ALEGO
ASSEMBLEIA LEGISLATIVA
DO ESTADO DE GOIÁS

Diretoria de Tecnologia
da Informação

POSIC

Política de Segurança
da Informação e Comunicações

1ª VERSÃO
SETEMBRO/2022

ALEGO
ASSEMBLEIA LEGISLATIVA
DO ESTADO DE GOIÁS

Sumário

1. ESCOPO 3
   1.1. OBJETIVO 3
   1.2. ABRANGÊNCIA 3
2. CONSIDERAÇÕES INICIAIS 3
3. CONCEITOS E DEFINIÇÕES 5
4. REFERÊNCIAS LEGAIS E NORMATIVAS 9
5. PRINCÍPIOS 10
6. DIRETRIZES GERAIS 11
7. DIRETRIZES ESPECÍFICAS 13
   7.1. GESTÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (GESIC) 13
   7.2. GESTÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDE COMPUTACIONAL GETIR 13
   7.3. GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (GRSIC) 13
   7.4. GESTÃO DE CONTINUIDADE DE NEGÓCIOS (GECON) 14
   7.5. GESTÃO DE ATIVOS DE INFORMAÇÃO 15
   7.6. TRATAMENTO DA INFORMAÇÃO 15
   7.7. CLASSIFICAÇÃO DA INFORMAÇÃO 16
   7.8. MONITORAMENTO, AUDITORIA E CONFORMIDADE 16
   7.9. CONTROLE DE ACESSO E USO DE SENHAS 16
   7.10. USO DE CORREIO ELETRÔNICO (E-MAIL) 17
   7.11. ACESSO À INTERNET 17
   7.12. USO DAS REDES SOCIAIS 17
   7.13. AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO 17
   7.14. CONSCIENTIZAÇÃO, SENSIBILIZAÇÃO E CAPACITAÇÃO EM SIC 18
   7.15. PLANO DE INVESTIMENTOS EM SIC 18
   7.16. PROPRIEDADE INTELECTUAL 18
   7.17. CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES 18
   7.18. USO DE COMPUTAÇÃO EM NUVEM 18
   7.19. USO DE DISPOSITIVOS MÓVEIS 19
8. COMPETÊNCIAS E RESPONSABILIDADES 19
   8.1. CABE AO CHEFE DA SEÇÃO DA SEGURANÇA DA INFORMAÇÃO 19
   8.2. CABE AO CONSELHO GESTOR DE TECNOLOGIA DA INFORMAÇÃO (CGTI) 20
   8.3. CABE À EQUIPE DE TRATAMENTO DE INCIDENTES EM REDES DE COMPUTADORES 20
   8.4. CABE AO PROPRIETÁRIO DE ATIVOS DE INFORMAÇÃO 21
   8.5. CABE AO CUSTODIANTE DOS ATIVOS DE INFORMAÇÃO 21
   8.6. CABE AOS TERCEIROS E FORNECEDORES 21
   8.7. CABE AOS USUÁRIOS 21
9. DIVULGAÇÃO E CONCIENTIZAÇÃO 22
10. ATUALIZAÇÃO E VALIDADE 22
   10.1. POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC): 22
   10.2. NOTAS TÉCNICAS DE SEGURANÇA DA INFORMAÇÃO: 22
   10.3. PROCEDIMENTOS OPERACIONAIS: 22
11. VALIDADE 23

12. PENALIDADES **23**

13. SIGLAS **23**

1. ESCOPO

1.1. Objetivo

A Política de Segurança da Informação e Comunicações - POSIC tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso da Assembleia Legislativa do Estado de Goiás - ALEGO contra ameaças e vulnerabilidades. Desse modo, a Política busca preservar os seus ativos de informação, assim como a sua imagem institucional.

O propósito da política é direcionar a ALEGO no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação e Comunicações (SIC), em conformidade com as disposições constitucionais, legais e regimentais vigentes.

A POSIC estabelece o comprometimento da alta direção organizacional da empresa, com vistas a prover apoio para a implantação da Gestão dos Riscos de Segurança da Informação e Comunicações (GRSIC).

1.2. Abrangência

Esta POSIC aplica-se à Assembleia Legislativa do Estado de Goiás - ALEGO, sendo de responsabilidade de todos os funcionários, colaboradores internos ou externos, bem como a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos da ALEGO o conhecimento desta POSIC. Todos esses atores são responsáveis por garantir a segurança das informações as que tenham acesso.

