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

INSTRUÇÃO

Nº do Processo: 161.00063624/2025-14

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

Assunto: Política de Segurança da informação

HISTÓRICO DE VERSÕES

Data	Versão	Descrição	Autor
03/2025	1.0	Política de Segurança da Informação	Leandro Timossi de Almeida

PROPÓSITO

Esta Política de Segurança da Informação tem como objetivo estabelecer os princípios, diretrizes, responsabilidades e práticas para a proteção das informações da Fundação CASA-SP. A Política visa garantir a confidencialidade, integridade e disponibilidade das informações, assegurando o seu uso adequado e a mitigação de riscos à segurança da informação, bem como o cumprimento da Lei Geral de Proteção de Dados Pessoais (LGPD) e de outras normas vigentes.

Esta Política está prevista na Portaria Normativa 468/2024 que institui a Política de Governança de Tecnologia da Informação (TI) no âmbito da Fundação CASA-SP.

ESCOPO

Instituir a Política de Segurança da Informação (PSI), no âmbito da Fundação CASA-SP, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações e controles que garantam a segurança das informações e de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

Esta Política se aplica a todos os ativos de informação da Fundação CASA-SP, incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, funcionários, contratados, parceiros e terceiros que acessam ou processam as informações da Fundação CASA-SP. Esta política se aplica em todas as instalações físicas administradas ou utilizadas pela Fundação CASA-SP.

TERMOS E DEFINIÇÕES

AMEAÇA CIBERNÉTICA: Potencial evento ou ação que pode causar danos a sistemas ou informações;

ATIVOS DE TIC: são todos os itens, físicos ou virtuais, que compõem a infraestrutura de TIC da instituição, ou seja, tudo que é hardware, software, redes e outras tecnologias fundamentais para a continuidade das operações de quase todo tipo de negócio;

CIBERSEGURANÇA: Conjunto de práticas e medidas destinadas a garantir a segurança física e lógica de sistemas, redes e dados, assegurando a confidencialidade, integridade e disponibilidade das informações;

CONFIDENCIALIDADE: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada à pessoa, ao sistema, ao órgão ou à entidade não autorizados nem credenciados;

CONTROLE DE ACESSO: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso à informação;

DADO PESSOAL: informação relacionada a pessoa natural identificada ou identificável;

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;

DIAGNÓSTICO DE CIBERSEGURANÇA: Avaliação da postura de segurança de um órgão ou entidade, identificando vulnerabilidades, ameaças e riscos em seus ativos tecnológicos

DISPONIBILIDADE: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

INTEGRIDADE: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

MODELO DAS 7 CAMADAS DE SEGURANÇA: Estabelece a implementação de múltiplas camadas de proteção, fundamentadas no princípio de Defesa em Profundidade, com o objetivo de garantir a segurança dos sistemas, redes e dados, abordando aspectos específicos, a saber:

Camada de Perímetro: Proteção da fronteira entre a rede interna e o ambiente externo, objetivando impedir que ameaças externas tenham acesso não autorizado ao sistema;

Camada de Rede: Proteção do tráfego de dados dentro da rede, objetivando controlar a comunicação interna, identificar e isolar ameaças;

Camada de Aplicação: Proteção das aplicações contra vulnerabilidades e acessos indevidos, objetivando garantir que as aplicações operem de forma segura, prevenindo falhas que possam ser exploradas;

Camada de Endpoint: Proteção dos dispositivos que acessam a rede, objetivando proteger os dispositivos contra malware e tentativas de acesso não autorizadas;

Camada de Ativos Críticos: Proteção dos sistemas e servidores críticos para a operação, objetivando assegurar que os sistemas essenciais estejam protegidos contra ataques e falhas;

Camada de Dados: Proteção dos dados em repouso e em trânsito, objetivando garantir que os dados estejam seguros contra acessos indevidos e vazamentos;

Camada Humana: Foco na conscientização e treinamento dos usuários, objetivando prevenir falhas humanas e comportamentos de risco cibernético.

IMPACTO: Consequência negativa resultante da exploração de uma vulnerabilidade, podendo incluir perdas financeiras, interrupção de serviços, danos à reputação e vazamento de dados.

