

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO – PSI





ESTADO DO RIO DE JANEIRO

PREFEITURA MUNICIPAL DE SAPUCAIA

PREFEITURA MUNICIPAL DE SAPUCAIA

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO — PSI

CONSIDERANDO que a manutenção de níveis adequados de segurança das informações tratadas pela Prefeitura Municipal de Sapucaia é requisito essencial para a continuidade, confiabilidade e qualidade dos serviços públicos prestados à sociedade;

CONSIDERANDO a necessidade de assegurar a integridade, disponibilidade, confidencialidade e autenticidade das informações tratadas pela Prefeitura Municipal de Sapucaia, de modo a preservar a confiabilidade de seus processos, sistemas e serviços;

CONSIDERANDO que as informações sob responsabilidade da Prefeitura Municipal de Sapucaia são armazenadas e tratadas em diferentes formatos e veiculadas por diferentes meios, físicos e digitais, estando sujeitas a riscos decorrentes de desastres naturais, acessos não autorizados, uso inadequado, falhas de equipamentos e sistemas, extravio, furto e outros eventos que possam comprometer sua segurança;

CONSIDERANDO a necessidade de aprimoramento contínuo das ações de governança e gestão da Segurança da Informação, de forma compatível com a evolução dos riscos e das ameaças cibernéticas que possam afetar a Administração Pública Municipal;

CONSIDERANDO a necessidade de integração entre as ações de Segurança da Informação, segurança cibernética, privacidade e proteção de dados pessoais, em conformidade com a legislação, as normas e os requisitos aplicáveis à Prefeitura Municipal de Sapucaia, tendo como referências a Política Nacional de Segurança da Informação, instituída pelo Decreto nº 12.572/2025, a Estratégia Nacional de Cibersegurança, instituída pelo Decreto nº 12.573/2025, o Programa de Privacidade e Segurança da Informação – PPSI do Governo Federal e a ABNT NBR ISO/IEC 27701, em sua edição vigente.

A PREFEITURA MUNICIPAL DE SAPUCAIA, por meio de sua Alta Administração,

ESTABELECE:

CAPÍTULO I

DISPOSIÇÕES INICIAIS

Art. 1º Esta Política institui a Política de Segurança da Informação — PSI no âmbito da Prefeitura Municipal de Sapucaia.

Parágrafo único. Todos os instrumentos normativos gerados a partir da Política de Segurança da Informação são partes integrantes desta e emanam dos princípios e diretrizes nela estabelecidos.

Art. 2º Esta Política e suas normas complementares aplicam-se a todas as áreas, órgãos e unidades da Prefeitura Municipal de Sapucaia, bem como aos seus agentes públicos, independentemente de cargo, função ou vínculo, e a prestadores de serviços, estagiários e demais pessoas físicas ou jurídicas que, por qualquer meio ou instrumento, tenham acesso, utilizem, armazenem, transmitam ou tratem informações sob responsabilidade da Prefeitura Municipal de Sapucaia.

Parágrafo único. Os prestadores de serviços e demais pessoas físicas ou jurídicas vinculadas à Prefeitura Municipal de Sapucaia por contratos, convênios, acordos ou instrumentos congêneres deverão observar as disposições desta Política e de suas normas complementares, naquilo que lhes for aplicável, especialmente quando houver acesso ou tratamento de informações da Prefeitura, observados os requisitos e prazos estabelecidos pela Administração Municipal.

Art. 3º Todos os processos de contratação de produtos e serviços, convênios, acordos e outros instrumentos congêneres celebrados pela Prefeitura Municipal de Sapucaia devem ser analisados quanto aos aspectos relacionados à Segurança da Informação, de forma que estejam sujeitos a requisitos de conformidade com esta Política e suas normas complementares.

