

DECRETO N.º 52.121, DE 27/10/2026.

DISPÕE SOBRE A POLÍTICA MUNICIPAL DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA NO ÂMBITO DA ADMINISTRAÇÃO PÚBLICA DIRETA E INDIRETA DO MUNICÍPIO DE ARACRUZ, ESTABELECE A ESTRUTURA DE GOVERNANÇA, OS PRINCÍPIOS, AS DIRETRIZES E AS RESPONSABILIDADES PARA A PROTEÇÃO DOS ATIVOS DE INFORMAÇÃO E DÁ OUTRAS PROVIDÊNCIAS.

O PREFEITO MUNICIPAL DE ARACRUZ, NO USO DAS ATRIBUIÇÕES QUE LHE CONFERE O ART. 84, INCISO IV, DA CONSTITUIÇÃO DA REPÚBLICA, O ART. 87, INCISOS I E II, DA CONSTITUIÇÃO DO ESTADO DO ESPÍRITO SANTO, E O ART. 9º DA LEI ORGÂNICA DO MUNICÍPIO DE ARACRUZ, E

CONSIDERANDO a necessidade de proteger os ativos de informação da Administração Pública Municipal Direta e Indireta;

CONSIDERANDO o disposto na Lei nº 13.709, de 14 de agosto de 2018 (LGPD), na Lei nº 12.527, de 18 de novembro de 2011 (LAI), na Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), na Lei nº 14.129, de 29 de março de 2021 (Governo Digital) e na Lei nº 14.133, de 1º de abril de 2021 (Licitações e Contratos Administrativos);

CONSIDERANDO o disposto no Decreto Municipal nº 50.611, de 2026, que institui a Política Municipal de Proteção de Dados Pessoais, da qual esta Política é complementar e com a qual coexiste, sem substituí-la;

CONSIDERANDO a necessidade de alinhar a gestão da segurança da informação às boas práticas nacionais e internacionais, em especial as normas ABNT NBR ISO/IEC 27001 e 27002, sem que delas dependa a validade desta Política;

DECRETA:

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 1º Fica instituída, na forma desta Política, a Política Municipal de Segurança da Informação e Segurança Cibernética, aplicável a toda a Administração Pública Municipal Direta e Indireta, abrangendo órgãos, entidades, agentes políticos, servidores efetivos e

comissionados, empregados públicos, estagiários, contratados, fornecedores, parceiros e demais pessoas que, a qualquer título, tenham acesso aos ativos de informação do Município.

Parágrafo único. Para os fins desta Política, consideram-se:

I - ativo de informação: todo dado, informação, knowledge ou recurso tecnológico, físico ou humano com valor institucional;

II - segurança da informação: as ações e controles que visam assegurar a confidencialidade, a integridade, a disponibilidade, a autenticidade e a conformidade das informações e dos serviços;

III - sistema de gestão de segurança da informação (SGSI): o conjunto de políticas, processos, procedimentos, controles e responsabilidades para a gestão da segurança da informação;

IV - incidente de segurança da informação: evento indesejado ou inesperado com probabilidade de comprometer a operação, os ativos ou os dados;

V - dado pessoal: dado relativo a pessoa natural identificada ou identificável, nos termos do art. 5º, I, da Lei nº 13.709/2018;

VI - Encarregado (DPO): o agente indicado pelo controlador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);

VII - documentos complementares: as normas, os procedimentos, os planos, os modelos e os registros que detalham e operacionalizam esta Política.

CAPÍTULO II

DA BASE LEGAL, DOS PRINCÍPIOS E DOS DIRETRIZES GERAIS

Art. 2º São fundamentos legais desta Política:

I - Constituição da República, arts. 5º, XXXIII e LXXII, e 37, caput;

II - Lei nº 13.709/2018 (LGPD);

III - Lei nº 12.527/2011 (LAI);

IV - Lei nº 12.965/2014 (Marco Civil da Internet);

V - Lei nº 14.129/2021 (Governo Digital);

VI - Lei nº 14.133/2021 (Licitações e Contratos Administrativos);

VII - Decreto Municipal nº 50.611/2026 (Política Municipal de Proteção de Dados Pessoais);

VIII - normas ABNT NBR ISO/IEC 27001 e 27002, como referências técnicas não vinculantes.

Art. 3º São princípio da segurança da informação: legalidade, interesse público, confidencialidade, integridade, disponibilidade, autenticidade, rastreabilidade, responsabilização, gestão de riscos, proteção de dados pessoais e melhoria contínua.

Art. 4º São diretrizes gerais desta Política:

I - a proteção dos ativos de informação como responsabilidade institucional compartilhada;

II - o tratamento da segurança da informação com base em riscos;

III - a promoção da cultura de segurança e da conscientização permanente;

IV - a garantia da continuidade dos serviços públicos;

V - a conformidade com a legislação aplicável, em especial a LGPD e a LAI;

VI - a segregação de funções e o princípio do menor privilégio;

VII - a avaliação periódica e a melhoria contínua do SGSI;

VIII - o incentivo ao uso responsável de tecnologias, incluída a inteligência artificial;

IX - a não dependência de certificação externa para a validade desta Política;

X - a implantação progressiva, por fases, desta Política e dos documentos complementares.

Art. 5º Esta Política integra-se aos demais instrumentos normativos municipais e não substitui o Decreto Municipal nº 50.611/2026, que permanece em plena vigência, coexistindo de forma complementar.

CAPÍTULO III **DA GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO**

Art. 6º A estrutura de governança da segurança da informação é composta por:

I - Alta Administração;

II - Comitê de Segurança da Informação e Proteção de Dados;

- III - Secretaria Municipal responsável pela Tecnologia da Informação;
- IV - Encarregado pelo Tratamento de Dados Pessoais (DPO) e sua equipe de apoio;
- V - gestores das unidades administrativas;
- VI - gestores de contratos;
- VII - usuários dos recursos tecnológicos.

Política: Art. 7º À Alta Administração compete, entre outras atribuições previstas nesta

- I - aprovar e revisar a Política e seus documentos complementares;
- II - assegurar recursos necessários à implantação e à manutenção do SGSI;
- III - promover a cultura de segurança da informação;
- IV - avaliar relatórios de riscos e incidentes de alta criticidade;
- V - patrocinar as ações de capacitação e conscientização;
- VI - designar os integrantes do Comitê;
- VII - prestar contas da gestão da segurança da informação.

Art. 8º Fica criado o Comitê de Segurança da Informação e Proteção de Dados, órgão colegiado de caráter consultivo e deliberativo no âmbito de sua competência, com fundamento no poder de auto-organização da Administração Pública (art. 37, caput, da Constituição da República), na Lei nº 13.709/2018 (arts. 41 e 50) e no Decreto Municipal nº 50.611/2026.

§ 1º O Comitê será composto por representantes da Secretaria Municipal responsável pela Tecnologia da Informação, da Procuradoria Geral do Município, da Controladoria-Geral do Município, da Secretaria Municipal de Governo e das unidades com maior exposição a riscos de segurança da informação, designados por ato do Chefe do Executivo.

§ 2º Compete ao Comitê:

- I - propor e revisar esta Política e os documentos complementares;
- II - avaliar e deliberar sobre riscos, incidentes e tratamentos prioritários;
- III - orientar a implantação progressiva e o monitoramento do SGSI;

IV - dirimir casos omissos, com apoio da Procuradoria Geral do Município;

V - apoiar o Encarregado (DPO) nas deliberações estratégicas de proteção de dados;

VI - zelar pela integração entre a segurança da informação e a proteção de dados pessoais.

§ 3º O Comitê contará com o apoio técnico da Secretaria Municipal responsável pela Tecnologia da Informação e da equipe de apoio do Encarregado (DPO), sem prejuízo das atribuições próprias de cada órgão.

Art. 9º Compete à Secretaria Municipal responsável pela Tecnologia da Informação:

I - coordenar a implantação e a operação do SGSI;

II - gerir a infraestrutura tecnológica e os ativos de informação;

III - conduzir a resposta técnica a incidentes;

IV - manter o inventário de ativos e a documentação correlata;

V - apoiar o Comitê e o Encarregado (DPO);

VI - executar as ações de conscientização e capacitação;

VII - propor melhorias e avaliar a conformidade técnica.

Art. 10. O Encarregado pelo Tratamento de Dados Pessoais (DPO), designado nos termos do art. 41 da Lei nº 13.709/2018 e do Decreto Municipal nº 50.611/2026, atua como canal de comunicação com os titulares e com a ANPD, devendo ser apoiado por equipe técnica designada, sem prejuízo da competência decisória do controlador.

Art. 11. Compete aos gestores das unidades administrativas, aos gestores de contratos e aos usuários dos recursos tecnológicos observar as diretrizes, os procedimentos e os documentos complementares desta Política, comunicar incidentes e zelar pela proteção dos ativos sob sua responsabilidade.

Art. 12. A segurança da informação observará a segregação de funções, a prestação de contas e a responsabilização administrativa, civil e criminal, na forma da legislação aplicável.

CAPÍTULO IV **DA GESTÃO DE ATIVOS DE INFORMAÇÃO**

Art. 13. A gestão de ativos de informação abrange a identificação, a classificação, o inventário, a propriedade, o ciclo de vida, o compartilhamento, a preservação, a retenção e o descarte seguro das informações e dos recursos tecnológicos, na forma dos documentos complementares.

CAPÍTULO V **DA GESTÃO DE RISCOS**

Art. 14. A gestão de riscos de segurança da informação observará processo estruturado de identificação, análise, avaliação, tratamento, monitoramento e comunicação dos riscos, com critérios de impacto financeiro, legal, operacional e reputacional, integrando-se à proteção de dados pessoais.

CAPÍTULO VI **DA GESTÃO DE PESSOAS, COMPETÊNCIAS, CONSCIENTIZAÇÃO E RESPONSABILIZAÇÃO**

Art. 15. A gestão de pessoas abrangerá admissão, concessão e revogação de acessos, alterações funcionais, desligamento, capacitação, conscientização, responsabilidades individuais, condutas vedadas, confidencialidade, gestão de terceiros e uso responsável de inteligência artificial, vedada a inserção de dados pessoais ou sensíveis em ferramentas de IA generativa não aprovadas pela Administração.

CAPÍTULO VII **DA GESTÃO DE IDENTIDADES, CONTROLE DE ACESSO E RESPONSABILIDADES DE ACESSO**

Art. 16. A gestão de identidades e de controle de acesso observará identidade digital individual e intransferível, ciclo de vida das identidades, revisão periódica de acessos, contas privilegiadas, autenticação multifator para acesso remoto, contas privilegiadas e sistemas críticos, gestão de credenciais, segregação de funções, registro e monitoramento, acesso por terceiros e acesso remoto.

CAPÍTULO VIII **DA SEGURANÇA FÍSICA, AMBIENTAL E PROTEÇÃO DA INFRAESTRUTURA**

Art. 17. A segurança física e ambiental abrangerá áreas seguras, controle de acesso físico, visitantes e prestadores, proteção de equipamentos, infraestrutura de energia, climatização, proteção contra incêndios, proteção das comunicações, arquivos físicos, transporte de equipamentos, gestão de incidentes físicos e continuidade da infraestrutura.

CAPÍTULO IX **DA SEGURANÇA DAS OPERAÇÕES E GESTÃO DA INFRAESTRUTURA TECNOLÓGICA**

Art. 18. A segurança das operações abrangerá gestão de operações, capacidade e desempenho, vulnerabilidades, atualizações e correções, proteção contra códigos maliciosos,

registros de eventos, monitoramento, gestão de mudanças, cópias de segurança (estratégia 3-2-1), sincronização de tempo, disponibilidade e serviços de terceiros.

CAPÍTULO X

DA SEGURANÇA DAS COMUNICAÇÕES E TRANSFERÊNCIA DE INFORMAÇÕES

Art. 19. A segurança das comunicações abrangerá proteção de redes, comunicações institucionais, correio eletrônico, compartilhamento de informações, intercâmbio com outros órgãos, serviços em nuvem (modelo de responsabilidade compartilhada), criptografia, transferência eletrônica, serviços de mensagens, trabalho remoto, monitoramento e incidentes de comunicação.

CAPÍTULO XI

DO DESENVOLVIMENTO, AQUISIÇÃO, MANUTENÇÃO E GESTÃO SEGURA DE SISTEMAS DE INFORMAÇÃO

Art. 20. O desenvolvimento, a aquisição, a manutenção e a gestão de sistemas de informação observarão os princípios de segurança e privacidade desde a concepção (security by design e privacy by design), o ciclo de vida seguro, o uso de referências técnicas como OWASP Top 10, a segregação de ambientes, a vedação ao uso de dados reais em ambientes de teste, a gestão de vulnerabilidades e o descarte seguro de sistemas.

CAPÍTULO XII

DA GESTÃO DE FORNECEDORES, SERVIÇOS TERCEIRIZADOS E RELAÇÕES CONTRATUAIS

Art. 21. As contratações que envolvam o tratamento de informações ou o acesso a ativos da Administração Pública Municipal observarão requisitos de segurança da informação, incluindo:

- I - avaliação prévia dos riscos;
- II - cláusulas de confidencialidade e de proteção de dados pessoais;
- III - obrigações de notificação de incidentes;
- IV - direito de auditoria e fiscalização;
- V - procedimentos para o encerramento da relação contratual.

Art. 22. Os fornecedores e prestadores de serviços responderão pelo cumprimento das obrigações de segurança da informação previstas nos instrumentos contratuais, sem prejuízo da responsabilidade dos órgãos contratantes.

CAPÍTULO XIII

DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E EVENTOS CIBERNÉTICOS

Art. 23. A gestão de incidentes de segurança da informação e de eventos cibernéticos abrangerá a identificação, o registro, a classificação, a comunicação, o tratamento, a resposta, a investigação e a recuperação de incidentes, alcançando servidores, agentes, estagiários, contratados, fornecedores, parceiros e demais pessoas que utilizem os ativos de informação do Município.

§ 1º Considera-se evento de segurança da informação a ocorrência identificada como desvio ou indício de desvio das diretrizes desta Política, e incidente de segurança da informação o evento indesejado ou inesperado com probabilidade de comprometer a operação, os ativos, os dados ou os serviços do Município.

§ 2º Os incidentes serão classificados segundo a criticidade, o impacto potencial, o alcance, a sensibilidade dos dados envolvidos e a urgência, na forma do documento complementar específico.

§ 3º A resposta aos incidentes observará as etapas de contenção, isolamento, mitigação, erradicação, recuperação e monitoramento pós-recuperação, com preservação de evidências e cadeia de custódia para fins de investigação administrativa e criminal.

§ 4º Os incidentes envolvendo dados pessoais observarão o disposto no art. 48 da Lei nº 13.709/2018: o controlador comunicará à Autoridade Nacional de Proteção de Dados (ANPD) e aos titulares afetados a ocorrência de incidente que possa acarretar risco ou dano relevante, no prazo legal, cabendo ao Encarregado (DPO) apoiar e assessorar o controlador na comunicação, sem substituir a sua competência decisória.

§ 5º Os incidentes envolvendo fornecedores e serviços terceirizados observarão as obrigações contratuais de comunicação e responsabilidade compartilhada, na forma do Capítulo XII.

§ 6º Ao final de cada incidente, serão registradas as lições aprendidas e adotadas as medidas de melhoria contínua do SGSI.

CAPÍTULO XIV

DA CONTINUIDADE DOS NEGÓCIOS, DA CONTINUIDADE DOS SERVIÇOS DE TIC E DA RECUPERAÇÃO DE DESASTRES

Art. 24. A continuidade dos serviços públicos e a recuperação de desastres serão asseguradas por planos e procedimentos que considerem a identificação dos serviços críticos, a análise de impacto nos negócios, as estratégias de continuidade, a recuperação de desastres, a gestão de crises, a comunicação em contingência, as cópias de segurança e a recuperação de dados, as dependências externas e a realização periódica de exercícios e testes.

§ 1º Os planos de continuidade e de recuperação de desastres serão mantidos atualizados, testados periodicamente e divulgados aos responsáveis pela sua execução.

§ 2º A gestão de crises observará procedimentos de acionamento, comando, comunicação e registro das decisões, envolvendo a Alta Administração, o Comitê, a Secretaria Municipal responsável pela Tecnologia da Informação e as demais unidades afetadas.

§ 3º As dependências externas, incluídas energia, telecomunicações, internet, serviços em nuvem e fornecedores estratégicos, serão monitoradas e consideradas nos planos de continuidade.

CAPÍTULO XV

DA CONFORMIDADE, DA AUDITORIA, DO MONITORAMENTO, DA RESPONSABILIZAÇÃO E DA MELHORIA CONTÍNUA

Art. 25. O SGSI observará processo de conformidade, auditoria, monitoramento, responsabilização e melhoria contínua, com avaliação periódica dos controles, das políticas, dos processos, dos riscos e dos indicadores de desempenho.

§ 1º A conformidade abrangerá o atendimento à legislação aplicável, às orientações da ANPD, às deliberações do Comitê e aos documentos complementares desta Política.

§ 2º As auditorias, internas e externas, avaliarão a adequação e a eficácia dos controles, podendo abranger políticas, padrões, procedimentos, infraestrutura, sistemas, contratos e gestão de riscos.

§ 3º As não conformidades serão registradas, analisadas quanto à causa raiz e tratadas por ações corretivas e preventivas, observado o documento complementar específico.

§ 4º A responsabilização pelo descumprimento desta Política dar-se-á nas esferas administrativa, civil e criminal, conforme a legislação aplicável, sem prejuízo das medidas disciplinares cabíveis.

§ 5º A Política será revista periodicamente e sempre que houver alterações legislativas, organizacionais, incidentes relevantes ou recomendações de auditoria.

CAPÍTULO XVI

DA HIERARQUIA DOCUMENTAL, DOS DOCUMENTOS COMPLEMENTARES E DA IMPLANTAÇÃO PROGRESSIVA

Art. 26. A documentação de segurança da informação observará a seguinte hierarquia:

I - nível estratégico: esta Política, o Decreto Municipal nº 50.611/2026, a Matriz Consolidada de Responsabilidades, o Catálogo de Documentos Complementares e o Cronograma de Implantação;

II - nível tático: as normas temáticas que detalham esta Política;

III - nível operacional: os procedimentos, os planos e os modelos operacionais;

IV - nível evidencial: os registros, os formulários, as atas e os relatórios que comprovam a execução dos controles.

Parágrafo único. Os documentos complementares integram esta Política, detalham e operacionalizam as suas disposições, e não podem criar sanções nem obrigações autônomas não previstas no Decreto ou nesta Política.

Art. 27. Fica instituído o Catálogo de Documentos Complementares da Política Municipal de Segurança da Informação e Segurança Cibernética, composto por até 27 (vinte e sete) documentos, incluídas normas de uso aceitável, de gestão de identidades, acessos e senhas, de classificação da informação, de gestão de incidentes, de cópias de segurança, de continuidade e recuperação de desastres, de dispositivos móveis e trabalho remoto, de serviços em nuvem, de controles criptográficos, de gestão de mudanças, de desenvolvimento seguro, de gestão de fornecedores e contratos, de registro de operações, de auditoria, de indicadores e de não conformidades, além dos planos, procedimentos e modelos correlatos.

Art. 28. Esta Política e os seus documentos complementares serão implantados de forma progressiva, em fases, conforme cronograma aprovado pela Alta Administração, observadas as prioridades e as dependências entre os documentos.

CAPÍTULO XVII

DA VIGÊNCIA, DAS REVOGAÇÕES E DAS DISPOSIÇÕES FINAIS

Art. 29. Esta Política entra em vigor na data da sua publicação, permanecendo vigente até ser revista, substituída ou revogada.

Parágrafo único. Integra este Decreto o Anexo Único que o acompanha.

Art. 30. Esta Política não substitui o Decreto Municipal nº 50.611/2026, que institui a Política Municipal de Proteção de Dados Pessoais, com a qual coexiste de forma complementar e harmônica, nem dele depende para a sua validade, e não condiciona a sua eficácia à obtenção de certificação externa, inclusive ISO.

Art. 31. Os casos omissos serão dirimidos pelo Comitê de Segurança da Informação e Proteção de Dados, com apoio da Procuradoria Geral do Município, observadas a legislação federal aplicável, as orientações da Autoridade Nacional de Proteção de Dados (ANPD) e os princípios estabelecidos nesta Política.

Art. 32. A segurança da informação é responsabilidade institucional compartilhada, essencial para a boa governança pública, a proteção dos ativos informacionais, a continuidade dos serviços públicos e o fortalecimento da confiança da sociedade, e sua implementação efetiva requer a ação integrada da Alta Administração, das Secretarias Municipais, das unidades administrativas, da Secretaria Municipal responsável pela Tecnologia da Informação, do Encarregado (DPO), dos gestores, dos servidores, dos colaboradores e dos fornecedores.

Av. Morobá, 20 | Bairro Morobá, Aracruz-ES | Cep 29192-733
Tel: (27) 3270-7013 | 3270-7014 | www.pma.es.gov.br | prefeito@aracruz.es.gov.br

ANEXO ÚNICO

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E SEGURANÇA CIBERNÉTICA

CAPÍTULO 1

APRESENTAÇÃO INSTITUCIONAL, OBJETIVO E FINALIDADE DA POLÍTICA

1.1 Apresentação

A Prefeitura Municipal de Aracruz reconhece que a informação constitui um dos ativos estratégicos mais relevantes para o desempenho de suas funções institucionais, para a prestação eficiente dos serviços públicos e para a promoção da transparência, da inovação e da transformação digital no âmbito da Administração Pública Municipal.