NIST Cybersecurity Framework: conjunto de diretrizes e boas práticas desenvolvido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (NIST) e oferecem uma abordagem estruturada para a gestão de riscos cibernéticos, auxiliando as organizações a identificar, proteger, detectar e responder a incidentes de segurança;

PSI: Política de Segurança da Informação;

RECURSOS DE TIC: consideram-se recursos de TIC o conjunto formado pelos bens e serviços de TIC que constituem a infraestrutura tecnológica de suporte automatizado ao ciclo da informação, que envolve as atividades de produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação;

RISCO CIBERNÉTICO: Probabilidade de ocorrência de uma ameaça explorando uma vulnerabilidade, causando impacto negativo;

SEGURANÇA DA INFORMAÇÃO: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

TIC: tecnologia da informação e comunicação;

TITULAR DO DADO: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

USUÁRIO: é qualquer pessoa, física ou jurídica, com vínculo formal direto ou indireto com a Fundação CASA-SP, ou em condição autorizada, que utiliza, de qualquer forma, algum recurso de TIC da instituição;

VULNERABILIDADE: Fragilidade que pode ser explorada para comprometer a segurança de um sistema.

DECLARAÇÕES DA POLÍTICA

Art. 1º. Fica instituída a Política de Segurança da Informação da Fundação CASA-SP, com a finalidade de estabelecer princípios, diretrizes, responsabilidades e competências para a gestão da segurança da informação.

Art. 2º. Esta Política de Segurança da Informação aplica-se a todas as unidades organizacionais da Fundação CASA-SP, e deverá ser observada por todos os usuários de informação, seja servidor ou equiparado, empregado, prestador de serviços ou pessoa habilitada pela administração, por meio da assinatura de Termo de Responsabilidade, para acessar os ativos de informação sob responsabilidade desta Fundação.

CAPÍTULO I - DISPOSIÇÕES GERAIS

Art. 3º. São objetivos da Política de Segurança da Informação:

I. estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

II. estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da

disponibilidade, integridade, confiabilidade e autenticidade das informações;

III. estabelecer competências e responsabilidades quanto à segurança da informação;

IV. nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;

V. promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional da Fundação CASA-SP.

CAPÍTULO II - DOS PRINCÍPIOS E DIRETRIZES

Art. 4º. As ações de segurança da informação da Fundação CASA-SP são norteadas pelos princípios constitucionais e administrativos que norteiam a Administração Pública, bem como pelos seguintes princípios:

I. abordagem sistêmica, com consideração integrada de todos os aspectos da segurança da informação;

II. gestão de riscos, com identificação e mitigação contínua de riscos cibernéticos;

III. defesa em profundidade, com implementação de múltiplas camadas de segurança para proteção reforçada;

IV. cooperação, com colaboração entre órgãos e entidades para compartilhamento de informações e estratégias;

V. cultura de segurança, com promoção de valores e comportamentos que priorizem a segurança em todas as atividades;

VI. disponibilidade, integridade, confidencialidade e autenticidade das informações;

VII. continuidade dos processos e serviços essenciais para o funcionamento da Fundação CASA-SP;

VIII. economicidade da proteção dos ativos de informação;

IX. respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

X. observância da publicidade como preceito geral e do sigilo como exceção;

XI. responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

XII. alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico da Fundação CASA-SP;

XIII. conformidade das normas e das ações de segurança da informação com a legislação regulamentos aplicáveis; e

XIV. educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

Art. 5º. Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito desta Fundação e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

Art. 6º. As normas, procedimentos, manuais e metodologias de segurança da informação da Fundação CASA-SP devem considerar, como referência, além dos normativos vigentes, as melhores práticas de segurança da informação.

Art. 7º. As ações de segurança da informação devem:

I. considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade da Fundação CASA-SP;

II. ser tratadas de forma integrada, respeitando as especificidades das áreas da Fundação CASA-SP;

III. ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;

IV. visar à prevenção da ocorrência de incidentes.

Art. 8º. O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos à Fundação CASA-SP.

Art. 9º. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada na Fundação CASA-SP compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

Parágrafo único. As informações citadas no caput, que tramitem pelo ambiente computacional da Fundação CASA-SP, são passíveis de monitoramento e auditoria pela Assessoria de Tecnologia da Informação, respeitados os limites legais.

