Art. 4º A POSIN-ITI aplica-se à todas as unidades organizacionais do ITI, bem como terceiros com o qual o ITI mantenha relações institucionais ou contratuais, abrangendo servidores públicos, empregados, estagiários, prestadores de serviços, colaboradores e quaisquer pessoas que, em caráter permanente ou temporário, acessem, tratem ou processem dados, informações ou recursos do ITI.

Parágrafo único. O acesso aos ativos de informação ou aos ambientes físicos ou lógicos do ITI somente poderá ocorrer mediante prévia assinatura de Termo de Conhecimento e Responsabilidade (TCR).

Art. 5º As unidades organizacionais poderão propor ao Subcomitê de Governança Digital e Segurança da Informação (SGDSI) normas especiais com a finalidade de atender demandas e requisitos específicos dos Ativos de Informação e Ambientes Tecnológicos do ITI.

Art. 6º 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 da informação.

Parágrafo único. A estrutura normativa será dividida em três categorias:

I. Política no nível estratégico;

II. Normas Complementares de Segurança da Informação (NCSI) no nível tático;

III. Regulamentos ou Manuais de Procedimentos no nível operacional.

Art. 7º Para efeito desta POSIN-ITI, aplicam-se os termos e definições constantes no Glossário de Segurança da Informação, aprovado pela Portaria GSI/PR nº 93, de 18 de outubro de 2021, e nas normas técnicas ABNT NBR ISO/IEC da família 27000.

CAPÍTULO II - ESTRUTURA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Seção I - Estrutura

Art. 8º A estrutura de Gestão de Segurança da Informação é composta por:

I. Comitê de Gestão Estratégica (CGE);

II. Subcomitê de Governança Digital e Segurança da Informação (SGDSI);

III. Gestor de Segurança da Informação (GSI);

IV. Gestor de Tecnologia da Informação e Comunicação,

V. Encarregado pelo Tratamento de Dados Pessoais

VI. Responsável pela Unidade de Controle Interno;

VII. Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR)

VIII. Oficiais de Segurança da Informação e Resposta a Incidentes (OSIRI) e;

IX. Usuários de Tecnologia da Informação.

Seção II - Competências e Responsabilidades

Art. 9º Compete ao Gestor de Segurança da Informação (GSI), sem prejuízo de outras atribuições dispostas na legislação vigente, em especial àquelas previstas na Instrução Normativa GSI/PR nº 1, de 27 de maio de 2020:

I. Coordenar os processos de gestão de segurança da informação e a elaboração/revisão da POSIN-ITI e de suas normas específicas;

II. Promover e incentivar a cultura de segurança da informação e o uso seguro dos ativos de informação no ITI;

III. Coordenar e acompanhar os trabalhos da ETIR e do SGDSI, nos temas relacionados à segurança da informação no ITI;

IV. Propor à Alta Administração a alocação coordenada dos recursos financeiros, tecnológicos e humanos necessários para a implementação e manutenção das ações de segurança da informação;

V. Acompanhar investigações e avaliações de danos decorrentes de incidentes ou quebras de segurança bem como a aplicação das ações corretivas e administrativas cabíveis;

VI. Articular ações de capacitação e profissionalização contínua de recursos humanos em temas relacionados à segurança da informação, em conjunto com as áreas de comunicação e gestão de pessoas;

VII. Monitorar a conformidade das práticas de segurança e os resultados de auditorias internas, avaliando a eficácia dos controles e propondo melhorias contínuas;

VIII. Atuar como ponto de contato principal com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República (GSI/PR) e Centro Integrado de Segurança Cibernética do Governo Digital (CISC Gov.br) para assuntos de segurança da informação;

IX. Avaliar e decidir sobre casos omissos e dúvidas referentes à interpretação da POSIN-ITI e seus normativos específicos.

Art. 10 Compete aos Oficiais de Segurança da Informação e de Resposta a Incidentes (OSIRI), compostos por servidores representantes de cada diretoria e do Gabinete, que atuarão de forma descentralizada e colaborativa como pontos focais nos assuntos de segurança da informação e resposta a incidentes em suas respectivas unidades, cujas competências e responsabilidades serão definidas em normativo específico.

§ 1º Os indicados a serem OSIRI terão prioridade nas capacitações, eventos e intercâmbios dentro do planejamento anual de capacitações do ITI, desde que relacionados às suas atividades e competências.

Parágrafo único. As competências e nomeação dos membros titulares e suplentes do OSIRI será formalizada por meio de ato administrativo específico.

Art. 11 Compete ao CGE fornecer os recursos necessários para assegurar o desenvolvimento e a implementação da Gestão de Segurança da Informação do ITI, bem como o tratamento das ações e decisões de segurança da informação em um nível de relevância e prioridade adequados, e formalizar e aprovar esta Política de Segurança da Informação do ITI, bem como suas alterações e atualizações.

Art. 12 A estrutura e competências do SGDSI são aquelas previstas no Art. 6º da Portaria ITI nº 52, de 11 de setembro de 2025.