O crescente processo de digitalização dos serviços públicos, a ampliação do uso de sistemas informatizados, a integração entre órgãos governamentais e a intensificação do tratamento de dados pessoais exigem a adoção de mecanismos permanentes de governança, gestão de riscos, proteção das informações e fortalecimento da segurança cibernética.

Nesse contexto, a presente Política de Segurança da Informação estabelece as diretrizes institucionais que orientam a proteção dos ativos de informação da Prefeitura Municipal de Aracruz, promovendo a utilização segura dos recursos tecnológicos, a preservação da continuidade dos serviços públicos, a proteção dos dados pessoais tratados pela Administração Municipal e a observância da legislação vigente.

Esta Política constitui o documento normativo de mais alto nível do Sistema de Gestão de Segurança da Informação (SGSI) da Prefeitura Municipal de Aracruz, servindo como referência para a elaboração das normas, procedimentos, padrões técnicos, processos administrativos e controles internos relacionados à segurança da informação e à proteção de dados.

1.2 Finalidade

A finalidade desta Política é estabelecer os princípios, diretrizes, responsabilidades e mecanismos de governança necessários para assegurar que as

informações produzidas, recebidas, armazenadas, processadas, transmitidas ou descartadas pela Prefeitura Municipal de Aracruz sejam protegidas de forma adequada durante todo o seu ciclo de vida, considerando sua importância para a Administração Pública, para os cidadãos e para a sociedade.

Esta Política busca promover uma cultura institucional de segurança da informação, fortalecendo a responsabilidade compartilhada entre gestores, servidores, colaboradores, terceirizados e demais usuários dos recursos tecnológicos da Administração Municipal, de forma a reduzir riscos, prevenir incidentes de segurança e garantir a continuidade dos serviços públicos.

Além disso, esta Política visa assegurar que todas as ações relacionadas à segurança da informação sejam conduzidas de forma integrada às estratégias institucionais, aos princípios da governança pública, à transformação digital e à proteção dos direitos fundamentais dos cidadãos.

1.3 Objetivos

Constituem objetivos desta Política:

- I – estabelecer as diretrizes institucionais para a gestão da segurança da informação no âmbito da Prefeitura Municipal de Aracruz;
- II – proteger a confidencialidade, a integridade, a disponibilidade, a autenticidade e a rastreabilidade das informações institucionais;
- III – fortalecer a governança da segurança da informação mediante definição clara de competências, responsabilidades e processos de tomada de decisão;
- IV – assegurar que a proteção da informação seja considerada em todas as atividades administrativas, técnicas e operacionais da Prefeitura;
- V – apoiar a continuidade dos serviços públicos por meio da implementação de controles administrativos, físicos e tecnológicos adequados aos riscos identificados;
- VI – promover a gestão sistemática dos riscos relacionados às informações, aos ativos tecnológicos e aos serviços digitais;
- VII – estabelecer diretrizes para a elaboração das normas complementares que compõem o Sistema de Gestão de Segurança da Informação;
- VIII – contribuir para a conformidade com a legislação aplicável à Administração Pública, especialmente quanto à proteção de dados pessoais, ao acesso à

informação, à transparência pública, à segurança digital e à governança de tecnologia da informação;

IX – promover ações permanentes de conscientização, capacitação e disseminação da cultura de segurança da informação entre todos os agentes públicos e usuários autorizados;

X – assegurar mecanismos de monitoramento, auditoria e melhoria contínua dos controles de segurança adotados pela Prefeitura.

1.4 Escopo Institucional da Política

Esta Política aplica-se a todos os órgãos, secretarias, fundos, autarquias, unidades administrativas e demais estruturas integrantes da Administração Pública Municipal de Aracruz que utilizem informações, ativos tecnológicos ou recursos de tecnologia da informação e comunicação sob responsabilidade da Prefeitura.

Estão igualmente sujeitos às disposições desta Política:

- agentes políticos;
- servidores efetivos;
- servidores comissionados;
- empregados públicos;
- estagiários;
- terceirizados;
- prestadores de serviços;
- consultores;
- fornecedores que possuam acesso a informações ou recursos tecnológicos da Prefeitura;
- quaisquer pessoas físicas ou jurídicas autorizadas a utilizar ativos de informação da Administração Municipal.

A aplicação desta Política estende-se a todas as informações, independentemente de seu meio de armazenamento ou transmissão, abrangendo documentos físicos, documentos digitais, sistemas corporativos, bancos de dados, equipamentos computacionais, serviços em nuvem, redes de comunicação, dispositivos móveis, mídias removíveis e quaisquer outros ativos relacionados ao tratamento da informação.

1.5 Hierarquia Documental

A presente Política constitui o documento institucional de mais alto nível da governança de segurança da informação da Prefeitura Municipal de Aracruz.

As diretrizes estabelecidas neste documento são complementadas por normas específicas, procedimentos operacionais, padrões técnicos, manuais, planos, registros e demais instrumentos administrativos que integram o Sistema de Gestão de Segurança da Informação.

Entre os principais documentos complementares destacam-se:

- Política Municipal de Proteção de Dados Pessoais;
- Norma de Uso Aceitável dos Recursos de Tecnologia da Informação e Comunicação;
- Norma de Gestão de Identidades, Acessos e Senhas;
- Norma de Classificação da Informação e Tratamento de Dados;
- Norma de Gestão de Dispositivos Móveis e Trabalho Remoto;
- Norma de Controles Criptográficos;
- Norma de Cópias de Segurança e Recuperação de Dados;
- Norma de Gestão de Mudanças;
- Procedimentos Operacionais de Segurança da Informação;
- Matriz de Riscos de Segurança da Informação;
- Declaração de Aplicabilidade (SoA);
- demais documentos institucionais relacionados à segurança da informação e à proteção de dados.

As normas complementares detalham requisitos específicos e procedimentos operacionais, não devendo reproduzir ou contrariar as diretrizes estabelecidas nesta Política.

CAPÍTULO 2 BASE LEGAL, PRINCÍPIOS E DIRETRIZES GERAIS

2.1 Base Legal

A presente Política de Segurança da Informação fundamenta-se nos princípios constitucionais da Administração Pública e nas normas legais que disciplinam a gestão da informação, a proteção de dados pessoais, a transformação digital, a transparência pública, a segurança cibernética e a governança da tecnologia da informação no âmbito da Administração Pública.

Constituem base legal desta Política, sem prejuízo da observância de outras normas aplicáveis:

I – Constituição da República Federativa do Brasil de 1988

Especialmente os princípios da legalidade, impessoalidade, moralidade, publicidade, eficiência, bem como os direitos fundamentais relacionados à intimidade, à vida privada, à proteção de dados pessoais, ao acesso à informação e à inviolabilidade das comunicações.

II – Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais (LGPD)

Estabelece regras para o tratamento de dados pessoais, inclusive em meios digitais, visando proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural, aplicando-se integralmente ao tratamento de dados realizado pela Administração Pública Municipal.

III – Lei nº 12.527, de 18 de novembro de 2011 – Lei de Acesso à Informação (LAI)

Regulamenta o direito constitucional de acesso às informações públicas, estabelecendo procedimentos para garantir a transparência ativa e passiva, sem prejuízo da proteção das informações sigilosas e dos dados pessoais.

IV – Lei nº 12.965, de 23 de abril de 2014 – Marco Civil da Internet

Define princípios, garantias, direitos e deveres para o uso da Internet no Brasil, disciplinando aspectos relacionados à privacidade, guarda de registros, segurança das comunicações e responsabilidade dos provedores.

V – Lei nº 14.129, de 29 de março de 2021 – Lei do Governo Digital

Dispõe sobre princípios, regras e instrumentos para o Governo Digital, promovendo a transformação digital da Administração Pública, a prestação de serviços digitais ao cidadão e o fortalecimento da segurança das informações utilizadas pelos órgãos públicos.

VI – Lei nº 14.133, de 1º de abril de 2021 – Lei de Licitações e Contratos Administrativos

Aplica-se especialmente às contratações relacionadas a serviços de tecnologia da informação, computação em nuvem, segurança cibernética, tratamento de dados pessoais e aquisição de soluções tecnológicas, exigindo gestão adequada dos riscos e fiscalização contratual.

VII – Decreto Municipal da Política Municipal de Proteção de Dados Pessoais

Institui a Política Municipal de Proteção de Dados Pessoais da Prefeitura Municipal de Aracruz, estabelecendo a estrutura de governança em privacidade, as atribuições do Encarregado pelo Tratamento de Dados Pessoais (DPO), as responsabilidades dos agentes públicos e as diretrizes para o tratamento de dados pessoais no âmbito da Administração Municipal.

As disposições relacionadas à governança da privacidade e à proteção de dados pessoais serão disciplinadas prioritariamente por aquele instrumento normativo, cabendo à presente Política apenas estabelecer sua integração ao Sistema de Gestão de Segurança da Informação.

VIII – Demais normas aplicáveis

Integram ainda o conjunto normativo desta Política todas as demais leis, decretos, regulamentos, orientações dos órgãos de controle, atos administrativos e normas internas aplicáveis à Administração Pública Municipal que tratem da segurança da informação, proteção de dados pessoais, transparência, continuidade dos serviços públicos, gestão documental e tecnologia da informação.

2.2 Referências Técnicas

Para fins de aperfeiçoamento contínuo da governança da Segurança da Informação, a Prefeitura poderá adotar como referência técnica boas práticas

reconhecidas nacional e internacionalmente, sempre que compatíveis com a legislação vigente e com a realidade da Administração Pública.

Essas referências técnicas possuem caráter orientativo e subsidiário, não substituindo nem se sobrepondo às disposições legais e regulamentares aplicáveis.

2.3 Princípios da Segurança da Informação

Todas as ações relacionadas à segurança da informação deverão observar os seguintes princípios:

I – Legalidade

O tratamento das informações deverá observar rigorosamente a legislação vigente, os regulamentos internos e as competências legalmente atribuídas aos agentes públicos.

II – Interesse Público

A segurança da informação constitui instrumento essencial para assegurar a prestação contínua, eficiente e segura dos serviços públicos, contribuindo para o atendimento do interesse coletivo e para a proteção do patrimônio público.

III – Confidencialidade

As informações deverão ser acessadas exclusivamente por pessoas autorizadas e somente quando houver necessidade funcional devidamente justificada.

IV – Integridade

As informações deverão permanecer íntegras, completas, exatas e protegidas contra alterações não autorizadas durante todo o seu ciclo de vida.

V – Disponibilidade

Os ativos de informação deverão permanecer disponíveis aos usuários autorizados sempre que necessários ao desempenho das atividades institucionais, observados os níveis de serviço estabelecidos.

VI – Autenticidade

Deverão ser adotados mecanismos que permitam assegurar a identificação inequívoca da origem das informações, dos usuários e das transações realizadas nos sistemas corporativos.

VII – Rastreabilidade

Os atos praticados nos ambientes tecnológicos deverão permitir registro, monitoramento e auditoria, garantindo a identificação das ações realizadas e dos respectivos responsáveis.

VIII – Responsabilização

Todo usuário responderá pelos atos praticados mediante utilização de suas credenciais de acesso e dos recursos tecnológicos disponibilizados pela Prefeitura, observado o devido processo legal.

IX – Gestão de Riscos

As decisões relacionadas à segurança da informação deverão considerar a identificação, análise, avaliação e tratamento dos riscos que possam comprometer os objetivos institucionais da Administração Municipal.

X – Proteção de Dados Pessoais

O tratamento de dados pessoais deverá observar os princípios, direitos e garantias estabelecidos na legislação vigente e na Política Municipal de Proteção de Dados Pessoais.

XI – Melhoria Contínua

Os processos de segurança da informação deverão ser permanentemente avaliados, monitorados e aperfeiçoados, considerando a evolução tecnológica, as mudanças organizacionais, as ameaças cibernéticas e os requisitos legais.

2.4 Diretrizes Gerais

Constituem diretrizes gerais desta Política:

I – promover a proteção dos ativos de informação da Prefeitura durante todo o seu ciclo de vida;

- II – assegurar que a segurança da informação seja considerada em todas as iniciativas relacionadas à tecnologia, inovação, governo digital e modernização administrativa;
- III – integrar a gestão da segurança da informação aos processos de governança institucional;
- IV – promover cultura organizacional baseada na responsabilidade compartilhada pela proteção das informações;
- V – garantir que todos os usuários conheçam suas responsabilidades antes de receber acesso aos recursos tecnológicos;
- VI – assegurar que normas, procedimentos e controles sejam proporcionais aos riscos identificados;
- VII – estimular a utilização segura das tecnologias digitais, preservando a continuidade dos serviços públicos;
- VIII – fortalecer mecanismos de prevenção, detecção, resposta e recuperação diante de incidentes de segurança da informação;
- IX – promover a integração entre segurança da informação, proteção de dados pessoais, gestão documental, transparência pública, continuidade dos serviços e transformação digital;
- X – manter estrutura documental organizada, atualizada e integrada, evitando duplicidade de normas e assegurando clareza na distribuição das responsabilidades.

2.5 Integração com os Demais Instrumentos Normativos

Esta Política estabelece as diretrizes estratégicas de Segurança da Informação da Prefeitura Municipal de Aracruz e deverá ser complementada por normas, procedimentos, planos e demais instrumentos específicos.

Os aspectos operacionais relacionados ao uso de recursos tecnológicos, gestão de acessos, classificação da informação, proteção de dados pessoais, dispositivos móveis, cópias de segurança, criptografia, gestão de mudanças, resposta a incidentes, continuidade dos serviços e demais controles serão disciplinados em documentos próprios, os quais passam a integrar formalmente o Sistema Municipal de Gestão de Segurança da Informação.

Na hipótese de conflito entre documentos, prevalecerão as disposições desta Política, da legislação vigente e da Política Municipal de Proteção de Dados Pessoais, cabendo às normas complementares disciplinar exclusivamente os aspectos técnicos e operacionais necessários à sua implementação.

2.6 Cláusula de Não Substituição do Decreto Municipal nº 50.611/2026

"Esta Política será aplicada de forma integrada à Política Municipal de Proteção de Dados Pessoais, instituída pelo Decreto Municipal nº 50.611/2026, não substituindo suas disposições, mas complementando-as no que tange à segurança técnica e administrativa. O Decreto permanece como instrumento jurídico autônomo de proteção de dados pessoais, e esta Política atua como instrumento complementar que fundamenta tecnicamente as medidas de segurança referidas no Art. 6º, inciso III, do referido Decreto."

2.7 Cláusula de Não Dependência de Certificação ISO

"A adoção de frameworks internacionais como ISO/IEC 27001 e ISO/IEC 27002 pela Prefeitura Municipal de Aracruz é facultativa e serve como referência técnica para a melhoria contínua do Sistema Municipal de Gestão da Segurança da Informação (SMGSI). A eficácia desta Política e do SMGSI não depende de certificação ISO, embora possa utilizá-la como referência para aprimoramento dos controles e processos de segurança."

2.8 Cláusula de Implantação Progressiva

"A implementação desta Política ocorrerá de forma progressiva, considerando a avaliação de riscos, a criticidade dos serviços públicos, a disponibilidade de recursos, a capacidade institucional e as prioridades definidas pela Administração. A ausência temporária de norma complementar não afasta a aplicação das diretrizes aqui estabelecidas. O Cronograma Geral de Implantação, Validação e Publicação (Documento Complementar nº 26) define as fases e prazos para a publicação progressiva dos documentos normativos complementares, estruturadas em quatro fases:

I —**Fase 1 (Imediata):** Publicação desta Política, da Norma de Uso Aceitável (Documento nº 01), da Matriz Consolidada de Responsabilidades (Documento nº 24) e do Cronograma de Implantação (Documento nº 26);

II —**Fase 2 (Alta Prioridade — D+30 a D+60):** Normas de Acessos (nº 02), Incidentes (nº 03), Classificação (nº 05), Contratos (nº 06), Atendimento aos Titulares (nº 04), Plano de Riscos (nº 07), Vulnerabilidades (nº 12), Inventário de Ativos (nº 16) e início do ROPA (nº 17);

III —**Fase 3 (Média Prioridade — D+60 a D+120):** Norma de Backup (nº 08), Plano de Continuidade (nº 09), DRP (nº 10), Logs (nº 11), Dispositivos Móveis (nº 13), Nuvem (nº 14), Gestão de Mudanças (nº 15), Desenvolvimento Seguro (nº 23) e Modelo de RIPD (nº 18);

IV —**Fase 4 (Governança e Melhoria Contínua — D+120 a D+180):** Plano de Capacitação (nº 19), Plano de Auditoria (nº 20), Procedimento de Não Conformidades (nº 21) e Procedimento de Indicadores (nº 22)."

CAPÍTULO 3

GOVERNANÇA DA SEGURANÇA DA INFORMAÇÃO

3.1 Objetivo da Governança

A Governança da Segurança da Informação da Prefeitura Municipal de Aracruz tem por finalidade estabelecer a estrutura organizacional, as competências, as responsabilidades e os mecanismos de tomada de decisão necessários para assegurar que a proteção das informações seja tratada como um processo permanente, integrado à gestão pública e alinhado aos objetivos estratégicos da Administração Municipal.

A governança da segurança da informação deverá promover a integração entre tecnologia, gestão, proteção de dados pessoais, continuidade dos serviços públicos, gestão de riscos, transparência, inovação e transformação digital, assegurando que as decisões relacionadas à segurança da informação sejam tomadas de forma coordenada, documentada e baseada em critérios técnicos e legais.

3.2 Estrutura de Governança

A Governança da Segurança da Informação da Prefeitura Municipal de Aracruz será composta pelos seguintes níveis institucionais:

I – Alta Administração

II – Comitê de Segurança da Informação e Proteção de Dados

III – Secretaria Municipal responsável pela Tecnologia da Informação

IV – Encarregado pelo Tratamento de Dados Pessoais (DPO)

V – Gestores das Secretarias Municipais

VI – Gestores de Contratos

VII – Servidores, empregados públicos, estagiários, terceirizados e demais usuários autorizados

Cada instância exercerá suas atribuições de forma integrada, observando as competências estabelecidas nesta Política e nos demais normativos institucionais.

3.3 Alta Administração

Compete à Alta Administração:

I – aprovar a Política de Segurança da Informação e suas alterações;

II – garantir recursos humanos, tecnológicos, financeiros e administrativos necessários à implementação das ações de segurança da informação;

III – promover a integração da segurança da informação às estratégias institucionais da Prefeitura;

IV – apoiar a cultura organizacional voltada à proteção das informações;

V – deliberar sobre riscos estratégicos relacionados à segurança da informação;

VI – acompanhar os resultados dos indicadores institucionais de segurança;

VII – apoiar as ações de melhoria contínua da governança da segurança da informação.

A Alta Administração permanece responsável pela governança institucional da segurança da informação, ainda que determinadas atividades sejam delegadas a outras unidades administrativas.

3.4 Comitê de Segurança da Informação e Proteção de Dados

O Comitê constitui órgão colegiado de natureza consultiva e deliberativa responsável por apoiar a governança da segurança da informação e da proteção de dados pessoais.

Compete ao Comitê:

- I – propor diretrizes estratégicas;
- II – acompanhar a implementação desta Política;
- III – analisar riscos estratégicos;
- IV – acompanhar incidentes relevantes;
- V – recomendar melhorias nos controles institucionais;
- VI – acompanhar indicadores;
- VII – apoiar a elaboração do Plano Anual de Segurança da Informação;
- VIII – acompanhar auditorias;
- IX – recomendar atualização dos documentos normativos;
- X – deliberar sobre assuntos que envolvam riscos institucionais relevantes.

O funcionamento do Comitê será regulamentado em ato próprio.

3.5 Secretaria Municipal responsável pela Tecnologia da Informação

Compete à unidade responsável pela Tecnologia da Informação:

- I – coordenar tecnicamente a implementação desta Política;
- II – administrar os recursos tecnológicos da Prefeitura;
- III – implementar controles técnicos de segurança;
- IV – manter mecanismos de monitoramento dos ambientes tecnológicos;
- V – administrar contas de usuários;
- VI – implementar controles de autenticação;
- VII – administrar cópias de segurança;
- VIII – apoiar investigações de incidentes;
- IX – manter registros técnicos necessários às auditorias;
- X – propor atualização das normas complementares.

A unidade de Tecnologia da Informação atuará como responsável pela coordenação técnica do Sistema Municipal de Gestão da Segurança da Informação.

3.6 Encarregado pelo Tratamento de Dados Pessoais (DPO)

As competências relacionadas à proteção de dados pessoais serão exercidas pelo Encarregado pelo Tratamento de Dados Pessoais, observadas as atribuições previstas na legislação vigente e na Política Municipal de Proteção de Dados Pessoais.

Compete ao Encarregado, entre outras atribuições:

- I – atuar como canal de comunicação com os titulares dos dados pessoais;
- II – atuar como canal de comunicação com a Autoridade Nacional de Proteção de Dados (ANPD);
- III – orientar as unidades administrativas quanto às boas práticas de proteção de dados;
- IV – apoiar avaliações de impacto relativas ao tratamento de dados pessoais;
- V – acompanhar incidentes envolvendo dados pessoais;
- VI – apoiar ações de conscientização e capacitação relacionadas à privacidade.

As competências específicas do Encarregado são disciplinadas pela Política Municipal de Proteção de Dados Pessoais, à qual esta Política faz referência.

3.7 Gestores das Secretarias Municipais

Cada Secretário Municipal responderá pela segurança das informações sob sua responsabilidade administrativa.

