Governo do Estado de São Paulo
Fundação Centro de Atendimento Socioeducativo ao Adolescente
ATI - Assessoria de Tecnologia da Informação

INSTRUÇÃO

Nº do Processo: 161.00076261/2025-79

Interessado: FUNDAÇÃO CASA, ATI - Assessoria de Tecnologia da Informação

Assunto: Política de Uso Aceitável de TI

Responsável	Assessoria de Tecnologia da Informação - ATI
Aprovado por:	Gabinete da Presidência.
Políticas Relacionadas	Política de Governança de TI, Política de Segurança da Informação, Política de Dados Pessoais e Privacidade, Política de Serviços de Mensageria e Telefonia
Localização de armazenamento	Processo SEI 161.00076261/2025-79
Data da Aprovação	Data da Assinatura
Data de revisão	
Versão	1.0

1. OBJETIVO

1.1. Esta Política de Uso Aceitável de Tecnologia da Informação (TI) tem como finalidade estabelecer diretrizes para a utilização adequada dos recursos tecnológicos disponibilizados pela Fundação CASA-SP, garantindo segurança, conformidade regulatória e eficiência operacional.

1.2. O uso adequado dos recursos de TI é fundamental para:

I. Proteger a integridade, confidencialidade e disponibilidade das informações institucionais;

II. Assegurar conformidade com a legislação vigente, incluindo a Lei Geral de Proteção de Dados Pessoais (Lei n 13.709/2018);

III. Garantir a utilização responsável e ética dos ativos de TI, prevenindo riscos operacionais, financeiros e reputacionais;

IV. Viabilizar um ambiente tecnológico seguro e eficiente, alinhado às melhores práticas de governança e segurança da informação, como ISO 27001, NIST e ITIL;

V. Estabelecer responsabilidades claras para todos os usuários no uso dos sistemas, dispositivos, redes e informações institucionais.

2. ABRANGÊNCIA

2.1. Esta política se aplica a todos os usuários que tenham acesso aos recursos tecnológicos da Fundação CASA-SP, incluindo, mas não se limitando a:

I. Servidores;

II. Estagiários e aprendizes;

III. Terceirizados e prestadores de serviço com acesso a sistemas, redes ou dados institucionais;

IV. Fornecedores e parceiros comerciais que utilizem ou tenham integração com os sistemas e infraestruturas da Fundação CASA-SP;

V. Qualquer outro indivíduo ou entidade que utilize os recursos de TI da Fundação CASA-SP mediante autorização formal.

2.2. Os usuários abrangidos por esta política são responsáveis por garantir que seu uso dos recursos de TI esteja em conformidade com as diretrizes estabelecidas, sendo passíveis de monitoramento e sanções em caso de descumprimento.

3. TERMOS E DEFINIÇÕES

I – Armazenamento Corporativo

Espaços de armazenamento disponibilizados na rede corporativa, incluindo servidores e diretórios compartilhados, utilizados para arquivamento e compartilhamento de arquivos institucionais.

II – Ataques Cibernéticos

Ações maliciosas com o objetivo de comprometer, danificar, interromper ou obter acesso não autorizado a sistemas, redes ou dispositivos da organização.

III – Categorização e Versionamento

Processo de organização e controle de versões de arquivos e documentos, garantindo que sejam corretamente identificados, classificados e mantidos conforme sua evolução.

IV – Comunicação Eletrônica

Mecanismos digitais de troca de informações, incluindo e-mails, sistemas de mensagens instantâneas e videoconferências.

V – Credenciais de Acesso

Usuário e senha, tokens, certificados digitais e demais mecanismos de autenticação utilizados para acesso aos sistemas e redes institucionais.

VI – Logs de Acesso

Registros automáticos das atividades realizadas pelos usuários nos sistemas e redes institucionais, contendo data, horário, endereço IP, identidade do usuário e ações executadas.

VII – Monitoramento e Auditoria

Processos de acompanhamento, registro e análise de logs de acesso e atividades, com o objetivo de garantir conformidade, segurança e desempenho adequado dos recursos de TI.

VIII – Phishing

Tentativa de fraude eletrônica em que criminosos se passam por entidades confiáveis para enganar usuários e obter informações sensíveis, como senhas e dados bancários.

IX – Recursos de Tecnologia da Informação (TI)

Conjunto de ativos tecnológicos disponibilizados pela organização, incluindo sistemas, dispositivos, redes, armazenamento corporativo e serviços de comunicação eletrônica.

