REGIMENTO INTERNO SOBRE A POLITICA DE SEGURANÇA DA INFORMAÇÃO NA SECRETARIA MUNICIPAL DE SAUDE

Institui a Política no âmbito da Secretaria Municipal de Saúde de Segurança da Informação com base na Lei Geral de Proteção de Dados Pessoais.

O Secretário Municipal de Saúde, usando os poderes conferidos administrativamente por Lei, faz instituir e publicar o presente regimento interno com força de norma administrativa de observância obrigatória, nos termos seguintes:

CAPÍTULO I – DA FINALIDADE

Art. 1º A presente Política de Segurança da Informação (PSI) tem por finalidade instituir o arcabouço normativo e técnico de governança em Segurança da Informação no âmbito da **Secretaria Municipal de Saúde de Afogados da Ingazeira**, estabelecendo princípios, diretrizes, responsabilidades e controles destinados à proteção dos ativos de informação e dos recursos tecnológicos utilizados na prestação dos serviços públicos de saúde.

Art. 2º A PSI fundamenta-se nas melhores práticas de governança e gestão de riscos em Segurança da Informação, alinhando-se:

I – Às diretrizes da norma ABNT NBR ISO/IEC 27001 – Sistema de Gestão de Segurança da Informação (SGSI);

II – À ABNT NBR ISO/IEC 27002 – Código de práticas para controles de Segurança da Informação;

III – Aos princípios de governança pública aplicáveis à Administração Pública Municipal;

IV – À legislação vigente, especialmente à Lei Geral de Proteção de Dados Pessoais (LGPD), considerando a natureza sensível dos dados tratados no contexto da saúde pública.

Art. 3º A presente Política estabelece diretrizes para:

I – Identificação, classificação e proteção dos ativos de informação;

II – Implementação de controles administrativos, técnicos e físicos adequados ao nível de risco identificado;

III – Gestão sistemática de riscos de Segurança da Informação;

IV – Prevenção, detecção, resposta e tratamento de incidentes de segurança;

V – Garantia da continuidade dos serviços essenciais de saúde, mediante mecanismos de contingência e recuperação;

VI – Monitoramento, auditoria e melhoria contínua dos controles implementados.

Art. 4º A Segurança da Informação será tratada como componente estratégico da governança institucional, devendo:

I – Integrar o planejamento estratégico e operacional da Secretaria;

II – Ser considerada na contratação de serviços, aquisição de tecnologias e desenvolvimento de sistemas;

III – Observar o ciclo de melhoria contínua (Planejar, Executar, Verificar e Agir – PDCA), conforme preconizado pelas normas de Sistema de Gestão;

IV – Ser conduzida com base na análise de riscos, priorizando ativos críticos e dados pessoais sensíveis relacionados à saúde.

Art. 5º A proteção das informações no âmbito da Secretaria Municipal de Saúde deverá observar, cumulativamente, os seguintes pilares:

I – Confidencialidade;
II – Integridade;
III – Disponibilidade;
IV – Autenticidade;
V – Responsabilização e prestação de contas.

CAPÍTULO II – DO OBJETIVO

Art. 8º A presente Política de Segurança da Informação tem como objetivo estabelecer diretrizes estratégicas, táticas e operacionais para a proteção dos ativos de informação no âmbito da **Secretaria Municipal de Saúde de Afogados da Ingazeira**, assegurando a adequada gestão de riscos, a continuidade dos serviços públicos de saúde e a conformidade com as normas legais e regulatórias aplicáveis.

Art. 9º Constituem objetivos específicos da PSI:

I – Garantir a proteção da confidencialidade, integridade, disponibilidade e autenticidade das informações institucionais;

II – Estabelecer critérios formais para identificação, avaliação e tratamento de riscos de Segurança da Informação;

III – Padronizar a implementação de controles técnicos, administrativos e físicos no âmbito da Secretaria;

IV – Promover a cultura de segurança da informação e proteção de dados entre servidores e colaboradores;

V – Assegurar a conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD), especialmente quanto ao tratamento de dados pessoais sensíveis relacionados à saúde;

VI – Minimizar impactos financeiros, operacionais, legais e reputacionais decorrentes de incidentes de segurança;

VII – Garantir a continuidade dos serviços essenciais de saúde mediante mecanismos de contingência e recuperação.

Art. 10. A Política deverá orientar o estabelecimento de metas e indicadores de desempenho relacionados à Segurança da Informação, incluindo, quando aplicável:

I – Percentual de ativos inventariados e classificados;

II – Percentual de usuários capacitados em Segurança da Informação;

III – Tempo médio de resposta a incidentes;

IV – Percentual de estações e servidores atualizados;

V – Taxa de conformidade com controles estabelecidos pelo SGSI.

Art. 11 A Segurança da Informação deverá integrar o planejamento estratégico da Secretaria, sendo considerada:

I – Na contratação de serviços e soluções tecnológicas;

II – No desenvolvimento ou aquisição de sistemas de informação;

III – Na formalização de parcerias e convênios;

IV – Na gestão de projetos institucionais.