Compete aos gestores:

- I – assegurar o cumprimento desta Política;
- II – apoiar a implementação das normas complementares;
- III – autorizar acessos aos sistemas de sua área;
- IV – comunicar alterações funcionais que impliquem revisão de acessos;
- V – comunicar incidentes de segurança;
- VI – assegurar a classificação adequada das informações produzidas por sua unidade;
- VII – apoiar auditorias internas;
- VIII – promover ações de conscientização junto às suas equipes.

3.8 Gestores de Contratos

Os gestores de contratos que envolvam serviços de tecnologia da informação, tratamento de dados pessoais ou acesso a informações institucionais deverão:

- I – assegurar que os instrumentos contratuais contemplem requisitos de segurança da informação e proteção de dados;
- II – acompanhar o cumprimento das obrigações assumidas pelos contratados;
- III – comunicar imediatamente qualquer descumprimento contratual relacionado à segurança da informação;
- IV – solicitar apoio técnico da Secretaria responsável pela Tecnologia da Informação sempre que necessário.

3.9 Usuários dos Recursos Tecnológicos

Todos os usuários dos recursos tecnológicos da Prefeitura possuem responsabilidade individual pela proteção das informações às quais tenham acesso.

Constituem deveres dos usuários:

- I – utilizar os recursos tecnológicos exclusivamente para fins institucionais;
- II – proteger suas credenciais de acesso;
- III – observar as normas internas;
- IV – preservar o sigilo das informações;
- V – comunicar incidentes imediatamente;
- VI – utilizar os recursos tecnológicos de forma ética, responsável e compatível com a legislação vigente.

As regras operacionais relacionadas ao uso dos recursos tecnológicos encontram-se disciplinadas na **Norma de Uso Aceitável dos Recursos de Tecnologia da Informação e Comunicação**, integrante do Sistema Municipal de Gestão da Segurança da Informação.

3.10 Segregação de Funções

A Prefeitura deverá adotar mecanismos de segregação de funções sempre que tecnicamente e administrativamente viável, visando reduzir riscos decorrentes da concentração de privilégios.

Sempre que possível, as atividades de solicitação, autorização, implementação, fiscalização e auditoria deverão ser desempenhadas por agentes distintos.

Quando a segregação integral não puder ser implementada em razão da estrutura organizacional, deverão ser adotados controles compensatórios, tais como supervisão, revisão periódica de atividades, registros de auditoria e monitoramento contínuo.

3.11 Prestação de Contas e Responsabilização

Todos os agentes públicos, colaboradores e terceiros que utilizem informações ou recursos tecnológicos da Prefeitura são responsáveis pelos atos praticados no exercício de suas atribuições.

O descumprimento desta Política ou das normas complementares poderá ensejar a adoção das medidas administrativas, disciplinares, civis e penais cabíveis, observados o contraditório, a ampla defesa e a legislação aplicável.

3.12 Integração da Governança

- Matriz Consolidada de Responsabilidades em Segurança da Informação e Proteção de Dados;
- Plano de Capacitação e Conscientização em Segurança da Informação e Proteção de Dados;
- Plano Anual de Auditoria e Conformidade em Segurança da Informação e Proteção de Dados;
- Procedimento de Indicadores, Monitoramento e Análise Crítica em segurança da informação e proteção de dados.

CAPÍTULO 4

GESTÃO DOS ATIVOS DE INFORMAÇÃO E PATRIMÔNIO INFORMACIONAL

4.1 Objetivo

A gestão dos ativos de informação tem por objetivo assegurar que as informações, os recursos tecnológicos e os demais ativos utilizados pela Prefeitura Municipal de Aracruz sejam identificados, inventariados, protegidos, utilizados de forma adequada e mantidos disponíveis durante todo o seu ciclo de vida, observadas a legislação vigente, as necessidades institucionais e os princípios estabelecidos nesta Política.

A proteção dos ativos de informação constitui responsabilidade compartilhada entre a Alta Administração, os gestores das unidades administrativas, a unidade responsável pela Tecnologia da Informação, o Encarregado pelo Tratamento de Dados Pessoais, os servidores, colaboradores e terceiros que, de qualquer forma, tenham acesso às informações institucionais.

4.2 Conceito de Ativo de Informação

Para os fins desta Política, considera-se ativo de informação qualquer recurso que possua valor para a Administração Pública Municipal e cuja perda de confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade possa comprometer o cumprimento das funções institucionais, a prestação dos serviços públicos, a continuidade das atividades administrativas ou os direitos dos cidadãos.

Constituem ativos de informação, entre outros:

- I – informações produzidas, recebidas, armazenadas, processadas ou compartilhadas pela Prefeitura;
- II – documentos físicos e digitais;
- III – bancos de dados;
- IV – processos administrativos eletrônicos;
- V – sistemas corporativos;
- VI – aplicações desenvolvidas internamente ou contratadas;
- VII – infraestrutura tecnológica;
- VIII – equipamentos computacionais;
- IX – dispositivos móveis;

- X – serviços em nuvem;
- XI – redes de comunicação;
- XII – mídias de armazenamento;
- XIII – credenciais de acesso;
- XIV – registros de auditoria e logs;
- XV – conhecimento técnico produzido pelos órgãos municipais;
- XVI – informações estratégicas, administrativas, financeiras, tributárias, educacionais, de saúde, assistência social, recursos humanos, planejamento urbano e demais informações produzidas pela Administração Pública.

4.3 Patrimônio Informacional

As informações produzidas ou custodiadas pela Prefeitura Municipal de Aracruz constituem patrimônio público institucional e deverão ser protegidas de forma compatível com seu valor, criticidade, finalidade e requisitos legais.

O patrimônio informacional deverá ser tratado como recurso estratégico da Administração Municipal, devendo receber proteção proporcional aos impactos decorrentes de seu uso inadequado, alteração indevida, indisponibilidade, destruição ou divulgação não autorizada.

A proteção do patrimônio informacional deverá observar simultaneamente:

- a necessidade de garantir transparência pública;
- a proteção de informações sigilosas;
- a proteção de dados pessoais;
- a preservação da memória institucional;
- a continuidade dos serviços públicos;
- a segurança jurídica dos atos administrativos.

4.4 Ciclo de Vida da Informação

Toda informação tratada pela Prefeitura Municipal de Aracruz deverá ser protegida durante todo o seu ciclo de vida, compreendendo, no mínimo, as seguintes etapas:

- I – produção ou recebimento;
- II – registro;

- III – classificação;
- IV – armazenamento;
- V – utilização;
- VI – compartilhamento;
- VII – transporte ou transmissão;
- VIII – arquivamento;
- IX – preservação;
- X – descarte ou eliminação.

Cada etapa deverá observar controles administrativos, físicos e tecnológicos compatíveis com a natureza da informação e com os riscos envolvidos.

Os critérios técnicos para classificação, armazenamento, compartilhamento, retenção e descarte serão disciplinados na **Norma de Classificação da Informação e Tratamento de Dados**, integrante do Sistema Municipal de Gestão da Segurança da Informação.

4.5 Inventário de Ativos

A Prefeitura deverá manter processo permanente de identificação e inventário dos ativos de informação considerados relevantes para o funcionamento da Administração Municipal.

O inventário deverá contemplar, sempre que aplicável:

- identificação do ativo;
- proprietário da informação;
- unidade responsável;
- localização;
- classificação;
- criticidade;
- dependências tecnológicas;
- requisitos legais aplicáveis;
- responsável operacional.

O inventário deverá ser revisado periodicamente e sempre que ocorrerem alterações significativas na infraestrutura, nos processos administrativos ou nos serviços públicos.

4.6 Proprietários da Informação

Toda informação institucional deverá possuir um proprietário claramente identificado.

O proprietário da informação é o gestor da unidade administrativa responsável pela produção, utilização ou custódia da informação.

Compete ao proprietário:

- I – definir a finalidade da informação;
- II – aprovar seu nível de classificação;
- III – autorizar o acesso quando necessário;
- IV – garantir que a informação permaneça atualizada;
- V – comunicar alterações relevantes;
- VI – apoiar processos de auditoria;
- VII – participar da avaliação dos riscos relacionados às informações sob sua responsabilidade.

A responsabilidade técnica pela administração dos sistemas não transfere à unidade de Tecnologia da Informação a propriedade das informações neles armazenadas.

4.7 Gestão dos Ativos Tecnológicos

A Secretaria responsável pela Tecnologia da Informação manterá mecanismos para administração dos ativos tecnológicos utilizados pela Prefeitura, abrangendo, entre outros:

- computadores;
- notebooks;
- servidores;
- equipamentos de rede;
- dispositivos móveis corporativos;
- soluções em nuvem;
- licenças de software;
- equipamentos de segurança;
- serviços tecnológicos contratados.

A gestão técnica desses ativos deverá observar critérios de disponibilidade, atualização tecnológica, manutenção preventiva, monitoramento, continuidade operacional e segurança.

Os procedimentos específicos para utilização dos recursos tecnológicos encontram-se disciplinados na **Norma de Uso Aceitável dos Recursos de Tecnologia da Informação e Comunicação**.

4.8 Compartilhamento de Informações

O compartilhamento de informações deverá observar:

- I – a finalidade institucional;
- II – o princípio da necessidade de conhecimento;
- III – as competências legais do órgão destinatário;
- IV – a legislação sobre proteção de dados pessoais;
- V – a legislação sobre acesso à informação;
- VI – os acordos ou instrumentos jurídicos aplicáveis.

Sempre que envolver dados pessoais, o compartilhamento deverá observar também as diretrizes estabelecidas na **Política Municipal de Proteção de Dados Pessoais**.

4.9 Preservação e Retenção das Informações

As informações institucionais deverão ser preservadas pelo período necessário ao cumprimento das obrigações legais, administrativas, fiscais, históricas e arquivísticas.

A retenção documental observará:

- legislação arquivística;
- tabelas de temporalidade;
- requisitos legais específicos;
- necessidades institucionais;
- decisões das autoridades competentes.

O descarte de documentos somente poderá ocorrer mediante observância dos procedimentos oficialmente estabelecidos pela Prefeitura.

4.10 Descarte Seguro

O descarte de informações, documentos, mídias e equipamentos deverá assegurar que informações institucionais, sigilosas ou dados pessoais não possam ser recuperados por pessoas não autorizadas.

Os procedimentos técnicos para descarte seguro serão disciplinados na **Norma de Classificação da Informação e Tratamento de Dados** e na **Norma de Descarte Seguro de Informações e Mídias**, quando existente.

4.11 Proteção dos Ativos por Terceiros

Os terceiros que, em razão de contratos, convênios, parcerias ou outros instrumentos jurídicos, tenham acesso a ativos de informação da Prefeitura deverão observar integralmente esta Política, as normas complementares e as cláusulas contratuais aplicáveis.

Sempre que necessário, deverão ser firmados termos de confidencialidade, responsabilidade e proteção de dados, bem como estabelecidos controles proporcionais aos riscos decorrentes da atividade contratada.

4.12 Diretrizes Gerais para Gestão dos Ativos

A gestão dos ativos de informação deverá observar, no mínimo, as seguintes diretrizes:

- I – identificação dos ativos essenciais à prestação dos serviços públicos;
- II – definição clara de responsabilidades sobre cada ativo;
- III – manutenção de inventário atualizado;
- IV – adoção de controles compatíveis com a criticidade dos ativos;
- V – proteção das informações durante todo o seu ciclo de vida;
- VI – integração entre gestão documental, segurança da informação e proteção de dados pessoais;
- VII – monitoramento contínuo dos riscos associados aos ativos;
- VIII – revisão periódica dos controles implementados;
- IX – promoção da cultura de proteção do patrimônio informacional.

4.13 Referências aos Documentos Complementares

- Procedimento de Inventário e Gestão de Ativos de Informação;
- Norma de Classificação e Tratamento da Informação;
- Registro de Operações de Tratamento de Dados Pessoais (ROPA).

CAPÍTULO 5

GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

5.1 Objetivo

A Gestão de Riscos de Segurança da Informação tem por objetivo identificar, analisar, avaliar, tratar, monitorar e comunicar os riscos que possam comprometer a confidencialidade, a integridade, a disponibilidade, a autenticidade e a rastreabilidade das informações sob responsabilidade da Prefeitura Municipal de Aracruz.

A gestão de riscos constitui processo permanente de governança e deverá subsidiar a tomada de decisão pela Administração Municipal, permitindo que os recursos institucionais sejam direcionados prioritariamente para os ativos, processos e serviços mais críticos.

5.2 Princípios da Gestão de Riscos

A gestão de riscos deverá observar, no mínimo, os seguintes princípios:

- I – integração aos processos de governança e gestão institucional;
- II – alinhamento aos objetivos estratégicos da Administração Municipal;
- III – abordagem preventiva e proativa;
- IV – proporcionalidade entre os riscos identificados e os controles adotados;
- V – melhoria contínua dos processos de gestão de riscos;
- VI – transparência na comunicação dos riscos às instâncias competentes;
- VII – responsabilidade compartilhada entre todas as unidades administrativas;
- VIII – utilização de critérios técnicos e objetivos para análise e priorização dos riscos.

A gestão de riscos deverá considerar não apenas os aspectos tecnológicos, mas também fatores humanos, organizacionais, jurídicos, financeiros, operacionais, ambientais e reputacionais.

5.3 Abrangência

A gestão de riscos deverá abranger todos os ativos de informação e processos que possam impactar as atividades da Administração Municipal, incluindo, entre outros:

- informações institucionais;
- dados pessoais;
- sistemas informatizados;
- infraestrutura tecnológica;
- redes de comunicação;
- serviços em nuvem;
- serviços terceirizados;
- documentos físicos;
- equipamentos de tecnologia;
- ambientes físicos;
- processos administrativos;
- serviços digitais oferecidos ao cidadão;
- integrações com órgãos externos.

5.4 Responsabilidades pela Gestão de Riscos

A gestão de riscos é responsabilidade institucional compartilhada.

Compete:

À Alta Administração

- I – aprovar a estratégia institucional de gestão de riscos;
- II – definir o nível de risco aceitável para a Administração Municipal;
- III – deliberar sobre riscos estratégicos que possam comprometer a continuidade dos serviços públicos;
- IV – assegurar recursos necessários para implementação das medidas de tratamento.

Ao Comitê de Segurança da Informação

Compete:

- I – acompanhar o processo institucional de gestão de riscos;
- II – analisar riscos críticos;

- III – propor prioridades de tratamento;
- IV – acompanhar a evolução dos planos de ação;
- V – recomendar medidas de mitigação.

À Secretaria responsável pela Tecnologia da Informação

Compete:

- I – coordenar tecnicamente o processo de avaliação dos riscos relacionados aos ativos tecnológicos;
- II – apoiar tecnicamente as unidades administrativas;
- III – manter registros dos riscos identificados;
- IV – apoiar a elaboração da Matriz de Riscos;
- V – acompanhar a implementação dos controles técnicos.

Aos Gestores das Unidades Administrativas

Compete:

- I – identificar riscos relacionados aos processos sob sua responsabilidade;
- II – comunicar novos riscos;
- III – apoiar a avaliação dos impactos;
- IV – implementar controles administrativos necessários;
- V – acompanhar os riscos residuais.

Aos Usuários

Compete comunicar situações que possam representar riscos à segurança da informação, colaborando com a prevenção de incidentes e com a melhoria contínua dos controles.

5.5 Processo de Gestão de Riscos

A gestão de riscos deverá ocorrer de forma sistemática e contínua, compreendendo, no mínimo, as seguintes etapas:

- I – estabelecimento do contexto;
- II – identificação dos ativos;
- III – identificação das ameaças;
- IV – identificação das vulnerabilidades;
- V – análise dos impactos;

- VI – avaliação da probabilidade;
- VII – determinação do nível de risco;
- VIII – definição da estratégia de tratamento;
- IX – implementação dos controles;
- X – monitoramento contínuo;
- XI – revisão periódica.

Os critérios metodológicos adotados pela Prefeitura serão disciplinados na **Metodologia de Gestão de Riscos** e na **Matriz Corporativa de Riscos de Segurança da Informação**, documentos integrantes do Sistema de Gestão da Segurança da Informação.

5.6 Critérios para Avaliação dos Riscos

Na avaliação dos riscos deverão ser considerados, sempre que aplicável:

- impactos financeiros;
- impactos legais;
- impactos operacionais;
- impactos reputacionais;
- impactos à continuidade dos serviços públicos;
- impactos ao cidadão;
- impactos à proteção de dados pessoais;
- impactos à transparência pública;
- impactos ambientais;
- impactos relacionados à saúde e segurança.

A avaliação deverá considerar tanto eventos intencionais quanto acidentais.

5.7 Tratamento dos Riscos

Após a avaliação, cada risco deverá possuir estratégia de tratamento formalmente definida.

As estratégias poderão compreender:

- I – eliminação do risco;
- II – redução do risco mediante implementação de controles;
- III – compartilhamento ou transferência do risco;

IV – aceitação formal do risco residual pela autoridade competente.

Toda decisão relativa ao tratamento dos riscos deverá ser registrada e documentada.

5.8 Plano de Tratamento dos Riscos

Os riscos considerados relevantes deverão integrar Plano de Tratamento contendo, no mínimo:

- identificação do risco;
- ativo afetado;
- controles existentes;
- controles a serem implementados;
- responsável pela implementação;
- prazo;
- prioridade;
- recursos necessários;
- indicadores de acompanhamento;
- situação da implementação.

O Plano de Tratamento será revisado periodicamente pelo Comitê de Segurança da Informação.

5.9 Monitoramento dos Riscos

Os riscos deverão ser monitorados continuamente.

O monitoramento deverá considerar:

- alterações tecnológicas;
- mudanças organizacionais;
- novas legislações;
- incidentes ocorridos;
- auditorias;
- testes realizados;
- mudanças na infraestrutura;
- novos serviços digitais;
- alterações contratuais;

- evolução das ameaças cibernéticas.

Sempre que ocorrer alteração significativa no ambiente institucional, deverá ser realizada nova avaliação dos riscos.

5.10 Indicadores

A Prefeitura deverá estabelecer indicadores para acompanhar a evolução da gestão de riscos.

Os indicadores poderão contemplar:

- quantidade de riscos identificados;
- percentual de riscos tratados;
- riscos críticos pendentes;
- tempo médio de implementação dos controles;
- incidentes relacionados a riscos conhecidos;
- percentual de planos concluídos;
- percentual de controles implementados;
- evolução da maturidade da gestão de riscos.

5.11 Integração com a Gestão da Segurança da Informação

A gestão de riscos deverá subsidiar:

- a definição dos controles administrativos;
- a implementação dos controles tecnológicos;
- a elaboração das normas complementares;
- a atualização dos procedimentos operacionais;
- a definição das prioridades de investimento em tecnologia;
- o Plano Diretor de Tecnologia da Informação;
- os planos de continuidade de negócios;
- os planos de resposta a incidentes;
- os programas de conscientização;
- os processos de contratação de soluções tecnológicas.

5.12 Integração com a Proteção de Dados Pessoais

Quando os riscos envolverem tratamento de dados pessoais, deverão ser observadas, além desta Política, as disposições da Política Municipal de Proteção de Dados Pessoais.

Sempre que necessário, poderão ser elaborados Relatórios de Impacto à Proteção de Dados Pessoais (RIPD), em conformidade com a LGPD e com as orientações da Autoridade Nacional de Proteção de Dados (ANPD).

A atuação conjunta entre a unidade responsável pela Tecnologia da Informação, o Encarregado pelo Tratamento de Dados Pessoais e os gestores das unidades administrativas deverá assegurar que os riscos à privacidade sejam avaliados de forma integrada aos riscos de segurança da informação.

Os riscos identificados que envolvam dados pessoais devem ser integrados ao Relatório de Impacto à Proteção de Dados Pessoais (RIPD — Modelo de Relatório de Impacto à Proteção de Dados) quando aplicável, e ao Registro de Operações de Tratamento de Dados Pessoais (ROPA — Registro de Operações de Tratamento de Dados Pessoais). O Encarregado (DPO) deve participar da avaliação de riscos de privacidade.

5.13 Documentos Complementares

Este capítulo é complementado pelos seguintes documentos:

- Plano de Tratamento de Riscos de Segurança da Informação e Privacidade;
- Registro de Operações de Tratamento de Dados Pessoais (ROPA);
- Modelo de Relatório de Impacto à Proteção de Dados (RIPD);
- Procedimento de Inventário e Gestão de Ativos de Informação.

5.14 Disposições Gerais

A gestão de riscos deverá ser compreendida como processo contínuo de aperfeiçoamento institucional, contribuindo para a proteção do patrimônio público, para a continuidade dos serviços prestados ao cidadão, para a conformidade legal e para o fortalecimento da governança da Prefeitura Municipal de Aracruz.

Todas as unidades administrativas deverão colaborar com a identificação, avaliação, tratamento e monitoramento dos riscos relacionados às suas atividades,

promovendo uma cultura organizacional baseada na prevenção, na responsabilidade e na melhoria contínua.

CAPÍTULO 6

GESTÃO DE PESSOAS, COMPETÊNCIAS, CONSCIENTIZAÇÃO E RESPONSABILIZAÇÃO

6.1 Objetivo

Este capítulo estabelece as diretrizes para a gestão de pessoas sob a perspectiva da Segurança da Informação, visando assegurar que todos os agentes públicos, colaboradores e terceiros compreendam suas responsabilidades quanto à proteção das informações institucionais, dos ativos tecnológicos e dos dados pessoais tratados pela Prefeitura Municipal de Aracruz.

A segurança da informação constitui responsabilidade de todos os usuários dos recursos institucionais, devendo fazer parte da cultura organizacional da Administração Pública Municipal.

