TÍTULO:	**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO - PSI**
Unidade Gestora:	**Diretoria de Tecnologia da Informação e Inovação - DTI**
Vigência:	27/05/2025
Público alvo:	Todas as unidades do CTM.
Relação com outras Instruções Normativas de TI:	Não se aplica.
Classificação:	#PÚBLICA
Atendimento de Dúvidas:	Coordenadoria de Tecnologia da Informação e Inovação - CTI

1 – Objetivo

1.1 – Padronizar e estabelecer princípios, diretrizes, responsabilidades e práticas para a proteção das informações, permitindo aos colaboradores do CTM seguirem padrões de comportamento relacionados à segurança da informação adequados às necessidades de negócio e da proteção legal da instituição, proporcionando condições que assegurem a integridade, a confidencialidade, a disponibilidade, bem como a legalidade da informação e do dado pessoal no âmbito do ambiente computacional da empresa.

2 – Definições

2.1 – IN – Instrução Normativa.

2.2 – DTI – Diretoria de Tecnologia da Informação.

2.3 – CTI – Coordenação de Tecnologia da Informação.

2.4 – CTM – Grande Recife Consórcio.

2.5 – GSIT – Gerência de Segurança Tecnológica, Infra e Telecomunicações.

2.6 – Integridade - garantia de que a informação seja mantida em seu estado original, visando protegê-la, na guarda ou transmissão, contra alterações indevidas, intencionais ou acidentais.

2.7 – Confidencialidade - garantia de que o acesso à informação seja obtido somente por pessoas autorizadas.

2.8 – Disponibilidade - garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário.

2.9 – Legalidade – aderência de ação ou ato a um conjunto normativo e legal vigentes.

2.10 – Informação - conhecimento registrado sob a forma escrita, oral ou audiovisual. É resultante do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema que a recebe.

2.11 – PSI – Política de Segurança da Informação.

2.12 – DPO – Data Protection Officer = Encarregado de Proteção de Dados.

2.13 – SEI – Sistema Eletrônico de Informações.

2.14 – Expresso PE – Correio eletrônico utilizado pelos órgãos do governo do estado de Pernambuco, inclusive, o Consórcio Grande Recife.

3 – Modificações em relação à Versão Anterior

3.1 – Diante do fato de ser a primeira versão da Instrução Normativa, tal item não se aplica.

4 – Referenciais Teóricos, Normativos e Legais

4.1 – Decreto Estadual 49.914/2020 – Política Estadual de Segurança da Informação do Poder Executivo Estadual – PESI.

4.2 – Norma Técnica ATI-SGR-PR/0001:24 – Resolução 001/2024 – Política de Segurança da Informação – ATI.

4.3 - Modelo de Política de Segurança da Informação (PPSI) – Versão 1.0 – Ministério da Gestão e Inovação – MGI.

4.4 – Lei Federal 13.709/2018 – Lei Geral de Proteção de Dados – LGPD.

5 – Contextualização

5.1 – A utilização da Tecnologia da Informação no Consórcio Grande Recife envolve amplo acervo de recursos computacionais, informações e dados pessoais que necessitam estar permanentemente protegidos contra perda da confidencialidade, integridade e disponibilidade.

5.2 – Neste contexto, torna-se essencial a definição e implantação de um instrumento normativo composto por uma Política de Segurança da Informação - PSI que estabeleça diretrizes gerais para a implantação de normas, regras, padrões e requisitos mínimos, sob diversos aspectos que envolvem direta e indiretamente, a manipulação, o trânsito e a guarda do acervo de informações e dados pessoais que se utilizam da sua infraestrutura de tecnologia no âmbito do CTM.

5.3 - Esta Política tem como objetivo expressar, pública e formalmente, as preocupações do CTM com a informação e os dados pessoais, norteando e proporcionando subsídios e condições que assegurem níveis mínimos adequados de integridade, confidencialidade e disponibilidade, englobando não apenas os requisitos de segurança lógica, mas, também, os de segurança física e de pessoal nos ambientes computacionais.

6 – Escopo da Política

6.1 – A presente Instrução Normativa institui a Política de Segurança da Informação (PSI), no âmbito do CTM, com a finalidade de estabelecer princípios e diretrizes para a implementação de ações e controles que garantam a segurança das informações e de dados pessoais, e no que couber, no relacionamento com outras entidades públicas ou privadas.

