POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

(PSI)

Prefeito Municipal
José Pessoa Leal

Presidente do IPMT
Kennedy Glauber Carvalho Leite

Diretor Administrativo e Financeiro
Ricardo Coelho Pereira

Diretor de Previdência Social
Edelman Medeiros Barbosa Santos

Diretor de Investimentos
José Ribamar Veloso Junior

Gerência de Tecnologia da Informação
Artur Luís da Conceição Silva

Teresina (PI)
maio / 2024

HISTÓRICO DE VERSIONAMENTO

Título	POLÍTICA DE SEGURANÇA DA INFORMAÇÃO
Número de Versão	2.0
Status	REVISÃO
Motivo	ADEQUAÇÃO AO PRÓ-GESTÃO
Autoria	GERÊNCIA DE T.I.
Pré-Aprovação	CONTROLADORIA
Data de Aprovação	30/04/2024
Instrumento de Homologação	PRÉ-APROVAÇÃO
Aprovação	CONSELHO ADMINISTRATIVO
Data de Aprovação	07/05/2024
Instrumento de Homologação	ATA DA REUNIÃO ORDINÁRIA DO CONSELHO DE ADMINISTRAÇÃO

Sumário

1 - INTRODUÇÃO

A Política de Segurança da Informação (PSI) tem por objetivo a instituição de diretrizes estratégicas que visam garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações, bem como atitudes adequadas para manuseio, tratamento, controle e proteção dos dados, informações, documentos e conhecimentos produzidos, armazenados, sob guarda ou transmitidos por qualquer meio ou recurso do Instituto de Previdência dos Servidores Municipais de Teresina - IPMT contra ameaças e vulnerabilidades. Desse modo, a Política busca preservar os seus ativos de informação, assim como a sua imagem institucional.

O propósito da Política é orientar o IPMT no que diz respeito à gestão de riscos e ao tratamento de incidentes de Segurança da Informação (SIN), em conformidade com as disposições constitucionais, legais e regimentais vigentes.

A PSI estabelece o comprometimento da alta direção organizacional do Instituto, com vistas a prover apoio para a implantação da Gestão dos Riscos de Segurança da Informação (GRSIN).

Esta PSI aplica-se a Sede do IPMT, sendo de responsabilidade de todos os servidores, colaboradores internos ou externos, devendo ser dado amplo conhecimento de seu teor a todas as pessoas ou organizações que utilizam os meios físicos ou lógicos do IPMT, por serem todos responsáveis por garantir a segurança das informações a que tenham acesso.

2 – CONCEITOS E DEFINIÇÕES

Para os efeitos desta PSI, são estabelecidos os seguintes conceitos e definições:

- **Acesso**: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a acessibilidade de usar os ativos de informação de um órgão ou entidade;
- **Ameaça**: qualquer evento que explore vulnerabilidades ou seja causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
- **Análise de Riscos**: uso sistemático de informações para identificar fontes e avaliar riscos;
- **Análise/Avaliação de Riscos**: processo completo de análise e avaliação de riscos;
- **Atividade**: processo ou conjunto de processos executados por um órgão ou entidade, ou em seu nome, que produzem ou suportem um ou mais produtos ou serviços;
- **Ativo**: qualquer componente (seja humano, tecnológico, software ou outros) que sustente uma ou mais atividades e que tenha valor para a organização;
- **Ativos de Informação**: os meios de armazenamento, transmissão e processamento; os sistemas de informação; além das informações em si, bem como os locais em que se encontram esses meios e as pessoas que têm acesso a eles;
- **Autenticidade**: propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, ou por um determinado sistema, órgão ou entidade;
- **Avaliação de Riscos**: processo de comparar o risco estimado com critérios predefinidos para determinar a importância do risco;
- **Celeridade**: as ações de segurança da informação devem oferecer respostas rápidas a incidentes e falhas;
- **Classificação da Informação**: identificação dos níveis de proteção que as informações demandam; atribuição de classes e formas de identificação, além de determinação dos controles de proteção necessários a cada uma delas;
- **Comunicação do Risco**: troca ou compartilhamento de informação sobre o risco entre o tomador de decisão e outras partes interessadas;
- **Confidencialidade**: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado ou não credenciado;
- **Controle de Acesso**: conjunto de procedimentos, recursos e meios utilizados com a finalidade de conceder ou bloquear o acesso;
- **Custodiante do Ativo de Informação**: é aquele que, de alguma forma, zela pelo armazenamento, operação, administração e preservação de ativos de informação que não lhe pertencem, mas que estão sob sua custódia;
- **Desastre**: evento repentino e não planejado que causa perda para toda ou parte da organização, com sérios impactos em sua capacidade de prestar serviços essenciais