6.2 Abrangência

As disposições deste capítulo aplicam-se a:

- I – agentes políticos;
- II – servidores efetivos;
- III – servidores ocupantes de cargos em comissão;
- IV – empregados públicos;
- V – estagiários;
- VI – aprendizes;
- VII – bolsistas;
- VIII – prestadores de serviços;
- IX – empresas contratadas;
- X – consultores;
- XI – fornecedores;
- XII – voluntários;
- XIII – qualquer pessoa física ou jurídica que possua acesso autorizado às informações ou aos recursos tecnológicos da Prefeitura.

O grau de acesso às informações deverá ser compatível com as atribuições desempenhadas por cada usuário.

6.3 Princípios

A gestão de pessoas em Segurança da Informação observará os seguintes princípios:

- I – responsabilidade individual;
- II – necessidade de conhecimento;
- III – menor privilégio;
- IV – segregação de funções;
- V – ética na utilização das informações;
- VI – transparência administrativa, observados os limites legais;
- VII – proteção dos dados pessoais;
- VIII – capacitação permanente;
- IX – melhoria contínua.

6.4 Competências Institucionais

Compete à Administração Municipal:

- I – promover ambiente institucional favorável à cultura de Segurança da Informação;
- II – disponibilizar normas e orientações atualizadas;
- III – promover programas permanentes de conscientização;
- IV – assegurar capacitação adequada aos usuários;
- V – disponibilizar canais para comunicação de incidentes;
- VI – manter mecanismos para registro e tratamento de ocorrências relacionadas ao comportamento dos usuários.

6.5 Processo de Admissão, Nomeação ou Contratação

Todo ingresso de servidor, colaborador, estagiário, terceirizado ou prestador de serviço que implique acesso às informações institucionais deverá observar procedimentos formais de autorização.

Antes da concessão de acesso aos recursos tecnológicos, o usuário deverá:

- I – receber orientações sobre suas responsabilidades;
- II – tomar ciência da Política de Segurança da Informação;

- III – tomar ciência da Norma de Uso Aceitável dos Recursos de Tecnologia da Informação;
- IV – tomar ciência da Política Municipal de Proteção de Dados Pessoais;
- V – firmar Termo de Ciência e Responsabilidade, quando aplicável;
- VI – receber somente os acessos estritamente necessários ao desempenho de suas atividades.

6.6 Concessão de Acessos

A concessão de acessos deverá observar:

- I – autorização do gestor responsável;
- II – necessidade funcional;
- III – perfil compatível com as atribuições;
- IV – registro formal da autorização;
- V – rastreabilidade das concessões.

As regras técnicas relacionadas à criação, alteração, bloqueio e revogação de contas são disciplinadas na **Norma de Gestão de Identidades, Acessos e Senhas**.

6.7 Alterações Funcionais

Sempre que ocorrer mudança de cargo, função, lotação, atribuições ou unidade administrativa, os acessos concedidos ao usuário deverão ser revisados tempestivamente.

Os gestores deverão comunicar formalmente à unidade responsável pela Tecnologia da Informação qualquer alteração que implique necessidade de concessão, modificação ou revogação de privilégios de acesso.

6.8 Desligamento

Nos casos de exoneração, demissão, aposentadoria, término de contrato, encerramento de estágio, rescisão contratual ou qualquer outra forma de desligamento, deverão ser adotadas medidas para assegurar a proteção das informações institucionais.

Sempre que aplicável, deverão ser providenciados:

- I – bloqueio ou exclusão das contas de acesso;

- II – recolhimento de equipamentos institucionais;
- III – devolução de documentos;
- IV – devolução de mídias;
- V – cancelamento de acessos remotos;
- VI – revogação de certificados digitais institucionais, quando existentes;
- VII – atualização dos registros administrativos.

6.9 Capacitação e Conscientização

A Prefeitura manterá programa permanente de conscientização em Segurança da Informação, destinado a promover o conhecimento das normas institucionais e estimular comportamentos seguros no ambiente de trabalho.

O programa poderá contemplar:

- I – treinamentos presenciais;
- II – cursos em ambiente virtual;
- III – palestras;
- IV – campanhas educativas;
- V – comunicados institucionais;
- VI – cartilhas;
- VII – simulados de incidentes;
- VIII – campanhas de prevenção ao phishing e à engenharia social;
- IX – ações específicas voltadas à proteção de dados pessoais.

As ações deverão considerar os diferentes perfis de usuários e os riscos associados às atividades desempenhadas.

6.10 Responsabilidades Individuais

Todo usuário dos recursos institucionais deverá:

- I – proteger suas credenciais de acesso;
- II – utilizar os recursos tecnológicos exclusivamente para finalidades institucionais, ressalvadas as hipóteses autorizadas em norma específica;
- III – preservar o sigilo das informações às quais tiver acesso;
- IV – comunicar imediatamente incidentes ou suspeitas de incidentes de segurança;

- V – observar as normas internas relacionadas à Segurança da Informação;
- VI – zelar pela integridade dos ativos sob sua responsabilidade;
- VII – utilizar equipamentos institucionais de forma diligente;
- VIII – colaborar com auditorias e investigações quando solicitado.

6.11 Condutas Vedadas

É vedado aos usuários:

- I – compartilhar credenciais de acesso;
- II – utilizar credenciais de terceiros;
- III – burlar controles de segurança;
- IV – instalar softwares sem autorização;
- V – utilizar equipamentos institucionais para fins ilícitos;
- VI – divulgar informações institucionais sem autorização;
- VII – remover informações institucionais sem necessidade funcional;
- VIII – armazenar informações institucionais em serviços não autorizados;
- IX – utilizar recursos tecnológicos para práticas discriminatórias, ofensivas ou incompatíveis com a legislação.

As condutas específicas relacionadas ao uso dos recursos tecnológicos encontram-se disciplinadas na **Norma de Uso Aceitável dos Recursos de Tecnologia da Informação e Comunicação**.

6.12 Cultura Organizacional

A Segurança da Informação deverá ser incorporada à cultura organizacional da Prefeitura, constituindo elemento permanente da gestão pública.

Os gestores deverão estimular boas práticas de proteção da informação em suas equipes, promovendo ambiente de confiança, responsabilidade e cooperação.

A cultura organizacional deverá incentivar a comunicação tempestiva de vulnerabilidades, falhas ou incidentes, sem prejuízo da apuração das responsabilidades quando houver dolo, fraude, negligência ou descumprimento das normas.

6.13 Confidencialidade e Sigilo

Os usuários deverão preservar o sigilo das informações classificadas ou protegidas por disposição legal, contratual ou administrativa.

A obrigação de confidencialidade permanecerá mesmo após o desligamento do usuário, observados os prazos e condições estabelecidos na legislação e nos instrumentos firmados com a Administração Municipal.

Sempre que necessário, poderão ser exigidos Termos de Confidencialidade específicos para atividades que envolvam informações sensíveis, estratégicas ou dados pessoais.

6.14 Gestão de Terceiros

As empresas contratadas e seus colaboradores deverão cumprir integralmente esta Política, as normas complementares e as cláusulas de segurança previstas nos instrumentos contratuais.

Os contratos que envolvam acesso a informações institucionais deverão prever, quando aplicável:

- obrigações de confidencialidade;
- requisitos mínimos de segurança da informação;
- proteção de dados pessoais;
- comunicação de incidentes;
- responsabilidades das partes;
- penalidades por descumprimento.

O gestor do contrato deverá acompanhar o cumprimento dessas obrigações.

6.15 Medidas Administrativas

O descumprimento desta Política ou das normas complementares poderá ensejar a adoção das medidas administrativas, disciplinares, civis e penais cabíveis, observados:

- a legislação vigente;
- o devido processo legal;
- o contraditório;
- a ampla defesa;

- os regulamentos internos da Prefeitura.

As sanções serão aplicadas de forma proporcional à natureza da infração, aos impactos causados e às circunstâncias do caso concreto.

6.16 Uso Responsável de Inteligência Artificial

O uso de ferramentas de inteligência artificial generativa no âmbito da Prefeitura Municipal de Aracruz deve observar rigorosos critérios de segurança e proteção de dados:

- I — É terminantemente VEDADA a inserção de dados pessoais, informações sigilosas, processos não públicos, segredos de Estado ou informações restritas em ferramentas de IA generativa externas não homologadas pela Secretaria de Transformação Digital;
- II — Todo conteúdo gerado por IA deve passar por validação humana antes de ser utilizado em atos administrativos ou documentos oficiais;
- III — É proibida a tomada de decisão administrativa automatizada baseada exclusivamente em IA sem governança específica, validação humana e autorização formal;
- IV — O uso de IA para gerar conteúdo que comprometa a imagem institucional, reproduza vieses discriminatórios ou viole direitos de propriedade intelectual é expressamente proibido;
- V — A Secretaria de Transformação Digital deverá homologar ferramentas de IA autorizadas para uso institucional, estabelecendo diretrizes técnicas específicas;
- VI — O uso responsável de IA será incluído como tema obrigatório no Plano de Capacitação e Conscientização (Documento Complementar nº 19)

6.17 Documentos Complementares

- Norma de Uso Aceitável dos Recursos de TIC;
- Plano de Capacitação e Conscientização em Segurança da Informação e Proteção de Dados;
- Matriz Consolidada de Responsabilidades.

6.18 Disposições Gerais

A efetividade da Segurança da Informação depende da participação ativa de todos os usuários dos recursos institucionais. A Prefeitura Municipal de Aracruz promoverá continuamente ações voltadas ao fortalecimento da cultura de segurança, à valorização das boas práticas e ao desenvolvimento de competências relacionadas à proteção das informações e dos serviços públicos digitais.

A conscientização permanente, aliada à definição clara de responsabilidades e ao cumprimento das normas institucionais, constitui elemento essencial para a redução dos riscos de segurança, para a proteção do patrimônio público e para o fortalecimento da confiança da sociedade na Administração Pública Municipal.

CAPÍTULO 7

GESTÃO DE IDENTIDADES, CONTROLE DE ACESSO E RESPONSABILIDADES DE ACESSO

7.1 Objetivo

Este capítulo estabelece as diretrizes institucionais para a gestão das identidades digitais, autenticação, autorização, controle de acesso e administração de privilégios no âmbito da Prefeitura Municipal de Aracruz, visando assegurar que o acesso às informações e aos recursos tecnológicos ocorra exclusivamente por usuários devidamente autorizados, observando os princípios da legalidade, necessidade de conhecimento, menor privilégio, segregação de funções, rastreabilidade e responsabilização.

O controle de acesso constitui um dos principais mecanismos para proteção dos ativos de informação da Administração Pública, devendo ser implementado de forma padronizada, documentada, auditável e compatível com os riscos associados aos serviços e processos institucionais.

7.2 Princípios da Gestão de Identidades

A gestão de identidades e acessos observará os seguintes princípios:

- I – identificação inequívoca de todos os usuários;
- II – autenticação adequada ao nível de risco da informação acessada;
- III – concessão de acessos baseada em necessidade funcional;

- IV – aplicação do princípio do menor privilégio;
- V – segregação de funções sempre que possível;
- VI – revisão periódica dos privilégios concedidos;
- VII – rastreabilidade de todas as operações relevantes;
- VIII – revogação tempestiva dos acessos quando cessar a necessidade de utilização;
- IX – proteção das credenciais de autenticação;
- X – responsabilização individual pelo uso das credenciais.

7.3 Abrangência

As diretrizes deste capítulo aplicam-se ao acesso a:

- sistemas corporativos;
- redes de computadores;
- serviços em nuvem;
- bancos de dados;
- correio eletrônico institucional;
- equipamentos computacionais;
- dispositivos móveis corporativos;
- aplicações web;
- portais administrativos;
- sistemas de terceiros utilizados pela Prefeitura;
- ambientes de desenvolvimento, homologação e produção;
- quaisquer recursos tecnológicos administrados ou utilizados pela Administração Municipal.

7.4 Identidade Digital

Todo usuário autorizado deverá possuir identidade digital individual, exclusiva e intransferível.

A identidade digital deverá permitir a identificação inequívoca do responsável pelas ações realizadas nos ambientes tecnológicos da Prefeitura, possibilitando a manutenção de registros de auditoria e a responsabilização pelos atos praticados.

É vedada a utilização de contas genéricas, compartilhadas ou anônimas para atividades que exijam identificação individual, ressalvadas situações excepcionais devidamente justificadas, autorizadas e controladas pela unidade responsável pela Tecnologia da Informação.

7.5 Gestão do Ciclo de Vida das Identidades

A gestão das identidades deverá abranger todo o ciclo de vida do usuário, compreendendo, no mínimo:

- I – solicitação de acesso;
- II – análise da necessidade funcional;
- III – autorização pelo gestor competente;
- IV – criação da identidade digital;
- V – concessão dos privilégios correspondentes;
- VI – revisão periódica dos acessos;
- VII – alteração de perfis quando houver mudança de função;
- VIII – suspensão temporária, quando aplicável;
- IX – revogação definitiva em caso de desligamento ou perda da necessidade de acesso.

Todo o processo deverá ser formalmente registrado e passível de auditoria.

7.6 Concessão de Acessos

A concessão de acessos deverá observar critérios objetivos, previamente definidos e compatíveis com as atribuições do usuário.

Nenhum acesso deverá ser concedido sem autorização formal da autoridade competente ou do gestor responsável pelo ativo de informação.

Os privilégios concedidos deverão limitar-se ao estritamente necessário para o desempenho das atividades institucionais.

Sempre que tecnicamente possível, deverão ser adotados mecanismos automatizados para gestão, aprovação, revisão e revogação dos acessos.

7.7 Revisão de Acessos

Os acessos concedidos deverão ser revisados periodicamente, de forma planejada e documentada, com o objetivo de verificar sua necessidade, adequação e conformidade.

As revisões deverão considerar, entre outros aspectos:

- I – mudanças de função;
- II – movimentações internas;
- III – afastamentos prolongados;
- IV – desligamentos;
- V – alterações organizacionais;
- VI – riscos identificados;
- VII – resultados de auditorias;
- VIII – incidentes de segurança.

Os gestores das unidades administrativas são corresponsáveis pela validação periódica dos acessos dos usuários sob sua responsabilidade.

7.8 Contas Privilegiadas

Os acessos administrativos ou privilegiados deverão receber tratamento diferenciado em razão do elevado potencial de impacto sobre os ativos de informação.

A utilização desses privilégios deverá observar controles adicionais, incluindo, sempre que possível:

- autorização específica;
- justificativa de uso;
- limitação das permissões;
- monitoramento contínuo;
- registro detalhado das atividades realizadas;
- revisão periódica;
- segregação entre contas administrativas e contas de uso cotidiano.

O uso de privilégios elevados deverá ocorrer apenas quando estritamente necessário à execução das atividades institucionais.

7.9 Autenticação

Os mecanismos de autenticação adotados pela Prefeitura deverão proporcionar nível de segurança compatível com a criticidade dos serviços acessados.

Sempre que tecnicamente viável e proporcional aos riscos, poderão ser utilizados mecanismos adicionais de autenticação, tais como autenticação multifator, certificados digitais ou outros métodos reconhecidos.

Os requisitos específicos relacionados à criação, utilização e proteção das credenciais encontram-se disciplinados na **Norma de Gestão de Identidades, Acessos e Senhas**.

7.10 Gestão de Credenciais

As credenciais de autenticação constituem responsabilidade exclusiva do usuário ao qual foram atribuídas.

É vedado:

- I – compartilhar credenciais;
- II – utilizar credenciais de terceiros;
- III – divulgar senhas ou outros fatores de autenticação;
- IV – armazenar credenciais de forma insegura;
- V – utilizar mecanismos destinados a contornar os controles de autenticação implementados.

Os usuários deverão comunicar imediatamente qualquer suspeita de comprometimento de suas credenciais.

7.11 Segregação de Funções

A Prefeitura adotará mecanismos de segregação de funções visando reduzir riscos decorrentes da concentração excessiva de privilégios.

Sempre que possível, atividades relacionadas à autorização, execução, administração, monitoramento e auditoria deverão ser atribuídas a pessoas distintas.

Quando a segregação completa não puder ser implementada, deverão ser estabelecidos controles compensatórios proporcionais ao risco.

7.12 Registro e Monitoramento

Os acessos aos ativos de informação deverão gerar registros que permitam:

- I – identificar o usuário responsável;
- II – identificar data e horário das operações;
- III – identificar os recursos acessados;
- IV – identificar eventos relevantes para investigação de incidentes;
- V – subsidiar auditorias e processos de responsabilização.

Os registros deverão ser protegidos contra alterações não autorizadas e preservados conforme os requisitos legais e institucionais.

7.13 Acesso por Terceiros

O acesso concedido a empresas contratadas, consultores, fornecedores ou outros terceiros deverá observar os mesmos princípios aplicáveis aos usuários internos.

Os contratos que envolvam acesso às informações institucionais deverão prever:

- responsabilidades das partes;
- confidencialidade;
- proteção de dados pessoais;
- comunicação de incidentes;
- devolução dos acessos ao término do contrato;
- possibilidade de auditoria pela Administração Municipal.

O acesso de terceiros deverá ser limitado ao período estritamente necessário para execução das atividades contratadas.

7.14 Acesso Remoto

O acesso remoto aos recursos tecnológicos da Prefeitura deverá ser autorizado, controlado e monitorado.

Sempre que aplicável, deverão ser utilizados mecanismos seguros de comunicação, autenticação e proteção das conexões.

As diretrizes específicas relacionadas ao trabalho remoto, dispositivos móveis e utilização de equipamentos particulares encontram-se disciplinadas na **Norma de Dispositivos Móveis, Trabalho Remoto e BYOD**.

7.15 Auditoria e Conformidade

A unidade responsável pela Tecnologia da Informação poderá realizar verificações periódicas para avaliar a conformidade da gestão de identidades e acessos.

As auditorias poderão abranger:

- concessão de acessos;
- contas privilegiadas;
- contas inativas;
- registros de autenticação;
- revisões periódicas;
- conformidade com esta Política e com as normas complementares.

Os resultados das auditorias deverão subsidiar ações de melhoria contínua.

O uso de Autenticação Multifator (MFA) é obrigatório para acessos remotos, contas privilegiadas e sistemas críticos, conforme detalhado na Norma de Gestão de Identidades, Acessos e Senhas.

7.16 Documentos Complementares

- Norma de Gestão de Identidades, Acessos e Senhas;
- Norma de Dispositivos Móveis, Trabalho Remoto e BYOD;
- Norma de Gestão de Logs, Monitoramento e Registros.

7.17 Disposições Gerais

A gestão adequada das identidades digitais e dos controles de acesso é condição essencial para a proteção dos ativos de informação da Prefeitura Municipal de Aracruz, devendo ser tratada como processo contínuo de governança.

Todos os usuários são responsáveis pela utilização adequada de suas credenciais e pelo cumprimento das normas institucionais relacionadas ao acesso aos recursos tecnológicos.

As diretrizes estabelecidas neste capítulo deverão ser observadas por todas as unidades administrativas, independentemente da tecnologia utilizada, contribuindo para a redução dos riscos, a proteção das informações institucionais e a continuidade dos serviços públicos.

CAPÍTULO 8

SEGURANÇA FÍSICA, AMBIENTAL E PROTEÇÃO DA INFRAESTRUTURA

8.1 Objetivo

Este capítulo estabelece as diretrizes para proteção física dos ativos de informação, das instalações, dos ambientes tecnológicos, dos equipamentos, das infraestruturas críticas e dos recursos utilizados pela Prefeitura Municipal de Aracruz, visando reduzir riscos decorrentes de acessos não autorizados, danos físicos, falhas ambientais, acidentes, desastres naturais, furtos, vandalismo, sabotagem e demais eventos capazes de comprometer a continuidade dos serviços públicos.

A proteção física constitui componente essencial da Segurança da Informação, devendo integrar as ações de gestão de riscos, continuidade dos serviços, proteção de dados pessoais e preservação do patrimônio público.

8.2 Abrangência

As diretrizes deste capítulo aplicam-se a todas as instalações utilizadas pela Prefeitura Municipal de Aracruz, incluindo:

- I – prédio da Administração Central;
- II – Secretarias Municipais;
- III – escolas municipais;
- IV – unidades de saúde;
- V – centros administrativos;
- VI – unidades descentralizadas;
- VII – almoxarifados;
- VIII – arquivos físicos;
- IX – centros de processamento de dados (CPDs);
- X – salas de equipamentos;

- XI – salas de telecomunicações;
- XII – datacenters próprios ou contratados;
- XIII – ambientes em nuvem, quando houver infraestrutura física sob responsabilidade contratual;
- XIV – quaisquer locais que armazenem informações institucionais ou ativos tecnológicos.

8.3 Princípios da Segurança Física

A proteção física observará os seguintes princípios:

- I – prevenção;
- II – proporcionalidade aos riscos;
- III – continuidade dos serviços públicos;
- IV – proteção do patrimônio público;
- V – disponibilidade dos ativos críticos;
- VI – controle de acesso;
- VII – monitoramento permanente;
- VIII – rastreabilidade dos acessos;
- IX – melhoria contínua.

8.4 Áreas Seguras

A Prefeitura deverá identificar e classificar as áreas que exijam níveis diferenciados de proteção física.

Poderão ser consideradas áreas seguras, entre outras:

- datacenters;
- CPDs;
- salas de servidores;
- salas de telecomunicações;
- centrais de monitoramento;
- salas de backup;
- arquivos permanentes;
- salas de equipamentos de segurança;

- ambientes que armazenem informações classificadas ou dados pessoais em grande volume.

As áreas seguras deverão possuir controles físicos compatíveis com sua criticidade.

8.5 Controle de Acesso Físico

O acesso às áreas protegidas deverá ser restrito às pessoas autorizadas.