Art. 12 A implementação dos objetivos estabelecidos nesta Política deverá observar o princípio da proporcionalidade administrativa, considerando o porte institucional do Município de **Afogados da Ingazeira**, a criticidade dos serviços de saúde prestados e a disponibilidade orçamentária.

CAPÍTULO III – DO ESCOPO E DA ABRANGÊNCIA

Art. 13 A presente Política de Segurança da Informação aplica-se a todas as unidades administrativas e assistenciais vinculadas à **Secretaria Municipal de Saúde de Afogados da Ingazeira**, incluindo seus órgãos internos, unidades básicas de saúde, centros especializados, setores administrativos e demais estruturas sob sua gestão.

Art. 14 Estão sujeitos às disposições desta Política:

I – Servidores públicos efetivos;
II – Servidores comissionados;
III – Empregados públicos;
IV – Estagiários;
V – Terceirizados e prestadores de serviço;
VI – Fornecedores e parceiros que tenham acesso a informações ou sistemas institucionais;
VII – Qualquer pessoa física ou jurídica que utilize, direta ou indiretamente, ativos de informação da Secretaria.

Art. 15 O escopo do Sistema de Gestão de Segurança da Informação – SGSI abrange:

I – Todos os ativos de informação, independentemente do meio de armazenamento, processamento ou transmissão;

II – Sistemas de informação, aplicações, bancos de dados e soluções tecnológicas;

III – Infraestrutura de tecnologia da informação, incluindo redes, servidores, estações de trabalho, dispositivos móveis e equipamentos de comunicação;

IV – Informações físicas e digitais, inclusive prontuários, relatórios, laudos, documentos administrativos e dados estatísticos;

V – Dados pessoais e dados pessoais sensíveis relacionados à saúde, tratados em conformidade com a Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 16 A aplicação desta Política estende-se:

I – Aos ambientes internos e externos onde informações institucionais sejam tratadas;

II – Aos dispositivos móveis e recursos tecnológicos utilizados para fins institucionais, ainda que de propriedade particular, quando autorizados;

III – Aos serviços contratados em ambiente de computação em nuvem ou hospedagem externa;

IV – Aos acessos remotos realizados por meio de redes privadas virtuais (VPN) ou outros mecanismos de conexão segura.

Art. 17 Sempre que houver contratação, convênio, parceria ou instrumento similar que envolva acesso a informações ou sistemas institucionais, deverão ser incluídas cláusulas específicas de:

I – Confidencialidade;
II – Proteção de dados pessoais;
III – Segurança da informação;
IV – Responsabilização por incidentes.

Art. 18 O descumprimento das disposições previstas nesta Política sujeitará o infrator às medidas administrativas, civis e penais cabíveis, sem prejuízo da apuração de responsabilidade funcional.

CAPÍTULO IV – DOS PRINCÍPIOS DA SEGURANÇA DA INFORMAÇÃO

Art. 19 A Segurança da Informação no âmbito da **Secretaria Municipal de Saúde de Afogados da Ingazeira** será regida pelos seguintes princípios fundamentais:

I – Confidencialidade

Garantia de que as informações sejam acessadas somente por pessoas devidamente autorizadas, prevenindo divulgação indevida, vazamentos ou exposição não autorizada.

II – Integridade

Garantia de que as informações permaneçam íntegras, completas e protegidas contra alterações não autorizadas, intencionais ou acidentais.

III – Disponibilidade

Garantia de que as informações e os serviços de saúde estejam acessíveis aos usuários autorizados sempre que necessário, assegurando a continuidade dos serviços públicos essenciais.

IV – Autenticidade

Garantia da veracidade da identidade dos usuários, sistemas e fontes de informação, assegurando que as transações e registros possam ser devidamente atribuídos a seus responsáveis.

V – Rastreabilidade e Auditoria

Garantia de que as ações realizadas nos sistemas institucionais possam ser registradas, monitoradas e auditadas, permitindo a identificação de responsabilidades e a detecção de incidentes.

VI – Gestão Baseada em Riscos

Adoção de abordagem sistemática de identificação, análise, avaliação e tratamento de riscos, priorizando ativos críticos e dados pessoais sensíveis relacionados à saúde.

VII – Conformidade Legal

Observância das normas constitucionais, legais e regulamentares aplicáveis, especialmente da Lei Geral de Proteção de Dados Pessoais (LGPD), bem como demais legislações pertinentes à Administração Pública.

VIII – Proporcionalidade e Necessidade

Aplicação de controles de segurança compatíveis com o porte institucional do Município de **Afogados da Ingazeira**, considerando a criticidade dos serviços prestados e a disponibilidade de recursos.

IX – Responsabilização e Prestação de Contas

Atribuição clara de responsabilidades quanto à proteção das informações, assegurando transparência e possibilidade de responsabilização em caso de descumprimento.