ou críticos, por um período superior ao prazo de recuperação;

- **Descarte**: eliminação correta de informações, documentos, mídias e acervos digitais;
- **Disponibilidade**: propriedade de que a informação esteja acessível e utilizável sob demanda por uma pessoa física ou determinado sistema, órgão ou entidade;
- **Estimativa de Riscos**: processo utilizado para atribuir valores à probabilidade e consequências de determinado risco;
- **Eficácia**: realização de um trabalho que atinja os resultados esperados;
- **Eficiência**: realização de um trabalho, com presteza, agilidade e eficácia;
- **Ética**: preservação dos direitos dos agentes públicos, sem comprometimento da Segurança da Informação;
- **Evento de Segurança da Informação**: ocorrência identificada de procedimento, sistema, serviço ou rede que indica possível perda de controle ou violação da política de segurança da informação, ou situação desconhecida que possa ser relevante para a segurança da informação;
- **Gerenciamento de Operações**: atividades, processos, procedimentos e recursos que visam disponibilizar e manter serviços, sistemas e infraestrutura que os suportem;
- **Gestão de Ativos**: processo de identificação dos ativos e de definição de responsabilidades pela manutenção apropriada de seu controle;
- **Gestão de Continuidade dos Negócios**: processo de gestão que identifica ameaças potenciais para uma organização, bem como os possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. Esse processo prevê a definição de estrutura para o aprimoramento da resiliência organizacional, de modo a se responder efetivamente às ameaças e salvaguardar os interesses das partes interessadas, a reputação e a marca da organização, assim como suas atividades de valor agregado;
- **Gestão de Riscos de Segurança da Informação**: conjunto de processos que permitem identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os seus ativos de informação, e equilibrá-los com os custos operacionais e financeiros envolvidos;
- **Gestão de Segurança da Informação**: ações e métodos que visam à integração das atividades de gestão de riscos, gestão de continuidade do negócio, tratamento de incidentes, tratamento da informação, conformidade, credenciamento, segurança cibernética, segurança física, segurança lógica, segurança orgânica e segurança organizacional aos processos institucionais estratégicos, operacionais e táticos, não se limitando, portanto, no âmbito da tecnologia da informação e comunicações;
- **Gestor de Segurança da Informação**: é o servidor público responsável pelas ações de segurança da informação do IPMT ;
- **Identificação de Riscos**: processo para localizar, listar e caracterizar elementos do risco;
- **Incidente de SIN**: evento adverso, confirmado ou sob suspeita, relacionado à segurança de sistemas de computação ou de redes de computadores;
- **Informação**: conjunto de dados, textos, imagens, métodos, sistemas ou quaisquer

formas de representação dotadas de significado em determinado contexto, independentemente do suporte em que resida ou da forma pela qual seja veiculado;