A Administração Municipal adotará mecanismos para controlar, registrar e, quando aplicável, monitorar os acessos físicos às áreas críticas.

Os mecanismos poderão incluir:

- identificação funcional;
- controle eletrônico de acesso;
- registro de visitantes;
- acompanhamento de visitantes por responsável designado;
- utilização de chaves, cartões ou credenciais;
- monitoramento por sistemas eletrônicos.

Os registros de acesso deverão ser mantidos pelo período definido nas normas internas e na legislação aplicável.

8.6 Visitantes e Prestadores de Serviço

O ingresso de visitantes, empresas contratadas e prestadores de serviço em áreas críticas deverá observar procedimentos previamente estabelecidos.

Sempre que aplicável, deverão ser adotadas as seguintes medidas:

- I – identificação do visitante;
- II – registro da entrada e saída;
- III – identificação do responsável pelo acompanhamento;
- IV – limitação do acesso às áreas estritamente necessárias;
- V – acompanhamento durante a permanência nas áreas críticas;
- VI – comunicação prévia à unidade responsável.

Os contratos de prestação de serviços deverão prever requisitos mínimos de segurança física compatíveis com os riscos envolvidos.

8.7 Proteção dos Equipamentos

Os equipamentos utilizados pela Prefeitura deverão ser protegidos contra riscos físicos que possam comprometer sua disponibilidade, integridade ou funcionamento.

Sempre que possível, deverão ser adotadas medidas relativas a:

- posicionamento adequado dos equipamentos;
- proteção contra impactos físicos;
- proteção contra poeira, umidade e calor excessivo;
- organização do cabeamento;
- controle de acesso aos equipamentos;
- manutenção preventiva;
- monitoramento das condições ambientais.

Os equipamentos críticos deverão possuir plano de manutenção compatível com sua importância para a continuidade dos serviços públicos.

8.8 Infraestrutura de Energia

A infraestrutura tecnológica deverá possuir mecanismos destinados a minimizar interrupções decorrentes de falhas no fornecimento de energia elétrica.

Sempre que tecnicamente viável, poderão ser utilizados:

- nobreaks (UPS);
- bancos de baterias;
- geradores;
- proteção contra surtos elétricos;
- aterramento elétrico;
- sistemas redundantes para ativos críticos.

Os equipamentos de proteção deverão ser submetidos a inspeções e manutenções periódicas.

8.9 Climatização e Condições Ambientais

Os ambientes destinados ao funcionamento de equipamentos tecnológicos deverão manter condições ambientais adequadas à sua operação.

Deverão ser observados, quando aplicável:

- temperatura adequada;
- controle de umidade;
- circulação de ar;
- limpeza periódica;
- monitoramento ambiental;
- prevenção contra infiltrações;
- prevenção contra condensação.

As condições ambientais deverão ser compatíveis com as recomendações dos fabricantes dos equipamentos.

8.10 Proteção Contra Incêndios e Outros Desastres

Os ambientes críticos deverão possuir medidas de prevenção e resposta a incêndios e outros eventos que possam comprometer a continuidade dos serviços.

As medidas poderão compreender:

- sistemas de detecção;
- extintores apropriados;
- sinalização de emergência;
- rotas de fuga;
- treinamento das equipes;
- planos de emergência;
- integração com os órgãos competentes.

Sempre que necessário, deverão ser realizados testes e inspeções periódicas.

8.11 Proteção das Comunicações

As infraestruturas de comunicação deverão ser protegidas contra danos físicos, interferências, interrupções e acessos não autorizados.

Sempre que possível, deverão ser adotadas medidas destinadas à proteção de:

- cabeamento estruturado;
- fibras ópticas;
- equipamentos de telecomunicações;
- enlaces de comunicação;

- racks;
- painéis de distribuição.

As alterações na infraestrutura deverão observar os procedimentos estabelecidos na **Norma de Gestão de Mudanças**.

8.12 Proteção dos Arquivos Físicos

Os documentos físicos sob responsabilidade da Prefeitura deverão ser armazenados em ambientes compatíveis com sua natureza, criticidade e requisitos legais.

Os controles poderão incluir:

- restrição de acesso;
- proteção contra incêndio;
- controle ambiental;
- organização documental;
- identificação dos responsáveis;
- controle de empréstimos;
- preservação histórica;
- observância das tabelas de temporalidade documental.

As informações classificadas ou protegidas por legislação específica deverão receber proteção adicional.

8.13 Transporte de Equipamentos e Informações

O transporte de equipamentos, mídias e documentos institucionais deverá observar medidas destinadas à preservação da confidencialidade, integridade e disponibilidade das informações.

Sempre que necessário, deverão ser adotados controles para:

- identificação do material transportado;
- registro da movimentação;
- definição de responsáveis;
- proteção física durante o transporte;
- rastreabilidade da entrega.

8.14 Gestão de Incidentes Físicos

Todo incidente que comprometa ou possa comprometer a segurança física dos ativos deverá ser comunicado imediatamente à autoridade competente.

Constituem exemplos de incidentes:

- invasões;
- furtos;
- vandalismo;
- incêndios;
- alagamentos;
- quedas prolongadas de energia;
- falhas de climatização;
- rompimento de fibras ópticas;
- danos estruturais;
- acesso físico não autorizado.

Os incidentes deverão ser tratados conforme o **Plano de Resposta a Incidentes de Segurança da Informação**.

8.15 Continuidade da Infraestrutura

A infraestrutura física deverá ser considerada nos processos de continuidade dos serviços públicos.

Sempre que possível, deverão ser avaliadas medidas relacionadas a:

- redundância de equipamentos críticos;
- redundância de comunicação;
- recuperação de ambientes;
- contingência operacional;
- recuperação de energia;
- recuperação das telecomunicações.

As estratégias específicas encontram-se disciplinadas no **Plano de Continuidade dos Serviços de Tecnologia da Informação**.

8.16 Auditoria e Inspeções

A Prefeitura poderá realizar inspeções periódicas destinadas a verificar a conformidade das instalações físicas com esta Política e com as normas complementares.

As inspeções poderão abranger:

- controle de acesso físico;
- organização dos ambientes;
- proteção dos equipamentos;
- funcionamento dos sistemas de segurança;
- condições ambientais;
- conformidade documental.

Os resultados deverão subsidiar ações de melhoria contínua.

Este capítulo é complementado pelos seguintes documentos:

- Plano de Continuidade dos Serviços de TIC;
- Plano de Recuperação de Desastres de TI (DRP);
- Norma de Dispositivos Móveis, Trabalho Remoto e BYOD.

8.18 Disposições Gerais

A proteção física e ambiental dos ativos de informação constitui requisito indispensável para a continuidade dos serviços públicos e para a preservação do patrimônio da Prefeitura Municipal de Aracruz.

Todas as unidades administrativas deverão adotar medidas compatíveis com os riscos existentes em seus ambientes, promovendo a proteção das pessoas, das instalações, dos equipamentos e das informações sob sua responsabilidade.

A segurança física deverá atuar de forma integrada aos demais componentes do Sistema de Gestão da Segurança da Informação, contribuindo para a redução dos riscos institucionais, para a conformidade legal e para o fortalecimento da confiança da sociedade na Administração Pública.

CAPÍTULO 9

SEGURANÇA DAS OPERAÇÕES E GESTÃO DA INFRAESTRUTURA TECNOLÓGICA

9.1 Objetivo

Este capítulo estabelece as diretrizes para a gestão segura das operações de Tecnologia da Informação e Comunicação (TIC) da Prefeitura Municipal de Aracruz, visando assegurar a continuidade dos serviços públicos, a proteção dos ativos de informação, a confiabilidade dos ambientes tecnológicos e a adequada administração da infraestrutura de TIC.

A gestão das operações deverá ser realizada de forma planejada, padronizada, documentada e monitorada, reduzindo os riscos operacionais e promovendo a disponibilidade, integridade, confidencialidade, autenticidade e rastreabilidade das informações institucionais.

9.2 Abrangência

As disposições deste capítulo aplicam-se a todos os recursos tecnológicos administrados ou utilizados pela Prefeitura Municipal de Aracruz, incluindo:

- I – infraestrutura de redes de comunicação;
- II – servidores físicos e virtuais;
- III – equipamentos de armazenamento;
- IV – estações de trabalho;
- V – dispositivos móveis corporativos;
- VI – sistemas corporativos;
- VII – aplicações desenvolvidas internamente ou adquiridas de terceiros;
- VIII – ambientes em nuvem;
- IX – bancos de dados;
- X – serviços de comunicação eletrônica;
- XI – ferramentas de monitoramento;
- XII – demais componentes da infraestrutura tecnológica institucional.

9.3 Princípios da Segurança das Operações

A gestão operacional da infraestrutura tecnológica observará os seguintes princípios:

- I – padronização dos processos operacionais;
- II – continuidade dos serviços públicos;
- III – disponibilidade dos ativos críticos;
- IV – prevenção de falhas operacionais;
- V – monitoramento contínuo;
- VI – gestão baseada em riscos;
- VII – rastreabilidade das operações relevantes;
- VIII – segregação de funções;
- IX – melhoria contínua dos processos operacionais.

9.4 Gestão das Operações

As atividades operacionais da infraestrutura tecnológica deverão ser executadas conforme procedimentos previamente estabelecidos, documentados e aprovados pela unidade responsável pela Tecnologia da Informação.

Os procedimentos operacionais deverão contemplar, sempre que aplicável:

- I – rotinas de operação dos ambientes tecnológicos;
- II – monitoramento dos serviços;
- III – administração da capacidade;
- IV – manutenção preventiva;
- V – tratamento de falhas;
- VI – atualização de componentes tecnológicos;
- VII – gerenciamento de recursos computacionais;
- VIII – gestão da disponibilidade dos serviços.

Sempre que possível, as atividades operacionais deverão ser automatizadas, reduzindo a possibilidade de erros humanos e aumentando a confiabilidade dos processos.

9.5 Gestão da Capacidade e Desempenho

A infraestrutura tecnológica deverá ser continuamente monitorada para assegurar que sua capacidade seja compatível com a demanda dos serviços prestados pela Administração Municipal.

A gestão da capacidade deverá considerar:

- I – utilização dos recursos computacionais;
- II – crescimento da demanda;
- III – evolução tecnológica;
- IV – disponibilidade dos serviços críticos;
- V – planejamento de expansão da infraestrutura.

Os resultados do monitoramento deverão subsidiar o planejamento de investimentos e a atualização da infraestrutura tecnológica.

9.6 Gestão de Vulnerabilidades

A Prefeitura deverá adotar processo contínuo para identificação, avaliação, tratamento e monitoramento das vulnerabilidades existentes em seus ambientes tecnológicos.

Sempre que aplicável, deverão ser realizadas atividades destinadas a:

- I – identificação de vulnerabilidades;
- II – análise de criticidade;
- III – definição de prioridades para correção;
- IV – implementação de medidas mitigadoras;
- V – acompanhamento da efetividade das ações adotadas.

As vulnerabilidades identificadas deverão ser tratadas de forma proporcional aos riscos envolvidos.

A gestão de vulnerabilidades, incluindo classificação CVSS, SLA de correção por severidade, varreduras periódicas e hardening, é detalhada no Documento Complementar nº 12 — Norma de Gestão de Vulnerabilidades, Atualizações e Correções.

9.7 Atualizações e Correções de Segurança

Os sistemas, equipamentos, aplicações e demais componentes tecnológicos deverão ser mantidos atualizados, observando critérios técnicos, operacionais e de continuidade dos serviços.

As atualizações deverão considerar:

- I – correções de segurança;
- II – atualizações de fabricantes;
- III – riscos associados às vulnerabilidades conhecidas;
- IV – impacto sobre os serviços institucionais;
- V – necessidade de homologação prévia, quando aplicável.

Os procedimentos específicos para implementação de atualizações deverão observar a **Norma de Gestão de Mudanças**.

9.8 Proteção contra Códigos Maliciosos

A Prefeitura adotará medidas destinadas à prevenção, detecção, contenção e tratamento de códigos maliciosos que possam comprometer seus ativos de informação.

As medidas poderão incluir:

- I – utilização de soluções de proteção contra malware;
- II – monitoramento contínuo dos ambientes tecnológicos;
- III – atualização das ferramentas de proteção;
- IV – conscientização dos usuários;
- V – isolamento de equipamentos comprometidos;
- VI – tratamento dos incidentes identificados.

As ações relacionadas à resposta a incidentes observarão o Plano de Resposta a Incidentes de Segurança da Informação.

9.9 Registros de Eventos (Logs)

Os sistemas e componentes tecnológicos deverão gerar registros de eventos compatíveis com sua criticidade e finalidade.

Os registros deverão possibilitar, sempre que aplicável:

- I – identificação do usuário responsável;

- II – data e horário da ocorrência;
- III – identificação do recurso afetado;
- IV – descrição do evento;
- V – apoio à investigação de incidentes;
- VI – suporte às auditorias;
- VII – comprovação de conformidade.

Os registros deverão ser protegidos contra alterações não autorizadas e preservados conforme os requisitos legais e institucionais.

9.10 Monitoramento dos Ambientes Tecnológicos

A infraestrutura tecnológica deverá ser monitorada continuamente, visando identificar falhas, indisponibilidades, degradação de desempenho, eventos de segurança e outras situações capazes de comprometer os serviços públicos.

O monitoramento poderá abranger:

- I – disponibilidade dos serviços;
- II – utilização de recursos computacionais;
- III – desempenho da infraestrutura;
- IV – eventos de segurança;
- V – funcionamento dos sistemas críticos;
- VI – integridade dos serviços.

Os eventos identificados deverão ser analisados e tratados conforme sua criticidade.

9.11 Gestão de Mudanças

As alterações na infraestrutura tecnológica, nos sistemas de informação e nos serviços de TIC deverão ser planejadas, avaliadas, autorizadas, implementadas e documentadas.

A gestão de mudanças deverá buscar:

- I – minimizar riscos operacionais;
- II – preservar a continuidade dos serviços;
- III – reduzir impactos aos usuários;
- IV – assegurar rastreabilidade das alterações realizadas;

V – manter histórico das mudanças implementadas.

Os procedimentos detalhados encontram-se estabelecidos na **Norma de Gestão de Mudanças**.

9.12 Cópias de Segurança

A Prefeitura deverá manter processo institucional para realização de cópias de segurança das informações e dos sistemas considerados necessários à continuidade das atividades administrativas.

As cópias de segurança deverão observar critérios de:

- I – periodicidade;
- II – integridade;
- III – disponibilidade;
- IV – proteção contra acessos não autorizados;
- V – armazenamento adequado;
- VI – testes periódicos de recuperação.

As diretrizes específicas encontram-se estabelecidas na **Norma de Cópias de Segurança e Recuperação de Dados**.

A estratégia de backup deve seguir o padrão 3-2-1 (3 cópias, 2 mídias diferentes, 1 fora do local), com pelo menos uma cópia imutável ou em air-gap para sistemas críticos. Os detalhes operacionais estão no Documento Complementar nº 08 — Norma de Cópias de Segurança, Restauração e Recuperação de Dados.

9.13 Sincronização de Tempo

Os sistemas e equipamentos que suportam processos institucionais relevantes deverão utilizar mecanismos adequados de sincronização de tempo, visando assegurar a consistência dos registros de eventos, das auditorias e das evidências digitais.

A sincronização deverá observar padrões técnicos compatíveis com a infraestrutura tecnológica adotada pela Prefeitura.

9.14 Gestão da Disponibilidade

A infraestrutura tecnológica deverá ser administrada de forma a assegurar níveis adequados de disponibilidade dos serviços públicos digitais.

Sempre que aplicável, deverão ser adotadas medidas destinadas a:

- I – reduzir pontos únicos de falha;
- II – aumentar a resiliência da infraestrutura;
- III – monitorar indisponibilidades;
- IV – estabelecer mecanismos de contingência;
- V – apoiar os planos de continuidade.

9.15 Serviços Prestados por Terceiros

Os serviços de TIC executados por terceiros deverão observar requisitos de segurança compatíveis com os riscos envolvidos.

Os contratos deverão prever, sempre que aplicável:

- I – requisitos mínimos de segurança;
- II – níveis de serviço;
- III – comunicação de incidentes;
- IV – proteção das informações institucionais;
- V – confidencialidade;
- VI – possibilidade de auditoria pela Administração Municipal.

9.16 Auditoria das Operações

A Prefeitura poderá realizar auditorias técnicas destinadas a verificar a conformidade das operações de TIC com esta Política, com as normas complementares e com a legislação vigente.

As auditorias poderão abranger:

- processos operacionais;
- registros de eventos;
- controles implementados;
- gestão de vulnerabilidades;
- gestão de mudanças;
- gestão de cópias de segurança;

- monitoramento dos ambientes tecnológicos.

Os resultados deverão subsidiar ações corretivas e de melhoria contínua.

9.17 Documentos Complementares

- Norma de Cópias de Segurança, Restauração e Recuperação de Dados;
- Norma de Gestão de Vulnerabilidades, Atualizações e Correções;
- Norma de Gestão de Logs, Monitoramento e Registros;
- Procedimento de Gestão de Mudanças em TI.

9.18 Disposições Gerais

A gestão segura das operações e da infraestrutura tecnológica constitui requisito essencial para assegurar a continuidade dos serviços públicos, a proteção das informações institucionais e a confiança dos cidadãos na Administração Municipal.

As atividades operacionais deverão ser conduzidas de forma integrada aos processos de gestão de riscos, continuidade dos serviços, proteção de dados pessoais, resposta a incidentes e governança de tecnologia da informação, observando as competências estabelecidas nesta Política e nos demais documentos que compõem o Sistema de Gestão da Segurança da Informação da Prefeitura Municipal de Aracruz.

CAPÍTULO 10

SEGURANÇA DAS COMUNICAÇÕES E TRANSFERÊNCIA DE INFORMAÇÕES

10.1 Objetivo

Este capítulo estabelece as diretrizes para a proteção das comunicações, das redes de dados e da transferência de informações no âmbito da Prefeitura Municipal de Aracruz, visando assegurar que o intercâmbio de informações institucionais ocorra de forma segura, íntegra, confiável, rastreável e em conformidade com a legislação vigente.

As comunicações institucionais deverão ser protegidas contra acessos não autorizados, interceptação, alteração indevida, perda de informações,

indisponibilidade dos serviços e demais ameaças que possam comprometer a prestação dos serviços públicos ou os direitos dos cidadãos.

10.2 Abrangência

As disposições deste capítulo aplicam-se a todas as formas de comunicação utilizadas pela Prefeitura Municipal de Aracruz, incluindo:

- I – redes locais (LAN);
- II – redes sem fio(Wi-Fi);
- III – redes metropolitanas e de longa distância;
- IV – conexões com a Internet;
- V – redes privadas virtuais (VPN);
- VI – serviços de correio eletrônico institucional;
- VII – sistemas corporativos;
- VIII – aplicações web;
- IX – plataformas em nuvem;
- X – serviços de mensagens institucionais;
- XI – integrações entre sistemas;
- XII – compartilhamento eletrônico de arquivos;
- XIII – troca de informações com outros órgãos públicos;
- XIV – comunicação com fornecedores e parceiros;
- XV – quaisquer outros meios utilizados para transmissão de informações institucionais.

10.3 Princípios

As comunicações institucionais deverão observar os seguintes princípios:

- I – confidencialidade;
- II – integridade;
- III – disponibilidade;
- IV – autenticidade;
- V – rastreabilidade;
- VI – necessidade de conhecimento;
- VII – proporcionalidade aos riscos;

VIII – conformidade legal;

IX – continuidade dos serviços públicos.

10.4 Proteção das Redes de Comunicação

A infraestrutura de redes deverá ser administrada de forma a garantir níveis adequados de segurança compatíveis com os riscos existentes.

A Prefeitura deverá adotar medidas destinadas a proteger suas redes contra:

I – acessos não autorizados;

II – interceptação de comunicações;

III – alterações indevidas;

IV – ataques cibernéticos;

V – indisponibilidade dos serviços;

VI – utilização inadequada dos recursos de rede.

A arquitetura da infraestrutura deverá considerar critérios de segmentação, monitoramento, disponibilidade e proteção dos ativos críticos.

10.5 Gestão das Comunicações Institucionais

As comunicações institucionais deverão ocorrer exclusivamente por meios autorizados pela Administração Municipal, observando os requisitos de segurança estabelecidos nesta Política e nas normas complementares.

Os usuários deverão utilizar os canais oficiais para o tratamento de assuntos relacionados às atividades da Prefeitura, preservando a confidencialidade das informações e evitando o uso de meios não autorizados para transmissão de dados institucionais.

10.6 Correio Eletrônico Institucional

O correio eletrônico institucional constitui ferramenta oficial de comunicação da Prefeitura Municipal de Aracruz.

Sua utilização deverá observar os princípios de legalidade, impessoalidade, moralidade, publicidade, eficiência e segurança da informação.

As mensagens eletrônicas deverão ser utilizadas exclusivamente para finalidades institucionais, ressalvadas as utilizações eventuais permitidas pela **Norma de Uso Aceitável dos Recursos de Tecnologia da Informação e Comunicação**.

A utilização do correio eletrônico não deverá comprometer a segurança da infraestrutura tecnológica, a imagem institucional da Prefeitura ou o cumprimento da legislação vigente.

10.7 Compartilhamento de Informações

O compartilhamento de informações deverá ocorrer apenas quando houver finalidade institucional legítima e autorização compatível com as competências legais dos envolvidos.

O compartilhamento deverá observar:

- I – classificação da informação;
- II – necessidade de conhecimento;
- III – proteção dos dados pessoais;
- IV – legislação sobre acesso à informação;
- V – requisitos contratuais, quando aplicáveis;
- VI – princípios da minimização e adequação.