Art. 13 Compete ao Gestor de Tecnologia da Informação e Comunicação, dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Portaria SGD/MGI nº 9.511/2025 planejar, desenvolver, executar e monitorar as medidas de privacidade e segurança da informação em soluções de tecnologia da informação e comunicação, considerando inclusive a cadeia de suprimentos relacionada à solução.

Art. 14 As competências do Encarregado pelo Tratamento dos Dados Pessoais, são aquelas dispostas na Política de Privacidade do ITI dentre outras atribuições dispostas na legislação vigente, em especial ao disposto na Lei nº 13.709/2018 e demais normativos e orientações emitidas pela Autoridade Nacional de Proteção de Dados, e nos normativos internos relacionados.

Parágrafo único. Compete ainda ao Encarregado pelo Tratamento de Dados Pessoais atuar como canal de comunicação exclusivo entre o ITI, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD), inclusive no que se refere à comunicação de incidentes de segurança que envolvam dados pessoais.

Art. 15 Compete ao Responsável pela Unidade de Controle Interno, dentre outras atribuições dispostas na legislação vigente, apoiar, supervisionar e monitorar as atividades desenvolvidas pela primeira linha de defesa prevista pela Instrução Normativa CGU nº 3, de 9 de junho de 2017.

Art. 16 Compete aos usuários dos ativos de informação conhecer, cumprir e fazer cumprir esta Política e às demais normas específicas de segurança da informação do ITI.

Parágrafo único. Todos os usuários são responsáveis pela segurança dos ativos de informação que estejam sob a sua responsabilidade.

Art. 17 Compete aos responsáveis por informações produzidas ou custodiadas pelo ITI assegurar a segurança das informações, classificar as informações e definir procedimentos e critérios de acesso observados os dispositivos legais e normativos relativos à confidencialidade e a outros critérios de classificação pertinentes, propor regras específicas para o uso das informações e definir os requisitos de segurança da informação necessários ao negócio com base em critérios de aceitação e tratamento de riscos inerentes aos processos de trabalho.

Art. 18 São responsabilidades do custodiante da informação assegurar a segurança da informação sob sua posse conforme os critérios definidos pelo respectivo responsável pela informação, comunicar tempestivamente ao responsável pela informação sobre eventos que comprometam a segurança das informações sob custódia e comunicar ao responsável pela informação eventuais limitações para o cumprimento dos critérios por ele definidos com vistas à proteção da informação.

Art. 19 São responsabilidades dos dirigentes das unidades e demais gestores do ITI, no que se refere à segurança da informação, conscientizar servidores e quaisquer colaboradores sob sua supervisão em relação aos conceitos e às práticas de segurança da informação, incorporar aos processos de trabalho de sua unidade ou de sua área práticas inerentes à segurança da informação e tomar as medidas administrativas necessárias para que sejam adotadas ações corretivas em tempo hábil em caso de comprometimento da segurança da informação.

CAPÍTULO III - PRINCÍPIOS E DIRETRIZES

Seção I - Princípios

Art. 20 As ações de segurança da informação do ITI são norteadas pelos princípios constitucionais e administrativos que regem a Administração Pública Federal, bem como pelos seguintes princípios específicos:

I. disponibilidade, integridade, confidencialidade e autenticidade das informações;

II. continuidade dos processos e serviços essenciais para o funcionamento do ITI;

III. economicidade da proteção dos ativos de informação;

IV. respeito ao acesso à informação, à proteção de dados pessoais e à proteção da privacidade;

V. observância da publicidade como preceito geral e do sigilo como exceção;

VI. responsabilidade do usuário de informação pelos atos que comprometam a segurança dos ativos de informação;

VII. alinhamento estratégico da Política de Segurança da Informação com o planejamento estratégico do ITI;

VIII. conformidade das normas e das ações de segurança da informação com a legislação e regulamentos aplicáveis;

IX. privilégio mínimo e necessidade de conhecer;

X. governança pública, em especial a segregação de funções e prevenção do conflito de interesses, e;

XI. educação, capacitação e comunicação como alicerces fundamentais para o fomento da cultura de segurança da informação.

Art. 21 As normas, procedimentos, manuais e metodologias de segurança da informação do ITI devem considerar, como referência, além da legislação aplicável, as melhores práticas de segurança da informação nacionais e internacionais.

Parágrafo único. As ações de segurança da informação devem considerar prioritariamente os objetivos estratégicos, os planos institucionais, a estrutura e a finalidade do ITI, ser tratadas de forma integrada respeitando as especificidades e a autonomia das unidades, ser adotadas proporcionalmente aos riscos existentes e à magnitude dos danos potenciais, e visar à prevenção da ocorrência de incidentes.

Seção II - Gestão de Ativos de Informação

Art. 22 Ativos de informação são todos os meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização

§ 1º Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no ITI compõe o seu rol de ativos de informação e deve ser protegida conforme normas em vigor.

§ 2º As informações que tramitem pelo ambiente computacional do ITI são passíveis de monitoramento e auditoria, respeitados os limites legais e os direitos e garantias individuais previstos em lei.

§ 3º Os ativos de informação do ITI devem ser inventariados, protegidos, possuir responsável definido para sua gestão e ter o acesso controlado para assegurar que somente pessoas autorizadas possam deles se utilizar.