- **Integridade**: propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;
- **Política de Segurança da Informação**: documento aprovado pela autoridade responsável do IPMT, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
- **Proprietário de Ativos de Informação**: unidade administrativa responsável por gerenciar determinado segmento de informação e todos os ativos relacionados;
- **Quebra de Segurança**: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação;
- **Recursos Criptográficos**: sistemas, programas, processos e equipamentos, isolados ou em rede, que utilizam algoritmo simétrico ou assimétrico, para realizar a cifração ou decifração de informações;
- **Resiliência**: poder de recuperação ou capacidade de uma organização resistir aos efeitos de um desastre;
- **Responsabilidade**: dever dos agentes públicos em conhecer e respeitar todas as normas de segurança da informação da respectiva instituição;
- **Risco de SIN**: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;
- **Segurança Física e do Ambiente**: processo referente à proteção de todos os ativos físicos da instituição, englobando instalações físicas, internas e externas, em todas as localidades em que a organização estiver presente;
- **Sistema Estruturante**: conjunto de sistemas informáticos fundamentais e imprescindíveis para a consecução das atividades administrativas, de forma eficaz e eficiente;
- **Terceiros**: quaisquer pessoas, físicas ou jurídicas, de natureza pública ou privada, externos ao IPMT;
- **Transferir Risco**: forma de tratamento de risco na qual a alta administração decide realizar a atividade, compartilhando com outra entidade o ônus associado a um risco;
- **Tratamento da Informação**: conjunto de ações referentes à recepção, produção, reprodução, utilização, acesso, transporte, transmissão, distribuição, armazenamento, eliminação e controle da informação;
- **Tratamento de Incidentes**: processo que consiste em receber, filtrar, classificar e responder às solicitações e alertas, bem como realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e a identificação de tendências potenciais futuras;
- **Tratamento dos Riscos**: processo e implementação de ações de segurança da informação, com o objetivo de evitar, reduzir, reter ou transferir um risco;
- **Usuário**: agente público que obteve autorização do responsável pela área interessada

para acesso aos ativos de informação;

- **Vulnerabilidade**: conjunto de fatores internos ou causas potenciais de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais devem ser evitados por ação interna de segurança da informação.

3 – REFERÊNCIAS LEGAIS E NORMATIVAS

- **Lei 8.159, de 8 de janeiro de 1991**: dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;
- **Lei nº 9.983, de 14 de julho de 2000**: dispõe sobre a responsabilidade administrativa, civil e criminal de usuários que cometam irregularidades em razão do acesso a dados, informações e sistemas informatizados da Administração Pública;
- **Lei nº 12.527, de 18 de novembro de 2011**: regulamenta o acesso às informações públicas;
- **Decreto nº 3.505, de 13 de junho de 2000**: institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;
- **Decreto nº 5.482, de 30 de junho de 2005**: dispõe sobre a divulgação de dados e informações pelos órgãos e entidades da Administração Pública Federal, por meio da Rede Mundial de Computadores – Internet;
- **Decreto nº 7.845, de 14 de novembro de 2012**: regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;
- **Decreto Nº 8.638, de 15 de janeiro de 2016**: institui a Estratégia de Governança Digital; h) Norma ABNT NBR ISO/IEC 27001:2013: estabelece os elementos de um Sistema de Gestão de Segurança da Informação e Comunicações;
- **Norma ABNT NBR ISO/IEC 27002:2013**: institui o código de melhores práticas para Gestão de Segurança da Informação e da Comunicação;
- **Norma ABNT NBR ISO/IEC 27005:2011**: estabelece diretrizes para o processo de gestão de riscos de segurança da informação.

4 – PRINCÍPIOS

Esta Política de Segurança da Informação e suas ações serão norteadas pelos seguintes princípios:

- **Celeridade**: as ações de SIN devem oferecer respostas rápidas a incidentes e falhas de segurança;
- **Ética**: os direitos e interesses legítimos dos usuários e agentes públicos devem ser preservados, sem comprometimento da SIN;
- **Clareza**: as regras de segurança dos ativos de SIN devem ser precisas, concisas e de fácil entendimento;
- **Legalidade**: as ações de segurança devem respeitar as atribuições regimentais, bem como as leis, normas e políticas organizacionais, administrativas, técnicas e operacionais do IPMT;
- **Publicidade**: transparência no trato da informação, observados os critérios legais.

5 – DIRETRIZES GERAIS

As diretrizes de segurança da informação estabelecidas nesta PSI aplicam-se às informações armazenadas, acessadas, produzidas e transmitidas pelo IPMT, e que devem ser seguidas pelos usuários, incumbindo a todos a responsabilidade e o comprometimento com sua aplicação.

Independentemente da forma ou do meio pelo qual a informação seja apresentada ou compartilhada, deverá ser sempre protegida adequadamente, de acordo com esta Política.