2. CONSIDERAÇÕES INICIAIS

A informação é um ativo, como qualquer outro considerado importante, essencial para os negócios de uma organização e consequentemente necessita ser adequadamente protegida. Na época em que as informações eram armazenadas apenas em documentos em papel, a segurança era relativamente simples. Bastava guardar os documentos em algum lugar e restringir fisicamente o acesso ao local. Com a chegada dos computadores pessoais e das redes de computadores, os aspectos de segurança passaram a exigir o desenvolvimento de equipes e de métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram grande importância para a sobrevivência da maioria das organizações modernas.

A administração pública, em todas as esferas e órgãos, processa informações consideradas sensíveis, que exigem proteção contra os riscos a que estão expostas, para garantir a confidencialidade, integridade, disponibilidade e a autenticidade delas. Consciente dessa importância, o Presidente da República editou o **Decreto nº 3.505, de 13 de junho de 2000**, por meio do qual foi instituída a Política Nacional de Segurança da Informação e que deveria ser implementada pelos órgãos e entidades da Administração Pública Federal, direta e indireta. Assim, o estabelecimento de uma Política de Segurança da Informação organizacional, implementada e formalmente divulgada a todos os servidores, terceiros, fornecedores ou indivíduos que possuam qualquer tipo de acesso à informação é o principal passo de estratégia de segurança das organizações.

Atualmente a informação pode existir em diversos formatos: impressa, armazenada eletronicamente, falada, transmitida via correio convencional, de voz ou eletrônico, entre outros. Seja qual for o formato, meio de armazenamento ou transmissão, recomenda-se que a informação seja protegida adequadamente. Sendo assim, é responsabilidade da segurança da informação protegê-la de vários tipos de ameaças.

A segurança da informação é obtida a partir da implementação de um conjunto de controles adequado, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de software e hardware. Este conjunto de controles é denominado Política de Segurança da Informação e Comunicação - POSIC. A POSIC precisa ser estabelecida, implementada, analisada criticamente e constantemente melhorada a fim de garantir que os objetivos do negócio e de segurança específicos da instituição sejam atendidos.

Convém que a direção apoie ativamente a segurança da informação dentro da organização, por meio de um claro direcionamento, demonstrando o seu comprometimento, definindo atribuições de forma explícita e reconhecendo as responsabilidades pela segurança da informação (NBR-ISO-27002). A POSIC declara o comprometimento da alta direção organizacional com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a gestão de segurança da informação na ALEGO.

O cumprimento desta Política depende do comprometimento de todos. Por outro lado, a inobservância às normas de segurança pode levar à execução de sanções definidas na POSIC.

3. CONCEITOS E DEFINIÇÕES

Para os efeitos desta POSIC, são estabelecidos os seguintes conceitos e definições:

a) Acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;
b) Ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
c) Análise de riscos: uso sistemático de informações para identificar fontes e estimar o risco;
d) Atividade: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;
e) Ativo: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha ou gere valor para a organização;
f) Ativo de Informação: São os meios de armazenamento, transmissão e processamento, os sistemas de informação, além das informações em si, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso, por exemplo o Data Center da Assembleia Legislativa, unidades de armazenamento externas utilizados por órgãos como TV Assembleia, Seção de Audiofonia, Seção de Taquigrafia e outros que fizerem parte da sede do Poder Legislativo Estadual;
g) Ativo de Processamento: É o patrimônio composto por todos os elementos de hardware e software necessários para a execução dos sistemas e processos da ALEGO, tanto os produzidos internamente quanto os adquiridos. Exemplos: banco de dados, softwares, equipamentos (computadores e notebooks), servidores, dispositivos de redes (roteadores, switches entre outros), pessoas, processos e serviços;
h) Autenticidade: Visa estabelecer a validade da transmissão, da mensagem e do seu remetente. O objetivo é que o destinatário possa comprovar a origem e a autoria de um determinado documento;
i) Celeridade: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas;
j) Classificação da informação: identificação de quais são os níveis de proteção que as informações demandam e estabelecimento de classes e formas de identificá-las, além de determinar os controles de proteção necessários a cada uma delas;
k) Comunicação do risco: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;
l) Confidencialidade: Garante que a informação somente será acessada por pessoas explicitamente autorizadas, em conformidade com a Lei Estadual

18.025/13 e a Lei Federal 12.527/11 que tratam sobre acesso à informação de dados públicos;

m) Controle de acesso: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;

n) Custodiante do ativo de informação: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;

o) Desastre: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período superior ao tempo objetivo de recuperação;

p) Descarte: eliminação correta de informações, documentos, mídias e acervos digitais;

q) Diretriz: Descrição que orienta o que deve ser feito e como, para que se alcancem os objetivos estabelecidos nas políticas;

r) Disponibilidade: Garantia de que a informação estará disponível e utilizável quando for solicitada por pessoas autorizadas.