Sempre que envolver dados pessoais, deverão ser observadas também as disposições da Política Municipal de Proteção de Dados Pessoais.

10.8 Compartilhamento com Outros Órgãos e Entidades

O intercâmbio de informações com órgãos públicos, entidades privadas, instituições parceiras ou demais organizações deverá ocorrer mediante instrumentos jurídicos ou administrativos adequados, observando:

- I – competência legal;
- II – finalidade específica;
- III – proteção das informações compartilhadas;
- IV – observância da LGPD, quando envolver dados pessoais;
- V – preservação do interesse público.

Sempre que necessário, deverão ser estabelecidos requisitos de segurança compatíveis com os riscos da informação compartilhada.

10.9 Serviços em Nuvem

A utilização de serviços em nuvem deverá observar critérios técnicos, jurídicos e administrativos destinados à proteção das informações institucionais.

A contratação ou utilização desses serviços deverá considerar, entre outros aspectos:

- I – requisitos de segurança da informação;
- II – proteção de dados pessoais;
- III – disponibilidade dos serviços;
- IV – continuidade operacional;
- V – localização dos dados, quando aplicável;
- VI – responsabilidades contratuais;
- VII – mecanismos de auditoria.

A adoção de soluções em nuvem deverá ser precedida de avaliação de riscos proporcional à criticidade dos serviços envolvidos.

A contratação e gestão de serviços em nuvem deve observar o modelo de responsabilidade compartilhada, exigir MFA, criptografia em repouso e trânsito, plano de saída e cláusulas de LGPD. Os detalhes estão no Documento Complementar nº 14 — Norma de Segurança e Governança de Serviços em Nuvem.

10.10 Criptografia

Sempre que a natureza da informação ou a avaliação de riscos indicar necessidade, deverão ser utilizados mecanismos criptográficos destinados à proteção das informações durante o armazenamento, processamento e transmissão.

Os critérios técnicos para utilização da criptografia encontram-se estabelecidos na **Norma de Controles Criptográficos**.

10.11 Transferência Eletrônica de Informações

A transferência eletrônica de informações deverá ocorrer mediante mecanismos que assegurem:

- I – identificação das partes envolvidas;
- II – integridade das informações transmitidas;

III – confidencialidade, quando necessária;

IV – rastreabilidade das operações;

V – proteção contra alterações indevidas.

Sempre que aplicável, deverão ser utilizados mecanismos de autenticação, validação da origem e proteção da comunicação.

10.12 Utilização de Serviços de Mensagens

A utilização de serviços de mensagens instantâneas para fins institucionais deverá observar as diretrizes estabelecidas pela Administração Municipal.

Informações classificadas, estratégicas, sigilosas ou que contenham dados pessoais não deverão ser compartilhadas por canais não autorizados.

Os gestores deverão orientar suas equipes quanto à utilização segura dessas ferramentas.

10.13 Trabalho Remoto

As comunicações realizadas em regime de trabalho remoto deverão observar os mesmos requisitos de segurança aplicáveis às atividades presenciais.

Os usuários deverão utilizar exclusivamente os meios autorizados pela Prefeitura para acesso aos recursos tecnológicos institucionais.

As diretrizes específicas encontram-se estabelecidas na **Norma de Dispositivos Móveis, Trabalho Remoto e BYOD**.

10.14 Monitoramento das Comunicações

A Administração Municipal poderá monitorar a utilização dos recursos de comunicação institucionais, observados:

I – a legislação vigente;

II – os princípios da proporcionalidade;

III – a finalidade institucional;

IV – a proteção dos direitos fundamentais;

V – a transparência dos controles adotados.

O monitoramento destina-se exclusivamente à proteção dos ativos institucionais, à continuidade dos serviços públicos, à prevenção de incidentes e ao atendimento das obrigações legais.

10.15 Incidentes nas Comunicações

Qualquer evento que comprometa ou possa comprometer a segurança das comunicações institucionais deverá ser comunicado imediatamente à unidade responsável pela Tecnologia da Informação.

Constituem exemplos de incidentes:

- interceptação de comunicações;
- indisponibilidade de redes;
- comprometimento do correio eletrônico;
- vazamento de informações;
- compartilhamento indevido de dados;
- utilização de canais não autorizados;
- comprometimento de serviços em nuvem;
- falhas em integrações entre sistemas.

Os incidentes deverão ser tratados conforme o Plano de Resposta a Incidentes de Segurança da Informação.

10.16 Auditoria e Conformidade

A Prefeitura poderá realizar auditorias destinadas a verificar a conformidade das comunicações institucionais com esta Política e com os demais documentos do Sistema de Gestão da Segurança da Informação.

As auditorias poderão abranger:

- utilização das redes;
- utilização do correio eletrônico;
- compartilhamento de informações;
- utilização dos serviços em nuvem;
- integrações entre sistemas;
- utilização de mecanismos criptográficos;
- conformidade contratual.

Os resultados das auditorias deverão subsidiar ações corretivas e de melhoria contínua.

10.17 Documentos Complementares

- Norma de Segurança e Governança de Serviços em Nuvem;
- Norma de Dispositivos Móveis, Trabalho Remoto e BYOD;
- Norma de Gestão de Logs, Monitoramento e Registros.

10.18 Disposições Gerais

A segurança das comunicações constitui elemento essencial para a proteção das informações institucionais e para a continuidade da prestação dos serviços públicos.

Todas as unidades administrativas da Prefeitura Municipal de Aracruz deverão utilizar os recursos de comunicação de forma segura, responsável e compatível com os objetivos institucionais, observando esta Política, as normas complementares e a legislação aplicável.

As medidas de proteção das comunicações deverão ser continuamente avaliadas e aperfeiçoadas, considerando a evolução tecnológica, as mudanças organizacionais, os riscos identificados e as necessidades da Administração Municipal.

CAPÍTULO 11

DESENVOLVIMENTO, AQUISIÇÃO, MANUTENÇÃO E GESTÃO SEGURA DE SISTEMAS DE INFORMAÇÃO

11.1 Objetivo

Este capítulo estabelece as diretrizes para assegurar que os sistemas de informação utilizados pela Prefeitura Municipal de Aracruz sejam planejados, adquiridos, desenvolvidos, implantados, mantidos, integrados, atualizados e descontinuados de forma segura, preservando a confidencialidade, integridade, disponibilidade, autenticidade e rastreabilidade das informações institucionais durante todo o seu ciclo de vida.

A segurança deverá ser considerada desde a concepção dos sistemas até sua desativação, integrando-se aos processos de governança de Tecnologia da Informação, gestão de riscos, proteção de dados pessoais e continuidade dos serviços públicos.

11.2 Abrangência

As disposições deste capítulo aplicam-se a:

- I – sistemas desenvolvidos internamente;
- II – sistemas adquiridos de terceiros;
- III – softwares como serviço (SaaS);
- IV – plataformas em nuvem;
- V – aplicativos móveis;
- VI – sistemas legados;
- VII – sistemas embarcados em equipamentos utilizados pela Prefeitura;
- VIII – integrações entre sistemas;
- IX – bancos de dados;
- X – interfaces de programação de aplicações (APIs);
- XI – soluções de inteligência artificial utilizadas pela Administração Municipal;
- XII – quaisquer outros sistemas responsáveis pelo tratamento de informações institucionais.

11.3 Princípios

O desenvolvimento e a gestão dos sistemas de informação observarão os seguintes princípios:

- I – segurança desde a concepção (*Security by Design*);
- II – proteção da privacidade desde a concepção (*Privacy by Design*);
- III – gestão baseada em riscos;
- IV – conformidade legal;
- V – continuidade dos serviços públicos;
- VI – interoperabilidade;
- VII – rastreabilidade das alterações;
- VIII – qualidade do software;

IX – melhoria contínua.

11.4 Segurança no Ciclo de Vida dos Sistemas

A segurança da informação deverá ser incorporada em todas as fases do ciclo de vida dos sistemas, compreendendo, no mínimo:

- I – planejamento;
- II – levantamento de requisitos;
- III – análise de riscos;
- IV – especificação técnica;
- V – desenvolvimento;
- VI – testes;
- VII – homologação;
- VIII – implantação;
- IX – operação;
- X – manutenção;
- XI – atualização;
- XII – descontinuação.

Cada etapa deverá contemplar controles proporcionais aos riscos identificados e à criticidade do sistema.

11.5 Requisitos de Segurança

Os requisitos de segurança deverão ser identificados e considerados desde o início dos projetos de desenvolvimento, aquisição ou evolução de sistemas.

Sempre que aplicável, deverão ser considerados requisitos relacionados à:

- I – autenticação;
- II – autorização;
- III – controle de acesso;
- IV – proteção contra alterações não autorizadas;
- V – registro de eventos;
- VI – disponibilidade;
- VII – continuidade dos serviços;
- VIII – proteção de dados pessoais;

- IX – requisitos legais;
- X – requisitos de auditoria.

11.6 Aquisição de Sistemas

A aquisição de soluções tecnológicas deverá observar critérios técnicos e requisitos mínimos de segurança compatíveis com os riscos associados ao tratamento das informações.

Os processos de contratação deverão considerar, entre outros aspectos:

- I – requisitos funcionais;
- II – requisitos de segurança;
- III – proteção de dados pessoais;
- IV – continuidade do serviço;
- V – suporte técnico;
- VI – atualização de segurança;
- VII – conformidade com a legislação vigente;
- VIII – possibilidade de auditoria.

Sempre que possível, os requisitos de segurança deverão integrar os documentos de planejamento da contratação e os instrumentos convocatórios.

11.7 Desenvolvimento Seguro

Os sistemas desenvolvidos pela Prefeitura ou por terceiros deverão observar práticas de desenvolvimento seguro compatíveis com a natureza do serviço prestado.

Sempre que aplicável, deverão ser adotadas medidas destinadas a:

- I – reduzir vulnerabilidades;
- II – prevenir falhas conhecidas;
- III – validar entradas de dados;
- IV – proteger informações sensíveis;
- V – controlar erros de processamento;
- VI – preservar registros de auditoria;
- VII – evitar exposição indevida de informações.

As práticas técnicas específicas serão disciplinadas em norma ou procedimento próprio.

O desenvolvimento deve seguir práticas de segurança incluindo revisão de código, OWASP Top 10, gestão de segredos (secrets management), privacy by design e segregação de ambientes (desenvolvimento, homologação e produção). É proibido usar dados reais em ambiente de teste. Os detalhes estão no Documento Complementar nº 23 — Norma de Desenvolvimento, Aquisição e Gestão Segura de Sistemas.

11.8 Ambientes de Desenvolvimento, Testes e Produção

Os ambientes utilizados para desenvolvimento, testes, homologação e produção deverão possuir segregação compatível com os riscos envolvidos.

Sempre que possível:

- I – ambientes distintos deverão ser utilizados para cada finalidade;
- II – alterações deverão ser previamente homologadas;
- III – dados de produção não deverão ser utilizados em ambientes de teste sem tratamento adequado e autorização formal;
- IV – o acesso aos ambientes deverá observar o princípio do menor privilégio.

11.9 Gestão das Mudanças em Sistemas

As alterações realizadas em sistemas de informação deverão observar processo formal de gestão de mudanças.

As mudanças deverão ser:

- I – registradas;
- II – avaliadas quanto aos riscos;
- III – autorizadas;
- IV – testadas;
- V – documentadas;
- VI – monitoradas após sua implementação.

As diretrizes específicas encontram-se estabelecidas na **Norma de Gestão de Mudanças**.

11.10 Testes de Segurança

Sempre que compatível com a criticidade do sistema, deverão ser realizados testes destinados a verificar a efetividade dos controles de segurança implementados.

Os testes poderão compreender:

- testes funcionais relacionados à segurança;
- testes de vulnerabilidades;
- avaliações de configuração;
- verificações de conformidade;
- testes de recuperação.

Os resultados deverão subsidiar ações corretivas antes da entrada do sistema em produção.

11.11 Proteção dos Dados

Os sistemas deverão ser projetados para assegurar tratamento adequado das informações institucionais e dos dados pessoais.

Sempre que aplicável, deverão ser observados:

- I – minimização de dados;
- II – controle de acesso;
- III – rastreabilidade das operações;
- IV – proteção durante armazenamento e transmissão;
- V – retenção adequada;
- VI – descarte seguro;
- VII – conformidade com a Política Municipal de Proteção de Dados Pessoais.

11.12 Integrações entre Sistemas

As integrações entre sistemas internos ou externos deverão observar critérios de segurança compatíveis com os riscos envolvidos.

Antes da implementação de integrações, deverão ser avaliados:

- I – requisitos de autenticação;
- II – autorização;
- III – integridade das informações;
- IV – disponibilidade dos serviços;

- V – responsabilidades das partes;
- VI – mecanismos de monitoramento.

11.13 Gestão de Vulnerabilidades em Sistemas

As vulnerabilidades identificadas nos sistemas deverão ser registradas, avaliadas e tratadas de acordo com sua criticidade.

Sempre que possível, deverão ser estabelecidos prazos proporcionais ao risco para implementação das correções necessárias.

As vulnerabilidades que possam comprometer significativamente os serviços públicos deverão receber tratamento prioritário.

11.14 Descontinuação de Sistemas

A desativação de sistemas deverá ocorrer de forma planejada e documentada.

O processo deverá considerar:

- I – preservação das informações;
- II – migração dos dados;
- III – continuidade dos serviços;
- IV – revogação de acessos;
- V – descarte seguro das informações remanescentes;
- VI – atualização dos inventários institucionais.

11.15 Contratações de Desenvolvimento e Manutenção

Os contratos que envolvam desenvolvimento, manutenção ou sustentação de sistemas deverão prever requisitos mínimos relacionados à segurança da informação e à proteção de dados pessoais.

Sempre que aplicável, deverão constar cláusulas relativas a:

- confidencialidade;
- propriedade intelectual;
- proteção de dados pessoais;
- comunicação de incidentes;
- atualização de vulnerabilidades;
- auditoria contratual;

- responsabilidade das partes.

11.16 Auditoria e Conformidade

A Prefeitura poderá realizar auditorias destinadas a verificar a conformidade dos sistemas com esta Política, com as normas complementares e com a legislação aplicável.

As auditorias poderão abranger:

- requisitos de segurança;
- registros de auditoria;
- controles implementados;
- proteção de dados pessoais;
- gestão de mudanças;
- gestão de vulnerabilidades;
- conformidade contratual.

Os resultados deverão subsidiar ações corretivas e de melhoria contínua.

11.17 Documentos Complementares

- Norma de Desenvolvimento, Aquisição e Gestão Segura de Sistemas;
- Norma de Segurança em Contratos e Terceirizações;
- Procedimento de Gestão de Mudanças em TI;
- Norma de Gestão de Vulnerabilidades, Atualizações e Correções.

11.18 Disposições Gerais

A segurança dos sistemas de informação constitui requisito indispensável para a prestação eficiente dos serviços públicos, para a proteção do patrimônio informacional da Prefeitura Municipal de Aracruz e para o cumprimento das obrigações legais relativas à segurança da informação e à proteção de dados pessoais.

Todos os projetos de desenvolvimento, aquisição, manutenção ou evolução de sistemas deverão incorporar requisitos de segurança desde sua concepção, promovendo uma abordagem preventiva, baseada em riscos e alinhada às necessidades institucionais da Administração Municipal.

CAPÍTULO 12

GESTÃO DE FORNECEDORES, SERVIÇOS TERCEIRIZADOS E RELAÇÕES CONTRATUAIS

12.1 Objetivo

Este capítulo estabelece as diretrizes para a gestão de fornecedores, prestadores de serviços, parceiros institucionais e demais terceiros que possuam acesso às informações, aos ativos de informação, aos sistemas, às redes ou à infraestrutura tecnológica da Prefeitura Municipal de Aracruz.

Seu objetivo é assegurar que as relações contratuais envolvendo Tecnologia da Informação e Comunicação (TIC), tratamento de informações institucionais ou dados pessoais sejam conduzidas de forma segura, transparente, documentada e em conformidade com a legislação vigente, preservando os princípios da segurança da informação, da continuidade dos serviços públicos e da proteção dos dados pessoais.

12.2 Abrangência

As disposições deste capítulo aplicam-se a:

- I – empresas contratadas;
- II – fornecedores de bens e serviços;
- III – empresas de outsourcing;
- IV – empresas de suporte técnico;
- V – prestadores de serviços especializados;
- VI – fornecedores de soluções em nuvem;
- VII – desenvolvedores de software;
- VIII – empresas de telecomunicações;
- IX – empresas responsáveis por manutenção de infraestrutura tecnológica;
- X – consultorias;
- XI – instituições parceiras;
- XII – quaisquer pessoas físicas ou jurídicas que tenham acesso, direto ou indireto, às informações ou aos recursos tecnológicos da Prefeitura Municipal de Aracruz.

12.3 Princípios

A gestão de fornecedores observará os seguintes princípios:

- I – legalidade;
- II – impessoalidade;
- III – transparência;
- IV – responsabilidade compartilhada;
- V – gestão baseada em riscos;
- VI – proteção das informações institucionais;
- VII – proteção de dados pessoais;
- VIII – continuidade dos serviços públicos;
- IX – melhoria contínua.

12.4 Avaliação de Riscos

Antes da contratação de fornecedores que possam acessar ativos de informação ou prestar serviços relacionados à Tecnologia da Informação e Comunicação, deverá ser realizada avaliação dos riscos envolvidos.

A avaliação deverá considerar, sempre que aplicável:

- I – natureza das informações tratadas;
- II – criticidade dos serviços;
- III – acesso a dados pessoais;
- IV – impacto potencial sobre os serviços públicos;
- V – dependência tecnológica;
- VI – requisitos legais;
- VII – requisitos regulatórios;
- VIII – histórico do fornecedor.

Os resultados deverão subsidiar a definição dos requisitos de segurança aplicáveis ao contrato.

12.5 Requisitos de Segurança nas Contratações

Os instrumentos convocatórios, contratos, termos de referência, estudos técnicos preliminares e demais documentos relacionados às contratações deverão

contemplar requisitos de segurança da informação compatíveis com os riscos da contratação.

Sempre que aplicável, deverão ser previstos requisitos relacionados a:

- I – confidencialidade;
- II – integridade;
- III – disponibilidade;
- IV – autenticação;
- V – controle de acesso;
- VI – proteção de dados pessoais;
- VII – gestão de incidentes;
- VIII – continuidade dos serviços;
- IX – auditoria;
- X – responsabilidades das partes.

12.6 Obrigações dos Fornecedores

Os fornecedores deverão cumprir integralmente as disposições desta Política, das normas complementares e das obrigações contratuais relacionadas à segurança da informação.

Constituem obrigações dos fornecedores, quando aplicáveis:

- I – proteger as informações institucionais;
- II – preservar o sigilo das informações;
- III – comunicar incidentes de segurança;
- IV – observar a legislação aplicável;
- V – utilizar controles de segurança compatíveis com os riscos;
- VI – cooperar com auditorias;
- VII – restringir o acesso às informações exclusivamente às pessoas autorizadas;
- VIII – assegurar que seus colaboradores conheçam as obrigações assumidas perante a Administração Municipal.

12.7 Acesso aos Ativos da Prefeitura

O acesso de fornecedores aos ativos de informação deverá ocorrer apenas quando necessário ao cumprimento das atividades contratadas.

Os acessos deverão observar:

- I – autorização formal;
- II – limitação ao escopo contratado;
- III – menor privilégio;
- IV – rastreabilidade;
- V – monitoramento;
- VI – revogação ao término da necessidade.

Os requisitos específicos relativos à gestão de identidades encontram-se estabelecidos na **Norma de Gestão de Identidades, Acessos e Senhas**.

12.8 Confidencialidade

Sempre que houver acesso a informações institucionais, o fornecedor deverá assumir compromisso formal de confidencialidade, observando as disposições legais e contratuais aplicáveis.

As obrigações de confidencialidade permanecerão válidas mesmo após o encerramento do contrato, observados os prazos estabelecidos na legislação e nos instrumentos firmados entre as partes.

12.9 Proteção de Dados Pessoais

Quando a execução contratual envolver tratamento de dados pessoais, deverão ser observadas as disposições da Lei Geral de Proteção de Dados Pessoais e da Política Municipal de Proteção de Dados Pessoais.

Os contratos deverão definir claramente:

- I – papéis e responsabilidades;
- II – finalidade do tratamento;
- III – medidas de segurança;
- IV – comunicação de incidentes;
- V – compartilhamento de dados;
- VI – retenção;
- VII – descarte;
- VIII – responsabilidades após o encerramento do contrato.

Todos os contratos que envolvam tratamento de dados pessoais devem conter cláusulas específicas de LGPD, incluindo: definição de controlador e operador, finalidade do tratamento, medidas de segurança, notificação de incidentes em prazo definido, subcontratação somente com autorização, devolução ou eliminação dos dados ao encerramento, e auditoria. Os detalhes estão no Documento Complementar nº 06 — Norma de Segurança em Contratos e Terceirizações.

12.10 Serviços em Nuvem

As contratações de serviços em nuvem deverão considerar requisitos específicos relacionados à segurança da informação e à proteção de dados.

Sempre que aplicável, deverão ser avaliados:

- I – disponibilidade dos serviços;
- II – localização das informações;
- III – mecanismos de continuidade;
- IV – requisitos de segurança;
- V – controles de acesso;
- VI – conformidade legal;
- VII – capacidade de auditoria;
- VIII – reversibilidade dos serviços ao término do contrato.

12.11 Gestão do Desempenho Contratual

Os contratos que envolvam ativos de informação deverão ser acompanhados durante toda sua execução.