Praça Governador Miguel Couto Filho nº 240

Centro – Sapucaia – RJ – CEP 25880-000



ESTADO DO RIO DE JANEIRO

PREFEITURA MUNICIPAL DE SAPUCAIA

CAPÍTULO II

DISPOSIÇÕES GERAIS

SEÇÃO I

Dos Objetivos

Art. 4º A Política de Segurança da Informação tem os seguintes objetivos:

- I – estabelecer princípios, diretrizes, responsabilidades e competências relacionados à Governança e à Gestão de Segurança da Informação no âmbito da Prefeitura Municipal de Sapucaia;
- II – orientar as áreas, órgãos e unidades da Prefeitura Municipal de Sapucaia na identificação, avaliação, tratamento e monitoramento dos riscos relacionados à Segurança da Informação, buscando mantê-los em níveis aceitáveis e compatíveis com os objetivos da Administração Municipal;
- III – proteger a disponibilidade, integridade, confidencialidade e autenticidade das informações que suportam as atividades, os processos e os serviços da Prefeitura Municipal de Sapucaia;
- IV – promover o comprometimento dos agentes públicos e demais usuários autorizados na adoção das diretrizes de Segurança da Informação e no desenvolvimento contínuo de uma cultura de segurança no âmbito da Prefeitura Municipal de Sapucaia;
- V – integrar a Segurança da Informação, a Privacidade e a Proteção de Dados Pessoais aos processos de governança, gestão de riscos e controles internos da Prefeitura Municipal de Sapucaia, promovendo uma gestão estruturada, verificável e orientada à melhoria contínua.

SEÇÃO II

Dos Princípios Básicos

Art. 5º As ações de Segurança da Informação devem observar os seguintes princípios:

- I – publicidade: garantir a divulgação de todas as medidas de gestão de riscos de Segurança da Informação, observando os critérios legais de sigilo apropriados;
- II – proporcionalidade: ser proporcionais ao valor da informação e ao nível de risco ao qual estiverem expostas;
- III – completude: cobrir todo o ciclo de vida da informação levando em conta todos os ativos que a suportam, sejam eles físicos, tecnológicos ou humanos;
- IV – privacidade: assegurar o direito à privacidade e à proteção de dados pessoais, em observância à legislação aplicável, incluindo a Lei Federal nº 13.709/2018 — Lei Geral de Proteção de Dados Pessoais (LGPD), quando aplicável;
- V – legalidade, finalidade e necessidade: assegurar que o tratamento de informações e dados pessoais observe finalidade legítima, compatibilidade com os objetivos institucionais e limitação ao mínimo necessário para sua execução;
- VI – privacidade desde a concepção: incorporar requisitos de privacidade e proteção de dados pessoais desde a definição, desenvolvimento, contratação e evolução de processos, sistemas e serviços;
- VII – segurança desde a concepção e por padrão: incorporar controles de segurança desde as etapas iniciais de projetos e manter, por padrão, configurações compatíveis com o nível de risco identificado;
- VIII – transparência e responsabilização: manter decisões, controles, avaliações e exceções devidamente documentados, com definição clara de responsabilidades e geração de evidências auditáveis;
- IX – melhoria contínua: revisar periodicamente riscos, controles e processos de Segurança da Informação e Privacidade, considerando mudanças de contexto, tecnologia, legislação, auditorias e incidentes.

Parágrafo único. Os princípios e diretrizes desta Política consideram, no que couber, as disposições da Política Nacional de Segurança da Informação, instituída pelo Decreto nº 12.572/2025, da Estratégia Nacional de Cibersegurança, instituída pelo Decreto nº 12.573/2025, as diretrizes do Programa de Privacidade e Segurança da Informação – PPSI do Governo Federal e os requisitos e orientações da ABNT NBR ISO/IEC 27701, em sua edição vigente, em harmonia com os arts. 46 a 50 da Lei nº 13.709/2018.

Praça Governador Miguel Couto Filho nº 240

Centro – Sapucaia – RJ – CEP 25880-000



ESTADO DO RIO DE JANEIRO

PREFEITURA MUNICIPAL DE SAPUCAIA

CAPÍTULO III

DOS TERMOS E DEFINIÇÕES

Art. 6º Para fins desta Política, considera-se:

I – acesso: capacidade de usar um ativo da informação, como por exemplo: ler, criar, modificar ou excluir um arquivo; executar um programa; se conectar a um dispositivo, a uma rede, a um sistema, a um serviço ou entrar em áreas de acesso restrito que hospedam informações sensíveis;

II – ameaça: evento que tem potencial em si próprio para comprometer os objetivos da Prefeitura Municipal de Sapucaia, seja trazendo danos diretos aos seus ativos ou prejuízos decorrentes de situações inesperadas, como por exemplo: incêndio, falha de equipamentos, indisponibilidade de sistemas ou serviços, destruição de informações sensíveis, dentre outros;

