades de coleta, uso, armazenamento, compartilhamento, retenção e descarte, de forma transparente, segura e em conformidade com a legislação vigente, especialmente a LGPD, a Política de Privacidade e Proteção de Dados Pessoais da Alece e os princípios da

autodeterminação informativa, finalidade, adequação, necessidade e minimização;

XXVII - Processo de trabalho: conjunto de atividades inter-relacionadas dentro da Alece (ou de seus órgãos), destinado a transformar entradas (recursos, informações ou materiais) em saídas (produtos ou resultados específicos), cujo controle é realizado por monitoramento e eventuais ajustes para garantir a conformidade e a eficiência de acordo com metas e exigências pré-estabelecidas;

XXVIII - Propriedades da informação: atributos que devem ser assegurados para a proteção adequada da informação, compreendendo a confidencialidade, a integridade, a disponibilidade, a autenticidade o não repúdio e a conformidade;

XXIX - Registros de segurança: documentos, arquivos ou logs que registram eventos, atividades e operações relacionadas à segurança da informação, utilizados para monitoramento, rastreabilidade, auditoria, investigação e resposta a incidentes ou ameaças, armazenados em banco de dados próprio;

XXX - Risco de segurança da informação: probabilidade de ocorrência de um incidente de segurança, resultante da exploração de vulnerabilidades por ameaças, associada ao impacto potencial sobre as propriedades da informação, os ativos institucionais e as operações da Alece;

XXXI - Segurança da informação: conjunto de princípios, políticas, práticas, processos, pessoas e mecanismos técnicos e administrativos destinados a proteger a informação e seus ativos, assegurando suas propriedades ao longo de todo o ciclo de vida, independentemente do meio ou suporte em que se encontrem;

XXXII - Sistema de gestão da segurança da informação (SGSI): conjunto integrado de estrutura organizacional, políticas, processos, responsabilidades, práticas, pessoas e recursos adotados pela Assembleia Legislativa do Estado do Ceará para planejar, implementar, operar, monitorar, revisar e melhorar continuamente a segurança da informação, com base em uma abordagem sistemática de gestão de riscos;

XXXIII - Usuário externo: qualquer pessoa natural ou jurídica não integrante do quadro funcional da Assembleia Legislativa do Estado do Ceará que, de forma autorizada, temporária, específica e restrita, possua credencial de acesso para utilizar ou consultar conteúdos informacionais ou serviços disponibilizados pela Alece;

XXXIV - Usuário interno: qualquer agente público, servidor efetivo ou comissionado, parlamentar, estagiário, colaborador terceirizado ou prestador de serviço da Alece que possua credencial de acesso autorizada para acessar conteúdos informacionais ou recursos de tecnologia da informação, em qualquer fase de seu ciclo de vida;

XXXV - Vulnerabilidade: fragilidade ou deficiência em ativos, processos, sistemas ou serviços que, quando explorada por uma ou mais

ameaças, pode resultar em impacto negativo à segurança da informação e à imagem institucional.

CAPÍTULO II

DOS PRINCÍPIOS, OBJETIVOS E DIRETRIZES

Seção I

Dos Princípios

Art. 4º Para orientar e nortear as ações de Segurança da Informação da Assembleia Legislativa do Estado do Ceará (Alece), a Política de Segurança da Informação (PSI) fundamenta-se nos seguintes princípios:

I - Responsabilidade compartilhada, cabendo a todos os usuários o dever de observar e zelar pela segurança da informação no exercício de suas atividades;

II - Participação ativa de usuários e custodiantes da informação na prevenção, detecção, comunicação e resposta a incidentes de segurança da informação;

III - Respeito aos direitos e legítimos interesses dos usuários, assegurando a proteção dos dados pessoais e da privacidade da informação, nos termos da legislação vigente;

IV - Observância da publicidade como regra geral e do sigilo como exceção, em conformidade com a Lei de Acesso à Informação e demais normas aplicáveis;

V - Garantia da continuidade dos processos, serviços e atividades essenciais da Alece, inclusive diante de incidentes ou situações adversas;