Art. 10. Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

Parágrafo único. É condição para acesso aos recursos de tecnologia da informação da Fundação CASA-SP a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, as responsabilidades e os compromissos em decorrência deste acesso, bem como as penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação da Fundação CASA-SP.

Art. 11. A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação da Fundação CASA-SP, devem ser divulgadas amplamente a todos os Usuários de Informação, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

§ 1º Os Usuários de Informação devem ser continuamente capacitados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atribuições, de modo a minimizar possíveis riscos à segurança da informação.

§ 2º As ações de capacitação previstas no § 1º devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

Art. 12. Todos os contratos de prestação de serviços firmados pela Fundação CASA-SP que envolvam acesso a sistemas, dados ou outros recursos de TI conterão cláusula específica sobre a obrigatoriedade de atendimento à esta Política de Segurança da Informação, bem como suas normas decorrentes.

CAPÍTULO III - DA GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Art. 13. A estrutura de Gestão de Segurança da Informação é composta por:

I. Gabinete da Presidência;

II. Assessoria de Tecnologia da Informação;

III. Gestor da Gerência de Infraestrutura e Segurança da Informação;

IV. Gestor da Seção de Segurança da Informação;

V. Equipe da Seção de Segurança da Informação;

VI. Equipe da Seção de Suporte Técnico;

VII. Núcleo de Apoio Tecnológico;

VIII. Encarregado pelo Tratamento de Dados Pessoais;

IX. Usuários de Informação.

Art. 14. Compete ao Gabinete da Presidência:

I. fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação da Fundação CASA-SP, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados; e

II. aprovar a Política de Segurança da Informação da Fundação CASA-SP, bem como suas alterações e atualizações.

Art. 15. Compete ao Gestor da Assessoria de Tecnologia da Informação:

I. assessorar na implementação das ações de segurança da informação;

II. constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

III. participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

IV. propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

V. deliberar sobre normas internas de segurança da informação;

VI. avaliar as ações propostas pelo gestor de segurança da informação;

VII. formalizar a Política de Segurança da Informação da Fundação CASA-SP, bem como suas alterações e atualizações.

Art. 16. Compete ao Gestor da Gerência de Infraestrutura e Segurança da Informação planejar, implementar e melhorar continuamente os controles de privacidade e segurança da informação em soluções de tecnologia da informação e comunicações, considerando a cadeia de suprimentos relacionada à solução.

Art. 17. Compete ao Gestor de Segurança da Informação:

I. coordenar a elaboração da Política de Segurança da Informação - PSI e das normas internas de

segurança da informação da Fundação CASA-SP, observadas a legislação vigente e as melhores práticas sobre o tema;

II. assessorar o Gestor da Gerência de Infraestrutura e Segurança da Informação na implementação da Política de Segurança da Informação;

III. estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

IV. promover a divulgação da política e das normas internas de segurança da informação da Fundação CASA-SP a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

V. incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

VI. propor recursos necessários às ações de segurança da informação;

VII. acompanhar os trabalhos da equipe da Seção de Segurança da Informação na Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

VIII. verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

IX. acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação.

Art. 18. Compete à Equipe da Seção de Segurança da Informação a Prevenção, Tratamento e Respostas a Incidentes Cibernéticos, atuando para:

I. facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos na Fundação CASA-SP;

II. monitorar continuamente as redes computacionais;

III. detectar e analisar ataques e intrusões;

IV. tratar incidentes de segurança da informação;

V. identificar vulnerabilidades e artefatos maliciosos;

VI. recuperar sistemas de informação;

VII. garantir a aplicação ágil de patches de segurança e atualizações nos servidores, protegendo aplicações e infraestrutura contra vulnerabilidades conhecidas;

VIII. promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação.

Art. 19. Compete à equipe da Seção de Suporte Técnico:

I. garantir a aplicação ágil de patches de segurança e atualizações nos endpoints, protegendo aplicações e infraestrutura contra vulnerabilidades conhecidas;

II. homologar softwares para instalação observando as vulnerabilidades de segurança.

Art. 20. Compete ao Núcleo de Apoio Tecnológico:

I. incorporar práticas de segurança em todas as etapas do desenvolvimento de software, incluindo análise de requisitos, implementação de controles e realização de testes de segurança;

II. projetar soluções alinhadas aos princípios de segurança da organização e em conformidade com a Política de Segurança da Informação;

III. adotar práticas de desenvolvimento seguro, como revisão de código, análise estática e dinâmica, e treinamento contínuo da equipe em segurança;

IV. manter sistemas seguros de gerenciamento de configuração e controle de versão, garantindo rastreabilidade e controle das alterações no código e infraestrutura;

V. realizar implantações e atualizações de forma segura e controlada, minimizando riscos de vulnerabilidades ou interrupções operacionais;

VI. estabelecer processos e sistemas para monitoramento contínuo, identificando e respondendo a incidentes de segurança em colaboração com as equipes de segurança e operações;

VII. garantir a aplicação ágil de patches de segurança e atualizações nos sistemas desenvolvidos internamente, protegendo aplicações e infraestrutura contra vulnerabilidades conhecidas;

VIII. implementar controles rigorosos de acesso e autenticação, assegurando que apenas usuários e sistemas autorizados possam acessar ou modificar ativos organizacionais.

Art. 21. Compete ao Encarregado pelo Tratamento dos Dados Pessoais, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os 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.

Art. 22. Compete aos Usuários de Informação conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação da Fundação CASA-SP.

Parágrafo único. Todos os Usuários de Informação são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

Art. 23. A Política de Segurança da Informação e demais normativos decorrentes desta Política integram o arcabouço normativo da Gestão de Segurança da Informação.

Art. 24. A Gestão da Segurança da Informação é constituída, 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 comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;

VI. controles de acesso;

VII. gestão de riscos;

VIII. gestão de continuidade;

IX. auditoria e conformidade;

Parágrafo único - Assessoria de Tecnologia da Informação poderá definir outros processos de Gestão de Segurança da Informação, desde que alinhados aos princípios e às diretrizes desta Política e destinados à implementação de ações de segurança da informação.

Art. 25. Os processos presentes no artigo 24 serão regulamentados em conformidade com a legislação vigente, com as boas práticas de segurança de informação e com a Portaria Normativa 468/2024, nas seguintes políticas:

I. Política de Backup e Recuperação de Dados

II. Política de Continuidade Operacional de TI

III. Política de Gestão de Acessos

IV. Política de Gestão de Ativos de TI

V. Política de Gestão de Capacidade e Desempenho

VI. Política de Gestão de Incidentes e Problemas

VII. Política de Gestão de Mudanças

VIII. Política de Gestão de Serviços de TI

IX. Política de Proteção de Dados e Privacidade

X. Política de Serviços de Mensageria e Telefonia

XI. Política de Uso Aceitável de TI

Art. 26. As políticas devem abordar, no mínimo, aspectos relacionados:

I. à inclusão das diretrizes e práticas do Framework NIST de Cibersegurança, abrangendo as funções de identificar, proteger, detectar, responder e recuperar, bem como a definição de responsabilidades e a periodicidade de revisão e atualização;

II. a conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;

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

IV. a 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;

V. ao uso aceitável da informação e a utilização de mídias de armazenamento;

VI. a entrada e saída de ativos de informação das instalações da Fundação CASA-SP;

VII. aos perímetros de segurança da Fundação CASA-SP;

VIII. aos controles de acesso baseados no princípio do menor privilégio;

IX. as etapas de identificação, contenção, erradicação e recuperação e atividades pós incidente;

X. aos critérios para a comunicação de incidentes aos titulares de dados pessoas e a ANPD;

XI. a Política de Gestão de Ativos da Fundação CASA-SP, abordando aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para o a organização; a manutenção de inventario atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança; uso aceitável de ativos, vedado o uso para fins particulares de seu responsável; o mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências; o monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade; a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;

XII. a utilização adequada dos recursos operacionais e de comunicações fornecidos pela Fundação CASA-SP, a serem utilizados para fins profissionais, relacionados às atividades da Fundação CASA-SP, em conformidade com os princípios éticos e profissionais da Fundação CASA-SP, evitando comportamentos antiéticos, discriminatórios, ofensivos ou que possam comprometer a reputação da Fundação CASA-SP;