Art. 20 Os princípios estabelecidos neste Capítulo deverão orientar:

I – A definição de normas complementares;
II – A implementação de controles técnicos e administrativos;
III – A análise e tratamento de riscos;
IV – A tomada de decisões estratégicas relacionadas à tecnologia da

informação;
V – A avaliação de incidentes de segurança.

CAPÍTULO V – DOS CONCEITOS E DEFINIÇÕES

Art. 21 Para os fins desta Política de Segurança da Informação, adotam-se os seguintes conceitos:

I – Ativo de Informação

Qualquer dado, informação, sistema, equipamento, recurso tecnológico, documento físico ou digital que possua valor para a **Secretaria Municipal de Saúde de Afogados da Ingazeira** e que deva ser protegido contra acessos não autorizados, perda, alteração ou indisponibilidade.

II – Ativo Crítico

Ativo de informação cuja indisponibilidade, perda ou comprometimento possa causar impacto significativo na prestação dos serviços públicos de saúde.

III – Informação

Conjunto de dados organizados que possuam significado e valor para a administração pública, podendo estar em meio físico ou digital.

IV – Dado Pessoal

Informação relacionada a pessoa natural identificada ou identificável, nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD).

V – Dado Pessoal Sensível

Dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação sindical, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a pessoa natural.

VI – Tratamento de Dados

Toda operação realizada com dados pessoais, como coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, armazenamento, eliminação ou avaliação.

VII – Segurança da Informação

Conjunto de práticas, controles e medidas destinadas a preservar a confidencialidade, integridade, disponibilidade e autenticidade da informação.

VIII – Sistema de Gestão de Segurança da Informação (SGSI)

Conjunto estruturado de políticas, processos, procedimentos e controles destinados à gestão sistemática da segurança da informação, com base na gestão de riscos e melhoria contínua.

IX – Incidente de Segurança da Informação

Evento adverso, confirmado ou sob suspeita, que comprometa ou tenha potencial de comprometer a segurança dos ativos de informação.

X – Risco de Segurança da Informação

Probabilidade de ocorrência de um evento que explore uma vulnerabilidade e cause impacto negativo aos ativos de informação.

XI – Vulnerabilidade

Fragilidade ou fraqueza em sistema, processo, pessoa ou tecnologia que possa ser explorada para comprometer a segurança da informação.

XII – Controle de Segurança

Medida administrativa, técnica ou física implementada com a finalidade de reduzir riscos de segurança da informação.

XIII – Usuário

Qualquer pessoa física ou jurídica que tenha acesso autorizado a ativos de informação da Secretaria.

XIV – Backup

Cópia de segurança realizada com o objetivo de garantir a recuperação de informações em caso de falhas, incidentes ou desastres.

Art. 22 Outros conceitos técnicos poderão ser definidos em normas complementares vinculadas a esta Política, sempre que necessário ao aprimoramento do Sistema de Gestão de Segurança da Informação.

CAPÍTULO VI – DA ESTRUTURA ORGANIZACIONAL DE SEGURANÇA DA INFORMAÇÃO

Seção I – Da Estrutura de Governança

Art. 23 A governança da Segurança da Informação no âmbito da **Secretaria Municipal de Saúde de Afogados da Ingazeira** será estruturada de forma hierarquizada, integrada e alinhada ao Sistema de Gestão de Segurança da Informação – SGSI.

Art. 24 A estrutura organizacional de Segurança da Informação será composta por:

I – Alta Administração;
II – Responsável pela Segurança da Informação;
III – Comitê de Segurança da Informação e Proteção de Dados;
IV – Área de Tecnologia da Informação;
V – Gestores de Área;
VI – Proprietários de Ativos de Informação;
VII – Usuários.

Seção II – Da Alta Administração

Art. 25 Compete à Alta Administração:

I – Aprovar a Política de Segurança da Informação e suas atualizações;
II – Garantir apoio institucional para a captação de recursos necessários para implementação do SGSI;
III – Deliberar sobre riscos críticos e incidentes de alto impacto;
IV – Promover cultura organizacional voltada à segurança e proteção de dados.

Seção III – Do Responsável pela Segurança da Informação

Art. 26 O Responsável pela Segurança da Informação será designado formalmente pela Secretaria, podendo ser exercido pelo Analista de Segurança da Informação ou servidor designado.

Art. 27 Compete ao Responsável pela Segurança da Informação:

I – Coordenar a implementação e manutenção do SGSI;
II – Propor políticas, normas e controles;
III – Conduzir análise e tratamento de riscos;
IV – Coordenar resposta a incidentes;
V – Elaborar relatórios periódicos à Alta Administração;
VI – Promover ações de conscientização.

Seção IV – Do Comitê de Segurança da Informação e Proteção de Dados

Art. 28 Fica instituído o Comitê de Segurança da Informação e Proteção de Dados Pessoais, com caráter consultivo e deliberativo, composto por representantes das áreas estratégicas da Secretaria.