O acompanhamento deverá considerar:

- I – cumprimento das obrigações de segurança;
- II – atendimento aos níveis de serviço;
- III – comunicação de incidentes;
- IV – conformidade contratual;
- V – atendimento às determinações da Administração Municipal.

Sempre que necessário, poderão ser adotadas medidas corretivas destinadas à mitigação dos riscos identificados.

12.12 Gestão de Incidentes Envolvendo Fornecedores

Os fornecedores deverão comunicar imediatamente à Prefeitura qualquer incidente de segurança da informação relacionado aos serviços contratados ou que possa impactar os ativos institucionais.

Os contratos deverão prever:

- I – canais de comunicação;
- II – prazos para notificação;
- III – responsabilidades das partes;
- IV – cooperação durante o tratamento do incidente;
- V – fornecimento das evidências necessárias à investigação.

Os incidentes serão tratados conforme o Plano de Resposta a Incidentes de Segurança da Informação.

12.13 Auditoria e Fiscalização

A Administração Municipal poderá realizar auditorias ou fiscalizações destinadas a verificar o cumprimento das obrigações contratuais relacionadas à segurança da informação.

As auditorias poderão abranger:

- controles implementados;
- proteção das informações;
- registros de auditoria;
- gestão de acessos;
- tratamento de incidentes;
- proteção de dados pessoais;
- conformidade com os instrumentos contratuais.

Sempre que cabível, os contratos deverão prever a possibilidade de auditoria pela Prefeitura ou por órgãos de controle competentes.

12.14 Alterações Contratuais

As alterações contratuais que possam impactar a segurança da informação deverão ser previamente avaliadas quanto aos riscos envolvidos.

Sempre que houver mudança relevante nos serviços prestados, deverão ser revisados:

- I – requisitos de segurança;
- II – controles implementados;
- III – níveis de acesso;
- IV – responsabilidades das partes;
- V – riscos associados ao contrato.

12.15 Encerramento da Relação Contratual

Ao término do contrato, deverão ser adotadas medidas destinadas a assegurar a proteção das informações institucionais.

Sempre que aplicável, deverão ser providenciados:

- I – revogação dos acessos concedidos;
- II – devolução dos ativos da Prefeitura;
- III – devolução ou eliminação das informações tratadas, conforme previsto contratualmente;
- IV – atualização dos registros administrativos;
- V – verificação do cumprimento das obrigações contratuais remanescentes.

O encerramento contratual deverá preservar a continuidade dos serviços públicos e a integridade das informações institucionais.

12.16 Auditoria e Conformidade

A unidade responsável pela gestão contratual e a unidade responsável pela Tecnologia da Informação poderão realizar avaliações periódicas para verificar a conformidade das contratações com esta Política, com as normas complementares e com a legislação aplicável.

Os resultados dessas avaliações deverão subsidiar ações corretivas, preventivas e de melhoria contínua, bem como orientar futuras contratações de bens e serviços de TIC.

12.17 Documentos Complementares

Este capítulo é complementado pelos seguintes documentos:

- Documento nº 06 — Norma de Segurança em Contratos e Terceirizações;
- Documento nº 14 — Norma de Segurança e Governança de Serviços em Nuvem;
- Documento nº 02 — Norma de Gestão de Identidades, Acessos e Senhas.

12.18 Disposições Gerais

A gestão de fornecedores constitui elemento essencial da governança da segurança da informação, devendo assegurar que todas as relações contratuais envolvendo ativos de informação, sistemas, infraestrutura tecnológica ou dados pessoais sejam conduzidas com níveis adequados de segurança, responsabilidade e transparência.

A Prefeitura Municipal de Aracruz deverá promover a integração entre os processos de contratação pública, gestão contratual, gestão de riscos, segurança da informação e proteção de dados pessoais, fortalecendo a capacidade institucional de prevenir incidentes, garantir a continuidade dos serviços públicos e preservar a confiança da sociedade na Administração Pública.

CAPÍTULO 13

GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO E EVENTOS CIBERNÉTICOS

13.1 Objetivo

Este capítulo estabelece as diretrizes para identificação, registro, classificação, comunicação, tratamento, resposta, investigação, recuperação e melhoria contínua relacionadas aos incidentes de Segurança da Informação no âmbito da Prefeitura Municipal de Aracruz.

Seu objetivo é assegurar que eventos capazes de comprometer a confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade das informações institucionais sejam tratados de forma coordenada, tempestiva e proporcional aos riscos envolvidos, minimizando impactos sobre os serviços públicos, os cidadãos, o patrimônio público e os dados pessoais tratados pela Administração Municipal.

13.2 Abrangência

As disposições deste capítulo aplicam-se a:

- I – todos os órgãos e unidades administrativas da Prefeitura Municipal de Aracruz;
- II – servidores públicos;
- III – agentes políticos;
- IV – empregados públicos;
- V – estagiários;
- VI – terceirizados;
- VII – fornecedores;
- VIII – empresas contratadas;
- IX – consultores;
- X – quaisquer pessoas físicas ou jurídicas que utilizem ou tenham acesso aos ativos de informação da Administração Municipal.

13.3 Princípios

A gestão de incidentes observará os seguintes princípios:

- I – resposta tempestiva;
- II – preservação das evidências;
- III – gestão baseada em riscos;
- IV – continuidade dos serviços públicos;
- V – comunicação adequada;
- VI – responsabilização;
- VII – melhoria contínua;
- VIII – cooperação entre as unidades administrativas;
- IX – conformidade legal.

13.4 Conceitos

Para os fins desta Política:

Evento de Segurança da Informação é qualquer ocorrência observada em sistemas, equipamentos, redes, processos ou serviços que possa indicar comportamento anormal, falha operacional, tentativa de ataque ou outra situação relevante para a segurança da informação.

Incidente de Segurança da Informação é um evento ou conjunto de eventos que comprometa, ou tenha potencial para comprometer, a confidencialidade, integridade, disponibilidade, autenticidade ou rastreabilidade das informações ou dos serviços institucionais.

Nem todo evento caracteriza um incidente, porém todo evento relevante deverá ser analisado para determinar seu impacto e necessidade de tratamento.

13.5 Diretrizes Gerais

A Prefeitura deverá manter processo institucional para gestão de incidentes de Segurança da Informação, contemplando todas as etapas necessárias para sua adequada condução.

Esse processo deverá assegurar:

- I – identificação dos eventos;
- II – registro das ocorrências;
- III – classificação da criticidade;
- IV – definição das prioridades;
- V – resposta coordenada;
- VI – recuperação dos serviços;
- VII – preservação de evidências, quando aplicável;
- VIII – análise das causas;
- IX – implementação de ações corretivas e preventivas;
- X – registro das lições aprendidas.

13.6 Comunicação de Incidentes

Todo usuário que identificar ou suspeitar da ocorrência de incidente de Segurança da Informação deverá comunicar imediatamente o fato pelos canais oficiais definidos pela Administração Municipal.

A comunicação deverá ocorrer independentemente da confirmação do incidente, permitindo sua avaliação tempestiva.

Sempre que possível, deverão ser informados:

- I – data e horário da ocorrência;
- II – local ou sistema afetado;

- III – descrição dos fatos observados;
- IV – impacto percebido;
- V – medidas já adotadas;
- VI – demais informações relevantes para análise.

13.7 Classificação dos Incidentes

Os incidentes deverão ser classificados conforme critérios previamente definidos, considerando, entre outros fatores:

- I – impacto sobre os serviços públicos;
- II – impacto sobre as informações;
- III – impacto sobre dados pessoais;
- IV – extensão da ocorrência;
- V – criticidade do ativo afetado;
- VI – urgência da resposta;
- VII – repercussão institucional;
- VIII – requisitos legais.

A classificação orientará a prioridade do tratamento e o nível de resposta necessário.

13.8 Resposta aos Incidentes

Os incidentes deverão ser tratados de forma coordenada, observando procedimentos previamente estabelecidos.

As ações poderão compreender:

- I – contenção;
- II – isolamento dos ativos comprometidos;
- III – mitigação dos impactos;
- IV – erradicação da causa;
- V – recuperação dos serviços;
- VI – monitoramento pós-recuperação;
- VII – documentação das ações realizadas.

A resposta deverá buscar reduzir os impactos sem comprometer a preservação das evidências quando necessárias para investigação ou responsabilização.

13.9 Preservação de Evidências

Sempre que houver possibilidade de investigação administrativa, civil, penal ou disciplinar, deverão ser adotadas medidas destinadas à preservação das evidências relacionadas ao incidente.

As evidências deverão ser tratadas de forma a preservar sua autenticidade, integridade, rastreabilidade e confiabilidade.

Quando aplicável, deverão ser observados procedimentos relacionados à cadeia de custódia das evidências digitais.

13.10 Comunicação Institucional

A divulgação de informações relacionadas a incidentes de Segurança da Informação deverá ocorrer exclusivamente pelos canais oficiais da Prefeitura Municipal de Aracruz e por autoridades formalmente designadas.

As comunicações deverão observar:

- I – interesse público;
- II – proteção das informações sensíveis;
- III – proteção de dados pessoais;
- IV – preservação das investigações;
- V – transparência compatível com a legislação vigente.

Nenhum usuário poderá divulgar informações sobre incidentes sem autorização da autoridade competente.

13.11 Incidentes Envolvendo Dados Pessoais

Quando o incidente envolver dados pessoais, deverão ser observadas as disposições da Lei Geral de Proteção de Dados Pessoais e da Política Municipal de Proteção de Dados Pessoais.

A Administração Municipal deverá avaliar, entre outros aspectos:

- I – natureza dos dados envolvidos;
- II – quantidade de titulares afetados;
- III – riscos aos direitos e liberdades dos titulares;
- IV – necessidade de comunicação aos órgãos competentes;

V – necessidade de comunicação aos titulares dos dados, quando exigida pela legislação.

O Encarregado pelo Tratamento de Dados Pessoais (DPO), ou a autoridade designada, deverá ser envolvido sempre que aplicável.

Caso o incidente envolva dados pessoais, o Encarregado (DPO) deve ser notificado imediatamente. A comunicação à ANPD e aos titulares ocorrerá conforme os critérios de risco e prazos estabelecidos pela LGPD e regulamentações da ANPD vigentes à época do fato. O fluxo de atendimento aos titulares está detalhado no Documento Complementar nº 04 — Procedimento de Atendimento aos Direitos dos Titulares.

13.12 Incidentes Envolvendo Fornecedores

Os fornecedores deverão comunicar imediatamente qualquer incidente que possa comprometer informações, sistemas ou serviços relacionados ao objeto contratual.

Os contratos deverão prever responsabilidades relativas:

- I – à comunicação do incidente;
- II – à cooperação técnica;
- III – ao fornecimento de evidências;
- IV – à recuperação dos serviços;
- V – às medidas corretivas.

13.13 Recuperação dos Serviços

Após a contenção do incidente, deverão ser adotadas medidas destinadas ao restabelecimento seguro dos serviços afetados.

A recuperação deverá observar:

- I – avaliação dos riscos remanescentes;
- II – verificação da integridade dos sistemas;
- III – validação dos serviços restaurados;
- IV – monitoramento reforçado após o retorno à operação.

Sempre que aplicável, deverão ser observadas as diretrizes estabelecidas no Plano de Continuidade dos Serviços de Tecnologia da Informação.

13.14 Lições Aprendidas e Melhoria Contínua

Após o encerramento do tratamento do incidente, deverá ser realizada análise destinada à identificação das causas, dos fatores contribuintes e das oportunidades de melhoria.

Sempre que aplicável, deverão ser avaliados:

- I – efetividade da resposta;
- II – adequação dos controles existentes;
- III – necessidade de atualização das normas;
- IV – necessidade de novos treinamentos;
- V – necessidade de revisão dos riscos;
- VI – atualização dos procedimentos operacionais.

As lições aprendidas deverão subsidiar a melhoria contínua do Sistema de Gestão da Segurança da Informação.

13.15 Capacitação e Conscientização

A Prefeitura promoverá ações periódicas destinadas a capacitar servidores, colaboradores e terceiros para identificação, comunicação e tratamento adequado dos incidentes de Segurança da Informação.

As ações poderão compreender treinamentos, campanhas educativas, exercícios simulados e outras iniciativas voltadas ao fortalecimento da cultura de segurança.

13.16 Auditoria e Avaliação

O processo de gestão de incidentes poderá ser submetido a auditorias internas ou externas destinadas a verificar sua conformidade com esta Política, com os documentos complementares e com a legislação vigente.

Os resultados dessas avaliações deverão subsidiar ações corretivas, preventivas e de melhoria contínua.

13.17 Documentos Complementares

- Norma de Gestão de Incidentes de Segurança da Informação e Eventos Cibernéticos;
- Norma de Gestão de Logs, Monitoramento e Registros;
- Plano de Continuidade dos Serviços de TIC;
- Plano de Recuperação de Desastres de TI (DRP);
- Procedimento de Atendimento aos Direitos dos Titulares;
- Registro de Operações de Tratamento de Dados Pessoais (ROPA);
- Modelo de Relatório de Impacto à Proteção de Dados (RIPD).

13.18 Disposições Gerais

A gestão de incidentes de Segurança da Informação constitui atividade permanente e essencial para a proteção dos ativos de informação da Prefeitura Municipal de Aracruz, para a continuidade da prestação dos serviços públicos e para o cumprimento das obrigações legais relacionadas à segurança da informação e à proteção de dados pessoais.

Todos os usuários dos recursos institucionais têm o dever de colaborar na prevenção, identificação e comunicação de incidentes, contribuindo para o fortalecimento da cultura de segurança, para a redução dos riscos institucionais e para a melhoria contínua do Sistema de Gestão da Segurança da Informação.

CAPÍTULO 14

CONTINUIDADE DOS NEGÓCIOS, CONTINUIDADE DOS SERVIÇOS DE TIC E RECUPERAÇÃO DE DESASTRES

14.1 Objetivo

Este capítulo estabelece as diretrizes para assegurar a continuidade dos serviços públicos, a resiliência operacional e a capacidade de recuperação da Prefeitura Municipal de Aracruz diante de incidentes, desastres, interrupções operacionais ou quaisquer eventos capazes de comprometer a disponibilidade dos serviços institucionais, dos ativos de informação e da infraestrutura tecnológica.

A continuidade deverá integrar os processos de gestão de riscos, governança, segurança da informação, proteção de dados pessoais e gestão institucional, garantindo que os serviços essenciais sejam restabelecidos em tempo compatível com sua criticidade.

14.2 Abrangência

As disposições deste capítulo aplicam-se a:

- I – todos os órgãos da Administração Direta;
- II – Secretarias Municipais;
- III – unidades administrativas;
- IV – unidades descentralizadas;
- V – infraestrutura tecnológica;
- VI – sistemas corporativos;
- VII – redes de comunicação;
- VIII – centros de processamento de dados;
- IX – serviços digitais;
- X – ambientes em nuvem;
- XI – fornecedores críticos;
- XII – ativos de informação essenciais;
- XIII – demais processos considerados críticos para o funcionamento da Administração Municipal.

14.3 Princípios

A gestão da continuidade observará os seguintes princípios:

- I – continuidade dos serviços públicos;
- II – proteção da vida e da integridade das pessoas;
- III – preservação do patrimônio público;
- IV – gestão baseada em riscos;
- V – resiliência organizacional;
- VI – proporcionalidade;
- VII – planejamento preventivo;
- VIII – melhoria contínua;

IX – coordenação institucional.

14.4 Diretrizes Gerais

A Prefeitura Municipal de Aracruz deverá manter processo institucional destinado à gestão da continuidade dos serviços públicos e da infraestrutura tecnológica.

Esse processo deverá integrar:

- I – gestão de riscos;
- II – segurança da informação;
- III – continuidade dos serviços;
- IV – resposta a incidentes;
- V – gestão de crises;
- VI – recuperação de desastres;
- VII – melhoria contínua.

As ações deverão priorizar a redução dos impactos à população e à prestação dos serviços públicos.

14.5 Identificação dos Serviços Críticos

Os órgãos municipais deverão identificar os serviços cuja interrupção possa causar impactos relevantes à Administração Pública, à população ou ao cumprimento das obrigações legais.

A identificação deverá considerar, entre outros aspectos:

- I – impacto financeiro;
- II – impacto operacional;
- III – impacto jurídico;
- IV – impacto sobre a prestação dos serviços públicos;
- V – impacto à imagem institucional;
- VI – impacto sobre dados pessoais;
- VII – impacto sobre a segurança da população.

Os serviços críticos deverão receber tratamento prioritário nas estratégias de continuidade.

14.6 Análise de Impacto nos Negócios

A Administração Municipal deverá realizar análises destinadas a identificar os impactos decorrentes da interrupção dos serviços institucionais.

A análise poderá considerar:

- I – tempo máximo aceitável de interrupção;
- II – dependências entre processos;
- III – dependências tecnológicas;
- IV – recursos humanos necessários;
- V – infraestrutura essencial;
- VI – requisitos legais;
- VII – prioridades de recuperação.

Os resultados deverão subsidiar a elaboração dos planos de continuidade.

14.7 Estratégias de Continuidade

A Prefeitura deverá estabelecer estratégias proporcionais aos riscos identificados para assegurar a continuidade dos serviços públicos.

As estratégias poderão contemplar:

- I – redundância tecnológica;
- II – ambientes alternativos;
- III – recuperação de sistemas;
- IV – comunicação emergencial;
- V – continuidade operacional das unidades administrativas;
- VI – utilização de serviços em nuvem;
- VII – contingências operacionais;
- VIII – acordos com fornecedores estratégicos.

14.8 Continuidade dos Serviços de Tecnologia da Informação

A unidade responsável pela Tecnologia da Informação deverá manter estratégias destinadas a assegurar a continuidade da infraestrutura tecnológica e dos serviços digitais.

As estratégias deverão contemplar, quando aplicável:

- I – servidores;

- II – redes;
- III – armazenamento;
- IV – bancos de dados;
- V – autenticação;
- VI – correio eletrônico;
- VII – conectividade;
- VIII – serviços em nuvem;
- IX – plataformas corporativas.

14.9 Recuperação de Desastres

A Administração Municipal deverá manter planejamento destinado à recuperação dos ambientes tecnológicos após eventos que comprometam significativamente sua operação.

O processo de recuperação deverá considerar:

- I – restauração da infraestrutura;
- II – recuperação das informações;
- III – recuperação dos sistemas;
- IV – validação dos ambientes restaurados;
- V – retorno seguro das operações;
- VI – documentação das ações executadas.

Os runbooks de recuperação, a avaliação de danos (damage assessment), os procedimentos de failover e failback, e a sanitização após ransomware estão detalhados no Documento Complementar nº 10 — Plano de Recuperação de Desastres de TI (DRP).

14.10 Gestão de Crises

Sempre que um incidente ultrapassar a capacidade normal de resposta operacional, poderá ser instituído processo formal de gestão de crise.

A gestão de crises deverá assegurar:

- I – coordenação institucional;
- II – definição de responsabilidades;
- III – tomada de decisões tempestivas;

IV – comunicação entre as unidades administrativas;

V – priorização dos serviços essenciais;

VI – acompanhamento da evolução do evento.

A autoridade competente poderá instituir comitê específico para condução das ações necessárias.

14.11 Comunicação em Situações de Contingência

A Prefeitura deverá estabelecer mecanismos destinados à comunicação durante situações de contingência.

A comunicação deverá observar:

I – tempestividade;

II – confiabilidade;

III – transparência;

IV – preservação das informações sensíveis;

V – proteção dos dados pessoais;

VI – coordenação entre os órgãos envolvidos.

As comunicações externas deverão ocorrer exclusivamente pelos canais oficiais e por autoridades competentes.

14.12 Cópias de Segurança e Recuperação

As estratégias de continuidade deverão considerar a disponibilidade das cópias de segurança necessárias à recuperação das informações institucionais.

Os processos de backup e restauração deverão observar as diretrizes estabelecidas na **Norma de Cópias de Segurança e Recuperação de Dados**, garantindo que as informações essenciais possam ser recuperadas dentro dos tempos definidos para os serviços críticos.

14.13 Dependências Externas

Os planos de continuidade deverão considerar dependências relacionadas a:

I – fornecimento de energia elétrica;

II – telecomunicações;

III – conectividade com a Internet;

- IV – serviços em nuvem;
- V – fornecedores estratégicos;
- VI – órgãos governamentais;
- VII – sistemas compartilhados;
- VIII – demais serviços indispensáveis ao funcionamento da Administração Municipal.

Sempre que possível, deverão ser previstas alternativas para redução dos impactos decorrentes da indisponibilidade dessas dependências.

14.14 Exercícios e Testes

Os planos de continuidade deverão ser submetidos a exercícios e testes periódicos destinados a verificar sua efetividade.

Os exercícios poderão contemplar:

- I – simulações de indisponibilidade;
- II – recuperação de sistemas;
- III – restauração de backups;
- IV – testes de comunicação;
- V – testes de contingência;
- VI – exercícios de gestão de crises.

Os resultados deverão ser registrados e utilizados para aperfeiçoamento dos planos.

14.15 Atualização dos Planos

Os planos de continuidade deverão ser revisados sempre que ocorrerem mudanças relevantes nos processos, na infraestrutura tecnológica, na legislação ou nos riscos institucionais.

Independentemente de alterações significativas, recomenda-se que sejam realizadas revisões periódicas para assegurar sua aderência à realidade operacional da Prefeitura.

14.16 Capacitação e Conscientização

A Prefeitura promoverá ações destinadas à capacitação dos servidores, gestores e equipes técnicas envolvidas nos processos de continuidade e recuperação.