III – ativo da informação: informação, processo ou ativo físico, tecnológico ou humano que suporta as operações de coleta, armazenamento, processamento, compartilhamento ou descarte de informações;

IV – ativo tecnológico: equipamento de TIC, software ou aplicação que suporta as atividades, processos de negócio e serviços da Prefeitura Municipal de Sapucaia;

V – autenticidade: garantia de que os ativos da informação identificados em um processo de comunicação como remetentes ou destinatários sejam realmente quem dizem ser, ou seja, diz respeito à veracidade das identidades dos ativos envolvidos em um processo de comunicação;

VI – classificação da informação: refere-se ao grau de sensibilidade de uma informação diante de uma possível quebra de segurança ou comprometimento dos princípios básicos de Segurança da Informação;

VII – confidencialidade: propriedade que garante que a informação só esteja disponível a indivíduos ou processos autorizados;

VIII – continuidade de negócios: capacidade estratégica e tática da Prefeitura Municipal de Sapucaia de se planejar e responder a incidentes que gerem interrupções em suas atividades ou serviços, visando minimizar impactos e manter suas operações em um nível aceitável de disponibilidade previamente definido;

IX – custodiante: pessoa física ou jurídica que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de informações que não lhe pertencem, mas que estão sob sua custódia;

X – disponibilidade: propriedade que garante que a informação esteja disponível às pessoas e aos processos autorizados a qualquer momento em que sejam requeridas;

XI – equipamento ou equipamento de TIC: componente da infraestrutura de Tecnologia da Informação e Comunicação – TIC, como por exemplo: computador, notebooks, tablets, smartphones, servidores, roteadores, switches, etc.;

XII – Grupo de Prevenção, Tratamento e Resposta a Incidentes: agentes responsáveis por receber, analisar e responder às notificações e atividades relacionadas a incidentes de Segurança da Informação;

XIII – integridade: propriedade que garante que a informação está intacta e protegida contra perda, dano ou modificação não autorizada;

XIV – plano de gerenciamento de incidentes: plano de ação claramente definido e documentado para ser usado quando ocorrer um incidente;

XV – risco: probabilidade de ameaças explorarem vulnerabilidades, comprometendo a confidencialidade, integridade ou disponibilidade da informação e causando impactos para as atividades da Prefeitura Municipal de Sapucaia;

XVI – sistema de informação: sistema composto por um conjunto de ativos da informação que tem por objetivo armazenar, transportar e processar informações visando suportar funções, serviços ou processos da Prefeitura Municipal de Sapucaia;

XVII – usuário: qualquer pessoa autorizada a ler, inserir ou atualizar informações em um sistema de informação;

XVIII – vulnerabilidade: fragilidade presente ou associada a ativos da informação que, ao ser explorada por ameaças, permite a ocorrência de um incidente de segurança comprometendo um ou mais princípios de segurança da informação;



ESTADO DO RIO DE JANEIRO

PREFEITURA MUNICIPAL DE SAPUCAIA

XIX – análise de impacto no negócio (BIA): processo utilizado para identificar impactos decorrentes da interrupção de atividades e subsidiar o planejamento de continuidade;

XX – declaração de aplicabilidade (SoA): documento do Sistema de Gestão da Segurança da Informação que registra os controles de segurança selecionados, aplicáveis e suas justificativas;

XXI – incidente de Segurança da Informação: ocorrência que compromete, ou possa comprometer, a confidencialidade, integridade, disponibilidade, autenticidade ou privacidade das informações;

XXII – risco inerente: nível de risco existente antes da consideração dos controles de segurança implementados, utilizado como referência inicial para priorização e tomada de decisão;

XXIII – risco residual: nível de risco remanescente após a consideração dos controles existentes ou planejados;

XXIV – vazamento de informação: divulgação, acesso ou exposição não autorizada de informação ou dado pessoal, decorrente de falha, erro ou ação maliciosa;

XXV – Sistema de Gestão da Segurança da Informação (SGSI): conjunto estruturado de políticas, processos, responsabilidades, controles e mecanismos de monitoramento destinados a implementar, manter e melhorar continuamente a Segurança da Informação.