VI - Proporcionalidade e economicidade na adoção de medidas de proteção aos ativos de informação, considerando os riscos envolvidos;

VII - Aplicação do princípio do mínimo privilégio, assegurando que o acesso a ativos de informação seja concedido apenas na extensão necessária ao desempenho das atribuições funcionais;

VIII - Observância do princípio da necessidade de conhecer, de modo que o acesso às informações seja restrito àquelas indispensáveis ao exercício das funções institucionais;

IX - Incorporação da segurança da informação como requisito essencial no planejamento, desenvolvimento, aquisição, implantação e operação de sistemas de informação, informatizados ou não;

X - Gestão sistêmica e integrada da segurança da informação, alinhada aos objetivos institucionais e baseada em abordagem de gestão de riscos; e

XI - Avaliação e aprimoramento contínuos da segurança da informação, mediante revisões periódicas da PSI e das demais políticas, normas, procedimentos e práticas correlatas.

Seção II

Dos Objetivos

Art. 5º Em conformidade com os princípios estabelecidos no art. 4º, a Política de Segurança da Informação (PSI) está voltada aos seguintes objetivos:

I - Instituir, desenvolver e manter uma cultura organizacional aderente à segurança da informação, compreendendo ações destinadas a fomentar entre os usuários a constante observância quanto às práticas destinadas à preservação dessa segurança;

II - Promover a contínua avaliação dos riscos a que a informação está sujeita, incluindo, entre outros, a medição de indicadores quantificáveis;

III - Estabelecer procedimentos eficazes de detecção, resposta e recuperação de incidentes de segurança da informação, com o objetivo de minimizar os impactos e garantir a continuidade dos serviços da Alece; e

IV - Implantar a gestão de segurança da informação para a implementação de mecanismos eficientes de monitoramento, análise e revisão contínua da PSI e dos controles de segurança, garantindo a melhoria contínua do Sistema de Gestão de Segurança da Informação (SGSI) e a adaptação às mudanças organizacionais e tecnológicas da Alece.

Seção III

Das Diretrizes

Art. 6º As diretrizes da Política de Segurança da Informação (PSI), que constituem os principais pilares da gestão de segurança da informação, norteiam a elaboração de políticas, planos e normas complementares no âmbito da Assembleia Legislativa do Estado do Ceará (Alece) e objetivam garantir os princípios básicos de segurança da informação estabelecidos no art. 4º, nos seguintes termos:

I - Direcionamento das ações de segurança da informação para: o alinhamento, prioritariamente, aos objetivos estratégicos, aos planos institucionais, à estrutura e à finalidade da Alece, de forma integrada, respeitando as especificidades e a autonomia de seus órgãos; a sua adoção proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação; e a prevenção da ocorrência de incidentes;

II - Capacitação adequada dos usuários e custodiantes frente às necessidades de segurança da informação;

III - Instituição de políticas e normas específicas, planos, procedimentos e práticas para a segurança da informação aderentes à PSI, devendo considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação;

IV - Observância de leis, regulamentos e obrigações contratuais aos quais os processos de trabalho estão sujeitos;

V - Investimento necessário em medidas de segurança da informação segundo o valor do ativo a ser protegido e o risco de potenciais prejuízos;

VI - Disposição para que todos os ativos **de** informação da Alece sejam rigorosamente protegidos e para que os dados que tramitem pelo seu ambiente computacional sejam passíveis de monitoramento e auditoria, respeitados os limites legais;

VII - Estabelecimento de limites a usuários e sistemas, concedendo-lhes, em regra, o menor privilégio e o mínimo acesso aos recursos necessários para a realização de uma dada tarefa;

VIII - Determinação da existência de cláusula específica em todos os contratos de prestação de serviços firmados pela Alece sobre a obrigatoriedade de atendimento a esta PSI, bem como às demais políticas e normas decorrentes dela;

IX - Manutenção de inventário atualizado dos ativos de informação da Alece, incluindo a identificação e a classificação das informações críticas que esses ativos armazenam, processam ou transmitem, de forma a subsidiar a adoção de controles de segurança compatíveis com sua criticidade.