Art. 29 Compete ao Comitê:

I – Avaliar riscos estratégicos;
II – Deliberar sobre incidentes relevantes;
III – Propor melhorias na Política;
IV – Apoiar decisões relacionadas à proteção de dados pessoais;
V – Recomendar investimentos em segurança da informação.

Parágrafo único. O Comitê reunir-se-á, ordinariamente, ao menos uma vez por ano, e extraordinariamente quando necessário.

Seção V – Da Área de Tecnologia da Informação

Art. 30 Compete à Área de Tecnologia da Informação:

I – Implementar controles técnicos de segurança;
II – Gerenciar infraestrutura tecnológica;
III – Manter sistemas atualizados;
IV – Executar rotinas de backup;
V – Monitorar eventos e registros de acesso;
VI – Apoiar tecnicamente o tratamento de incidentes.

Seção VI – Dos Gestores de Área

Art. 31 Compete aos Gestores de Área:

I – Garantir cumprimento da Política em sua unidade;
II – Classificar informações sob sua responsabilidade;
III – Solicitar concessão e revogação de acessos;
IV – Comunicar incidentes imediatamente.

Seção VII – Dos Proprietários de Ativos de Informação

Art. 32 O Proprietário do Ativo é o responsável pela definição do nível de classificação e das regras de acesso às informações sob sua gestão.

Seção VIII – Dos Usuários

Art. 33 Todos os usuários são responsáveis pelo uso adequado dos ativos de informação, devendo:

I – Cumprir esta Política;
II – Proteger credenciais de acesso;

III – Reportar incidentes;
IV – Participar de treinamentos obrigatórios.

CAPÍTULO VII – DA GESTÃO DE RISCOS DE SEGURANÇA DA INFORMAÇÃO

Seção I – Das Disposições Gerais

Art. 34 A Gestão de Riscos de Segurança da Informação no âmbito da **Secretaria Municipal de Saúde de Afogados da Ingazeira** será conduzida de forma sistemática, estruturada e contínua, como elemento central do Sistema de Gestão de Segurança da Informação – SGSI.

Art. 35 A metodologia de gestão de riscos deverá estar alinhada às boas práticas internacionais, especialmente à norma ISO/IEC 27001 e à ISO/IEC 27005, considerando:

I – O contexto organizacional;
II – A criticidade dos serviços públicos de saúde;
III – A natureza dos dados pessoais tratados;
IV – A capacidade operacional do Município de **Afogados da Ingazeira**.

Seção II – Do Processo de Gestão de Riscos

Art. 36 O processo de gestão de riscos compreenderá, no mínimo, as seguintes etapas:

I – Estabelecimento do contexto;
II – Identificação de ativos;
III – Identificação de ameaças e vulnerabilidades;
IV – Análise de riscos;
V – Avaliação de riscos;
VI – Tratamento de riscos;
VII – Aceitação formal de riscos residuais;
VIII – Monitoramento e revisão periódica.

Seção III – Da Identificação e Classificação dos Ativos

Art. 37 Todos os ativos de informação deverão ser identificados, inventariados e classificados quanto à sua criticidade e sensibilidade.

Art. 38 A classificação da informação deverá considerar, no mínimo:

I – Grau de confidencialidade;
II – Impacto da perda de integridade;
III – Impacto da indisponibilidade;
IV – Existência de dados pessoais ou dados pessoais sensíveis, nos termos da Lei Geral de Proteção de Dados Pessoais (LGPD).

Seção IV – Da Análise e Avaliação de Riscos

Art. 39 A análise de riscos deverá considerar:

I – Probabilidade de ocorrência;
II – Impacto potencial;
III – Nível de exposição;
IV – Controles existentes.

Art. 40 Os riscos identificados deverão ser classificados em níveis (baixo, médio, alto ou crítico), conforme metodologia definida em norma complementar.

Seção V – Do Tratamento de Riscos

Art. 41 O tratamento de riscos poderá envolver:

I – Mitigação, mediante implementação de controles;
II – Transferência, quando aplicável;
III – Evitação do risco;
IV – Aceitação formal do risco residual.

Art. 42 A aceitação de riscos classificados como altos ou críticos deverá ser formalmente registrada e submetida à Alta Administração.

Seção VI – Do Monitoramento e Melhoria Contínua

Art. 43 A gestão de riscos deverá ser revisada:

I – Periodicamente, ao menos uma vez por ano;
II – Sempre que houver mudança significativa em sistemas, processos ou estrutura organizacional;
III – Após a ocorrência de incidentes relevantes.

Art. 44 O processo de gestão de riscos deverá observar o princípio da melhoria contínua, garantindo atualização constante dos controles de segurança.

CAPÍTULO VIII – DA CLASSIFICAÇÃO E TRATAMENTO DA INFORMAÇÃO

Seção I – Das Disposições Gerais

Art. 45 A informação produzida, recebida, armazenada ou custodiada pela **Secretaria Municipal de Saúde de Afogados da Ingazeira** deverá ser classificada quanto ao seu grau de sensibilidade, criticidade e necessidade de proteção.