CAPÍTULO IV

DAS COMPETÊNCIAS E RESPONSABILIDADES

SEÇÃO I

Das Competências

Art. 7º Compete à Unidade Técnica de Tecnologia da Informação — TI:

I – consolidar e coordenar as ações de gestão de riscos em Segurança da Informação no âmbito da Prefeitura Municipal de Sapucaia;

II – elaborar, revisar e propor as Normas Complementares necessárias para suplementar e detalhar as diretrizes desta Política de Segurança da Informação, submetendo-as à deliberação do Comitê Multidisciplinar de Segurança da Informação – CMSI;

III – definir e estabelecer metodologias, critérios e diretrizes para a gestão de riscos relacionados à Segurança da Informação;

IV – promover a divulgação das políticas, normas, diretrizes e boas práticas relacionadas à gestão de riscos em Segurança da Informação para as áreas, órgãos e unidades da Prefeitura Municipal de Sapucaia;

V – definir as estratégias para a implementação desta Política e de suas normas complementares;

VI – receber, analisar e consolidar os resultados das auditorias e avaliações de conformidade realizadas nas áreas, órgãos e unidades da Prefeitura Municipal de Sapucaia quanto à observância das políticas, normas e diretrizes de Segurança da Informação;

VII – atualizar periodicamente a Política de Segurança da Informação, observando o processo institucional de revisão e aprovação;

VIII – realizar a análise técnica dos planos de gerenciamento de incidentes e de continuidade de negócios relacionados à Tecnologia da Informação, emitindo parecer técnico e submetendo-os à apreciação do Comitê Multidisciplinar de Segurança da Informação – CMSI;

Parágrafo único. Para os fins desta Política, a Unidade Técnica de Tecnologia da Informação — TI acumula a função de Unidade Gestora de Segurança da Informação — UGSI, cabendo-lhe exercer as competências previstas nos arts. 8º, IV, 16, I, e 20 desta Política.

Art. 8º Compete à Unidade Técnica de Tecnologia da Informação — TI, em seu âmbito de atuação:

I – instituir e coordenar o Grupo de Prevenção, Tratamento e Resposta a Incidentes;

II – elaborar, implementar e gerenciar os planos técnicos de continuidade e recuperação dos serviços, sistemas e recursos de Tecnologia da Informação sob sua responsabilidade, submetendo-os à análise técnica e à posterior



ESTADO DO RIO DE JANEIRO

PREFEITURA MUNICIPAL DE SAPUCAIA

apreciação do Comitê Multidisciplinar de Segurança da Informação – CMSI, visando assegurar a continuidade e a recuperação dos serviços essenciais da Prefeitura Municipal de Sapucaia;

III – executar, gerenciar e prover suporte técnico às atividades de TIC, garantindo a conformidade operacional dos ativos sob sua gestão a esta Política e às suas normas complementares;

IV – elaborar e encaminhar à instância competente a previsão orçamentária das necessidades tecnológicas de Segurança da Informação relativas à infraestrutura sob sua administração;

V – oferecer apoio operacional nas ações corretivas em casos de descumprimento da Política de Segurança da Informação ou de suas normas complementares, nas áreas e unidades da Prefeitura Municipal de Sapucaia.

Parágrafo único. Compete ao Grupo de Prevenção, Tratamento e Resposta a Incidentes:

I – executar as atividades de prevenção, tratamento e resposta a incidentes de segurança por intermédio de processos em conformidade com as melhores práticas relacionadas à matéria;

II – elaborar e manter atualizado o Plano de Gerenciamento de Incidentes de Segurança da Informação;

III – executar as atividades de recuperação dos sistemas e serviços comprometidos por incidentes de segurança de forma integrada com as respectivas equipes de administração dos ativos que os suportam.

Art. 9º Sempre que um incidente de segurança da informação gerenciado sob as diretrizes desta PSI envolver indícios ou confirmação de vazamento ou comprometimento de dados pessoais, o Grupo de Prevenção, Tratamento e Resposta a Incidentes notificará imediatamente o Encarregado pelo Tratamento de Dados Pessoais e o Comitê Multidisciplinar de Segurança da Informação – CMSI.