X – Spam

Envio não autorizado e em massa de mensagens eletrônicas, geralmente de caráter publicitário, fraudulento ou contendo ameaças à segurança da informação.

XI – Uso Aceitável

Forma adequada de utilização dos sistemas, dispositivos e redes, conforme as diretrizes estabelecidas nesta política, garantindo segurança, conformidade legal e eficiência operacional.

XII – Uso Não Aceitável

Qualquer utilização dos recursos de TI que viole as disposições desta política, incluindo práticas que envolvam uso inadequado, atividades ilegais ou antiéticas, acesso não autorizado, uso indevido de credenciais e armazenamento irregular de dados.

XIII – Usuário

Qualquer pessoa autorizada a utilizar os recursos de TI da organização, incluindo servidores, terceirizados, prestadores de serviço, estagiários e demais colaboradores.

4. REFERÊNCIAS LEGAIS E BOAS PRÁTICAS

Referência	Descrição
Lei Geral de Proteção de Dados (LGPD) - Lei nº 13.709/2018	Princípios da proteção de dados pessoais, segurança e sigilo, necessidade de comunicação de incidentes de segurança.
ISO/IEC 27001 (Norma de Segurança da Informação)	Gestão de acessos, boas práticas de segurança da informação, regras de uso aceitável e monitoramento de atividades.

NIST Special Publication 800-53 (Segurança de Sistemas e Controle de Acessos)	Políticas de segurança, controle de acessos, restrição ao uso de dispositivos não autorizados, gestão de credenciais.
ITIL (Gerenciamento de Serviços de TI)	Regras para uso eficiente dos recursos de TI, boas práticas de suporte e atendimento de incidentes, organização do armazenamento.
Marco Civil da Internet (Lei nº 12.965/2014)	Direitos e deveres dos usuários no uso da internet corporativa, monitoramento e auditoria, privacidade e proteção de dados.
ISO/IEC 27002 (Código de Boas Práticas para Segurança da Informação)	Definição de responsabilidades dos usuários, controle de acessos e proibição de disseminação de software malicioso.
Resolução CGPAR nº 2/2016 (Boas Práticas de Segurança Cibernética no Setor Público)	Proibição de uso de credenciais de terceiros, boas práticas no armazenamento de dados, manutenção da integridade de equipamentos.

5. PRINCÍPIOS GERAIS

5.1. O uso dos recursos de TI da organização deve ser guiado pelos seguintes princípios:

I – Segurança da Informação

a) Garantir a proteção dos ativos digitais da organização contra acessos não autorizados, vazamentos, fraudes, ataques cibernéticos e quaisquer outras ameaças.

b) Adotar boas práticas de gerenciamento de senhas, autenticação e restrição de acessos.

c) Proteger dispositivos, redes e sistemas contra malwares, phishing e outras vulnerabilidades.

II – Conformidade Legal e Regulatória

a) Atender às exigências da legislação aplicável, incluindo a **LGPD (Lei n 13.709/2018)**, que regulamenta o tratamento de dados pessoais.

b) Cumprir normas internas e frameworks de governança de TI, como **ISO 27001 (Gestão de Segurança da Informação)** e **ITIL (Gestão de Serviços de TI)**.,

c) Respeitar as políticas institucionais de privacidade, proteção de dados e segurança da informação.

III – Responsabilidade dos Usuários

a) Utilizar os recursos de TI exclusivamente para fins institucionais, evitando usos indevidos que possam comprometer a organização.

b) Zelar pela confidencialidade, integridade e disponibilidade das informações acessadas.

c) Reportar incidentes de segurança, tentativas de fraude ou usos indevidos dos sistemas e dispositivos institucionais.

IV – Uso Racional dos Recursos

a) Evitar desperdício de recursos computacionais, como armazenamento desnecessário de arquivos, consumo excessivo de banda e processamento indevido.

b) Priorizar o uso de ferramentas institucionais para comunicação e colaboração, reduzindo dependência de soluções externas não autorizadas.

c) Seguir boas práticas na gestão e organização dos arquivos armazenados na rede corporativa, evitando sobrecarga de espaço e garantindo rastreabilidade da informação.

CAPÍTULO I – DAS REGRAS GERAIS DE USO ACEITÁVEL

Seção I – Das Disposições Gerais

Artigo 1º O uso aceitável dos recursos de Tecnologia da Informação (TI) compreende a utilização responsável, ética e segura dos sistemas, dispositivos, redes e informações institucionais, em conformidade com as diretrizes estabelecidas nesta Política**.**

Artigo 2º A presente Política aplica-se a todos os usuários, sendo de caráter obrigatório e vinculante.