Art. 46 A classificação da informação tem por finalidade:

I – Assegurar proteção adequada aos ativos de informação;
II – Reduzir riscos de vazamento, perda ou uso indevido;
III – Garantir conformidade com a legislação vigente;
IV – Apoiar a definição de controles técnicos e administrativos.

Seção II – Dos Níveis de Classificação

Art. 47 As informações serão classificadas nos seguintes níveis:

I – Informação Pública

Informação que pode ser divulgada sem restrições, observadas as normas de transparência pública.

II – Informação de Uso Interno

Informação destinada ao uso exclusivo da Secretaria, cuja divulgação externa não autorizada pode causar prejuízos administrativos.

III – Informação Restrita

Informação cujo acesso deve ser limitado a usuários autorizados, podendo incluir dados pessoais.

IV – Informação Sigilosa ou Sensível

Informação cuja divulgação não autorizada pode causar danos graves à Administração Pública, aos cidadãos ou envolver dados pessoais sensíveis, especialmente dados relacionados à saúde, conforme definido na Lei Geral de Proteção de Dados Pessoais (LGPD).

Seção III – Das Responsabilidades pela Classificação

Art. 48 A classificação da informação é de responsabilidade do Proprietário do Ativo ou do Gestor da Área responsável pela sua geração ou custódia.

Art. 49 A revisão da classificação deverá ocorrer:

I – Periodicamente;
II – Quando houver alteração na natureza da informação;
III – Em caso de mudança normativa.

Seção IV – Do Tratamento da Informação

Art. 50 O tratamento da informação deverá observar o nível de classificação atribuído, devendo ser aplicadas medidas proporcionais de proteção.

Art. 51 Para informações classificadas como Restritas ou Sigilosas, deverão ser adotadas, no mínimo:

I – Controle de acesso baseado no princípio do menor privilégio;
II – Autenticação individualizada;
III – Registro de acessos (logs);
IV – Criptografia, quando aplicável;
V – Proteção contra cópias não autorizadas.

Seção V – Do Armazenamento, Transmissão e Descarte

Art. 52 O armazenamento de informações deverá ocorrer apenas em sistemas e locais autorizados pela Área de Tecnologia da Informação.

Art. 53 A transmissão de informações sensíveis deverá ocorrer por meios seguros, com uso de protocolos protegidos ou mecanismos equivalentes.

Art. 54 O descarte de informações deverá:

I – Garantir a impossibilidade de recuperação indevida;
II – Observar prazos legais de retenção;
III – Seguir procedimentos formais de eliminação segura.

Seção VI – Da Reclassificação e Desclassificação

Art. 55 Informações poderão ser reclassificadas ou desclassificadas quando cessarem as condições que justificaram sua proteção.

Parágrafo único. A reclassificação deverá ser formalmente registrada.

CAPÍTULO IX – DO CONTROLE DE ACESSO

Seção I – Das Disposições Gerais

Art. 56 O acesso aos ativos de informação deverá ser concedido com base nos princípios:

I – Do menor privilégio;
II – Da necessidade de conhecer;
III – Da segregação de funções;
IV – Da responsabilidade individual e rastreabilidade.

Art. 57 O controle de acesso deverá abranger:

I – Sistemas informatizados;
II – Redes corporativas;
III – Equipamentos institucionais;
IV – Documentos físicos e digitais;
V – Ambientes físicos restritos.

Seção II – Da Concessão de Acesso

Art. 58 A concessão de acesso deverá:

I – Ser formalmente solicitada pelo gestor da área;
II – Ser autorizada pelo responsável competente;
III – Estar vinculada às atribuições do cargo ou função;
IV – Ser registrada para fins de auditoria.

Art. 59 É vedada a criação de contas genéricas ou compartilhadas, salvo justificativa técnica formalmente aprovada.

Seção III – Da Gestão de Identidades

Art. 60 Todo usuário deverá possuir identificação individual e intransferível para acesso aos sistemas institucionais.

Art. 61 As credenciais de acesso:

I – São de uso pessoal e intransferível;
II – Não poderão ser compartilhadas;
III – Devem ser protegidas contra divulgação indevida.

Seção IV – Das Senhas e Autenticação

Art. 62 As senhas deverão atender a requisitos mínimos de complexidade definidos em norma complementar.

Art. 63 Sempre que tecnicamente viável, deverá ser adotada autenticação multifator para acesso a:

I – Sistemas críticos;
II – Sistemas que tratem dados pessoais sensíveis;
III – Acesso remoto à rede institucional.

Seção V – Da Revisão e Revogação de Acessos

Art. 64 Os acessos concedidos deverão ser revisados periodicamente, ao menos uma vez por ano.

Art. 65 O acesso deverá ser imediatamente revogado nos casos de:

I – Desligamento do servidor ou colaborador;
II – Mudança de função;
III – Identificação de uso indevido;
IV – Determinação da autoridade competente.