s) Ética: os direitos dos agentes públicos devem ser preservados sem comprometimento da Segurança da Informação e Comunicações;

t) Equipe de Tratamento de Incidentes em Redes de Computadores (ETIR): Grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

u) Evento de segurança da informação: ocorrência identificada de um sistema, serviço ou rede que indica uma possível violação da política de segurança da informação, ou falta de controle, ou situação previamente desconhecida que possa ser relevante para a segurança da informação;

v) Gerenciamento de operações e comunicações: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suporte, satisfazendo os acordos de níveis de serviço;

w) Gestão de ativos: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada dos controles desses ativos;

x) Gestão de continuidade dos negócios: processo abrangente de gestão que identifica ameaças potenciais para uma organização e os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo fornece uma estrutura para que se desenvolva uma resiliência

organizacional que seja capaz de responder efetivamente e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização e suas atividades de valor agregado;

y) Gestão de Riscos de Segurança da Informação e Comunicações: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;

z) Gestão de segurança da informação e comunicações: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;

aa) Gestor de segurança da informação e comunicações: é o servidor público responsável pelas ações de segurança da informação e comunicações;

bb) Identificação de riscos: processo para localizar, listar e caracterizar elementos do risco;

cc) Incidente de Segurança da Informação: É um evento de segurança da informação indesejado ou inesperado que tenha uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

dd) Incidente de SIC: evento que tenha causado algum dano, colocado em risco algum ativo de informação crítico ou interrompido a execução de alguma atividade crítica por um período inferior ao tempo objetivo de recuperação;

ee) Integridade: Garante que a informação não será modificada ou destruída por pessoas não autorizadas, seja acidental ou propositalmente;

ff) Política de Segurança da Informação: É um documento que engloba um conjunto de princípios, diretrizes, critérios e suporte administrativos suficientes à implementação da Segurança da Informação e que deve ser observado pelo corpo técnico e gerencial e pelos usuários internos;

gg) Proprietário de ativos de informação: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;

hh) Quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;

ii) Recursos criptográficos: sistemas, programas, processos e equipamento isolado ou em rede que utilizam algoritmo simétrico ou assimétrico para realizar a cifração ou decifração;

jj) Resiliência: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;

kk) Responsabilidade: os agentes públicos devem conhecer e respeitar todas as normas de segurança da informação e comunicações da instituição;

ll) Risco de SIC: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

mm) Segurança da Informação: É a proteção da informação contra muitos ameaças, de forma a assegurar sua confidencialidade, integridade e disponibilidade; adicionalmente, outras propriedades como autenticidade, responsabilidade, não repúdio e confiabilidade, podem também ser envolvidas;

nn) Segurança física e do ambiente: processo que trata da proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização está presente;

oo) Sistema estruturante: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;

pp) Terceiros: Quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos à ALEGO;

qq) Transferir risco: uma forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;

rr) Tratamento da informação: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;

ss) Tratamento de incidentes: é o processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências;

tt) Tratamento dos riscos: processo e implementação de ações de segurança da informação e comunicações para evitar, reduzir, reter ou transferir um risco;

uu) Usuário: agente público que obteve autorização do responsável pela área interessada para acesso aos ativos de Informação;

vv) Vulnerabilidade: Conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação;

ww) Computação em Nuvem: Em inglês, *cloud computing* refere-se à utilização da memória e da capacidade de armazenamento e cálculo de computadores e servidores compartilhados e interligados por meio da Internet, seguindo o princípio da computação em grade.

4. REFERÊNCIAS LEGAIS E NORMATIVAS

a) **Lei 8.159, de 8 de janeiro de 1991:** dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;
b) **Lei nº 9.983, de 14 de julho de 2000:** dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;
c) **Lei nº 12.527, de 18 de novembro de 2011:** regulamenta o acesso às informações públicas;
d) **Lei Federal nº 13.709, de 14 de agosto de 2018**, que dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural;
e) **Norma ABNT NBR ISO/IEC 27001:2013:** estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;
f) **Norma ABNT NBR ISO/IEC 27002:2013:** institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação;
g) **Norma ABNT NBR ISO/IEC 27005:2011:** estabelece diretrizes para o processo de gestão de riscos de segurança da informação.