CAPÍTULO III

DA GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

Seção I

Do Sistema de Gestão da Segurança da Informação (SGSI)

Art. 7º A composição da estrutura de agentes responsáveis pelo Sistema de Gestão de Segurança da Informação (SGSI) da Assembleia Legislativa do Estado do Ceará (Alece) inclui:

I - Diretoria-Geral, na qualidade de Controladora de Dados Pessoais para os dados da gestão;

II - Coordenadoria de Tecnologia da Informação (COTI);

III - Procuradoria-Geral;

IV - Coordenadoria de Desenvolvimento Institucional (CODINS);

V - Coordenadoria do Sistema Alece de Comunicação (CSAC);

VI - Usuários Internos e Externos de Informação.

§ 1º A estruturação dos cargos e funções será realizada por meio de norma específica.

§ 2º O órgão ou unidade administrativa afetada por incidente de segurança da informação detectado ou reportado pelo SGSI deverá colaborar integral e prioritariamente com todas as determinações e orientações dos agentes responsáveis pela contenção do incidente, visando à mitigação de riscos e ao restabelecimento da normalidade dentro do menor prazo possível.

Art. 8º A PSI e demais políticas, normas, procedimentos e práticas decorrentes dela integram o arcabouço normativo do Sistema de Gestão de Segurança da Informação (SGSI).

Art. 9º O Sistema de Gestão de Segurança da Informação (SGSI) será constituído, no mínimo, pelos seguintes processos:

I - Tratamento da informação;

II - Segurança física e do ambiente;

III - Gestão de incidentes em segurança da informação;

IV - Gestão de ativos;

V - Gestão do uso dos recursos operacionais e de comunicação, incluindo e-mail, internet, mídias sociais e computação em nuvem;

VI - Controles de acesso;

VII - Gestão de riscos;

VIII - Gestão de continuidade; e

IX - Auditoria e conformidade.

Parágrafo único. Para cada um dos processos que constituem o Sistema de Gestão de Segurança da Informação (SGSI), deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o entendimento desses processos em conformidade com a legislação vigente, com as boas práticas de segurança **da** informação e com o disposto no Manual de Gerenciamento de Riscos e na Metodologia de Gestão por Processos Baseada em Riscos (GPR) da Assembleia Legislativa do Estado do Ceará.

Art. 10. As políticas, normas, procedimentos, orientações ou manuais de que trata o parágrafo único do art. 9º devem abordar, no mínimo, aspectos relacionados:

I - À conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidos pela Agência Nacional de Proteção de Dados - ANPD;

II - À classificação da informação de acordo com seu nível de confidencialidade e criticidade, entre outros fatores, com vistas a determinar os controles de segurança adequados;

III - À proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

IV - Ao uso aceitável da informação e à utilização de mídias de armazenamento;

V - À entrada e saída de ativos de informação das instalações da organização;

VI - Aos perímetros de segurança da organização;

VII - Aos controles de acesso baseados no princípio do menor privilégio;

VIII - Às etapas de identificação, contenção, erradicação e recuperação e às atividades pós-incidente;

IX - Aos critérios para a comunicação de incidentes aos titulares de dados pessoais e à ANPD;

X - Ao Plano de Gestão de Incidentes de Segurança, considerando diferentes cenários;

XI - À Política de Gestão de Ativos, abordando aspectos relacionados à proteção dos ativos; à classificação do ativo de acordo com a sua criticidade para a Assembleia Legislativa do Estado do Ceará; à manutenção de inventário atualizado desse ativo, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança; ao uso aceitável de ativos, vedado o uso para fins particulares de seu responsável; ao mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências; ao monitoramento de ativos de acordo com os princípios legais de segurança da informação e privacidade e à investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;

XII - À utilização adequada dos recursos operacionais e de comunicações fornecidos pela Assembleia Legislativa do Estado do Ceará (Alece), a serem utilizados para fins profissionais, relacionados às atividades desse órgão, em conformidade com os seus princípios éticos e profissionais, evitando comportamentos antiéticos, discriminatórios, ofensivos ou que possam comprometer a sua reputação;