6.2 - Esta Política se aplica a todos os ativos de informação do CTM, incluindo dados, sistemas, aplicativos, dispositivos e redes. A Política se aplica a todos os colaboradores, empregados, comissionados, terceirizados, estagiários e Jovens Aprendizes que acessam ou processam as informações do Consórcio, ou ainda, ou por qualquer pessoa e ou empresa que venha a ter acesso a dados ou informações e em qualquer meio ou suporte.

6.3 - Esta política se aplica em todas as instalações físicas administradas ou utilizadas pelo CTM, em caráter temporário ou permanente.

6.4 – A PSI dá ciência a todos os colaboradores e parceiros do CTM de que os ambientes, sistemas, computadores e redes do órgão poderão ser monitorados e gravados conforme previsto nas leis brasileiras.

7 – Normas Gerais

7.1 – São **objetivos específicos** da Política de Segurança da Informação do CTM:

7.1.1 - Estabelecer princípios e diretrizes a fim de proteger ativos de informação e conhecimentos gerados ou recebidos;

7.1.2. - Estabelecer orientações gerais de segurança da informação e, desta forma, contribuir para a gestão eficiente dos riscos, limitando-os a níveis aceitáveis, bem como preservar os princípios da disponibilidade, integridade, confiabilidade e autenticidade das informações;

7.1.3 - Estabelecer competências e responsabilidades quanto à segurança da informação;

7.1.4 - Nortear a elaboração das normas necessárias à efetiva implementação da segurança da informação;

7.1.5 - Promover o alinhamento das ações de segurança da informação com as estratégias de planejamento organizacional do CTM.

7.2 – Princípios e Diretrizes:

7.2.1 - As ações de segurança da informação do CTM são norteadas pelos princípios constitucionais e administrativos que regem a Administração Pública, assim como pelos seguintes princípios:

7.2.1.1 - Disponibilidade, integridade, confidencialidade e autenticidade das informações;

7.2.1.2 - Continuidade dos processos e serviços essenciais para o funcionamento do CTM;

7.2.1.3 – Racionalidade e economicidade da proteção dos ativos de informação;

7.2.1.4 - Respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

7.2.1.5 - Observância da publicidade como preceito geral e do sigilo como exceção;

7.2.1.6 - Responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

7.2.1.7 - Alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico do CTM, além do Plano Diretor de Tecnologia da Informação e Comunicação, assim como demais normas específicas de segurança da informação;

7.2.1.8 - Conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis;

7.2.1.9 - Educação e comunicação como alicerces fundamentais para o fomento da cultura e segurança da informação.

7.2.1.10 - Todos os mecanismos de proteção utilizados para a segurança da informação devem ser mantidos para preservar a continuidade do negócio.

7.2.1.11 - Toda informação gerada pelos colaboradores, utilizando integralmente ou parcialmente recursos do CTM, é de propriedade do órgão.

7.2.1.12 - O acesso às informações, produzidas ou recebidas pelo CTM, deve ser limitado às atribuições necessárias ao desempenho das respectivas atividades dos usuários internos.

7.2.1.13 - Os processos de aquisição ou contratação de bens e serviços de tecnologia da informação e comunicação, a qualquer título, devem refletir esta PSI, sem prejuízo da observância da legislação em vigor.

7.2.1.14 - Os equipamentos de informática e comunicação, sistemas e informações deverão ser utilizados para a realização das atividades profissionais de seus colaboradores.

7.2.2 - Estas diretrizes constituem os principais pilares da gestão de segurança da informação norteando a elaboração de políticas, planos e normas complementares no âmbito do CTM e objetivam a garantia dos princípios básicos de segurança da informação estabelecidos nesta Política.

7.2.3 - As normas, procedimentos, manuais e metodologias de segurança da informação do CTM devem considerar, como referência, além da normatização e legislação vigentes, as melhores práticas de segurança da informação.

7.2.4 - Os colaboradores devem evitar a circulação das informações e/ou mídias consideradas confidenciais e/ou restritas e/ou que possuam dado pessoal, como também não deixar documentos com dados pessoais, relatórios nas impressoras, e mídias em locais de fácil acesso, tendo sempre em mente

o conceito “mesa limpa”, ou seja, ao terminar o trabalho não deixar nenhum documento com dado pessoal, relatório e/ou mídia confidencial e/ou restrito sobre suas mesas.