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações e suas ações serão norteadas pelos seguintes princípios:

a) **Celeridade:** As ações de SIC devem oferecer respostas rápidas à incidentes e falhas de segurança;
b) **Ética:** Os direitos e interesses legítimos dos usuários e agentes públicos devem ser preservados, sem comprometimento da SIC;
c) **Clareza:** As regras de segurança dos ativos de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;
d) **Legalidade:** As ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais da ALEGO;
e) **Publicidade:** Transparência no trato da informação, observados os critérios legais;
f) **Finalidade:** a realização do tratamento deve ocorrer para propósitos legítimos, específicos, explícitos e informados ao(à) titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
g) **Adequação:** compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
h) **Necessidade:** o tratamento deve se limitar à realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
i) **Livre acesso:** garantia dada aos(às) titulares de consulta livre, de forma facilitada e gratuita, à forma e à duração do tratamento, bem como à integralidade de seus dados pessoais;
j) **Qualidade dos dados:** garantia dada aos(às) titulares de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
k) **Transparência:** garantia dada aos(às) titulares de que terão informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
l) **Segurança:** trata-se da utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
m) **Prevenção:** compreende a adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;

n) **Não discriminação:** o tratamento de dados não pode ser realizado para fins discriminatórios ilícitos ou abusivos;
o) **Responsabilização e Prestação de Contas:** demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

6. DIRETRIZES GERAIS

6.1. Para a uniformidade da informação, esta POSIC deverá ser comunicada a todos os servidores, fornecedores e provedores de serviços que, de alguma forma, tenham acesso aos ativos da ALEGO visando o cumprimento da POSIC dentro e fora da instituição;
6.2. Toda informação produzida ou recebida pelos servidores como resultado da atividade contratada pela ALEGO pertence à referida instituição. As exceções devem ser explicitadas e formalizadas em contrato entre as partes;
6.3. Os equipamentos de informática e comunicação são utilizados pelos servidores para a realização das atividades profissionais. O uso pessoal dos recursos é permitido desde que não prejudique o desempenho dos servidores;
6.4. A ALEGO, por meio de sua Diretoria de Tecnologia da Informação, poderá monitorar e registrar todo o uso dos sistemas, serviços e computadores, visando garantir a disponibilidade e a segurança das informações e sistemas;
6.5. Os usuários de computador devem utilizar apenas software homologado ou pelo menos autorizado pela ALEGO, ficando vedada a instalação de softwares não autorizados pela Diretoria de Tecnologia da Informação;
6.6. É proibido todo o procedimento de manutenção física ou lógica, instalação ou desinstalação, configuração ou modificação, de qualquer equipamento ou software ligado a tecnologia da informação, sem o conhecimento prévio e a anuência da Diretoria de Tecnologia da Informação através da Seção de Suporte ao Usuário;
6.7. Os arquivos pessoais e/ou não pertinentes à ALEGO não deverão ser mantidos em unidades de rede, backup ou estações de trabalho, caso identificada a existência de tais arquivos, eles poderão ser excluídos definitivamente sem prévia comunicação ao usuário;
6.8. Documentos imprescindíveis para as atividades dos servidores da ALEGO deverão ser salvos em unidades de rede ou de backup. Tais arquivos, se gravados apenas localmente, não terão garantia de backup e poderão ser perdidos caso ocorra alguma falha no computador;
6.9. Todo incidente que afete a segurança da informação deverá ser comunicado imediatamente à Diretoria de Tecnologia da Informação por meio da Seção de Suporte ao Usuário;

6.10. As senhas de acesso, bem como outros mecanismos de identificação são de uso pessoal e intransferível, sendo o usuário de computador responsável pelos atos e acessos realizados com sua identificação no ambiente informatizado;

6.11. O uso de senhas e/ou mecanismos de identificação de outra pessoa constitui crime tipificado no artigo nº 307 do código penal brasileiro;

6.12. Será de inteira responsabilidade de cada servidor, todo prejuízo ou dano que vier a sofrer ou causar à ALEGO e/ou a terceiros, em decorrência da não obediência às diretrizes e normas aqui referidas;

6.13. A ALEGO exonera-se de toda e qualquer responsabilidade decorrente do uso indevido, negligente ou imprudente dos recursos e serviços concedidos aos seus servidores, reservando-se o direito de analisar dados e evidências para obtenção de provas a serem utilizadas nos processos investigatórios, bem como adotar as medidas legais cabíveis;

6.14. Deverá constar em todos os contratos da ALEGO o anexo de Acordo de Confiabilidade, como condição imprescindível para que possa ser concedido o acesso aos ativos de informação disponibilizados pela instituição;