XIII - Aos procedimentos para o uso de correio eletrônico (e-mail), o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

XIV - Ao acesso à internet, quanto ao download de arquivos, sendo vedado o uso de sítios inadequados e a instalação de software não autorizado;

XV - Ao uso de mídias sociais no que se refere à divulgação de informações, ao uso de contas pessoais para fins profissionais e à interação com estranhos;

XVI - Às políticas e procedimentos para o uso da computação em nuvem, a seleção de provedores de serviços em nuvem, a segurança dos dados na nuvem e a conformidade com as leis e regulamentos aplicáveis;

XVII - Às políticas e procedimentos para o uso de inteligência artificial e tecnologias similares e à conformidade com as leis e regulamentos aplicáveis;

XVIII - Às políticas e procedimentos para o controle de acesso, tais como o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização baseados no princípio do menor privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de

acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação da Alece;

XIX - Às políticas e procedimentos para a Gestão de Riscos de Segurança da Informação que possam afetar seus ativos de informação, abordando a análise do ambiente da Alece, dos seus ativos de informação e das ameaças à segurança da informação; a adoção de uma metodologia estruturada para identificar riscos; a documentação dos riscos identificados, incluindo sua descrição, origem, impacto potencial e probabilidade de ocorrência; a avaliação de riscos, de forma a determinar o risco de se concretizar e o impacto potencial nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento e o tratamento dos riscos identificados e avaliados, o que pode incluir a mitigação de riscos, por meio da implementação de controles de segurança, ou a aceitação de riscos;

XX - Às políticas e procedimentos para a Gestão de Continuidade de Negócios, incluindo o Plano de Continuidade de Negócios (PCN), para garantir que a Assembleia Legislativa do Estado do Ceará (Alece) possa continuar suas atividades em caso de um incidente de segurança da informação, e a realização de testes e exercícios periódicos baseados nesse plano para garantir sua eficácia;

XXI - Às políticas e aos procedimentos para a Gestão de Mudanças nos ativos de informação, respaldados pelas informações dos relatórios de avaliação e tratamento de risco de segurança da informação, com a designação de papéis e responsabilidades para a avaliação, aprovação e implementação de mudanças e a criação de um processo formal para solicitação e documentação de mudanças; e

XXII - Às políticas e aos procedimentos para a auditoria e conformidade da Alece, abordando o Plano de Verificação de Conformidade, que considere as unidades abrangidas, os aspectos para verificação da conformidade, as ações e atividades a serem realizadas, os documentos necessários para a fundamentação da verificação de conformidade e das responsabilidades, bem como o Relatório de Avaliação de Conformidade, que considere o detalhamento das ações e das atividades com identificação do responsável, o parecer de conformidade e as recomendações.

§ 1º Os órgãos da Alece devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com a PSI de que trata este Ato e com outros requisitos de segurança da informação aplicáveis.

§ 2º Todas as ações realizadas pelos órgãos da Alece que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis a esta temática.

§ 3º As atividades, produtos e serviços desenvolvidos na Alece devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, normas internas, estatutos e contratos

vigentes.

Seção II

Das Instâncias de Governança e Competências

Art. 11. Compete à Diretoria-Geral:

I - Fornecer os recursos necessários para assegurar o desenvolvimento e a implementação do SGSI, bem como o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados;

II - Formalizar, aprovar e publicar a Política de Segurança da Informação (PSI) da Alece, bem como suas alterações e atualizações;

III - Supervisionar, juntamente com o CGTI, a implantação e a execução da PSI; e

IV - Promover a cultura da segurança da informação e o envolvimento de todos os órgãos da Alece na consecução dos objetivos e diretrizes da PSI.

