ANEXO

CAPÍTULO I

DO ESCOPO

Art. 1º - Instituir diretrizes estratégicas, responsabilidades e competências, visando assegurar a integridade, confidencialidade, disponibilidade e autenticidade das informações custodiadas e de propriedade do Instituto, de modo a preservar seus ativos e sua imagem institucional.

Art. 2º - Trata-se do uso e compartilhamento do conteúdo de dados, informações e documentos no âmbito do Instituto, em todo o seu ciclo de vida - criação, manuseio, divulgação, armazenamento, transporte e destinação final, visando à continuidade de seus processos críticos, em conformidade com a legislação vigente, normas pertinentes, requisitos regulamentares e contratuais, valores éticos e as melhores práticas de segurança da informação e comunicações.

Art. 3º - Aplica-se a todas as unidades da estrutura regimental do Instituto, podendo ser estendida às demais unidades eventualmente por ele atendidas

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 4º - Para efeitos desta POSIC, entende-se por:

I - acesso: ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade;
II - agente público: todo aquele que exerce cargo, emprego ou função no Instituto, ainda que transitoriamente, com ou sem remuneração, por nomeação, designação, contratação ou qualquer outra forma de vínculo (servidores públicos, militares, servidores temporários regidos pela Lei nº 8.745, de 9 de dezembro de 1993 e colaboradores);
III - ameaça: conjunto de fatores externos ou causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou organização;
IV - assinatura eletrônica: geração, por computador, de qualquer símbolo ou série de símbolos executados, adotados ou autorizados legalmente equivalentes à assinatura manual do indivíduo;
V - ativo classificado: ativo de informação com informação classificada como sigilosa;
VI - ativo de informação: qualquer componente (humano, tecnológico, físico ou lógico) que sustenta um ou mais processos de negócio de uma unidade ou área de negócio. Inclui meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;
VII - ativo sob restrição de acesso: ativo de informação com informação institucional não pública ou com informação de acesso transitoriamente restrito;
VIII - auditabilidade: atributo que garante a rastreabilidade dos diversos passos de um processo informatizado, identificando os participantes, ações e horários de cada etapa;
IX - auditoria: atividade que engloba o exame das operações, processos, sistemas e responsabilidades gerenciais, com o intuito de verificar sua conformidade com os objetivos e políticas institucionais, orçamentos, regras, normas e padrões;
X - autenticidade: qualidade da informação que tenha sido produzida, expedida, recebida ou modificada por determinado indivíduo, equipamento ou sistema;
XI - classificação: grau de sigilo atribuído por autoridade competente a dados, informações, documentos, materiais, áreas ou instalações;
XII - colaborador: pessoa jurídica ou pessoa física que desempenhe atividade de interesse do Instituto, realize estágio ou preste serviço, em caráter permanente ou eventual;
XIII - Comitê de Segurança da Informação e Comunicações - CSIC: comitê instituído com a responsabilidade de assessorar a implementação das ações de segurança da informação e comunicações no âmbito da estrutura regimental do Instituto e dos órgãos por ela atendidos;
XIV - confidencialidade: propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado;
XV - continuidade de negócios: capacidade estratégica e tática de um órgão ou entidade de se planejar e responder a incidentes e interrupções de negócios, minimizando seus impactos e recuperando perdas de ativos de informação das atividades críticas, de forma a manter suas operações em um nível aceitável, previamente definido;
XVI - custodiante do ativo de informação: 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;
XVII - desastre: evento repentino e não planejado que causa perda para toda ou parte da organização e gera sérios impactos em sua capacidade de entregar serviços essenciais ou críticos por um período de tempo superior ao tempo objetivo de recuperação;
XVIII - disponibilidade: qualidade da informação que pode ser conhecida e utilizada por indivíduos, equipamentos ou sistemas autorizados;
XIX - documento: unidade de registro de informações, qualquer que seja o suporte ou formato;
XX - documento classificado: documento com informação classificada como sigilosa;
XXI - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR: grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em computadores;
XXII - Gestão da Segurança da Informação e Comunicações: 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 à tecnologia da informação e comunicações;