Os recursos de Tecnologia da Informação (TI) disponibilizados pelo IPMT serão utilizados estritamente para propósito institucional.

É vedado a qualquer usuário do IPMT o uso dos recursos de Tecnologia da Informação para fins pessoais (próprios ou de terceiros), entretenimento, veiculação de opiniões político-partidárias, bem como para perpetrar ações que, de qualquer modo, possam constranger, assediar, ofender, caluniar, ameaçar, violar direito autoral ou causar prejuízos a qualquer pessoa física ou jurídica, assim como aquelas que atentem contra a moral e a ética, ou que prejudiquem o cidadão ou a imagem da instituição, comprometendo a integridade, a confidencialidade, a confiabilidade, autenticidade ou a disponibilidade das informações.

As diretrizes desta PSI constituem os principais pilares da Gestão de Segurança da Informação do IPMT, sendo norteadoras da elaboração das normas de SIC.

Os casos omissos e as dúvidas decorrentes da aplicação do disposto nesta PSI, devem ser direcionados a Gerência de Tecnologia da Informação (GTI).

6 – DIRETRIZES ESPECÍFICAS

6.1 – GESTÃO DA SEGURANÇA DA INFORMAÇÃO (GESIN)

Todos os mecanismos de proteção utilizados para a SIN devem ser mantidos com o objetivo de garantir a continuidade dos negócios do IPMT.

As medidas de proteção devem ser planejadas e os gastos da aplicação de controles devem ser compatíveis com o valor do ativo protegido.

Os requisitos de segurança da informação e comunicações do IPMT devem ser explicitamente citados em todos os termos de compromisso celebrados entre a instituição e terceiros, por meio de cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta Política, devendo também ser exigido termo de confidencialidade.

6.2 – GESTÃO DE TRATAMENTO DE INCIDENTES DE SEGURANÇA EM REDE COMPUTACIONAL (GETIR)

A Gerência de TI (GTI) deverá criar e manter Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR), com a responsabilidade de receber, analisar e responder notificações e atividades relacionadas a incidentes de segurança em redes de computadores.

Os eventos e incidentes de SIN devem ser comunicados, registrados e tratados de acordo com um Plano de Gerenciamento de Incidentes específico.

6.3 – GESTÃO DE RISCOS E SEGURANÇA DA INFORMAÇÃO (GRSIN)

A GRSIN é um conjunto de processos que permite identificar e implementar as medidas de proteção necessárias para minimizar ou eliminar os riscos a que estão sujeitos os ativos de informação do IPMT, e equilibrá-los com os custos operacionais e financeiros envolvidos.

As áreas responsáveis por ativos de informação deverão implementar processo contínuo de Gestão de Riscos, que será aplicado na implementação e operação da GRSIN.

A GRSIN deve ser implementada no âmbito do IPMT, visando identificar os ativos relevantes e determinar ações de gestão apropriadas, devendo ser atualizada periodicamente, no mínimo 01 (uma) vez por ano, ou oportunamente, em função de inventários de ativos, mudanças, ameaças ou vulnerabilidades. Trata-se de instrumento do programa de Gestão de Riscos que deve incluir um Plano de Continuidade de Negócios (PCN) e um Plano de Gerenciamento de Incidentes (PGI).

O Plano de Continuidade de Negócios deverá complementar a análise de riscos, visando limitar os impactos do incidente e garantir que as informações requeridas para os processos do negócio estejam prontamente disponíveis.

O Plano de Gerenciamento de Incidentes definirá responsabilidades e procedimentos para assegurar respostas rápidas, efetivas e ordenadas perante incidentes de SIN.

6.4 – Gestão de Continuidade de Negócios (GECON)

A GECON é um processo abrangente de gestão que identifica ameaças potenciais aos ativos de informação do IPMT, assim como possíveis impactos nas operações de negócio, caso essas ameaças se concretizem. A GECON, portanto, prevê a definição de uma estrutura para que se aprimore a resiliência organizacional, com vistas a responder efetivamente aos incidentes de SIN e minimizar os impactos decorrentes de falhas, desastres ou indisponibilidades significativas sobre as atividades do IPMT, além de recuperar perdas de ativos de informação.