Seção VI – Do Monitoramento e Registro

Art. 66 Os acessos a sistemas e informações classificadas como Restritas ou Sigilosas deverão ser registrados em logs.

Art. 67 Os registros de acesso deverão ser:

I – Protegidos contra alteração indevida;
II – Mantidos pelo prazo definido em norma interna;
III – Utilizados para fins de auditoria e investigação de incidentes.

Seção VII – Do Acesso Físico

Art. 68 O acesso a ambientes físicos que contenham ativos críticos de informação deverá ser controlado por meio de mecanismos apropriados, tais como:

I – Controle de chaves;
II – Registro de entrada e saída;
III – Monitoramento por câmeras, quando aplicável.

Seção VIII – Do Acesso Remoto

Art. 69 O acesso remoto aos sistemas institucionais deverá:

I – Utilizar conexões seguras;
II – Ser autorizado formalmente;
III – Ser restrito a dispositivos previamente configurados e protegidos.

CAPÍTULO X – DA SEGURANÇA EM TECNOLOGIA DA INFORMAÇÃO

Seção I – Das Diretrizes Gerais

Art. 70 A infraestrutura tecnológica da Secretaria deverá ser protegida por controles técnicos e administrativos compatíveis com a criticidade dos serviços públicos de saúde prestados.

Art. 71 A segurança em Tecnologia da Informação deverá observar:

I – Gestão baseada em riscos;
II – Princípios de defesa em profundidade;
III – Atualização contínua de sistemas;
IV – Monitoramento e registro de eventos;
V – Conformidade com o Sistema de Gestão de Segurança da Informação – SGSI.

Seção II – Da Segurança de Redes

Art. 72 A rede institucional deverá ser protegida por mecanismos de segurança, incluindo, quando aplicável:

I – Firewall;
II – Segmentação de rede;
III – Controle de acesso à rede;
IV – Monitoramento de tráfego.

Art. 73 Redes sem fio deverão:

I – Utilizar criptografia adequada;
II – Possuir autenticação individualizada;
III – Ser segregadas da rede administrativa quando destinadas a visitantes.

Seção III – Da Segurança de Servidores e Sistemas

Art. 74 Servidores físicos e virtuais deverão:

I – Permanecer atualizados com correções de segurança;
II – Possuir controle de acesso restrito;
III – Estar protegidos contra softwares maliciosos;
IV – Ser submetidos a rotinas de backup.

Art. 75 Sistemas que tratem dados pessoais sensíveis, especialmente dados de saúde, deverão adotar controles reforçados de segurança, incluindo criptografia quando tecnicamente viável, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD).

Seção IV – Da Segurança de Estações de Trabalho

Art. 76 As estações de trabalho deverão:

I – Utilizar antivírus ou solução equivalente;
II – Estar protegidas por senha individual;
III – Possuir bloqueio automático de sessão;
IV – Não permitir instalação de softwares não autorizados.

Seção V – Da Gestão de Atualizações e Vulnerabilidades

Art. 77 A Área de Tecnologia da Informação deverá implementar processo de:

I – Atualização periódica de sistemas operacionais e aplicações;
II – Correção de vulnerabilidades críticas;
III – Avaliação de exposição a riscos tecnológicos.

Seção VI – Da Segurança de Backup

Art. 78 A Secretaria deverá manter política formal de backup contemplando:

I – Periodicidade das cópias;
II – Armazenamento seguro;
III – Testes periódicos de restauração;
IV – Proteção contra acesso não autorizado.

Art. 79 Backups que contenham dados pessoais sensíveis deverão receber proteção reforçada.

Seção VII – Da Segurança no Uso de Dispositivos Móveis

Art. 80 O uso de dispositivos móveis institucionais deverá observar:

I – Proteção por senha ou biometria;
II – Criptografia de armazenamento, quando possível;
III – Proibição de compartilhamento com terceiros;
IV – Comunicação imediata em caso de perda ou furto.

Seção VIII – Da Segurança na Aquisição e Desenvolvimento de Sistemas

Art. 81 A aquisição ou desenvolvimento de sistemas deverá considerar requisitos de segurança desde sua concepção (Security by Design).

Art. 82 Sistemas contratados deverão atender a requisitos mínimos de proteção de dados e segurança da informação.

Seção IX – Da Terceirização de Serviços de TI

Art. 83 Contratos com fornecedores de tecnologia deverão conter cláusulas específicas sobre:

I – Confidencialidade;
II – Proteção de dados pessoais;
III – Responsabilidade por incidentes;
IV – Conformidade com a legislação vigente.

CAPÍTULO XI – DA CONSCIENTIZAÇÃO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO

Seção I – Das Diretrizes Gerais

Art. 84 A **Secretaria Municipal de Saúde de Afogados da Ingazeira** deverá promover programa contínuo de conscientização e capacitação em Segurança da Informação, como parte integrante do Sistema de Gestão de Segurança da Informação – SGSI.