XXIII - Gestor de Segurança da Informação e Comunicações: servidor responsável pelas ações de segurança da informação e comunicações;
XXIV - Gestor do Ativo de Informação: autoridade legal responsável pela concessão de acesso a terceiros (pode ser a autoridade marcadora, a autoridade classificadora ou a autoridade instituidora do processo);
XXV - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;
XXVI - informações institucionais públicas: informações geradas ou custodiadas pelo Instituto ou por seus colaboradores, no exercício de suas funções, às quais o acesso será permitido, observando-se eventual restrição temporária. Dividem-se em:
a) de acesso ostensivo: aquelas que não estão sujeitas a nenhuma restrição de acesso;
b) de acesso transitoriamente restrito: aquelas referentes a documentos utilizados como fundamento de decisões e atos administrativos, às quais o acesso será franqueado após a edição do correspondente ato decisório, conforme previsto no parágrafo 3º do art. 7º da Lei nº 12.527, de 18 de novembro de 2011, salvo se forem, posteriormente, objeto de classificação como sigilosas.
XXVII - informações institucionais não públicas: informações geradas ou custodiadas pelo ou por seus colaboradores, no exercício de suas funções, sujeitas a restrição de acesso. Dividem-se em:
a) informações pessoais: aquelas relacionadas à pessoa natural identificada ou identificável e que diga respeito à sua intimidade, vida privada, honra e imagem, cujo tratamento é regulado pelo art. 31 da Lei nº 12.527, de 18 de novembro de 2011;
b) informações sujeitas a outros tipos de sigilo: aquelas sob segredo de justiça ou protegidas por sigilo comercial, bancário, fiscal, industrial ou outros, na forma da legislação vigente, conforme o disposto no art. 22 da Lei nº 12.527, de 18 de novembro de 2011;
c) informação classificada: informação sigilosa em poder dos órgãos e entidades públicas, observado o seu teor e em razão de sua imprescindibilidade à segurança da sociedade ou do Estado, classificada como ultrassecreta, secreta ou reservada;
d) registros: informações contidas em anotações, levantamentos e análises preliminares, ou seja, aquelas de produção e guarda dos agentes públicos no exercício de suas funções, e que não integrem processo ou expediente que subsidie decisão administrativa editada.

XXVIII - informação sob restrição de acesso: informação institucional não pública ou informação de acesso transitoriamente restrito;
XXIX - integridade: qualidade da informação não modificada, inclusive quanto à origem, trânsito e destino;
XXX - legalidade: atributo que garante a legalidade jurídica da informação, assegurando que todos os seus dados estão de acordo com as cláusulas contratuais pactuadas ou com a legislação vigente;
XXXI - não repúdio: propriedade da informação que não possa ter seu envio ou conteúdo contestados, rejeitados ou repudiados por seu emissor ou por seu receptor;
XXXII - Política de Segurança da Informação e Comunicações: documento aprovado pela autoridade responsável pelo órgão com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações;
XXXIII - princípios: são ideias centrais que estabelecem diretrizes a um dado sistema, conferindo-lhe um sentido lógico, harmonioso e racional;
XXXIV - privacidade: propriedade da informação privada que só possa ser acessada por terceiros com conhecimento e autorização prévios das pessoas de que ela trata;
XXXV - quebra de segurança: ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação e das comunicações;
XXXVI - recurso criptográfico: sistema, programa, processo, equipamento isolado ou em rede que utiliza algoritmo simétrico ou assimétrico para realizar cifração ou decifração;
XXXVII - recursos de tecnologia da informação: servidores de rede, estações de trabalho, equipamentos de conectividade, todo e qualquer hardware e software que compõem soluções e aplicações de Tecnologia da Informação;
XXXVIII - segurança da informação e comunicações: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;
XXXIX - tratamento da informação: conjunto de ações referentes à produção, classificação, utilização, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação;
XL - usuário: agente público, auditores e quaisquer outros entes que podem acessar ativos de informação do Instituto, mediante autorização de um gestor de ativo de informação;
XLI - vulnerabilidade: conjunto de fatores internos ou causa potencial de um incidente indesejado, que podem resultar em risco para um sistema ou organização, os quais podem ser evitados por uma ação interna de segurança da informação.