Parágrafo único. A atuação da área técnica de Tecnologia da Informação nos incidentes cibernéticos restringe-se ao suporte tecnológico e à mitigação de riscos à infraestrutura, cabendo à área responsável por privacidade e proteção de dados e ao Encarregado pelo Tratamento de Dados Pessoais as deliberações sobre impactos administrativos, legais e regulatórios, incluindo eventual comunicação à Agência Nacional de Proteção de Dados – ANPD, quando aplicável, observados o art. 48 da LGPD e a Resolução CD/ANPD nº 15/2024.

Art. 10. Compete às áreas e unidades da Prefeitura Municipal de Sapucaia, em seus respectivos âmbitos de atuação:

I – implementar a Política de Segurança da Informação;

II – apoiar a elaboração da estratégia de gestão de riscos de segurança da Informação;

III – implementar o programa de gestão de riscos de Segurança da Informação e Privacidade;

IV – disseminar esta Política e suas normas complementares;

V – aplicar as ações corretivas, com apoio operacional da Unidade Técnica de Tecnologia da Informação – TI, e as medidas administrativas cabíveis nos casos de descumprimento da Política de Segurança da Informação ou de suas normas complementares.

Art. 11. Compete ao Controle Interno auditar periodicamente o cumprimento da Política de Segurança da Informação e de suas normas complementares, analisando e avaliando a eficácia das medidas de implementação.

Art. 11-A. Compete ao Encarregado pelo Tratamento de Dados Pessoais, no âmbito desta Política, exercendo as atribuições do art. 41 da Lei nº 13.709/2018 e da Resolução CD/ANPD nº 18/2024:

I – atuar como ponto de interlocução com titulares de dados pessoais e com a autoridade competente, nos termos da legislação aplicável;

II – orientar a Prefeitura Municipal de Sapucaia quanto ao cumprimento das obrigações relacionadas à proteção de dados pessoais e à privacidade;

III – apoiar a gestão de incidentes que envolvam dados pessoais, em articulação com o Grupo de Prevenção, Tratamento e Resposta a Incidentes e com as áreas responsáveis por privacidade, jurídico, riscos e conformidade;

IV – apoiar a definição de requisitos de privacidade aplicáveis a processos, sistemas, contratos e avaliações de impacto.

Art. 11-B. A Prefeitura Municipal de Sapucaia manterá Sistema de Gestão da Segurança da Informação – SGSI destinado a assegurar a implementação, o monitoramento e a melhoria contínua dos controles necessários à proteção de seus ativos de informação, considerando, no que couber, as diretrizes da Política Nacional de Segurança da Informação, instituída pelo Decreto nº 12.572/2025, da Estratégia Nacional de Cibersegurança, instituída pelo Decreto nº 12.573/2025, do Programa de Privacidade e Segurança da Informação – PPSI do Governo Federal e da ABNT NBR ISO/IEC 27701, em sua edição vigente.



ESTADO DO RIO DE JANEIRO

PREFEITURA MUNICIPAL DE SAPUCAIA

Parágrafo único. O SGSI contemplará, no mínimo, gestão de riscos, auditorias internas, revisão periódica de controles, registros auditáveis e Declaração de Aplicabilidade — SoA, quando adotada pela Prefeitura Municipal de Sapucaia.

SEÇÃO II

Das Responsabilidades

Subseção I

Dos usuários

Art. 12. É de responsabilidade dos usuários dos ativos da informação:

- I – gerenciar os ativos da informação sob sua responsabilidade e garantir que sejam utilizados exclusivamente para os fins previstos;
- II – realizar suas competências funcionais em aderência a todas as políticas, normas e procedimentos de segurança da informação a eles relacionados;
- III – comunicar prontamente ao seu gestor imediato, ou ao responsável contratual no caso de prestadores de serviço, quaisquer desvios das políticas, normas e procedimentos estabelecidos ou incidentes de segurança de que tenha conhecimento;
- IV – tratar a informação de acordo com a sua classificação, adotando as medidas de proteção previstas para o tratamento dos riscos a que estão sujeitos os ativos de informação sob sua custódia, sem prejuízo do cumprimento das salvaguardas e rotinas de privacidade e proteção de dados aplicáveis;
- V – manter-se atualizado quanto a esta Política e normas complementares.