7.2.5 - Esta política de Segurança da Informação pode ser revisada periodicamente e eventualmente revista sempre que eventos ou fatos relevantes ocorram.

7.3 - **As ações de segurança da informação** devem:

7.3.1 - Considerar, prioritariamente, os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do CTM;

7.3.2 - Ser tratadas de forma integrada, respeitando as especificidades e a autonomia das unidades do CTM;

7.3.3 - Ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, considerados o ambiente, o valor e a criticidade da informação;

7.3.4 - Visar à prevenção da ocorrência de incidentes.

7.4 – Normas Gerais

7.4.1 - O investimento necessário em medidas de segurança da informação deve ser dimensionado segundo o valor do ativo a ser protegido e de acordo com o risco de potenciais prejuízos ao CTM.

7.4.2 - Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no CTM compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

7.4.2.1 - As informações citadas no item 7.4.2 (anterior), que tramitem pelo ambiente computacional do CTM, são passíveis de monitoramento e auditoria pelo CTM, respeitados os limites legais.

7.4.3 - As pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa.

7.4.3.1 - É condição para acesso aos recursos de tecnologia da informação do CTM a assinatura, preferencialmente eletrônica, de Termo de Responsabilidade indicando a ciência aos termos desta Política, bem como as responsabilidades e os compromissos em decorrentes desse acesso, além das penalidades cabíveis pela inobservância das regras previstas nas normas de segurança da informação do CTM.

7.4.4 - A Política de Segurança da Informação e suas atualizações, bem como normas específicas de segurança da informação do CTM, devem ser divulgadas amplamente a todos os Usuários de Informação, conforme definido por portaria que regulamenta a implementação das Instruções Normativas, a fim de promover sua observância, seu conhecimento, bem como a formação da cultura de segurança da informação.

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

7.4.4.2 - As ações de capacitação previstas no item 7.4.4.1 (anterior) devem ser conduzidas de modo a possibilitar o compartilhamento de materiais educacionais sobre segurança da informação.

7.4.5 - Todos os contratos de prestação de serviços firmados pelo CTM conterão cláusula específica sobre a obrigatoriedade de atendimento a esta Política de Segurança da Informação, bem como às normas dela decorrentes.

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

7.4.7 - A Gestão da Segurança da Informação é constituída, no mínimo, pelos seguintes processos:

a) Tratamento da informação;

b) Segurança física e do ambiente;

c) Gestão de incidentes em segurança da informação;

d) Gestão de ativos;

e) Gestão do uso dos recursos de tecnologia e de comunicações, tais como e-mail, acesso à internet, mídias sociais e computação em nuvem;

f) Controles de acesso;

g) Gestão de riscos;

h) Gestão de continuidade;

i) Auditoria e conformidade.

7.4.8 - Para cada um dos processos que constituem a Gestão de Segurança da Informação, deve ser observada a pertinência de elaboração de políticas, normas, procedimentos, orientações ou manuais que disciplinem ou facilitem o seu entendimento em conformidade com a legislação vigente e boas práticas de segurança de informação.

7.4.9 - As políticas, normas, procedimentos, orientações ou manuais de que trata o item 7.4.8 (anterior) devem abordar, no mínimo, aspectos relacionados:

7.4.9.1 - A conformidade com as diretrizes dispostas na LGPD e demais normativos e orientações emitidas pela ANPD;

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

7.4.9.3 - A proteção dos dados contra acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito;

7.4.9.4 - O uso aceitável da informação e a utilização de mídias de armazenamento;

7.4.9.5 - A entrada e saída de ativos de informação das instalações da organização;

7.4.9.6 - Os controles de acesso baseados no princípio do menor privilégio;

7.4.9.7 - O Plano de Gestão de Incidentes de Segurança, de forma a considerar diferentes cenários;

7.4.9.8 - A Política de Gestão de Ativos da organização, abordando aspectos relacionados à proteção dos ativos, sua classificação de acordo com a criticidade do ativo para o a organização;

7.4.9.9 - A manutenção de inventário atualizado de ativos da organização, contendo o tipo de ativo, sua localização, seu proprietário ou custodiante e seu status de segurança;

7.4.9.10 - O mapeamento de vulnerabilidades, ameaças e suas respectivas interdependências;

7.4.9.11 - O monitoramento de ativos, de acordo com os princípios legais de Segurança da Informação e privacidade; a investigação de sua operação e uso quando houver indícios de quebra de segurança e/ou privacidade;

7.4.9.12 - A utilização adequada dos recursos operacionais e de comunicações fornecidos pelo CTM, a serem utilizados para fins profissionais, relacionados às atividades do órgão, em conformidade com os princípios éticos e profissionais.