Art. 12. Compete à Coordenadoria de Tecnologia da Informação (COTI), dentre outras atribuições dispostas na legislação vigente, incluindo a Portaria da Diretoria-Geral nº 800/2024 (Política de Privacidade e Proteção de Dados Pessoais – LGPD):

I - Planejar, implementar e melhorar continuamente os controles de segurança da informação e de privacidade em soluções de tecnologia da informação e comunicação, juntamente com os agentes responsáveis pelo Sistema de Gestão de Segurança da Informação (SGSI) da Assembleia Legislativa do Estado do Ceará (Alece), considerando a cadeia de suprimentos relacionada à solução;

II - Facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos na Alece;

III - Monitorar as redes computacionais;

IV - Detectar e analisar ataques e intrusões;

V - Tratar incidentes de segurança da informação;

VI - Identificar vulnerabilidades e artefatos maliciosos; e

VII - Recuperar sistemas de informação.

Art. 13. Compete à Procuradoria-Geral, dentre as atribuições dispostas na Resolução nº 780/2025 e suas alterações, assessorar e orientar juridicamente, sempre que solicitada, os agentes responsáveis pelo Sistema de Gestão de Segurança da Informação (SGSI) da Assembleia Legislativa do Estado do Ceará (Alece), constantes no art. 7º desta Política de Segurança da Informação (PSI).

Art. 14. Compete ao Encarregado de Proteção de Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na LGPD e demais normativos e orientações emitidas pela Agência Nacional de Proteção de Dados (ANPD), conduzir, com o auxílio da COTI, o

diagnóstico de privacidade, bem como orientar, no que couber, os órgãos e gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis, além de auxiliar a supervisionar a implantação e a execução da PSI.

Art. 15. Compete à Coordenadoria de Desenvolvimento Institucional (CODINS), dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha, que é responsável por identificar, avaliar, controlar e mitigar os riscos, guiando o desenvolvimento e a implementação de políticas e procedimentos internos destinados a garantir que as atividades sejam realizadas de acordo com as metas e objetivos da Alece.

Art. 16. Compete à Coordenadoria do Sistema Alece de Comunicação (CSAC), dentre outras atribuições dispostas na legislação vigente:

I - Atuar conjuntamente na elaboração de publicações externas e internas;

II - Gerenciar a comunicação interna e externa, com apoio do Encarregado de Proteção de Dados Pessoais e da Célula de Governança da COTI, durante incidentes, garantindo transparência e proteção da imagem institucional;

III - Disseminar orientações e comunicações relacionadas à segurança da informação, com o apoio do Encarregado de Proteção de Dados Pessoais e da Célula de Governança da COTI;

IV - Promover campanhas de conscientização e capacitação sobre a Política de Segurança da Informação (PSI) e normas de segurança, visando tornar os colaboradores cientes de suas responsabilidades;

V - Divulgar as atualizações e novas versões da PSI.

CAPÍTULO IV

DOS DEVERES, DIREITOS E RESPONSABILIDADES

Seção I

Dos Deveres dos Órgãos da Alece

Art. 17. Compete a todos os órgãos da Assembleia Legislativa do Estado do Ceará (Alece):

I - Participar da implantação e da execução da PSI;

II - Zelar pela segurança da informação no âmbito dos processos de trabalho e atividades sob sua responsabilidade;

III - Comunicar, imediatamente ou tão logo tenha conhecimento, por meio de seu gestor, à Coordenadoria de Tecnologia da Informação (COTI), quaisquer ocorrências ou suspeitas de incidentes de segurança da informação na estrutura sob sua responsabilidade;

IV - Garantir que os servidores, os colaboradores e os terceiros participem dos treinamentos e atividades educativas de Segurança da Informação propostas pela Alece;

V - Elaborar propostas de regulamentação relacionadas à segurança da informação em seus processos de trabalho, em consonância com a PSI, submetendo-**as** à apreciação do Comitê de Governança de Tecnologia da Informação (CGTI); e

VI - Participar da definição e validação dos requisitos e funcionalidades de segurança da informação dos aplicativos e sistemas de informação vinculados aos seus processos de trabalho.