Subseção II

Dos Custodiantes

Art. 13. Ao custodiante da informação cabem as seguintes responsabilidades:

- I – zelar pela disponibilidade, integridade e confidencialidade das informações sob sua custódia;
- II – utilizar os ativos da informação sob sua custódia exclusivamente para os fins previstos;
- III – comunicar prontamente ao seu gestor imediato, ou ao responsável contratual no caso de prestadores de serviço, quaisquer desvios das políticas, normas e procedimentos estabelecidos ou incidentes de segurança de que tenha conhecimento;
- IV – preservar a classificação dos ativos da informação aos quais tiver acesso em decorrência do exercício de suas funções, adotando as medidas de proteção previstas para o tratamento dos riscos a que estejam sujeitos.

SEÇÃO III

Das Diretrizes de Governança, Riscos, Conformidade e Privacidade

Art. 13-A. Classificação e Tratamento da Informação

As informações serão classificadas conforme sua criticidade e sensibilidade, observada a Política de Classificação da Informação do Município. A rotulagem, o armazenamento, a transferência, a retenção, o compartilhamento e o descarte seguro serão disciplinados em norma complementar. A ausência de rotulagem não implicará presunção de caráter público ou irrestrito.

Art. 13-B. Continuidade do Negócio e Recuperação de Desastres

A Prefeitura Municipal de Sapucaia manterá processos de Análise de Impacto no Negócio — BIA, Planos de Continuidade de Negócio — BCP e Planos de Recuperação de Desastres — DRP, com responsabilidades, níveis de serviço e testes periódicos definidos em normas e planos específicos, de modo a preservar a resiliência dos serviços e a custódia das informações críticas.

Art. 13-C. Controle de Acesso e Identidades

Praça Governador Miguel Couto Filho nº 240

Centro – Sapucaia – RJ – CEP 25880-000



ESTADO DO RIO DE JANEIRO

PREFEITURA MUNICIPAL DE SAPUCAIA

O acesso a informações e recursos será concedido com base nos princípios do menor privilégio e da necessidade de saber, com revisões periódicas e revogações tempestivas. Normas complementares definirão processos de concessão, alteração e revogação, autenticação, gestão de credenciais, trilhas de auditoria e adoção de múltiplos fatores de autenticação — MFA, quando aplicável.

Art. 13-D. Inovação e Uso de Novas Tecnologias

A adoção de novas tecnologias deverá observar avaliação prévia de riscos e os princípios de privacy by design e security by design, mediante processos formais previstos em normas complementares.

Art. 13-E. Monitoramento, Auditoria e Registro de Evidências

A eficácia dos controles será monitorada e auditada periodicamente. Registros de eventos relevantes à segurança deverão ser gerados e protegidos contra alteração não autorizada, com critérios de acesso, retenção e guarda definidos em norma complementar, observadas a legislação aplicável e as obrigações específicas de conservação de registros, quando aplicáveis.

Art. 13-F. Proteção de Dados Pessoais

O tratamento de dados pessoais observará a legislação aplicável — em especial os arts. 46 a 50 da Lei nº 13.709/2018 — e os princípios de minimização, privacidade e segurança desde a concepção, em articulação com a Política de Proteção de Dados Pessoais — PPDP do Município. Normas complementares detalharão, quando aplicável, registros de tratamento, atendimento aos direitos dos titulares, avaliações de impacto e requisitos contratuais para operadores e terceiros.

Art. 13-G. Relacionamento com Terceiros e Cadeia de Suprimentos

A seleção, contratação e gestão de terceiros considerarão avaliação de riscos e exigirão requisitos mínimos de Segurança da Informação e Privacidade, incluindo obrigações de confidencialidade, notificação de incidentes, controle de subcontratação, continuidade e desligamento seguro ao término da relação contratual, observados os arts. 39 a 42 da LGPD.

Art. 13-H. Resposta a Incidentes de Segurança da Informação

A Prefeitura Municipal de Sapucaia manterá processo formal de gestão de incidentes para comunicação, classificação, tratamento, recuperação e lições aprendidas. Normas complementares definirão fluxo, critérios de severidade, responsabilidades, comunicação às partes competentes e preservação de evidências, em alinhamento com o Plano de Resposta a Incidentes e com o art. 48 da LGPD e a Resolução CD/ANPD nº 15/2024.