CAPÍTULO III
DAS REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 5º - Esta POSIC observa a legislação vigente e normas específicas, destacando-se:
I - Leis Federais, Estaduais e Municipais;
II - Acórdãos do TCU;
III - Instruções Normativas e Normas Complementares aprovadas pelo CGSI/PR; e
IV - Normas ABNT.

CAPÍTULO IV
DOS PRINCÍPIOS

Art. 6º - As ações de Segurança da Informação e Comunicações são norteadas pelos seguintes princípios:
I - Alinhamento Estratégico: deve haver um alinhamento entre a POSIC e a missão institucional e seu planejamento estratégico;
II - Propriedade da informação: toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo IPREM é considerada seu patrimônio e deve ser protegida conforme normas em vigor.
III - Responsabilidade: os agentes públicos devem conhecer e respeitar a POSIC;
IV - Ética: os direitos dos agentes públicos devem ser preservados, sem o comprometimento da segurança da informação e comunicações;

V - Celeridade: as ações de segurança da informação e comunicações devem oferecer respostas rápidas a incidentes e falhas de segurança;
VI - Clareza: as regras de segurança da informação e comunicações devem ser precisas, concisas e de fácil entendimento;
VII - Privacidade: informação que fira o respeito à intimidade e à honra dos cidadãos não pode ser divulgada;
VIII - Publicidade: dar transparência no trato da informação, observados os critérios legais;
IX - Domínio: É vedado o domínio exclusivo, por apenas um colaborador, de um processo de negócio ou recurso; e
X - Serão observados ainda, sem prejuízo das demais, outros princípios constitucionais que regem a Administração Pública Municipal.

CAPÍTULO V
DAS DIRETRIZES GERAIS
Seção I

Da Gestão da Segurança da Informação e Comunicações

Art. 7º - A gestão da segurança da informação e comunicações compreende a preservação dos ativos do Instituto, quanto aos aspectos de confidencialidade, integridade, disponibilidade e autenticidade, independentemente do meio que se encontrem.
Art. 8º - De forma a promover a gestão e fomentar os aspectos de segurança da informação, o Instituto deve:
I - Instituir uma estrutura para a gestão de segurança da informação e comunicações;
II - Nomear um gestor de segurança da informação e comunicações;
III - Estabelecer o comitê de segurança da informação e comunicações;
IV - Instituir normas e procedimentos que garantam a segurança da informação em ambientes de computação móvel e de trabalho remoto;
V - Instituir normas e procedimentos que estabeleçam critérios de acesso e uso de internet, redes sociais, sistemas corporativos, banco de dados, rede de comunicações, uso de dispositivos de armazenamento (pendrive, cartões de memória, discos rígidos externos e dispositivos similares);
VI - Instituir normas e procedimentos que estabeleçam a Gestão de Continuidade do Negócio para minimizar os impactos decorrentes de eventos que causem a indisponibilidade sobre os serviços sob responsabilidade do Instituto; e
VII - Resguardar todo ativo de informação contra acesso e manipulação indevidos.

Seção II
Do Tratamento da Informação

Art. 9º - Toda informação criada, adquirida ou custodiada pelo agente público, no exercício de suas atividades para o Instituto, é considerada um bem e deve estar protegida de acordo com as regulamentações de segurança existentes.
Art. 10 - As informações devem ser protegidas de acordo com as diretrizes descritas nesta POSIC e demais regulamentações em vigor.
Art. 11 - As informações do Instituto produzidas ou custodiadas pelo Setor de Comunicações e Tecnologia devem ter destinação final, conforme o seu nível de classificação.

Seção III
Da Relação com Terceiros

Art. 12 - Nos editais de licitação, nos contratos ou acordos de cooperação técnica com entidades prestadoras de serviços para o Instituto deverá constar cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, bem como deverá ser exigida, da entidade contratada, a assinatura do termo de confidencialidade.
Parágrafo único - As particularidades das relações com terceiros deverão ser definidas em norma interna específica.