Art. 85 O programa de conscientização tem como objetivos:

I – Reduzir riscos decorrentes de falhas humanas;
II – Fortalecer a cultura organizacional de segurança;
III – Garantir conformidade com normas internas e legislação aplicável;
IV – Promover boas práticas no tratamento de dados pessoais.

Seção II – Do Programa de Conscientização

Art. 86 O programa deverá contemplar, no mínimo:

I – Treinamentos periódicos para servidores e colaboradores;
II – Orientações sobre uso adequado de sistemas e recursos tecnológicos;
III – Boas práticas de criação e proteção de senhas;
IV – Prevenção contra phishing e engenharia social;
V – Procedimentos de comunicação de incidentes;

VI – Diretrizes sobre proteção de dados pessoais, conforme a Lei Geral de Proteção de Dados Pessoais (LGPD).

Seção III – Da Capacitação Técnica

Art. 87 A Secretaria deverá assegurar que servidores que atuem diretamente na gestão de ativos de informação ou na área de Tecnologia da Informação possuam capacitação compatível com suas responsabilidades.

Art. 88 Sempre que possível, deverão ser promovidas:

I – Atualizações técnicas sobre ameaças emergentes;
II – Capacitação em gestão de riscos;
III – Treinamento em resposta a incidentes;
IV – Atualização sobre requisitos normativos e boas práticas internacionais.

Seção IV – Da Responsabilidade Individual

Art. 89 Todos os servidores, estagiários, terceirizados e colaboradores são responsáveis por:

I – Participar das ações de conscientização;
II – Cumprir as orientações recebidas;
III – Aplicar as boas práticas no exercício de suas funções;
IV – Comunicar situações de risco ou incidentes.

Seção V – Do Registro e Monitoramento

Art. 90 As ações de capacitação deverão:

I – Ser registradas formalmente;
II – Ter periodicidade definida;
III – Ser avaliadas quanto à sua efetividade.

Parágrafo único. A participação poderá ser considerada requisito para concessão ou manutenção de acessos a sistemas críticos.

CAPÍTULO XII – DA GESTÃO DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO

Seção I – Das Disposições Gerais

Art. 91 A **Secretaria Municipal de Saúde de Afogados da Ingazeira** deverá estabelecer processo formal de gestão de incidentes de Segurança da Informação, integrado ao Sistema de Gestão de Segurança da Informação – SGSI.

Art. 92 Considera-se incidente de segurança qualquer evento adverso, confirmado ou sob suspeita, que comprometa ou possa comprometer:

I – A confidencialidade;
II – A integridade;
III – A disponibilidade;
IV – A autenticidade das informações institucionais.

Seção II – Da Comunicação de Incidentes

Art. 93 Todo servidor, colaborador ou prestador de serviço que identificar ou suspeitar de incidente deverá comunicar imediatamente ao Responsável pela Segurança da Informação ou à Área de Tecnologia da Informação.

Art. 94 A omissão na comunicação de incidentes poderá ensejar responsabilização administrativa.

Seção III – Da Classificação dos Incidentes

Art. 95 Os incidentes deverão ser classificados conforme seu nível de impacto:

I – Baixo;
II – Médio;
III – Alto;
IV – Crítico.

Parágrafo único. A classificação considerará impacto operacional, financeiro, jurídico e reputacional.

Seção IV – Do Tratamento de Incidentes

Art. 96 O tratamento de incidentes deverá seguir, no mínimo, as seguintes etapas:

I – Registro formal do evento;
II – Análise preliminar;
III – Contenção;
IV – Erradicação da causa;
V – Recuperação dos serviços;
VI – Análise pós-incidente.

Art. 97 Sempre que necessário, poderão ser adotadas medidas emergenciais para contenção de danos, incluindo bloqueio de acessos e isolamento de sistemas.

Seção V – Dos Incidentes Envolvendo Dados Pessoais

Art. 98 Incidentes que envolvam dados pessoais ou dados pessoais sensíveis deverão ser tratados com prioridade máxima.

Art. 99 Nos casos que possam acarretar risco ou dano relevante aos titulares de dados, deverão ser adotadas medidas cabíveis, conforme previsto na Lei Geral de Proteção de Dados Pessoais (LGPD).

Seção VI – Do Registro e Documentação

Art. 100 Todos os incidentes deverão ser registrados em sistema ou relatório formal, contendo:

I – Data e hora da ocorrência;
II – Descrição do incidente;
III – Sistemas afetados;
IV – Medidas adotadas;
V – Responsáveis pelo tratamento;
VI – Avaliação de impacto.

Seção VII – Da Melhoria Contínua

Art. 101 Após o encerramento do incidente, deverá ser realizada análise crítica para:

I – Identificação de falhas processuais ou técnicas;
II – Atualização da matriz de riscos;
III – Implementação de controles adicionais;
IV – Revisão de procedimentos, quando necessário.