Art. 13-I. Segurança de Redes e Sistemas

Devem ser adotadas medidas de proteção proporcionais ao risco nos ambientes de rede, infraestrutura, nuvem e aplicações, incluindo práticas de desenvolvimento seguro, proteção contra código malicioso e controles sobre mídias removíveis. Requisitos técnicos e procedimentos serão definidos em normas específicas.

Art. 13-J. Gestão de Riscos de Segurança da Informação e Privacidade

A avaliação de riscos seguirá princípios padronizados, auditáveis e consistentes, integrando Segurança da Informação e Privacidade. O risco inerente será utilizado como referência inicial para priorização e tomada de decisão, considerando a exposição antes dos controles. Probabilidade e impacto serão determinados de forma estruturada conforme metodologia aprovada pela Prefeitura Municipal de Sapucaia, e reavaliações posteriores determinarão o risco residual após a aplicação dos controles.

§ 1º Cada avaliação de riscos deverá gerar registros auditáveis, com trilhas que permitam identificar, no mínimo, quem realizou a avaliação, quando ela foi executada, qual objeto foi avaliado, quais critérios foram aplicados, quais controles foram considerados e quais decisões foram tomadas, assegurando consistência e comparabilidade entre ciclos.

§ 2º O processo de gestão de riscos integra-se ao SGSI e deverá prever reavaliações sempre que houver mudanças relevantes de contexto, tecnologia, legislação, processos, fornecedores ou em decorrência de incidentes e auditorias.

Art. 13-K. Uso Aceitável, Monitoramento e Conduta

Os ativos de informação e recursos tecnológicos da Prefeitura Municipal de Sapucaia destinam-se prioritariamente a fins institucionais. Regras de uso aceitável, canais oficiais de comunicação, uso de dispositivos pessoais, monitoramento e condutas vedadas serão disciplinados em normas complementares e instrumentos próprios, observada a legislação aplicável.



ESTADO DO RIO DE JANEIRO

PREFEITURA MUNICIPAL DE SAPUCAIA

Art. 13-L. Conformidade e Gestão de Exceções

Exceções a esta Política ou às suas Normas Complementares somente serão admitidas mediante processo formal, devidamente justificado, com avaliação de riscos, definição de controles compensatórios quando aplicáveis, responsável pela aceitação e prazo de vigência definido, sujeitas à aprovação da instância competente.

CAPÍTULO V

DO COMITÊ MULTIDISCIPLINAR DE SEGURANÇA DA INFORMAÇÃO — CMSI

SEÇÃO I

Disposições Iniciais

Art. 14. Fica instituído o Comitê Multidisciplinar de Segurança da Informação — CMSI, órgão colegiado de natureza consultiva e deliberativa, responsável pela governança estratégica de Segurança da Informação e segurança cibernética na Prefeitura Municipal de Sapucaia.

SEÇÃO II

Da Composição e Diretrizes

Art. 15. O CMSI atuará em consonância com os princípios da Política de Segurança da Informação — PSI e com as salvaguardas de privacidade e proteção de dados estabelecidas na legislação e nas normas internas aplicáveis.

Art. 16. O Comitê será composto por membros titulares e suplentes indicados pelas seguintes áreas:

I – Unidade Técnica de Tecnologia da Informação — TI, que acumula a função de Unidade Gestora de Segurança da Informação — UGSI e exercerá a Presidência do Comitê;

II – Controle Interno;

III – Procuradoria-Geral do Município;

IV – Encarregado pelo Tratamento de Dados Pessoais, com direito a voz e voto nas matérias que envolvam proteção de dados pessoais.

Parágrafo único. A participação no CMSI será considerada atividade institucional relevante e não implicará remuneração adicional.