7.4.9.13 Os procedimentos para o uso de e-mail, o envio de informações confidenciais, a instalação de software antivírus e a abertura de anexos de e-mail;

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

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

7.4.9.16 - As políticas e procedimentos para o controle de acesso, tais como o uso de Múltiplo Fator de Autenticação (MFA), controles de autorização, baseados no princípio do menor privilégio, controles de segregação de funções, trilhas de auditoria, rastreamento, acompanhamento, controle e verificação de acessos para os ativos de informação, desligamento ou afastamento de colaboradores e parceiros que utilizam ou operam os ativos de informação do CTM;

7.4.9.17 - As políticas e procedimentos para a gestão dos riscos de segurança da informação que possam afetar seus ativos de informação, abordando a análise do ambiente do CTM, dos seus ativos de informação e das ameaças à segurança da informação;

7.4.9.18 - As políticas e procedimentos para Gestão de Continuidade de Negócios da organização, incluindo o Plano de Continuidade para garantir que o CTM possa continuar suas atividades em caso de um incidente de segurança da informação e a realização de testes e exercícios periódicos baseados no Plano de Continuidade para garantir sua eficácia;

7.4.9.19 - As políticas e procedimentos para a Gestão de Mudanças nos ativos de informação da organização, respaldado pelas informações dos relatórios de avaliação e tratamento de risco de segurança da informação, com a designação de papéis e responsabilidades para a avaliação, aprovação e implementação de mudanças e a criação de um processo formal para solicitação e documentação de mudanças;

7.4.9.20 - As políticas e procedimentos para a auditoria e conformidade da organização, abordando o Plano de Verificação de Conformidade, que considere as unidades abrangidas, os aspectos para verificação da conformidade, as ações e atividades a serem realizadas, os documentos necessários para a fundamentação da verificação de conformidade e as responsabilidades e o Relatório de Avaliação de Conformidade, que considere o detalhamento das ações e das atividades com identificação do responsável, o parecer de conformidade e as recomendações.

7.4.10 - Todas as ações, realizadas pelas unidades do CTM, que envolvem a segurança da informação devem estar em conformidade com as leis e regulamentos aplicáveis a esta temática.

7.4.11 - As atividades, os produtos e os serviços desenvolvidos no CTM devem estar em conformidade com requisitos de privacidade e proteção de dados pessoais constantes em leis, regulamentos, resoluções, normas, estatutos e contratos jurídicos vigentes.

7.5 – Estrutura de Gestão da Segurança da Informação

7.5.1 - A estrutura de Gestão de Segurança da Informação é composta por:

a) Alta Administração (Diretor-Presidente e demais Diretores);

b) Comitê de Segurança da Informação;

c) Gestor de Segurança da Informação;

d) Encarregado pelo Tratamento de Dados Pessoais (DPO);

e) Assessor Especial de Controle Interno;

f) Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos;

g) Usuários de Informação.

7.5.2 – O Comitê de Segurança da Informação será criado por portaria da Presidência do CTM, e será composto por um integrante de cada diretoria, com exceção da DTI, que contará com a participação do Coordenador de Tecnologia da Informação e Inovação e do Gerente da GSIT, sob a condução do Gestor de Segurança da Informação.

7.5.3 - O Gestor de Segurança da Informação do CTM será designado em Portaria da Presidência do órgão, de acordo com a legislação vigente.

7.5.4 – A Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos será composta por profissionais com conhecimento especializado no tema, por definição do gerente da GSIT.

7.5.5 – Os Usuários da Informação são todos os empregados, comissionados, terceirizados, estagiários e jovens aprendizes, que têm acesso ao ambiente computacional e seus dados e informações, seja de forma temporária, seja de forma contínua.

8 – Considerações Finais

8.1 - É vedada a utilização dos recursos de tecnologia da informação disponibilizados pelo CTM para acesso, guarda e divulgação de material incompatível com ambiente do serviço, que viole direitos autorais ou que infrinja a legislação vigente.