Seção II

Dos Deveres e Direitos dos Usuários

Art. 18. Compete aos Usuários Internos da Assembleia Legislativa do Estado do Ceará:

I - Conhecer e cumprir a PSI de que trata este Ato e suas normas e procedimentos complementares;

II - Comunicar, tão logo tenha conhecimento, à chefia imediata, à COTI e ao Encarregado de Proteção de Dados Pessoais quaisquer vulnerabilidades, ameaças ou ações indevidas relacionadas à segurança da informação de que tiver conhecimento ou suspeita;

III - Seguir as orientações fornecidas pelos setores competentes em relação ao uso dos recursos computacionais e conteúdos informacionais da Alece; e

IV - Utilizar de forma ética, legal e consciente os recursos computacionais e conteúdos informacionais da Alece com que lidam, zelando pela garantia das propriedades desses conteúdos informacionais.

Art. 19. Compete aos Usuários Externos da Alece:

I - Conhecer e cumprir seus deveres específicos descritos neste Ato, incluindo o que estiver previsto no Capítulo V (Das Vedações) e na Portaria nº 800/2024, da Diretoria-Geral da Alece (Política de Privacidade e Proteção de Dados Pessoais), e eventuais normas e procedimentos complementares que lhes disserem respeito;

II - Reportar imediatamente a um representante do órgão que lhe concedeu credenciais de acesso, vulnerabilidades, ameaças ou ações indevidas de que tiver conhecimento ou suspeita, relacionadas à segurança da informação; e

III - Utilizar de forma ética, legal e consciente os recursos computacionais e conteúdos informacionais da Assembleia Legislativa do Estado do Ceará.

Art. 20. São direitos dos servidores da Assembleia Legislativa do Estado do Ceará em relação à PSI:

I - Receber capacitação adequada ao exercício de suas atribuições; e

II - Propor aperfeiçoamento da PSI e de seus instrumentos de gestão.

Art. 21. Aos direitos dos titulares de dados pessoais aplica-se o art. 18 da Lei nº 13.709, de 14 de agosto de 2018.

CAPÍTULO V

DAS VEDAÇÕES

Seção Única

Das Condutas Vedadas

Art. 22. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pela Alece para acessar, armazenar, transmitir ou divulgar qualquer material incompatível com o ambiente institucional, incluindo, mas não se limitando a conteúdos tais como:

I - Discriminatórios ou ofensivos, relacionados à saúde, raça, gênero, orientação sexual, condição social, religiosa ou política;

II - Obscenos, pornográficos, ou que incitem violência, ódio ou práticas ilegais;

III - Que infrinjam direitos autorais ou propriedade intelectual; ou

IV - Que violem as normas internas da Alece ou legislações vigentes, especialmente a Lei Geral de Proteção de Dados Pessoais (LGPD), a Lei de Acesso à Informação (LAI) e demais normas relativas à segurança da informação e privacidade.

Art. 23. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados, adquiridos e/ou expressamente autorizados pela Coordenadoria de Tecnologia da Informação, incluindo, mas não se limitando a:

I - Arquivos, softwares ou programas não autorizados ou de procedência duvidosa, incluindo ferramentas para invasão ou quebra de segurança; ou

II - Dispositivos eletrônicos e digitais, tais como notebooks, tablets, smartphones, mídias removíveis (pendrives, discos rígidos externos e similares) ou qualquer outro dispositivo eletrônico que possa se conectar à rede interna da Alece.

Art. 24. É vedada, a todos os usuários indicados na Política de que trata este Ato, a divulgação de mecanismos de identificação, autenticação e

autorização, cujo uso tenha sido classificado como pessoal e intransferível, que lhes tenham sido fornecidos.

Art. 25. É proibido explorar eventuais falhas e vulnerabilidades sem a devida autorização expressa e por escrito fornecida pela COTI.