SEÇÃO III

Das Regras de Funcionamento e Prazos

Art. 17. Compete ao Comitê:

I – analisar, deliberar e homologar propostas de novas Normas Complementares à PSI antes de sua publicação;

II – apreciar e aprovar os planos de gerenciamento de incidentes e de continuidade de negócios, considerando a análise técnica realizada pela Unidade Técnica de Tecnologia da Informação – TI, quando aplicável;

III – reunir-se de forma ordinária a cada bimestre, ou extraordinariamente por convocação de seu Presidente;

IV – deliberar sobre exceções a esta Política e às Normas Complementares, observada a avaliação formal de riscos e o prazo de vigência da exceção;

V – supervisionar a eficácia do SGSI e acompanhar a evolução dos riscos de Segurança da Informação e Privacidade;

VI – aprovar as metodologias e critérios institucionais aplicáveis à gestão de riscos de Segurança da Informação e Privacidade.

Art. 18. Os responsáveis pelas áreas indicadas no art. 16 deverão nomear seus respectivos representantes no prazo definido pela Alta Administração a partir da aprovação desta Política.

Art. 19. Todas as reuniões do Comitê deverão, obrigatoriamente, ser registradas em atas circunstanciadas, devidamente registradas e aprovadas pelos membros presentes em meio físico ou sistema eletrônico oficial, servindo como evidência para auditorias internas e externas.

CAPÍTULO VI

Praça Governador Miguel Couto Filho nº 240

Centro – Sapucaia – RJ – CEP 25880-000



ESTADO DO RIO DE JANEIRO

PREFEITURA MUNICIPAL DE SAPUCAIA

DISPOSIÇÕES FINAIS

Art. 20. A Política de Segurança da Informação será regulamentada e detalhada por meio de Normas Complementares – NC específicas, editadas pela Unidade Gestora de Segurança da Informação no prazo máximo de 180 (cento e oitenta) dias a contar da vigência desta Política, priorizando-se as NCs de classificação da informação, gestão de identidade e controle de acessos, resposta a incidentes e proteção de dados pessoais.

§ 1º As Normas Complementares disciplinarão, obrigatoriamente, os seguintes temas essenciais à suplementação desta PSI, sem prejuízo da edição de novas normas a qualquer momento, sempre que constatada a necessidade institucional ou a evolução dos cenários de risco:

- I – gestão de fornecedores e operadores;
- II – uso de recursos tecnológicos da Prefeitura Municipal de Sapucaia e diretrizes de BYOD;
- III – gestão de identidade e controle de acessos;
- IV – padrões técnicos e complexidade de senhas;
- V – classificação da informação, em associação aos requisitos legais, regulatórios e internos aplicáveis;
- VI – Política de Mesa Limpa e Tela Limpa;
- VII – gestão de riscos de Segurança da Informação e Privacidade;
- VIII – resposta e gerenciamento de incidentes de Segurança da Informação;
- IX – segurança de redes, infraestrutura, ambientes em nuvem e sistemas;
- X – criptografia e proteção de informações em trânsito e em repouso;
- XI – desenvolvimento seguro e gestão de vulnerabilidades;
- XII – monitoramento, auditoria, registros de eventos e preservação de evidências;
- XIII – continuidade de negócios, recuperação de desastres e backup;
- XIV – gestão de mudanças;
- XV – dispositivos móveis, trabalho remoto e teletrabalho;
- XVI – proteção de dados pessoais, privacidade e gestão de operadores;
- XVII – gestão documental, retenção e descarte seguro de informações;
- XVIII – gestão de exceções e aceitação de riscos;
- XIX – uso de mídias removíveis e proteção contra código malicioso.

§ 2º Os atos normativos e as Normas Complementares editadas deverão ser revisados com periodicidade máxima de 2 (dois) anos a contar da data de sua aprovação, ou antes, sempre que houver mudanças relevantes no contexto organizacional, tecnológico, legal ou de riscos.

Art. 21. Fica estabelecido prazo de transição de até 180 (cento e oitenta) dias, contados da publicação de cada Norma Complementar, para que áreas, processos e sistemas legados se adéquem integralmente às novas exigências operacionais estabelecidas pelas respectivas Normas Complementares, podendo a Unidade Gestora de Segurança da Informação prorrogá-lo uma única vez, mediante justificativa formal registrada.

Art. 22. As ações que violem esta Política ou suas normas complementares são passíveis de medidas administrativas, disciplinares, contratuais e legais cabíveis, conforme os normativos internos e a legislação aplicável, observado o devido processo.

Art. 23. Esta Política entra em vigor na data de sua aprovação e permanecerá aplicável até que seja formalmente revisada, revogada ou substituída.