Artigo 3º São princípios norteadores do uso aceitável dos recursos de TI:

I. **Legalidade**: observância das normas legais vigentes, incluindo a Lei Geral de Proteção de Dados Pessoais (Lei n 13.709/2018);

II. **Segurança**: preservação da confidencialidade, integridade e disponibilidade das informações institucionais;

III. **Responsabilidade**: dever dos usuários de zelar pelo correto uso dos recursos de TI, evitando riscos operacionais e legais para a organização;

IV. **Uso institucional**: utilização dos ativos de TI para fins exclusivamente relacionados às atividades institucionais, vedado o uso pessoal indevido ou que comprometa a eficiência operacional.

Artigo 4º O descumprimento das diretrizes desta Política poderá resultar em penalidades administrativas, civis e criminais.

Seção II – Das Regras de Utilização dos Recursos de TI

Artigo 5º Os sistemas, dispositivos e redes da organização devem ser utilizados exclusivamente para fins institucionais, sendo vedado o uso para atividades pessoais, ilícitas ou que violem normas de segurança.

Artigo 6º O uso de impressoras institucionais deve ser realizado exclusivamente para fins profissionais, respeitando critérios de necessidade e redução de desperdício, devendo, sempre que possível, utilizar a função de impressão frente e verso e a impressora preto e branco.

Artigo 7º É permitido o uso dos sistemas corporativos de TI, incluindo plataformas de gestão, bancos de dados e aplicações especializadas, desde que:

I. Respeitem as diretrizes de segurança e conformidade da Fundação CASA-SP;

II. Não comprometam o desempenho, disponibilidade ou integridade dos serviços de TI;

III. Sejam utilizados conforme os perfis e permissões atribuídos a cada usuário.

Artigo 8º A comunicação eletrônica por meio de e-mails institucionais, mensageria e videoconferências deve seguir as seguintes regras:

I. O e-mail corporativo deve ser utilizado exclusivamente para fins institucionais, sendo vedado seu uso para inscrição em serviços pessoais, disseminação de conteúdos inapropriados ou comunicação não autorizada;

II. O uso de ferramentas de mensagens instantâneas e videoconferência deve observar as diretrizes de privacidade, confidencialidade e conduta profissional;

III. É proibido o compartilhamento de informações sigilosas ou restritas por meios não autorizados ou sem a devida proteção;

IV. O usuário é responsável pelo conteúdo das mensagens enviadas e pela adoção de medidas para evitar phishing, spam e ataques cibernéticos.

Parágrafo único – O detalhamento das regras se encontra na **Política de Serviços de Mensageria e Telefonia**.

Artigo 9º O armazenamento e compartilhamento de arquivos devem seguir as seguintes diretrizes:

I. Os arquivos institucionais devem ser armazenados nos diretórios e plataformas autorizadas;

II. É proibido o armazenamento de arquivos pessoais em servidores e dispositivos corporativos;

III. O compartilhamento de arquivos deve ser realizado por canais oficiais e respeitando os níveis de acesso e classificação da informação;

IV. Dados sensíveis e informações sigilosas devem ser protegidos por medidas de segurança adequadas.

Artigo 10 O uso de software e instalação de aplicativos seguem as seguintes regras:

I. É vedada a instalação de softwares, aplicativos ou extensões não autorizadas pela ATI;

II. Todo software utilizado deve possuir licença válida e estar alinhado com as diretrizes institucionais;

III. Aplicações em nuvem e serviços de terceiros devem ser previamente avaliados quanto à conformidade com as normas internas e regulatórias;

IV. A equipe da ATI poderá revogar o acesso ou desinstalar softwares que comprometam a segurança ou o desempenho dos sistemas.

Artigo 11 O uso de dispositivos de TI no teletrabalho deve observar diretrizes que garantam a proteção dos ativos de TI e a segurança da informação, incluindo:

I. Segurança física do local de teletrabalho:

a) O usuário deve garantir que o ambiente de trabalho remoto seja seguro e protegido contra acessos indevidos;

b) Dispositivos corporativos devem ser armazenados de forma segura, evitando riscos de furto, roubo ou danos físicos;

c) Sempre que possível, recomenda-se o uso de dispositivos de segurança, como travas para notebooks e armazenamento em locais protegidos.