CAPÍTULO VI

DAS DISPOSIÇÕES FINAIS

Seção Única

Art. 26. As demandas prioritárias para elaboração e revisão de normas e procedimentos relativos à segurança da informação serão conduzidas pelo Comitê de Governança de Tecnologia da Informação (CGTI), com a participação da Diretoria-Geral como Controladora de Dados Pessoais, e terão como prioridade os seguintes temas, sem prejuízo de eventuais necessidades já existentes:

I - Acesso, proteção e guarda da informação, em especial, a sigilosa e a pessoal;

II - Aquisição, desenvolvimento e manutenção de sistemas informatizados;

III - Autenticação, autorização e controle de acesso à rede de dados, aos serviços de tecnologia da informação e comunicação e aos sistemas de informação da Alece;

IV - Classificação da informação, observado o disposto na Lei de Acesso à Informação (LAI) e na Tabela de Classificação e Temporalidade da Alece;

V - Coleta e preservação de registros de segurança;

VI - Cópias de segurança de dados e de sistemas informatizados;

VII - Gestão de incidentes de segurança da informação;

VIII - Inventário dos recursos computacionais e dos conteúdos informacionais, enfatizando os aspectos de responsabilidades e de uso aceitável;

IX - Proposição de um Plano de Continuidade de Negócio (PCN), incluindo um Plano de Recuperação de Desastres (PRD);

X - Segregação de ambientes de tecnologia da informação e comunicação, com a implementação de ambientes distintos de desenvolvimento, teste, homologação e produção de sistemas computacionais, feita em atendimento ao princípio da separação de funções, com a definição de papéis e responsabilidades específicos para cada ambiente; e

XI - Segurança das instalações que hospedam os conteúdos informacionais e os recursos computacionais para os quais a normatização seja necessária.

Art. 27. A inobservância dos dispositivos constantes deste Ato pode acarretar, isolada ou cumulativamente, sanções administrativas, civis ou penais, nos termos da legislação vigente, assegurando-se o contraditório e a ampla defesa.

Art. 28. Este Ato deverá ser revisado ordinariamente a cada biênio ou, extraordinariamente, sempre que ocorrer algum dos seguintes eventos ou situações específicas:

I - Ocorrência de incidentes significativos de segurança da informação ou violações de dados institucionais e/ou pessoais que evidenciem fragilidades ou lacunas nas políticas e procedimentos atualmente vigentes;

II - Alterações relevantes na legislação ou normativos que afetem diretamente a segurança da informação, privacidade ou proteção de dados pessoais, especialmente nas diretrizes estabelecidas pela Agência Nacional de Proteção de Dados (ANPD);

III - Mudanças significativas nas atividades, estrutura organizacional ou processos internos da Alece que demandem adaptação dos controles previstos nesta PSI;

IV - Adoção de novas tecnologias, ferramentas ou sistemas de informação que exijam redefinição ou complementação dos mecanismos de segurança atualmente adotados;

V - Resultados negativos recorrentes identificados em auditorias internas ou externas relativas à segurança da informação e proteção de dados pessoais; ou

VI - Recomendação fundamentada pelo Comitê de Governança de Tecnologia da Informação (CGTI) ou pela Diretoria-Geral, através do Encarregado de Proteção de Dados Pessoais, motivada pela identificação de vulnerabilidades ou riscos críticos emergentes.

Art. 29. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação – PSI e demais documentos integrantes da estrutura normativa do Sistema de Gestão de Segurança da Informação (SGSI) serão dirimidos pelo Comitê de Governança de Tecnologia da Informação (CGTI), com apoio da Coordenadoria de Tecnologia da Informação e, quando couber, da Diretoria-Geral.

Art. 30. A implementação da PSI de que trata este Ato será realizada de forma gradual, conforme a priorização estratégica, a disponibilidade de recursos e a aprovação dos atos administrativos competentes.

Art. 31. Este Ato Normativo entra em vigor na data de sua publicação.

PAÇO DA ASSEMBLEIA LEGISLATIVA DO ESTADO DO CEARÁ, em Fortaleza, aos 15 dias do mês de abril do ano de 2026.

DEPUTADO ROMEU ALDIGUERI
PRESIDENTE

DEPUTADO DANNIEL OLIVEIRA
1º VICE PRESIDENTE

DEPUTADA LARISSA GASPAR
2ª VICE PRESIDENTE

DEPUTADO DE ASSIS DINIZ
1º SECRETÁRIO

DEPUTADO JEOVÁ MOTA
2º SECRETÁRIO

DEPUTADO FELIPE MOTA
3º SECRETÁRIO

DEPUTADO JOÃO JAIME
4º SECRETÁRIO