XIII. aos procedimentos para o uso de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

XIV. o acesso à internet, o download de arquivos da internet, vedado o uso de sites inadequados e a instalação de software não autorizado;

XV. o uso de mídias sociais, a divulgação de informações nas mídias sociais, o uso de contas pessoais para fins profissionais e a interação com estranhos nas mídias sociais;

XVI. as 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. as 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 Fundação CASA;

XVIII. as políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando a análise do ambiente da Fundação CASA-SP, 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 a se concretizar e o impacto potencial nos ativos de informação, bem como quais riscos devem ser priorizados para tratamento; 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;

XIX. as políticas e procedimentos para Gestão de Continuidade Operacional da Fundação CASA-SP, incluindo o Plano de Continuidade para garantir que a Fundação CASA-SP possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Continuidade para garantir sua eficácia;

XX. as políticas e procedimentos para a Gestão de Mudanças nos ativos de informação da organização, respaldado 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.

§ 1º As unidades organizacionais da Fundação CASA-SP devem realizar periodicamente auditorias internas de sua segurança da informação para assegurar que ela esteja em conformidade com esta Política e com outros requisitos de segurança da informação aplicáveis.

§ 2º Todas as ações, realizadas pelas unidades organizacionais da Fundação CASA-SP, que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis à esta temática.

§ 3º As atividades, produtos e serviços desenvolvidos na Fundação CASA-SP devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes de leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

CAPÍTULO IV - DO DIAGNÓSTICO E AVALIAÇÃO DE MATURIDADE EM CIBERSEGURANÇA E RECOMENDAÇÕES

Art. 27. Devem ser realizados diagnósticos periódicos de cibersegurança, com o objetivo de identificar vulnerabilidades, ameaças e riscos nos ambientes tecnológicos, abrangendo hardware, software, redes, dados, processos e pessoas.

Art. 28. O diagnóstico de cibersegurança deverá contemplar, no mínimo, as seguintes etapas:

I. Análise de Vulnerabilidades: Identificação de fragilidades em sistemas, aplicações e infraestrutura de rede, utilizando ferramentas e metodologias adequadas;

II. Avaliação de Risco: Análise do potencial impacto das vulnerabilidades identificadas, considerando a probabilidade de ocorrência e o possível dano aos ativos;

III. Análise de Superfície de Ataque: Mapeamento dos pontos de entrada e vetores de ataque potenciais, incluindo endpoints, aplicações, usuários e infraestrutura de rede;

IV. Monitoramento de Tráfego de Rede: Análise do tráfego de rede para identificar comportamentos anômalos, tentativas de intrusão e comunicações com fontes maliciosas;

V. Análise de Logs: Coleta e exame dos registros de segurança para identificar eventos suspeitos e investigar incidentes.

Art. 29. A avaliação de maturidade em cibersegurança deve ser realizada com base no modelo das 7 (sete) Camadas de Segurança, considerando os seguintes aspectos:

I. Camada de Perímetro: Proteção da fronteira da rede contra acessos não autorizados;

II. Camada de Rede: Segurança do tráfego interno e detecção de atividades maliciosas;

III. Camada de Aplicação: Garantia da integridade e segurança dos sistemas e aplicações;

IV. Camada Humana: Conscientização e treinamento dos usuários para prevenir erros e ações maliciosas;

V. Camada de Endpoint: Proteção dos dispositivos finais que acessam a rede;

VI. Camada de Ativos Críticos: Segurança reforçada em sistemas e servidores essenciais;

VII. Camada de Dados: Salvaguarda das informações, assegurando confidencialidade, integridade e disponibilidade.

Art. 30. Ao final do diagnóstico e da avaliação de maturidade, recomenda-se a elaboração de um relatório contendo:

I. Resultados Encontrados: Detalhamento das vulnerabilidades e riscos identificados;

II. Recomendações de Cibersegurança: Sugestões de medidas para mitigar riscos e corrigir vulnerabilidades;

III. Plano de Ação: Proposta de cronograma e responsabilidades para a implementação das melhorias necessárias.

CAPÍTULO V - DAS VEDAÇÕES E DISPOSIÇÕES FINAIS

Art. 31. É vedada a utilização dos recursos de tecnologia da informação disponibilizados pela Fundação CASA-SP para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

Art. 32. São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pela Fundação CASA-SP.