II. Controle de acesso a dispositivos corporativos no teletrabalho:

a) O uso dos dispositivos corporativos e senhas é restrito ao colaborador autorizado, sendo vedado o compartilhamento com terceiros, incluindo familiares e visitantes;

b) O usuário deve adotar medidas para impedir que terceiros tenham acesso a informações sensíveis exibidas na tela do dispositivo ou deixadas em documentos físicos;

c) Durante ausências temporárias, o usuário deve bloquear a sessão ou desligar o dispositivo para evitar acessos indevidos;

d) É proibida a conexão de dispositivos não autorizados aos equipamentos corporativos, como pen drives, HDs externos e outros acessórios de armazenamento não homologados pela TI.

III. Uso de VPN e conexões seguras:

a) O acesso remoto a sistemas corporativos deve ser realizado exclusivamente por meio da VPN oficial fornecida pela Assessoria de Tecnologia da Informação (ATI);

b) O usuário é responsável por garantir que a VPN esteja ativa durante todo o período de trabalho remoto ao acessar sistemas internos da organização;

c) É proibido o uso de redes Wi-Fi públicas ou inseguras para conexão com sistemas corporativos, salvo se utilizado em conjunto com VPN e demais camadas de segurança indicadas pela ATI;

d) A instalação e configuração da VPN devem seguir as orientações da ATI, sendo vedado o uso de softwares ou serviços de VPN não autorizados;

e) O usuário deve se desconectar da VPN ao finalizar o expediente ou sempre que não estiver utilizando sistemas corporativos, evitando exposição desnecessária da rede interna.

CAPÍTULO II – DAS RESTRIÇÕES E USO NÃO ACEITÁVEL

Seção I – Das Proibições Gerais

Artigo 12 São consideradas práticas vedadas no uso dos recursos de Tecnologia da Informação

(TI) da Fundação CASA-SP:

I. **Uso inadequado dos recursos tecnológicos**, incluindo atividades que comprometam a segurança, o desempenho dos sistemas ou a disponibilidade dos serviços institucionais;

II. **Utilização de recursos de TI para fins não institucionais**, como navegação em sites de entretenimento, jogos online, redes sociais pessoais e qualquer outro uso que não esteja alinhado às atividades laborais;

III. **Ações que possam comprometer a organização**, incluindo disseminação de informações falsas, conteúdo ofensivo, difamação ou qualquer prática que prejudique a imagem institucional;

IV. **Uso de tecnologia para atividades ilegais ou antiéticas**, tais como pirataria de software, disseminação de malware, envio de spam, violação de direitos autorais, assédio virtual e qualquer outra conduta ilegal;

V. **Instalação e uso de softwares não autorizados**, incluindo programas que possam comprometer a segurança da informação, aplicativos não licenciados ou serviços de armazenamento em nuvem não aprovados;

VI. **Alteração, exclusão ou manipulação indevida de registros institucionais**, sem a devida autorização ou justificativa operacional;

VII. **Atividades que comprometam a integridade da rede**, como tentativas de sobrecarga de servidores, criação de redes sem fio (Wi-Fi) paralelas dentro do ambiente corporativo, ataques cibernéticos, uso de VPNs não autorizadas, exploração de vulnerabilidades ou ações que comprometam o desempenho do ambiente computacional;

VIII. **Modificar ou remover componentes de hardware** sem autorização expressa da Gerência de Suporte ao Usuário;

IX. **Realizar por conta própria manutenção, formatação ou conserto** em ativo de TI sem autorização expressa da Gerência de Suporte ao Usuário;

X. **Exposição dos dispositivos a riscos**, como quedas, derramamento de líquidos ou ambientes inadequados;

XI. **Instalação** de repetidores, roteadores, switches ou qualquer outro equipamento de rede sem a devida homologação e autorização;

XII. **Remoção, transporte, movimentação ou transferência** de computadores e demais equipamentos de TI do local instalado sem autorização prévia da área responsável da ATI;

XIII. **Utilização de dispositivos pessoais**, como notebooks próprios, pendrives, HDs externos e smartphones, para armazenar informações institucionais sem autorização formal da área da ATI;

XIV. **Compartilhamento de dados sensíveis, pessoais ou sigilosos com ferramentas de inteligência artificial**, bem como a utilização de IA para acessar, modificar ou extrair informações de sistemas corporativos sem autorização formal da ATI.