6.15. Excetuam-se neste caso os ativos regidos pela **Lei Federal nº 12.527 de 18/11/11**.

6.16. Deverá ser atribuída aos servidores e prestadores de serviços, no ato da posse ou formalização de contratos individuais de trabalho, de prestação de serviços ou de parceria, a responsabilidade do cumprimento desta POSIC. Para efetivar tal responsabilidade, o servidor, ou prestador de serviço, deverá assinar o termo de Compromisso e Ciência, assumido o dever de seguir as normas estabelecidas;

6.17. Servidores e prestadores de serviços, no ato da posse ou da formalização de contratos individuais de trabalho, de prestação de serviços ou de parceria, deverão assinar o Acordo de Confidencialidade;

6.18. O não cumprimento dos requisitos previstos nesta POSIC e das Normas de Segurança da Informação acarretará violação às regras internas da instituição e sujeitará o usuário às medidas administrativas e legais cabíveis, assegurando-se o direito à ampla defesa e ao contraditório.

6.19. Ocorrendo o desligamento do servidor ou alteração na sua lotação, será responsabilidade da Diretoria de Gestão de Pessoas - DGP comunicar a Seção de Segurança da Informação, com o intuito de assegurar que os chefes não sejam responsabilizados por atos ilícitos dos servidores não pertencentes ao departamento;

6.20. Esta POSIC será implementada na ALEGO por meio de procedimentos específicos, obrigatórios para todos os servidores, independente da categoria funcional, do cargo ou seu tipo de provimento.

7. DIRETRIZES ESPECÍFICAS

7.1. Gestão da Segurança da Informação e Comunicações (GESIC)

Todos os mecanismos de proteção utilizados para a SIC devem ser mantidos com o objetivo de garantir a continuidade do negócio.

As medidas de proteção devem ser planejadas e os gastos da aplicação de controles devem ser compatíveis com o valor do ativo protegido.

Os requisitos de segurança da informação e comunicações da ALEGO devem ser explicitamente citados em todos os termos de compromisso celebrados entre a instituição e terceiros, por meio de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta política, bem como deverá ser exigido um termo de confidencialidade, aprovado pelo Conselho Gestor de Tecnologia da Informação (CGTI).

7.2. Gestão de Tratamento de Incidentes de Segurança em Rede Computacional (GETIR)

O Conselho Gestor de Tecnologia da Informação, instituído pelo **Decreto Administrativo nº 3048 de 10 de dezembro de 2019**, deverá criar e manter **Equipe de tratamento e resposta a Incidentes em Redes Computacionais (ETIR)**, com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Os eventos e incidentes de SIC devem ser tratados de acordo com um Plano de Gerenciamento de Incidentes específico, comunicados e registrados.

7.3. Gestão de Riscos de Segurança da Informação e Comunicações (GRSIC)

A GRSIC é um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação e equilibrá-los com os custos operacionais e financeiros envolvidos.

As áreas responsáveis por ativos de informação deverão implementar processo contínuo de Gestão de Riscos, que será aplicado na implementação e operação da GRSIC.

A GRSIC deve ser realizada no âmbito da ALEGO, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, e deve ser atualizada periodicamente, no mínimo 01 (uma) vez por ano, ou tempestivamente, em função de inventários de ativos, de mudanças, ameaças ou vulnerabilidades. Trata-se de um instrumento do programa de Gestão de Riscos que deve incluir um Plano de Continuidade de Negócio (PCN) e um Plano de Gerenciamento de Incidentes (PGI).

O Plano de Continuidade de Negócio deverá complementar a análise de riscos, visando limitar os impactos do incidente e garantir que as informações requeridas para que os processos do negócio estejam prontamente disponíveis.

O Plano de Gerenciamento de Incidentes definirá responsabilidade e procedimentos para assegurar respostas rápidas, efetivas e ordenadas a incidentes de SIC.

7.4. Gestão de Continuidade de Negócios (GECON)

A GECON é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação da ALEGO e possíveis impactos nas operações de negócio, caso estas ameaças se concretizem. Este processo fornece uma estrutura para que se desenvolva uma resiliência organizacional que seja capaz de responder efetivamente aos incidentes de SIC e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades da ALEGO, além de recuperar perdas de ativos de informação a um nível aceitável, por intermédio de ações de prevenção, resposta e recuperação, objetivando salvaguardar os interesses da ALEGO e da sociedade.