As ações poderão compreender:

- I – treinamentos;
- II – exercícios simulados;
- III – capacitações técnicas;
- IV – campanhas de conscientização;
- V – reuniões de avaliação pós-incidente.

14.17 Auditoria e Avaliação

- Plano de Continuidade dos Serviços de TIC;
- Plano de Recuperação de Desastres de TI (DRP);
- Norma de Cópias de Segurança, Restauração e Recuperação de Dados;
- Cronograma Geral de Implantação, Validação e Publicação.

14.18 Documentos Complementares

As diretrizes estabelecidas neste capítulo são complementadas pelos seguintes documentos institucionais:

- Plano de Continuidade dos Serviços de Tecnologia da Informação (PCSTI);
- Plano de Recuperação de Desastres (Disaster Recovery Plan – DRP);
- Plano de Resposta a Incidentes de Segurança da Informação (PRISI);
- Plano de Gestão de Crises;
- Norma de Cópias de Segurança e Recuperação de Dados;
- Norma de Gestão de Riscos de Segurança da Informação;
- Política Municipal de Proteção de Dados Pessoais;
- Procedimento Operacional de Recuperação de Serviços Críticos;
- Procedimento Operacional de Testes de Continuidade.

Esses documentos estabelecem os procedimentos técnicos, operacionais e administrativos necessários para a implementação das diretrizes previstas neste capítulo.

14.19 Responsabilidades

Compete à Alta Administração assegurar os recursos necessários para a implementação das estratégias de continuidade dos serviços.

Compete às Secretarias Municipais identificar seus processos críticos, participar da elaboração e da atualização dos planos de continuidade e assegurar a execução das medidas sob sua responsabilidade.

Compete à unidade responsável pela Tecnologia da Informação coordenar os aspectos tecnológicos da continuidade dos serviços, manter os planos relacionados à infraestrutura de TIC, apoiar os testes periódicos e monitorar a capacidade de recuperação dos serviços tecnológicos.

Compete a todos os usuários colaborar com a execução das medidas de contingência, observar as orientações emitidas durante situações de crise e comunicar prontamente qualquer evento que possa comprometer a continuidade dos serviços.

14.20 Disposições Gerais

A continuidade dos serviços públicos constitui requisito essencial para o cumprimento da missão institucional da Prefeitura Municipal de Aracruz e para a manutenção da confiança da sociedade na Administração Pública.

As estratégias de continuidade deverão ser continuamente aperfeiçoadas, considerando a evolução dos riscos, as mudanças organizacionais, as transformações tecnológicas, as lições aprendidas decorrentes de incidentes e os resultados dos exercícios e auditorias realizados.

A gestão da continuidade deverá atuar de forma integrada ao Sistema de Gestão da Segurança da Informação, à gestão de riscos, à proteção de dados pessoais e à governança institucional, fortalecendo a capacidade da Prefeitura de responder a eventos adversos e assegurar a prestação dos serviços públicos essenciais.

CAPÍTULO 15

CONFORMIDADE, AUDITORIA, MONITORAMENTO, RESPONSABILIZAÇÃO E MELHORIA CONTÍNUA

15.1 Objetivo

Este capítulo estabelece as diretrizes para assegurar a conformidade do Sistema de Gestão da Segurança da Informação (SGSI) da Prefeitura Municipal de Aracruz, mediante a implementação de mecanismos de monitoramento, auditoria, avaliação de desempenho, tratamento de não conformidades, responsabilização e melhoria contínua.

Seu objetivo é garantir que os controles de Segurança da Informação permaneçam adequados às necessidades institucionais, às exigências legais, aos riscos identificados e à evolução tecnológica, promovendo a eficiência administrativa, a proteção das informações institucionais e a continuidade dos serviços públicos.

15.2 Abrangência

As disposições deste capítulo aplicam-se:

- I – a todos os órgãos da Administração Direta;
- II – às Secretarias Municipais;
- III – às unidades administrativas;
- IV – às unidades de Tecnologia da Informação;
- V – aos servidores públicos;
- VI – aos empregados públicos;
- VII – aos estagiários;
- VIII – aos colaboradores;
- IX – aos fornecedores;
- X – aos terceiros que utilizem ativos de informação da Prefeitura.

15.3 Princípios

A verificação da conformidade observará os seguintes princípios:

- I – legalidade;
- II – transparência;

- III – responsabilidade;
- IV – prestação de contas;
- V – melhoria contínua;
- VI – gestão baseada em riscos;
- VII – eficiência administrativa;
- VIII – rastreabilidade;
- IX – evidência objetiva.

15.4 Gestão da Conformidade

A Prefeitura Municipal de Aracruz deverá manter processo permanente destinado à verificação da conformidade das atividades relacionadas à Segurança da Informação.

A gestão da conformidade deverá assegurar que:

- I – as normas institucionais sejam observadas;
- II – os controles sejam implementados;
- III – os riscos sejam tratados;
- IV – as obrigações legais sejam cumpridas;
- V – as responsabilidades estejam claramente definidas;
- VI – as não conformidades sejam tratadas tempestivamente.

15.5 Monitoramento do SGSI

O Sistema de Gestão da Segurança da Informação deverá ser monitorado continuamente para verificar sua efetividade.

O monitoramento poderá abranger:

- I – implementação dos controles;
- II – cumprimento das políticas;
- III – desempenho dos processos;
- IV – tratamento dos riscos;
- V – indicadores de segurança;
- VI – incidentes registrados;
- VII – vulnerabilidades identificadas;
- VIII – evolução das ações de melhoria.

Os resultados deverão subsidiar a tomada de decisões da Administração Municipal.

15.6 Indicadores de Desempenho

A unidade responsável pela Segurança da Informação deverá estabelecer indicadores destinados a avaliar o desempenho do SGSI.

Os indicadores poderão abranger:

- I – quantidade de incidentes;
- II – tempo médio de resposta aos incidentes;
- III – tempo médio de recuperação dos serviços;
- IV – percentual de atualizações de segurança realizadas;
- V – percentual de servidores capacitados;
- VI – percentual de revisões de acesso concluídas;
- VII – conformidade das cópias de segurança;
- VIII – evolução do tratamento dos riscos;
- IX – percentual de ações concluídas nos planos de ação.

Os indicadores deverão ser revisados periodicamente para assegurar sua aderência às necessidades institucionais.

O catálogo completo de indicadores (KPIs e KRIs), os critérios SMART, o ciclo de monitoramento (coleta, análise, análise crítica, ações de melhoria), a escala de maturidade do SMGSI (níveis 1 a 5) e o rito de análise crítica pela Alta Administração estão detalhados no Documento Complementar nº 22 — Procedimento de Indicadores, Monitoramento e Análise Crítica.

15.7 Auditorias

A Prefeitura poderá realizar auditorias internas ou externas destinadas à avaliação da conformidade dos controles de Segurança da Informação.

As auditorias poderão abranger:

- I – políticas;
- II – normas;
- III – procedimentos;
- IV – infraestrutura tecnológica;

- V – sistemas;
- VI – processos administrativos;
- VII – contratos;
- VIII – gestão de riscos;
- IX – proteção de dados pessoais;
- X – continuidade dos serviços.

As auditorias deverão observar critérios objetivos, independência técnica e documentação adequada das evidências.

15.8 Avaliações de Conformidade

Sempre que necessário, poderão ser realizadas avaliações específicas para verificar:

- I – atendimento à legislação;
- II – cumprimento das normas internas;
- III – aderência aos requisitos contratuais;
- IV – implementação dos controles de segurança;
- V – conformidade dos sistemas de informação;
- VI – proteção dos dados pessoais;
- VII – maturidade do SGSI.

Os resultados deverão subsidiar o planejamento das ações corretivas.

15.9 Gestão das Não Conformidades

Toda não conformidade identificada deverá ser registrada, analisada e tratada de forma proporcional aos riscos envolvidos.

O tratamento deverá considerar:

- I – identificação da causa;
- II – avaliação dos impactos;
- III – definição das ações corretivas;
- IV – implementação das medidas;
- V – verificação da efetividade;
- VI – encerramento formal da ocorrência.

As não conformidades recorrentes deverão ser objeto de análise específica pela Alta Administração.

A diferenciação entre correção imediata (contém o dano) e ação corretiva (elimina a causa raiz), o fluxo de tratamento de NCs, a análise de causa raiz (5 Porquês ou Ishikawa) e a verificação de eficácia estão detalhados no Documento Complementar nº 21 — Procedimento de Gestão de Não Conformidades e Ações Corretivas.

15.10 Ações Corretivas e Preventivas

Sempre que identificadas oportunidades de melhoria ou falhas nos controles existentes, deverão ser planejadas ações corretivas ou preventivas.

As ações deverão possuir, sempre que possível:

- I – responsável definido;
- II – prazo para implementação;
- III – recursos necessários;
- IV – critérios de acompanhamento;
- V – verificação da efetividade.

15.11 Gestão Documental

Os documentos que compõem o Sistema de Gestão da Segurança da Informação deverão possuir controle de versão, aprovação, publicação, revisão e arquivamento.

Cada documento deverá conter, quando aplicável:

- I – identificação;
- II – versão;
- III – data de aprovação;
- IV – responsável pela elaboração;
- V – responsável pela aprovação;
- VI – histórico de revisões.

Os documentos obsoletos deverão ser tratados conforme as normas de gestão documental da Prefeitura.

15.12 Revisão da Política

Esta Política deverá ser revisada sempre que ocorrer:

- I – alteração significativa na legislação;
- II – mudança relevante na estrutura organizacional;
- III – alteração dos processos institucionais;
- IV – mudanças tecnológicas relevantes;
- V – ocorrência de incidentes significativos;
- VI – recomendações de auditorias;
- VII – determinação da Alta Administração.

Independentemente dessas situações, recomenda-se revisão periódica para assegurar sua atualização e aderência às necessidades institucionais.

15.13 Responsabilização

O descumprimento desta Política e das normas complementares poderá sujeitar o responsável às medidas administrativas, civis e penais previstas na legislação aplicável, sem prejuízo da apuração de responsabilidades pelos órgãos competentes.

A responsabilização observará:

- I – devido processo legal;
- II – contraditório;
- III – ampla defesa;
- IV – proporcionalidade;
- V – razoabilidade.

15.14 Capacitação e Cultura Organizacional

A melhoria contínua do SGSI dependerá da manutenção de programas permanentes de capacitação e conscientização.

A Prefeitura deverá estimular:

- I – desenvolvimento das competências em Segurança da Informação;
- II – disseminação das boas práticas;
- III – fortalecimento da cultura organizacional;
- IV – participação das unidades administrativas;

V – compartilhamento das lições aprendidas.

15.15 Melhoria Contínua

O Sistema de Gestão da Segurança da Informação deverá ser continuamente aperfeiçoado, considerando:

- I – resultados das auditorias;
- II – indicadores de desempenho;
- III – incidentes registrados;
- IV – avaliações de riscos;
- V – evolução tecnológica;
- VI – alterações legais;
- VII – necessidades institucionais;
- VIII – recomendações dos órgãos de controle;
- IX – lições aprendidas.

As ações de melhoria deverão ser documentadas e acompanhadas até sua conclusão.

15.16 Integração com a Governança Institucional

O SGSI deverá atuar de forma integrada aos processos de:

- Governança de Tecnologia da Informação;
- Gestão de Riscos;
- Governança de Dados;
- Proteção de Dados Pessoais;
- Gestão Documental;
- Controle Interno;
- Gestão da Qualidade;
- Planejamento Estratégico;
- Continuidade dos Serviços;
- Transformação Digital.

Essa integração deverá fortalecer a capacidade institucional de prevenir riscos, proteger ativos estratégicos e melhorar continuamente os serviços públicos prestados à sociedade.

15.17 Documentos Complementares

- Plano Anual de Auditoria e Conformidade em Segurança da Informação e Proteção de Dados;
- Procedimento de Gestão de Não Conformidades e Ações Corretivas;
- Procedimento de Indicadores, Monitoramento e Análise Crítica;
- Plano de Capacitação e Conscientização em Segurança da Informação e Proteção de Dados;
- Catálogo Final de Documentos Normativos Complementares.

15.18 Vigência

Esta Política entra em vigor na data de sua aprovação pela autoridade competente da Prefeitura Municipal de Aracruz e permanecerá vigente até que seja formalmente revisada, substituída ou revogada.

Todas as unidades administrativas deverão adotar as providências necessárias para sua implementação e cumprimento.

15.19 Revogações

Com a entrada em vigor desta Política, ficam revogados os atos normativos internos que disponham sobre matéria conflitante, sem prejuízo da manutenção das normas complementares compatíveis com este documento.

As normas existentes deverão ser revisadas gradativamente para adequação às diretrizes estabelecidas nesta Política.

15.20 Disposições Finais

A Segurança da Informação constitui responsabilidade institucional compartilhada e elemento essencial para a boa governança pública, para a proteção do patrimônio informacional, para a continuidade dos serviços públicos e para o fortalecimento da confiança da sociedade na Administração Municipal.

A implementação desta Política dependerá da atuação integrada da Alta Administração, das Secretarias Municipais, das unidades administrativas, da unidade

responsável pela Tecnologia da Informação, do Encarregado pelo Tratamento de Dados Pessoais, dos gestores, dos servidores públicos, dos colaboradores e dos fornecedores, observando-se os princípios da legalidade, eficiência, transparência, responsabilidade e melhoria contínua.

Esta Política deverá orientar todas as decisões relacionadas à Segurança da Informação no âmbito da Prefeitura Municipal de Aracruz, servindo como documento central do Sistema de Gestão da Segurança da Informação e referência para a elaboração, atualização e aplicação das normas complementares, procedimentos operacionais e demais instrumentos de governança.

CAPÍTULO 16

HIERARQUIA DOCUMENTAL, DOCUMENTOS COMPLEMENTARES E IMPLANTAÇÃO PROGRESSIVA

16.1 Hierarquia Documental

"O Sistema Municipal de Gestão da Segurança da Informação (SMGSI) estrutura-se em quatro níveis hierárquicos:

I —**Nível Estratégico:** Esta Política Municipal de Segurança da Informação e Segurança Cibernética, o Decreto Municipal nº 50.611/2026, a Matriz Consolidada de Responsabilidades (Documento nº 24), o Catálogo de Documentos Normativos Complementares (Documento nº 25) e o Cronograma Geral de Implantação (Documento nº 26);

II —**Nível Tático:** Normas temáticas que detalham regras obrigatórias para domínios específicos da tecnologia e do tratamento de dados;

III —**Nível Operacional:** Procedimentos, Planos e Modelos que orientam a execução técnica e administrativa;

IV —**Nível Evidencial:** Registros, formulários, atas e relatórios que comprovam a execução dos controles para fins de auditoria e prestação de contas."

16.2 Catálogo de Documentos Complementares

"Esta Política é complementada por 27 (vinte e sete) documentos normativos que detalham operacionalmente as diretrizes aqui estabelecidas. O Catálogo Final de Documentos Normativos Complementares (Documento Complementar nº 25)

consolida o índice mestre da arquitetura documental, indicando para cada documento: nível hierárquico, tipo, responsável pela manutenção, aprovador, status de elaboração, prioridade de publicação, fundamentação legal e periodicidade de revisão."

16.3 Lista de Documentos Complementares

Nº	Título do Documento	Nível	Responsável
01	Norma de Uso Aceitável dos Recursos de TIC	Tático	TI
02	Norma de Gestão de Identidades, Acessos e Senhas	Tático	TI
03	Norma de Gestão de Incidentes de SI e Eventos Cibernéticos	Tático	TI / CSIRT
04	Procedimento de Atendimento aos Direitos dos Titulares	Operacional	DPO
05	Norma de Classificação e Tratamento da Informação	Tático	Comitê
06	Norma de Segurança em Contratos e Terceirizações	Tático	Compras / Jurídico
07	Plano de Tratamento de Riscos de SI e Privacidade	Operacional	TI / DPO
08	Norma de Cópias de Segurança, Restauração e Recuperação	Tático	TI
09	Plano de Continuidade dos Serviços de TIC	Operacional	TI / Negócio
10	Plano de Recuperação de Desastres de TI (DRP)	Operacional	TI
11	Norma de Gestão de Logs, Monitoramento e Registros	Tático	TI
12	Norma de Gestão de Vulnerabilidades e Correções	Tático	TI
13	Norma de Dispositivos Móveis, Trabalho Remoto e BYOD	Tático	TI

Nº	Título do Documento	Nível	Responsável
14	Norma de Segurança e Governança de Serviços em Nuvem	Tático	TI
15	Procedimento de Gestão de Mudanças em TI	Operacional	TI
16	Procedimento de Inventário e Gestão de Ativos	Operacional	TI / Patrimônio
17	Registro de Operações de Tratamento de Dados (ROPA)	Evidencial	DPO / Áreas
18	Modelo de Relatório de Impacto (RIPD)	Evidencial	DPO / Áreas
19	Plano de Capacitação e Conscientização	Operacional	RH / TI / DPO
20	Plano Anual de Auditoria e Conformidade	Operacional	Controladoria
21	Procedimento de Gestão de Não Conformidades	Operacional	Qualidade / TI
22	Procedimento de Indicadores e Análise Crítica	Operacional	Comitê
23	Norma de Desenvolvimento e Aquisição Segura	Tático	TI / Dev
24	Matriz Consolidada de Responsabilidades	Estratégico	Comitê
25	Catálogo Final de Documentos Complementares	Estratégico	TI / DPO
26	Cronograma Geral de Implantação e Publicação	Estratégico	Alta Adm.
27	Plano de Ação para Revisão e Consolidação	Estratégico	Comitê

16.4 Implantação Progressiva

"A implementação desta Política e de seus documentos complementares ocorrerá de forma progressiva, em quatro fases, conforme o Cronograma Geral de Implantação, Validação e Publicação (Documento Complementar nº 26):

I —**Fase 1 (Imediata)**: Publicação desta Política, da Norma de Uso Aceitável (nº 01), da Matriz de Responsabilidades (nº 24) e do Cronograma (nº 26);

II —**Fase 2 (Alta Prioridade)**: Normas de Acessos, Incidentes, Classificação, Contratos, Titulares, Riscos, Vulnerabilidades, Inventário e ROPA;

III —**Fase 3 (Média Prioridade)**: Backup, Continuidade, DRP, Logs, Dispositivos Móveis, Nuvem, Mudanças, Desenvolvimento Seguro e RIPD;

IV —**Fase 4 (Governança)**: Capacitação, Auditoria, Não Conformidades e Indicadores."

16.5 Dependências entre Documentos

"A arquitetura documental é interdependente e sistêmica. As dependências críticas incluem:

I — O Plano de Tratamento de Riscos (nº 07) depende do Inventário de Ativos (nº 16);

II — O RIPD (nº 18) depende do ROPA (nº 17);

III — A Norma de Incidentes (nº 03) requer a Norma de Logs (nº 11);

IV — O Plano de Continuidade (nº 09) depende da Norma de Backup (nº 08) e do DRP (nº 10);

V — O Plano de Auditoria (nº 20) e o Procedimento de Indicadores (nº 22) monitoram o cumprimento de todas as normas."

CAPÍTULO 17

VIGÊNCIA, REVOGAÇÕES E DISPOSIÇÕES FINAIS

17.1 Vigência

"Esta Política entra em vigor na data de sua aprovação pela autoridade competente, permanecendo em vigor até formalmente revisada, substituída ou revogada. Todas as unidades administrativas da Administração Direta e Indireta deverão adotar as medidas necessárias à sua implementação, observado o cronograma de implantação progressiva definido no Capítulo 16."

17.2 Revogações

As normas complementares existentes deverão ser gradualmente revisadas para alinhamento com esta Política. A revogação produz efeitos apenas a partir da publicação oficial desta Política no Diário Oficial do Município."

17.3 Não Substituição do Decreto Municipal nº 50.611/2026

"Esta Política não substitui nem revoga o Decreto Municipal nº 50.611/2026 (Política Municipal de Proteção de Dados Pessoais). Ambos os instrumentos coexistem e se complementam: o Decreto estabelece a política de proteção de dados pessoais; esta Política estabelece a política de segurança da informação e segurança cibernética que fundamenta tecnicamente as medidas de proteção referidas no Art. 6º, inciso III, do referido Decreto."

17.4 Casos Omissos

"Os casos omissos serão dirimidos pelo Comitê de Segurança da Informação e Proteção de Dados, com apoio da Procuradoria Geral do Município, observada a legislação federal aplicável, as orientações da Autoridade Nacional de Proteção de Dados (ANPD) e os princípios estabelecidos nesta Política."

17.5 Responsabilidade Compartilhada

"A segurança da informação é uma responsabilidade institucional compartilhada, essencial para a boa governança pública, a proteção dos ativos informacionais, a continuidade dos serviços públicos e o fortalecimento da confiança da sociedade. Sua implementação efetiva requer a ação integrada de toda a Administração Municipal: Alta Administração, Secretarias Municipais, unidades administrativas, unidade de Tecnologia da Informação, Encarregado de Dados Pessoais, gestores, servidores públicos, colaboradores e fornecedores."



Documento assinado digitalmente
BRUNO ANGEL ANGRA BARBOSA
Data: 26/10/2026 16:35:32-0300
Verifique em <https://validar.iti.gov.br>

BRUNO ANGEL ANGRA BARBOSA

Subsecretário de Inovação e Serviços

Decreto N.º 49.198, DE 03/07/2025

Presidente Comissão Municipal De Proteção De Dados – CMPD

Decreto N.º 51.589, de 16/07/2026

Encarregado Pelo Tratamento De Dados Pessoais (LGPD)

Portaria N.º 21.002, de 04/05/2026.