Art. 33. É vedada a divulgação a terceiros de mecanismos de identificação, autenticação e autorização baseados em conta e senha ou certificação digital, de uso pessoal e intransferível, que são fornecidos aos usuários.

Art. 34. É vedada a exploração de eventuais vulnerabilidades, as quais devem ser comunicadas às instâncias superiores assim que identificadas.

Art. 35. As unidades organizacionais da Fundação CASA-SP devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

Parágrafo único. A conscientização, a capacitação e a sensibilização em segurança da informação devem ser adequadas aos papéis e responsabilidades dos colaboradores.

Art. 36. As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através do seguinte canal: ati@fundacaocasa.sp.gov.br

Art. 37. O cumprimento desta Política, bem como dos normativos que a complementam devem ser avaliados pela Assessoria de Tecnologia da Informação periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de segurança da informação e da garantia de cláusula de responsabilidade e sigilo constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 38. A não observância do disposto nesta Política, bem como em seus instrumentos normativos correlatos, sujeita o infrator à aplicação de sanções administrativas conforme a legislação vigente, sem prejuízo das responsabilidades penal e civil, assegurados sempre aos envolvidos o contraditório e a ampla defesa.

Art. 39. Esta Política será revisada periodicamente, pelo menos a cada quatro anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente da Fundação CASA-SP, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

Art. 40. Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos devem ser submetidas à Assessoria de Tecnologia da Informação.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27701:2019: **Técnicas de segurança — Extensão da ABNT NBR ISO/IEC 27001 e ABNT NBR ISO/IEC 27002 para gestão da privacidade da informação** — Requisitos e diretrizes. Rio de Janeiro, 2019.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27001:2022: **Segurança da informação, segurança cibernética e proteção à privacidade — Sistemas de gestão da segurança da informação — Requisitos**. Rio de Janeiro, 2022.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS: ABNT NBR ISO/IEC 27002:2022: **Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação— Requisitos**. Rio de Janeiro, 2023.

BRASIL. Presidência da República. Gabinete de Segurança Institucional. **Decreto nº 9.637, de 26 de dezembro de 2018. Política Nacional de Segurança da Informação – PNSI**. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015- 2018/2018/Decreto/D9637.html. Acesso em: 17 jun. 2024.

DIRETORIA DE PRIVACIDADE E SEGURANÇA DA INFORMAÇÃO DA SECRETARIA DE GOVERNO DIGITAL – DPSI/SGD. **Guia do Framework de Privacidade e Segurança da Informação. Março 2024**. Disponível em:https://www.gov.br/governodigital/pt-br/privacidade-e-seguranca/ppsi/guia_framework_psi.pdf . Acesso em: 25 jun. 2024.

BRASIL. Presidência da República. Agência Nacional de Proteção de Dados - ANPD. **Guia Orientativo - Tratamento de dados pessoais pelo Poder Público. Junho 2023.** Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/guia-poder-publico-anpd-versao-final.pdf. Acesso em: 01 jul. 2022.

SÃO PAULO (ESTADO). Secretaria de Gestão e Governo Digital do Estado de São Paulo. Fundação CASA-SP Resolução SGGD nº 33, de 07-10-2024. Institui o Guia de Boas Práticas em Cibersegurança no âmbito da Administração Pública direta e autárquica do Estado de São Paulo.

SÃO PAULO (ESTADO). Fundação CASA-SP. Portaria Normativa 468 de 2024. Institui a Política de Governança de Tecnologia da Informação (TI) no âmbito da Fundação CASA-SP.

Raelen Bego Luiz
Chefe de Gabinete

Leandro Timossi de Almeida
Assessor da Presidência

São Paulo, na data da assinatura digital.

Documento assinado eletronicamente por **Leandro Timossi de Almeida**, **Assessor da Presidência II**, em 13/03/2025, às 16:28, 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 18/03/2025, às 22:30, 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 **0059261952** e o código CRC **E30495D7**.