As áreas da ALEGO deverão manter processo de gestão de continuidade de negócios, visando permitir que os negócios baseados em Tecnologia da Informação não sejam interrompidos e, também, assegurar a sua retomada em tempo hábil, quando for o caso.

A resiliência contra possíveis interrupções de sua capacidade em atingir seus principais objetivos deve ser uma prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional da ALEGO.

Todas as áreas da ALEGO que dependam de recursos de Tecnologia da Informação e da Comunicação - TIC deverão criar Planos de Gerenciamento de Incidentes, por meio do Comitê Gestor de Segurança da Informação e Comunicações (CGSIC), de acordo com o grau de probabilidade de ocorrências de eventos ou sinistros e estabelecer um conjunto de estratégias e procedimentos que deverá ser adotado em situações que

comprometam o andamento normal dos processos e a consequente prestação dos serviços.

As medidas constantes do Plano de Gerenciamento de Incidentes deverão assegurar disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto sofrido diante do acontecimento de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

7.5. Gestão de Ativos de Informação

A gestão de ativos de informação deverá observar normas operacionais/complementares e procedimentos específicos para garantir a sua operação segura e contínua.

Os ativos de informação da ALEGO deverão ser inventariados, atribuídos aos respectivos responsáveis e seu uso deve estar em conformidade com os princípios e normas de SIC e são destinados ao uso corporativo, sendo vedada a utilização para fins em desconformidade com os interesses institucionais.

Todos os ativos deverão ser classificados em termos de valor, requisitos legais, sensibilidade e criticidade da informação para a instituição.

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo de normas e legislação específica de classificação de informação.

É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pela ALEGO.

7.6. Tratamento da Informação

A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços da ALEGO.

Os dados, as informações e os sistemas de informação da ALEGO devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

A informação deve ser protegida de acordo com o seu valor, sensibilidade e criticidade, elaborando-se, para tanto, sistema de classificação da informação.

7.7. Classificação da Informação

Toda informação criada, manuseada, armazenada, transportada ou descartada da ALEGO será classificada de acordo com a Lei Federal nº 12.527, de 18 de novembro 2011.

O usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pela ALEGO e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas. O usuário será informado/treinado através de treinamento e material informativo espalhados nos murais de divulgação da ALEGO.

As informações sob gestão da ALEGO terão segurança de maneira a serem adequadamente protegidas quanto ao acesso e uso. Para as consideradas de alta criticidade, serão necessárias medidas especiais de tratamento com o objetivo de limitar a exploração às informações exclusivas da instituição.

7.8. Monitoramento, Auditoria e Conformidade

O monitoramento, auditoria e conformidade observarão o seguinte:

a) O uso dos recursos de tecnologia da informação e comunicações disponibilizados pela ALEGO é passível de monitoramento e auditoria e devem ser implementados e mantidos, sempre que possível, mecanismos que permitam a sua rastreabilidade;
b) A entrada e saída de ativos de informação da ALEGO serão registradas e autorizadas por autoridade competente mediante procedimento formal;
c) A Diretoria de Tecnologia da Informação manterá registros e procedimentos, como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas corporativos, à rede interna e à internet;

7.9. Controle de Acesso e Uso de Senhas

As regras de controle de acesso a todos os sistemas corporativos, intranet, internet, informações, dados e às instalações físicas da ALEGO deverão ser definidas e regulamentadas, por meio de normas internas, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da instituição.

As credenciais de acesso para cadastro em sites externos, cursos online e afins, perfis sociais e outros meios de comunicação em nome da Assembleia Legislativa do Estado de Goiás, deverão ser feitos somente por meio de e-mail corporativo, com prévia autorização do diretor da área e comunicado ao Conselho Gestor de Tecnologia da Informação (CGTI).

O órgão que fizer o cadastro acima mencionado, será responsável por todas as informações e atualizações cadastrais, devendo comunicar qualquer alteração ao CGTI e zelando pelos limites estabelecidos nesta Política e legislação pertinente.

7.10. Uso de Correio Eletrônico (E-Mail)

O correio eletrônico é um recurso de comunicação corporativa da ALEGO e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta POSIC e das normas específicas e complementares, além das demais diretrizes da ALEGO.

7.11. Acesso à Internet

O acesso à rede mundial de computadores (internet), no ambiente de trabalho, deve ser regido por normas e procedimentos específicos, atendendo às determinações desta POSIC, e demais orientações governamentais e legislação em vigor.

7.12. Uso das Redes Sociais

A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações da ALEGO, deve ser regido por normas internas específicas e estar alinhada tanto à POSIC quanto aos objetivos da instituição.