Artigo 13 É expressamente proibido o acesso não autorizado a sistemas, sites, aplicativos e informações institucionais, sendo vedado:

I. **Tentativa de burlar ou contornar mecanismos de segurança** para obter acesso privilegiado a sistemas, sites, aplicativos, redes ou informações restritas;

II. **Acesso a dados confidenciais sem a devida autorização**, ainda que o usuário possua

credenciais técnicas que permitam a visualização ou manipulação dos dados;

III. **Compartilhamento de informações sensíveis ou sigilosas** sem a devida autorização, independentemente do meio utilizado (e-mail, mídias removíveis, mensageria, entre outros).

Artigo 14 O uso de credenciais de terceiros é estritamente proibido, sendo vedado:

I. **Compartilhar senhas ou credenciais de acesso**, incluindo tokens, cartões de segurança e autenticação multifator, com qualquer outro usuário, independentemente do nível hierárquico ou da relação funcional;

II. **Utilizar credenciais de outro usuário** para acessar sistemas ou recursos institucionais, mesmo que autorizado verbalmente pelo titular da conta;

III. **Permitir que terceiros acessem sistemas utilizando credenciais próprias** ou dispositivos autenticados em seu nome.

Seção II – Das Restrições à Armazenagem de Dados

Artigo 15 O espaço de armazenamento na rede corporativa deve ser utilizado de forma responsável, visando à eficiência, segurança e conformidade com as diretrizes institucionais, sendo vedado:

I. O armazenamento de arquivos pessoais, como fotos, vídeos, músicas, programas ou qualquer outro conteúdo que não seja estritamente necessário para a execução das atividades institucionais;

II. A duplicação desnecessária de arquivos e documentos, comprometendo o espaço disponível e a eficiência da gestão da informação;

III. A utilização extensiva do armazenamento para guarda de documentos criados digitalmente no SEI-SP;

IV. Armazenamento de arquivos institucionais no desktop ou no computador;

V. O uso de servidores institucionais para backup de dispositivos pessoais ou armazenamento de dados externos sem autorização da equipe de TI.

Artigo 16 O armazenamento e organização de arquivos devem seguir padrões estabelecidos para facilitar a recuperação da informação e evitar desperdício de espaço, incluindo:

I. Adoção de nomenclaturas padronizadas para arquivos e pastas;

II. Adoção de nomenclatura padronizada para pastas, baseada em assuntos ou temas institucionais, como competências, projetos, processos, unidades organizacionais ou outros critérios que facilitem a identificação, organização e recuperação das informações, em vez de nomes individuais de servidores das áreas;

III. Utilização de diretórios institucionais definidos pela ATI para cada setor, evitando a fragmentação desnecessária da informação;

IV. Aplicação de categorização e versionamento adequado para evitar arquivos desatualizados ou redundantes;

a. A categorização deve seguir critérios padronizados, como tipo de documento, data, área responsável e status de uso;

b. O versionamento deve adotar convenções claras de nomenclatura, como inclusão de número de versão (v1, v2, v3) ou data de última modificação, evitando múltiplas cópias desnecessárias do mesmo arquivo.

V. Evitar nomes extensos para pastas e arquivos.

Artigo 17 É proibido armazenar os seguintes tipos de dados nos ambientes corporativos:

I. Arquivos de caráter pessoal que não tenham relação com as atividades institucionais;

II. Software ou scripts não licenciados, cracks, keygens ou qualquer ferramenta que possa comprometer a segurança da organização;

III. Dados sigilosos em diretórios de acesso irrestrito, sem mecanismos adequados de controle de acesso;

IV. Documentos que violem direitos autorais ou normativas de proteção de dados.

Artigo 18 A retenção e exclusão de arquivos devem seguir as diretrizes estabelecidas pela ATI, observando-se as seguintes regras:

I. Arquivos institucionais devem ser mantidos pelo período mínimo determinado nas normas internas e legislações aplicáveis;

II. Dados considerados obsoletos ou desnecessários devem ser excluídos de forma segura, garantindo a proteção contra recuperação indevida;

III. O usuário deve monitorar regularmente a utilização de espaço em caixas de e-mail e pastas de armazenamento para evitar congestionamento e falhas operacionais;

IV. A equipe da ATI poderá realizar auditorias e campanhas de limpeza periódicas para garantir o uso adequado do espaço de armazenamento;

V. Informações sigilosas devem ser excluídas conforme os padrões de descarte seguro.

CAPÍTULO III – DO MONITORAMENTO E DA AUDITORIA

Seção I – Do Direito de Monitoramento e Auditoria

Artigo 19 A Fundação CASA-SP detém o direito de monitorar e auditar o uso dos recursos de Tecnologia da Informação (TI), visando à segurança da informação, à conformidade com normas internas e externas, e à prevenção de atividades indevidas, garantindo a continuidade dos serviços institucionais.