Seção III - Controle de Acesso e Gestão de Credenciais

Art. 23 Pessoas e sistemas devem ter o menor privilégio e o mínimo acesso aos recursos necessários para realizar uma dada tarefa, observado o princípio da necessidade de conhecer.

§1º. O acesso aos ativos de informação ou aos ambientes físicos ou lógicos do ITI somente poderá ocorrer mediante a prévia assinatura do Termo de Conhecimento e Responsabilidade (TCR), na forma do Anexo II.

§2º O TCR deverá ser assinado digitalmente, com o uso de assinatura qualificada ou avançada Gov.br.

Seção IV - Plano de Conscientização em Segurança da Informação

Art. 24 A POSIN-ITI e suas atualizações, bem como normas específicas de segurança da informação e privacidade do ITI, devem ser objeto de ampla e constante divulgação, a fim de promover sua observância, seu conhecimento e a formação da cultura de segurança da informação.

Parágrafo único. Deverá ser instituído um plano de conscientização, proposto pelo GSI e aprovado pelo CGE, que abrangerá ações e cursos sobre os procedimentos de segurança, boas práticas e uso adequado dos ativos de informação necessários ao desempenho de suas atribuições, de modo a capacitar, treinar e conscientizar continuamente os usuários de informação a fim de fortalecer o comportamento seguro, reduzir vulnerabilidades humanas e minimizar potenciais riscos à segurança da informação e à privacidade.

Seção V - Contratos e Aquisições

Art. 25 Os contratos de prestação de serviços, convênios, acordos de cooperação e outros instrumentos congêneres firmados pelo ITI conterão cláusula específica sobre a obrigatoriedade de atendimento a esta POSIN-ITI e adequação à LGPD, bem como às suas normas decorrentes.

Parágrafo único. A contratação de serviços deve considerar os critérios de segurança da informação definidos nesta POSIN-ITI, incluindo requisitos específicos quando houver tratamento de informações classificadas ou de dados pessoais, sem prejuízo de necessidades específicas das unidades organizacionais demandantes.

CAPÍTULO IV - SISTEMA DE GESTÃO DE SEGURANÇA DA INFORMAÇÃO

Seção I - Processos do Sistema de Gestão de Segurança da Informação

Art. 26 O Sistema de Gestão de Segurança da Informação (SGSI) do ITI deverá ser constituído por processos baseados nos guias de melhores práticas de segurança da informação e normas nacionais e internacionais correlatas, que devem ser adaptadas às necessidades e especificidades do ITI.

§ 1º Os processos do SGSI são interdependentes, poderão ser implementados gradativamente, e devem ser monitorados de forma a permitir sua melhoria contínua.

§ 2º O Subcomitê de Governança Digital e Segurança da Informação (SGDSI) definirá o SGSI, em especial sua estrutura e processos, que devem estar alinhados aos princípios e às diretrizes desta POSIN-ITI e destinados à implementação de ações de segurança da informação.

§ 4º O SGSI deve se comunicar e ser executado de maneira coordenada com o Sistema de Gestão da Proteção de Dados (SGPD) a ser estabelecido pelo ITI.

Seção II - Classificação da Informação e Governança de Dados

Art. 27 A Classificação da Informação tem por objetivo assegurar que a informação receba um nível adequado de proteção, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização, observando os princípios estabelecidos na legislação aplicável.

Art. 28 A Governança de Dados é definida como o exercício de autoridade, controle e tomada de decisão compartilhada (planejamento, monitoramento e fiscalização) sobre o gerenciamento de ativos de dados e tem por objetivo estabelecer um ecossistema de dados sustentável, confiável e seguro.

Parágrafo único. As diretrizes acerca da classificação e tratamento da informação e governança de dados serão objeto de regulamentação específica pelo SGDSI.

Seção III - Privacidade e Proteção de Dados Pessoais

Art. 29 A proteção de dados pessoais tem o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, em conformidade com a Lei nº 13.709/2018.

Parágrafo único. As diretrizes acerca de proteção de dados pessoais serão objeto de regulamentação específica pela SGDSI

Seção IV - Gestão de Riscos de Segurança da Informação

Art. 30 A gestão de riscos de segurança da informação tem por objetivo identificar os riscos que possam comprometer a confidencialidade, a integridade, a disponibilidade ou a autenticidade da informação, priorizando seu tratamento com base em critérios para aceitação de riscos compatíveis com os objetivos institucionais.

§ 1º Os controles de segurança da informação devem ser planejados, aplicados, implementados e, periodicamente, avaliados de acordo com os objetivos institucionais e os riscos para o ITI.

§ 2º O processo de gestão de riscos de segurança da informação deve ser contínuo e aplicado na implementação e operação da Gestão de Segurança da Informação, contemplando inclusive as contratações de soluções de Tecnologia da Informação.

§ 3º A gestão de riscos de segurança da informação deve resultar na identificação de requisitos de segurança da informação e na seleção de controles de segurança, com o objetivo de redução do risco ao nível aceitável.