7.13. Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação devem observar critérios e controles de segurança para garantir o respeito aos atributos básicos de segurança da informação.

7.14. Conscientização, Sensibilização e Capacitação em SIC

A ALEGO deverá promover continuamente a capacitação, reciclagem e o aperfeiçoamento de todos os usuários da instituição por meio de programas de divulgação, sensibilização, conscientização e capacitação em segurança da informação e comunicação, com o propósito de criar uma cultura de segurança dentro da instituição.

7.15. Plano de Investimentos em SIC

Os investimentos em segurança da informação e comunicações serão realizados de forma planejada e consolidados no que couber, no **Plano Diretor de Tecnologia da Informação e Comunicações – PDTIC**.

O Plano de Investimentos em SIC deverá ser reavaliado quando houver revisão orçamentária ou revisão de prioridades das ações de SIC.

7.16. Propriedade Intelectual

As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual da ALEGO e não cabe a seus criadores qualquer forma de direito autoral, ressalvando o direito de autoria, se for o caso.

É vedada a utilização de patrimônio intelectual da ALEGO em quaisquer projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica.

7.17. Contratos, Convênios, Acordos e Instrumentos Congêneres

Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter cláusulas que estabeleçam a obrigatoriedade de observância desta POSIC.

O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta política e suas normas complementares aos empregados, prepostos e todos os envolvidos em atividades vinculadas à ALEGO.

7.18. Uso de Computação em Nuvem

O uso de recursos de Computação em Nuvem para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por normas específicas, atendendo à determinações desta POSIC e demais orientações governamentais e legislação em

vigor, visando garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento de um prestador de serviço.

7.19. Uso de Dispositivos Móveis

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mail da ALEGO, devem considerar, prioritariamente, os requisitos legais e a estrutura da Instituição, atendendo a esta Política de Segurança da Informação e Comunicações e regidas por normas específicas, a qual contemplará recomendações sobre o uso desses dispositivos.

8. COMPETÊNCIAS E RESPONSABILIDADES

8.1. Cabe ao Chefe da Seção da Segurança Da Informação

a) Promover a cultura de segurança da informação e comunicações;
b) Coordenar a elaboração da Política de Segurança da Informação e Comunicações;
c) Coordenar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);
d) Coordenar as ações de segurança da informação e comunicações;
e) Promover e disseminar a cultura da Segurança da Informação e Comunicações;
f) Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e submeter à Diretoria de Tecnologia da Informação e Secretaria-Geral da Presidência da ALEGO os resultados consolidados de tais investigações e avaliações;
g) Propor recursos necessários às ações de Segurança da Informação e Comunicações;
h) Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação e comunicações;
i) Propor normas e procedimentos relativos à Segurança da Informação e Comunicações;
j) Manter contato permanente e estreito com grupos técnicos responsáveis por resolver incidentes relacionados à segurança em sistemas computacionais (CSIRTs), para o trato de assuntos relativos à segurança da informação e comunicações, quando necessário;
k) Encaminhar os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação e Comunicações à Diretoria de Tecnologia da Informação - DTI e Secretaria-Geral da Presidência da ALEGO;

l) Prover os meios necessários para capacitação, o aperfeiçoamento técnico dos membros da ETIR, bem como prover a infraestrutura necessária para o seu funcionamento;

m) Providenciar a divulgação interna desta POSIC.

8.2. Cabe ao Conselho Gestor De Tecnologia Da Informação (CGTI)

a) Promover a cultura de segurança da informação e comunicações;

b) Implementar, acompanhar, avaliar e propor alterações desta POSIC e de suas normas;

c) Definir diretrizes estratégicas para aplicação da POSIC na ALEGO;

d) Propor normas e procedimentos relativos à SIC em conformidade com as legislações existentes sobre o tema;

e) Assessorar na implementação das ações de SIC da ALEGO;

f) Propor penações à Presidência da ALEGO em caso de violação desta POSIC;

g) Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;

h) Solicitar apurações quando da suspeita de ocorrências de quebras de SIC;

i) Avaliar, revisar e analisar criticamente a POSIC e suas normas complementares, visando a sua aderência aos objetivos institucionais da ALEGO e às legislações vigentes;

j) Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à POSIC;

k) Aprovar Plano de Investimentos em Segurança da Informação e Comunicações;

8.3. Cabe à Equipe de Tratamento de Incidentes em Redes de Computadores

a) Facilitar e coordenar as atividades de tratamento e resposta a incidentes de SIC;

b) Promover a recuperação de sistemas;

c) Agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de SIC e avaliando condições de segurança de redes por meio de verificações de conformidade;

d) Realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos, buscando causas, danos e responsáveis;

e) Analisar ataques e intrusões na rede da ALEGO;

f) Executar as ações necessárias para tratar quebras de segurança;

g) Obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causa, data da ocorrência, frequência e custos resultantes;

h) Cooperar com outras equipes de tratamento e resposta a incidentes;
i) Participar de fóruns, redes nacionais e internacionais relativas à SIC.