As áreas do IPMT deverão manter processo de GECON, de modo a não permitir que os negócios baseados em Tecnologia da Informação sejam interrompidos, e assegurar a sua retomada em tempo hábil, quando for o caso.

A resiliência contra possíveis interrupções na capacidade de atingir os principais objetivos institucionais deve ser prática proativa de todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional do IPMT.

Todas as áreas do IPMT que dependam de recursos de Tecnologia da Informação deverão elaborar, com o apoio da GTI, Planos de Gerenciamento de Incidentes, de acordo com o grau de probabilidade de ocorrência de eventos ou sinistros, bem como estabelecer um conjunto de estratégias e procedimentos que deverá ser adotado em situações que comprometam o andamento normal dos processos e a consequente prestação dos serviços.

As medidas constantes do Plano de Gerenciamento de Incidentes deverão assegurar a disponibilidade dos ativos de informação e a recuperação de atividades críticas à normalidade, com o objetivo de minimizar o impacto de situações inesperadas, desastres, falhas de segurança, entre outras, até que se retorne à normalidade.

6.5 – Gestão de Ativos de Informação

A gestão de ativos de informação do IPMT deverá observar normas operacionais e procedimentos específicos para garantir a sua operação segura e contínua.

Os ativos de informação do Instituto deverão ser inventariados, com a classificação em termos de valor, requisitos legais, sensibilidade e criticidade da informação para o IPMT, e

serão atribuídos aos respectivos responsáveis. Seu uso deverá estar em conformidade com os princípios e normas operacionais de SIN, sendo destinados exclusivamente ao uso institucional, vedada a utilização para fins em desconformidade com os interesses do IPMT.

O usuário deve ter acesso apenas aos ativos necessários e indispensáveis ao seu trabalho, respeitando as recomendações de sigilo, conforme disposto em normas e legislação específica de classificação de informação.

É vedado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo IPMT.

6.6 – Tratamento da Informação

A informação deve ser protegida de forma preventiva, com o objetivo de minimizar riscos às atividades e serviços do IPMT. Essa proteção deve ser de acordo com o valor, sensibilidade e criticidade da informação, devendo ser desenvolvido, para este fim, sistema de classificação da informação. Os dados, as informações e os sistemas de informação do IPMT devem ser protegidos contra ameaças e ações não autorizadas, acidentais ou não, de modo a reduzir riscos e garantir a disponibilidade, integridade, confidencialidade e autenticidade desses bens.

6.7 – Classificação da Informação

Toda informação criada, manuseada, armazenada, transportada ou descartada do IPMT será classificada de acordo com a Lei nº 12.527, de 18 de novembro 2011.

O usuário deverá ser capaz de identificar a classificação atribuída a uma informação tratada pelo IPMT e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

As informações sob gestão do IPMT devem dispor de segurança, de maneira a serem adequadamente protegidas quanto ao acesso e uso. Para aquelas consideradas de alta criticidade, serão necessárias medidas especiais de tratamento, com o objetivo de limitar a exploração de informações exclusivas da instituição.

6.8 – Monitoramento, Auditoria e Conformidade

O monitoramento, auditoria e conformidade de ativos de informações observarão o seguinte:

a) O uso dos recursos de tecnologia da informação disponibilizados pelo IPMT é passível de monitoramento e auditoria, devendo ser implementados e mantidos, à medida do possível, mecanismos que permitam a sua rastreabilidade;
b) A entrada e saída de ativos de informação do IPMT deverá ser registrada e autorizada por autoridade competente mediante procedimento formal;
c) A GTI deverá manterá registros e procedimentos específicos, tais como trilhas de auditoria e outros que assegurem o rastreamento, acompanhamento, controle e verificação de acessos a todos os sistemas institucionais, à rede interna e à internet;
d) A Ouvidoria do IPMT será responsável por manter canal de comunicação para recebimento de denúncias de infração a qualquer parte desta PSI.

6.9 – Controle de Acesso e Uso de Senhas

As regras de controle de acesso a todos os sistemas institucionais, intranet, internet, informações, dados e às instalações físicas do IPMT deverão ser definidas e regulamentadas, por meio de normas internas, com o objetivo de garantir a segurança dos usuários e a proteção dos ativos da instituição.