Artigo 20 O monitoramento e auditoria serão conduzidos com base nos seguintes princípios:

I. **Legalidade:** As atividades de monitoramento e auditoria seguirão as normativas legais, incluindo a **Lei Geral de Proteção de Dados Pessoais (LGPD – Lei n 13.709/2018)** e demais regulamentos aplicáveis;

II. **Proporcionalidade:** O monitoramento será realizado de forma razoável, observando-se a necessidade, finalidade e minimização de impacto sobre a privacidade dos usuários;

III. **Transparência:** A organização comunicará previamente aos usuários, por meio desta política e outros instrumentos normativos, sobre a existência do monitoramento e suas finalidades;

IV. **Confidencialidade:** As informações coletadas durante os processos de auditoria e

monitoramento serão protegidas e utilizadas exclusivamente para os fins institucionais previstos nesta política.

Artigo 21 O uso dos recursos de TI disponibilizados pela Fundação CASA-SP não configura privacidade individual irrestrita, sendo permitida a inspeção dos dados, tráfego e atividades realizadas nos dispositivos, redes e sistemas institucionais.

Seção II – Do Registro e Análise de Logs

Artigo 22 O registro de logs de acesso e atividades será realizado de forma contínua, visando à detecção de incidentes, auditoria de conformidade e análise de segurança.

Artigo 23 A obtenção e retenção dos registros de logs seguirá as diretrizes da **Política de Dados Pessoais e Privacidade**, sendo vedada a eliminação prematura sem justificativa formal e autorização dos responsáveis da Seção de Segurança da Informação.

Seção III – Dos Procedimentos para Fiscalização e Conformidade

Artigo 24 A ATI poderá realizar auditorias periódicas e monitoramento contínuo durante as atividades de trabalho para avaliar a conformidade do uso dos recursos de TI.

Artigo 25 Caso sejam identificadas irregularidades ou infrações às diretrizes desta política, serão adotadas as seguintes medidas:

I. Notificação do usuário responsável e gestor para esclarecimento e eventual correção da conduta;

II. Aplicação de medidas corretivas, incluindo revogação de acessos ou suspensão de contas, conforme a gravidade da infração;

III. Encaminhamento do caso às instâncias disciplinares e administrativas competentes para avaliação e aplicação de sanções, quando necessário;

IV. Comunicação às autoridades competentes em casos de violação de normas legais.

Artigo 26 As auditorias e fiscalizações poderão ser realizadas por equipes internas da ATI, conforme necessidade.

CAPÍTULO IV – DAS DISPOSIÇÕES FINAIS

Artigo 27 Qualquer incidente, falha ou comportamento anômalo relacionado ao uso dos recursos de TI deve ser comunicado imediatamente à Seção de Atendimento ao Usuário, incluindo, mas não se limitando a:

I. Tentativas de acesso não autorizado a recursos, sistemas ou dados institucionais;

II. Falhas de funcionamento em softwares ou equipamentos que impactem a produtividade ou segurança;

III. Mensagens suspeitas de phishing, ataques cibernéticos ou tentativas de engenharia social;

IV. Incidentes de segurança relacionados ao uso indevido de credenciais, como suspeitas de invasão, comprometimento de contas ou tentativas de acesso não autorizado;

V. Qualquer problema ou dano observado nos dispositivos de TI.

Artigo 28 Esta política será revisada periodicamente, conforme a necessidade e evolução das

melhores práticas de governança de TI, segurança da informação e mudanças na legislação aplicável.

Artigo 29 Alterações na Política deverão ser submetidas à aprovação do Gabinete da Presidência.

São Paulo, na data da assinatura digital.

Raelen Bego Luiz
Chefe de Gabinete

Leandro Timossi de Almeida
Assessor da Presidência

Documento assinado eletronicamente por **Leandro Timossi de Almeida**, **Assessor da Presidência II**, em 24/03/2025, às 12:51, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

Documento assinado eletronicamente por **Raelen Bego Luiz**, **Chefe de Gabinete**, em 24/03/2025, às 17:21, conforme horário oficial de Brasília, com fundamento no Decreto Estadual nº 67.641, de 10 de abril de 2023.

A autenticidade deste documento pode ser conferida no site https://sei.sp.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0 , informando o código verificador **0060869675** e o código CRC **4FC8C177**.