8.2 - São vedados o uso e a instalação de recursos de tecnologia da informação que não tenham sido homologados ou adquiridos pelo CTM.

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

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

8.5 - As unidades organizacionais do CTM devem promover ações de treinamento e conscientização para que os seus colaboradores entendam suas responsabilidades e procedimentos voltados à segurança da informação e à proteção de dados.

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

8.7 - As denúncias de violação a esta Política podem ser comunicadas ao Gestor de Segurança da Informação e feitas através dos seguintes canais: SEI ou Expresso.

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

8.9 - Esta Política será revisada periodicamente, pelo menos a cada dois anos, ou com mais frequência se necessário, para refletir as mudanças no ambiente do CTM, nos riscos à segurança da informação e nas melhores práticas de segurança da informação.

8.10 - Os casos omissos e as dúvidas sobre a Política de Segurança da Informação e seus documentos devem ser submetidos ao Comitê de Segurança da Informação.

9 – Responsabilidades

9.1 - Alta Administração – Diretor-Presidente e demais Diretores:

9.1.1 - Fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do CTM, bem como com o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados.

9.1.2 - Aprovar a Política de Segurança da Informação do CTM, bem como suas alterações e atualizações, em última instância.

9.2 - Comitê de Segurança da Informação:

9.2.1 - Aprovar a Política de Segurança da Informação do CTM, bem como suas alterações e atualizações, em primeira instância;

9.2.2 - Assessorar na implementação das ações de segurança da informação;

9.2.3 - Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação;

9.2.4 - Participar da elaboração da Política de Segurança da Informação e das normas internas de segurança da informação;

9.2.5 - Propor alterações à Política de Segurança da Informação e às normas internas de segurança da informação;

9.2.6 – Opinar e sugerir sobre normas internas de segurança da informação;

9.2.7 - Avaliar as ações propostas pelo gestor de segurança da informação.

9.3 - Gestor de Segurança da Informação:

9.3.1 - Coordenar o Comitê de Segurança da Informação;

9.3.2 - Coordenar a elaboração da Política de Segurança da Informação - PSI e das normas internas de segurança da informação do órgão, observadas a legislação vigente e as melhores práticas sobre o tema;

9.3.3 - Assessorar a Alta Administração na implementação da Política de Segurança da Informação;

9.3.4 - Estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à segurança da informação;

9.3.5 - Promover a divulgação da política e das normas internas de segurança da informação do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no órgão;

9.3.6 - Incentivar estudos de novas tecnologias, e seus eventuais impactos relacionados à segurança da informação;

9.3.7 - Propor recursos necessários às ações de segurança da informação;

9.3.8 - Acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos;

9.3.9 - Verificar os resultados dos trabalhos de auditoria sobre a gestão da segurança da informação;

9.3.10 - Acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da segurança da informação;

9.4 - Encarregado pelo Tratamento dos Dados Pessoais (DPO):

9.4.1 - Dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709/2018 (Lei Geral de Proteção de Dados - LGPD) e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados (ANPD), conduzir o diagnóstico de privacidade, bem como orientar, no que couber, os gestores proprietários dos ativos de informação, responsáveis pelo planejamento, implementação e melhoria contínua dos controles de privacidade em ativos de informação que realizem o tratamento de dados pessoais ou dados pessoais sensíveis.

9.5 – Assessor Especial de Controle Interno:

9.5.1 - Dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista perante a Segurança da Informação do CTM.

9.6 - Equipe de Prevenção, Tratamento e Respostas a Incidentes Cibernéticos:

9.6.1 - Facilitar, coordenar e executar as atividades de prevenção, tratamento e resposta a incidentes cibernéticos no CTM;

9.6.2 - Monitorar as redes computacionais;

9.6.3 - Detectar e analisar ataques e intrusões;

9.6.4 - Tratar incidentes de segurança da informação;

9.6.5 - Identificar vulnerabilidades e artefatos maliciosos;

9.6.6 - Recuperar sistemas de informação;

9.6.7 - Promover a cooperação com outras equipes, e participar de fóruns e redes relativas à segurança da informação.

9.7 - Usuários de Informação:

9.7.1 - Conhecer, cumprir e fazer cumprir esta Política e as demais normas específicas de segurança da informação do CTM.

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