CAPÍTULO XIII – DAS SANÇÕES E RESPONSABILIZAÇÕES

Seção I – Das Disposições Gerais

Art. 102 O descumprimento das disposições desta Política de Segurança da Informação sujeitará o infrator às sanções administrativas cabíveis, sem prejuízo das responsabilidades civil e penal aplicáveis.

Av. Rio Branco, nº296 – Centro
CEP: 56800-000
CNPJ:11.308.823/0001-03 (87)3838-1575 saude@afogadosdaingazeira.pe.gov.br saudeafogadosdaingazeira

Art. 103 As sanções serão aplicadas conforme a natureza da infração, sua gravidade, a extensão do dano causado e a reincidência.

Seção II – Da Responsabilização de Servidores e Colaboradores

Art. 104 O servidor público que descumprir esta Política poderá responder administrativamente, nos termos do regime jurídico aplicável ao Município.

Art. 105 Constituem, entre outras, infrações relacionadas à Segurança da Informação:

I – Compartilhamento indevido de credenciais;
II – Acesso não autorizado a informações;
III – Vazamento intencional ou culposo de dados;
IV – Omissão na comunicação de incidentes;
V – Uso inadequado de recursos tecnológicos institucionais;
VI – Descumprimento de normas de classificação e tratamento da informação.

Seção III – Da Responsabilização de Terceiros e Fornecedores

Art. 106 Fornecedores e prestadores de serviços que tenham acesso a ativos de informação da **Secretaria Municipal de Saúde de Afogados da Ingazeira** responderão contratualmente por violações às normas de segurança da informação.

Art. 107 Os contratos firmados deverão prever:

I – Cláusulas de confidencialidade;
II – Obrigações específicas de proteção de dados;
III – Penalidades por descumprimento;
IV – Responsabilidade por incidentes decorrentes de falhas de segurança.

Seção IV – Das Infrações Relacionadas à Proteção de Dados Pessoais

Art. 108 O tratamento inadequado de dados pessoais poderá ensejar responsabilização administrativa, civil e penal, conforme previsto na Lei Geral de Proteção de Dados Pessoais (LGPD).

Art. 109 Incidentes que envolvam dados pessoais sensíveis, especialmente dados de saúde, serão considerados de maior gravidade para fins de apuração interna.

Seção V – Do Processo de Apuração

Art. 110 A apuração de infrações deverá observar:

I – O contraditório e a ampla defesa;
II – A legislação municipal aplicável;
III – A formalização do procedimento administrativo.

Art. 111 O Responsável pela Segurança da Informação deverá comunicar formalmente à autoridade competente sempre que identificar indícios de infração relevante.

Seção VI – Das Medidas Corretivas

Art. 112 Independentemente da aplicação de sanções, poderão ser adotadas medidas corretivas, tais como:

I – Suspensão ou revogação de acessos;
II – Reforço de treinamento obrigatório;
III – Revisão de processos internos;
IV – Atualização de controles técnicos.

CAPÍTULO XIV – DAS DISPOSIÇÕES FINAIS E VIGÊNCIA

Seção I – Das Disposições Finais

Art. 113 Esta Política de Segurança da Informação aplica-se a todos os servidores públicos, estagiários, colaboradores, terceirizados, fornecedores e quaisquer pessoas físicas ou jurídicas que tenham acesso a ativos de informação da **Secretaria Municipal de Saúde de Afogados da Ingazeira**.

Art. 114 As disposições desta Política deverão ser observadas em conjunto com:

I – Normas internas complementares;
II – Regulamentos municipais aplicáveis;
III – Contratos administrativos firmados pela Secretaria;
IV – A Lei Geral de Proteção de Dados e demais legislações pertinentes.

Art. 115 Normas complementares poderão ser editadas pelo Responsável pela Segurança da Informação ou pela autoridade competente, com a finalidade de detalhar procedimentos técnicos e operacionais necessários à implementação do Sistema de Gestão de Segurança da Informação – SGSI.

Art. 116 A presente Política deverá ser revisada:

I – Periodicamente, no mínimo a cada dois anos;
II – Sempre que houver alteração significativa na estrutura organizacional;

tecnológica ou normativa;
III – Após incidentes relevantes que demandem aprimoramento dos controles existentes.

Art. 117 A Alta Administração deverá garantir os recursos necessários à implementação e manutenção desta Política, observadas as disponibilidades orçamentárias do Município de **Afogados da Ingazeira**.

Seção II – Da Vigência

Art. 118 Esta Política de Segurança da Informação entra em vigor na data de sua publicação oficial.

Art. 119 Revogam-se as disposições em contrário.

Publique-se. Cumpra-se.

Afogados da Ingazeira-PE, 22 de maio de 2026

Artur Belarmino de Amorim
SECRETARIO DE SAÚDE
Mat. 7580-6

ARTUR BELARMINO DE AMORIM
Secretário Municipal de Saúde

PUBLICAÇÃO
Nesta data fiz a publicação deste ato no local de costume.
Af. da Ingazeira 29/05/2026
Funcionário (a) Emanuela Vitória