6.10 – Uso de E-mail

O correio eletrônico é um recurso de comunicação institucional do IPMT e as regras de acesso e utilização do e-mail devem atender a todas as orientações desta PSI e das normas específicas, além das demais diretrizes da Prefeitura Municipal de Teresina (PI).

6.11 – Acesso à Internet

O acesso à rede mundial de computadores (internet), no ambiente de trabalho, deve ser regido por normas e procedimentos específicos, atendendo às determinações desta PSI, e demais orientações governamentais e legislação em vigor.

6.12 – Uso das Redes Sociais

A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgando ou compartilhando informações do IPMT, deve ser regida por normas internas especificas e deve estar em consonância tanto com a PSI quanto com os objetivos estratégicos da instituição.

6.13 – Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

As atividades de aquisição, manutenção e desenvolvimento de sistemas de informação devem observar critérios e controles de segurança, com vistas a garantir o respeito aos atributos básicos de segurança da informação.

6.14 – Conscientização, Sensibilização e Capacitação em SIN

O IPMT deverá promover continuamente a capacitação, reciclagem e o aperfeiçoamento de todos os usuários da instituição, por meio de programas de divulgação, sensibilização, conscientização e capacitação em segurança da informação e comunicações, com o propósito de criar uma cultura de segurança dentro da instituição.

6.15 – Plano de Investimento em SIN

Os investimentos em segurança da informação serão realizados de forma planejada e consolidados em um Plano de Investimentos em SIN e, no que couber, no Plano Diretor de Tecnologia da Informação e Comunicação (PDTIC).
O Plano de Investimentos em SIN deverá ser reavaliado quando houver revisão orçamentária ou revisão de prioridades das ações de SIN.

6.16 – Propriedade Intelectual

As informações produzidas por usuários internos e colaboradores, no exercício de suas funções, são patrimônio intelectual do IPMT e não cabe a seus criadores qualquer forma de direito autoral, ressalvado o direito de autoria, quando for o caso.

É vedada a utilização de patrimônio intelectual do IPMT em quaisquer projetos ou atividades de uso diverso do estabelecido pela instituição, salvo autorização específica.

6.17 – Contratos, Convênios, Acordos e Instrumentos Congêneres

Todos os contratos, convênios, acordos e instrumentos congêneres deverão conter cláusulas que estabeleçam a obrigatoriedade de observância desta PSI.

O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta Política, bem como suas normas complementares, aos empregados, prepostos e todos os envolvidos em atividades vinculadas ao IPMT.

6.18 – Uso de Computação em Nuvem

O uso de recursos de Computação em Nuvem, para suprir demandas de transferência e armazenamento de documentos, processamento de dados, aplicações, sistemas e demais tecnologias da informação, deve ser regido por normas específicas, atendendo a determinações desta PSI, e demais orientações governamentais e legislação em vigor, com vistas a garantir a disponibilidade, integridade, confidencialidade e autenticidade das informações armazenadas na nuvem, em especial aquelas sob custódia e gerenciamento de prestador de serviço.

6.19 – Uso de Dispositivos Móveis

As diretrizes gerais de uso de dispositivos móveis para acesso às informações, sistemas, aplicações e e-mails do IPMT devem considerar, prioritariamente, os requisitos legais e a estrutura da instituição, atendendo a esta Política de Segurança da Informação, e devem ser regidas por normas específicas, as quais contemplarão recomendações sobre o uso desses dispositivos.

7 – Penalidades

Ações que violem esta Política ou quaisquer de suas diretrizes, normas ou procedimentos, ou que infrinjam os controles de Segurança da Informação (SIN) serão devidamente apuradas, sendo aplicadas aos responsáveis as sanções penais, administrativas e civis cabíveis.

O usuário responderá disciplinarmente e/ou civilmente pelo prejuízo que vier a ocasionar à instituição, podendo culminar com o seu desligamento e, se aplicáveis, eventuais processos criminais.