8.4. Cabe ao Proprietário de Ativos de Informação

a) Descrever o ativo de informação;
b) Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com esta POSIC;
c) Garantir a segurança dos ativos de informação sob sua responsabilidade por meio de monitoramento contínuo;
d) Comunicar as exigências de POSIC do ativo de informação a todos os custodiantes e usuários;
e) Conceder e revogar acessos aos ativos de informação;
f) Comunicar à ETIR os riscos e a ocorrência de incidentes de POSIC; e
g) Designar custodiante dos ativos de informação, quando aplicável.

8.5. Cabe ao Custodiante dos Ativos de Informação

a) Proteger e manter os ativos de informação;
b) Controlar o acesso, conforme requisitos definidos pelo proprietário da informação e em conformidade com esta POSIC;
c) Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com esta POSIC;

8.6. Cabe aos Terceiros e Fornecedores

a) Tomar conhecimento desta POSIC;
b) Fornecer listas atualizadas da documentação dos ativos, licenças, acordos ou direitos relacionados aos ativos de informação objetos do contrato; e
c) Fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

8.7. Cabe aos Usuários

a) Conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta POSIC, bem como os demais normativos e resoluções relacionados à Segurança da Informação e Comunicações;
b) Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e
c) Comunicar os incidentes que afetam à segurança dos ativos de informação e comunicações à ETIR.

9. DIVULGAÇÃO E CONCIENTIZAÇÃO

A divulgação das regras e orientações de segurança aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na Intranet, seminários de conscientização e quaisquer outros meios, como forma de ser criada uma cultura de segurança dentro da ALEGO.

Cabe ao Gestor de Segurança da Informação e Comunicações providenciar a divulgação interna desta POSIC e das normas, inclusive com publicação permanente na página da intranet da ALEGO, para que seu conteúdo possa ser consultado a qualquer momento e desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à POSIC.

10. ATUALIZAÇÃO E VALIDADE

A POSIC, seja ela digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

Os instrumentos normativos gerados a partir desta POSIC deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Legislativo Estadual, ou conforme os seguintes critérios:

10.1. Política de Segurança da Informação e Comunicações (POSIC):

a) Nível de Aprovação: Mesa Diretora;
b) Periodicidade de Revisão: Anual;

10.2. Notas Técnicas de Segurança da Informação:

a) Nível de Aprovação: Conselho Gestor de Tecnologia da Informação (CGTI);
b) Periodicidade de Revisão: Semestral.

10.3. Procedimentos Operacionais:

a) Nível de Aprovação: Área Técnica;
b) Periodicidade de Revisão: Semestral.

11. VALIDADE

Esta POSIC entra em vigor na data de sua publicação e tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

12. PENALIDADES

Ações que violem esta Política ou quaisquer de suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de Segurança da Informação e Comunicações serão devidamente apuradas, sendo aplicadas aos responsáveis as sanções penais, administrativas e civis cabíveis.

O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar à instituição, podendo culminar com o seu desligamento e, se aplicáveis, eventuais processos criminais.

13. SIGLAS

ABNT	Associação Brasileira de Normas Técnicas
CSIRTs	*Computer Security Incident Response Teams*
ETIR	Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
GETIR	Gestão de Tratamento de Incidentes de Segurança em Rede Computacional
GECON	Gestão de Continuidade de Negócios em Segurança da Informação e Comunicações
GESIC	Gestão de Segurança da Informação e Comunicações
GRSIC	Gestão de Riscos de Segurança da Informação e Comunicações
IEC	*International Electrotechnical Commission*
ISO	*International Organization for Standardization*
PDTIC	Plano Diretor de Tecnologia da Informação e Comunicações
POSIC	Política de Segurança da Informação e Comunicações
SIC	Segurança da Informação e Comunicações
DTI	Diretoria de Tecnologia da Informação
TI	Diretoria de Tecnologia da Informação
TIC	Tecnologia da Informação e Comunicação
DGP	Diretoria de Gestão de Pessoas
SGP	Secretaria-Geral da Presidência