8 – Competências e Responsabilidades

8.1 – Conselho Deliberativo do IPMT

- Aprovar a Política de Segurança da Informação (PSI)

8.2 – Diretorias do IPMT

- Dar suporte à promoção da cultura de segurança da informação;
- Aprovar a Política de Segurança da Informação (PSI);
- Aprovar programa orçamentário específico para as ações de SIN, conforme proposto pela Gerência de Tecnologia da Informação (GTI).

8.3 – Presidência do IPMT

- Dar suporte à promoção da cultura de segurança da informação;
- Nomear o Gestor de Segurança da Informação;
- Aplicar ações corretivas e disciplinares cabíveis nos casos de quebra de segurança.

8.4 – Gestor de Segurança da Informação

- Promover e disseminar a cultura de segurança da informação;
- Coordenar a elaboração da Política de Segurança da Informação;
- Instituir e coordenar a Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR);

- Coordenar as ações de segurança da informação;
- Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança e submeter à Presidência do IPMT, após análise da GTI, os resultados consolidados de tais investigações e avaliações;
- Propor recursos necessários às ações de Segurança da Informação;
- Realizar e acompanhar estudos de novas tecnologias, quanto aos possíveis impactos na segurança da informação;
- Propor normas e procedimentos relativos à Segurança da Informação;
- Encaminhar os resultados consolidados dos trabalhos de auditoria de Gestão de Segurança da Informação à Presidência do IPMT;
- Prover os meios necessários para capacitação e aperfeiçoamento técnico dos membros da ETIR,
- bem como prover a infraestrutura necessária para o seu funcionamento;
- Providenciar a divulgação interna desta PSI.

8.5 – GERÊNCIA DE TI (GTI)

- Prover todas as informações de Gestão de Segurança da Informação do IPMT;
- Prover ampla divulgação desta Política de Segurança da Informação e das Normas de Segurança da Informação, para todos os colaboradores e prestadores de serviços do IPMT;
- Promover ações de conscientização sobre Segurança da Informação para todos os colaboradores e prestadores de serviços do IPMT;
- Propor projetos e iniciativas relacionados ao aperfeiçoamento da segurança da informação, nos termos do Plano Diretor de Tecnologia da Informação e Comunicação do IPMT (PDTIC);
- Elaborar e manter política de classificação da informação, com temporalidade para guarda;
- Promover a cultura de segurança da informação;
- Implementar, acompanhar, avaliar e propor alterações desta PSI e de suas normas;
- Propor normas e procedimentos relativos à SIN em conformidade com as legislações existentes sobre o tema;
- Assessorar na implementação das ações de SIN do IPMT;
- Propor à Presidência do IPMT penalidades em caso de violação desta PSI;
- Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação e comunicações;
- Solicitar apurações quando da suspeita de ocorrências de quebras de SIN;
- Avaliar, revisar e analisar criticamente a PSI e suas normas complementares, visando à aderência aos objetivos institucionais do IPMT e às legislações vigentes;
- Dirimir eventuais dúvidas e deliberar sobre assuntos relativos à PSI;
- Aprovar Plano de Investimentos em Segurança da Informação;
- Propor programa orçamentário específico para as ações de SIN;

- Definir e atualizar seu Regimento Interno.

8.6 – Equipe de Tratamento de Incidentes em Redes de Computadores

- Facilitar e coordenar as atividades de tratamento e resposta a incidentes de SIN;
- Promover a recuperação de sistemas;
- Agir proativamente com o objetivo de tratar incidentes de segurança, divulgando práticas e recomendações de SIN e avaliando condições de segurança de redes por meio de verificações de conformidade;
- Realizar ações reativas, tais como recebimento de notificações de incidentes, orientação de equipes no reparo a danos e na análise de sistemas comprometidos, avaliando causas e responsáveis;
- Analisar ataques e intrusões na rede do IPMT;
- Executar as ações necessárias para tratar violações de segurança;
- Obter informações quantitativas acerca dos incidentes ocorridos, com a descrição da natureza, causa, data da ocorrência, frequência e custos resultantes;
- Participar de fóruns, redes nacionais e internacionais relativas à SIN.

8.7 – Proprietário de Ativos de Informação

- Descrever o ativo de informação;
- Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com esta PSI;
- Garantir a segurança dos ativos de informação sob sua responsabilidade, por meio de monitoramento contínuo;
- Comunicar as exigências de SIN do ativo de informação a todos os custodiantes e usuários;
- Conceder e revogar acessos aos ativos de informação;
- Comunicar à ETIR os riscos e a ocorrência de incidentes de SIN;
- Designar custodiante dos ativos de informação, quando aplicável.

8.8 – Custodiante dos Ativos de Informação

- Proteger e manter os ativos de informação;
- Controlar o acesso, conforme requisitos definidos pelo proprietário da informação e em conformidade com esta PSI;
- Definir e gerir os requisitos de segurança para os ativos de informação sob sua responsabilidade em conformidade com esta PSI.

8.9 – Terceiros e Fornecedores

- a) Tomar conhecimento desta PSI;
- b) Fornecer listas atualizadas de documentação dos ativos, licenças, acordos ou

direitos relacionados aos ativos de informação objetos do contrato; e

- c) Fornecer toda a documentação dos sistemas, produtos e serviços relacionados às suas atividades.

8.10 – Usuários

- Conhecer e cumprir todos os princípios, diretrizes e responsabilidades desta PSI, bem como os demais normativos e resoluções relacionados à Segurança da Informação;
- Obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação; e
- Comunicar os incidentes que afetam à segurança dos ativos de informação à Ouvidoria ou à ETIR.

9 – Divulgação e Conscientização

A divulgação das regras e orientações de segurança da informação aplicadas aos usuários deve ser objeto de campanhas internas permanentes, disponibilização integral e contínua na Intranet, seminários de conscientização e quaisquer outros meios, com vistas à criação de uma cultura de segurança da informação no âmbito do IPMT.

Cabe a Gerência de TI (GTI) providenciar a divulgação interna desta PSI e das normas dela decorrentes, inclusive com publicação na intranet do IPMT, e desenvolver processo permanente de divulgação, sensibilização, conscientização e capacitação dos usuários sobre os cuidados e deveres relacionados à SIN.

10 – Atualização e Validade

A SIN, digital ou física, é tema de permanente acompanhamento e aperfeiçoamento, devendo ser constantemente revista e atualizada, visando à melhoria contínua da qualidade dos processos internos.

Os instrumentos normativos gerados a partir desta PSI deverão ser revisados sempre que se fizer necessário, em função de alterações na legislação pertinente ou de diretrizes políticas do Governo Federal e/ou Municipal, conforme os seguintes critérios:

10.1 – Política de Segurança da Informação (PSI)

- Nível de Aprovação: Diretoria Executiva;
- Periodicidade de Revisão: Anual, não podendo exceder 3 anos;

10.2 – Normas de Segurança da Informação

- Nível de Aprovação: Gerência de Tecnologia da Informação (GTI);

- Periodicidade de Revisão: Semestral;

10.3 – Procedimentos Operacionais

- a) Nível de Aprovação: Área Técnica;
- b) Periodicidade de Revisão: Semestral;

10.4 – Validade

Esta PSI tem prazo de validade indeterminado, portanto, sua vigência se estenderá até a edição de outro marco normativo que a atualize ou a revogue.

11 – Principais Siglas

ABNT - Associação Brasileira de Normas Técnicas
CGSIN - Comitê Gestor de Segurança da Informação
ETIR - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais
GETIR - Gestão de Tratamento de Incidentes de Segurança em Rede Computacional
GECON - Gestão de Continuidade de Negócios em Segurança da Informação
GESIN - Gestão de Segurança da Informação
GRSIN - Gestão de Riscos de Segurança da Informação
IEC - International Electrotechnical Commission
ISO - International Organization for Standardization
PSI - Política de Segurança da Informação
SIN - Segurança da Informação
SISP - Sistema de Administração dos Recursos de Informação e Informática
TI - Tecnologia da Informação
GTI – Gerência de Tecnologia da Informação
PDTIC - Plano Diretor de Tecnologia da Informação e Comunicação

Teresina (PI), 7 de maio de 2024