Seção IV
Da Classificação da Informação

Art. 13 - As informações custodiadas ou de propriedade do Instituto devem ser classificadas quanto aos aspectos de sigilo, disponibilidade e integridade de forma implícita ou explícita e receber o nível de proteção condizente com sua classificação, conforme normas e legislação específica em vigor.
Art. 14 - O gestor da informação é responsável por atribuir o nível de classificação das informações sob sua responsabilidade.
Art. 15 - A classificação deve ser respeitada durante todo o ciclo de vida da informação, ou seja, criação, manutenção, armazenamento, transporte e descarte.
Art. 16 - Todo agente público deve ser capaz de identificar a classificação atribuída a uma informação custodiada ou de propriedade do Instituto e, a partir dela, conhecer e obedecer às restrições de acesso e divulgação associadas.

Seção V
Da Sensibilização, Conscientização e Capacitação

Art. 17 - Deve ser adotado processo permanente de divulgação, sensibilização, conscientização e capacitação dos agentes públicos sobre os cuidados e deveres relacionados à segurança da informação e comunicações.

Seção VI
Da Gestão de Riscos

Art. 18 - Deve ser adotado processo contínuo de gestão de riscos, o qual será aplicado na implantação e operação da gestão de segurança da informação e comunicações.

Seção VII
Da Gestão de Continuidade

Art. 19 - Deve ser adotado processo de gestão de continuidade das atividades e processos críticos, visando não permitir que estes sejam interrompidos e assegurar a sua retomada em tempo hábil.
Art. 20 - As ações de continuidade devem ser observadas por todos os titulares das unidades administrativas, de forma a proteger a reputação e a imagem institucional.
Art. 21 - As informações de propriedade ou custodiadas pelo Instituto, quando armazenadas em meio eletrônico, devem ser providas de cópia de segurança de forma a garantir a continuidade das atividades do Instituto. As informações armazenadas em outros meios devem possuir mecanismos de proteção que preservem sua integridade, conforme o nível de classificação atribuído.

Seção VIII
Do Tratamento de Incidentes de Rede Computacional

Art. 22 - A Coordenação-Geral de Tecnologia da Informação do Instituto deve 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 rede de computadores.
Parágrafo único - A regulamentação da ETIR deve ser realizada por meio de portaria específica.

Seção IX
Do Uso de Recursos Computacionais e de Comunicações

Art. 23 - O uso de recursos computacionais e de comunicações do Instituto pelos agentes públicos deve ser direcionado prioritariamente para realização das atividades profissionais desempenhadas para o Instituto nos limites dos princípios da ética, razoabilidade e legalidade.
§ 1º - A área de tecnologia do Instituto poderá monitorar o acesso à internet e restringir acesso aos sítios que possam oferecer riscos à segurança da rede ou ao ambiente computacional.
§ 2º - Só poderão ser utilizados no ambiente computacional softwares homologados ou autorizados pela área de tecnologia do Instituto.
§ 3º - Não devem ser permitidos usuários com privilégios de administrador de sistema operacional nos computadores do Instituto.

Seção X
Da Auditoria e Conformidade

Art. 24 - Devem ser criados e mantidos registros e procedimentos, como trilhas de auditoria que possibilitem o rastreamento, acompanhamento, controle e verificação de acessos aos sistemas corporativos e rede interna do Instituto.
Art. 25 - Periodicamente deve-se promover verificação de conformidade às regulamentações de segurança e legislações em vigor.

Seção XI
Dos Controles de Acesso

Art. 26 - Devem ser sistematizados procedimentos para a concessão de acesso como forma de evitar a quebra de segurança da informação e comunicações.
Art. 27 - Devem ser implementados mecanismos de controle de acesso como consequência do processo de gestão de riscos de segurança da informação e comunicações.
Art. 28 - O acesso às informações custodiadas ou de propriedade do Instituto pelos agentes públicos deve ser restrito ao necessário para desempenho de suas funções.
Art. 29 - O acesso físico às instalações do Instituto deverá ser regulamentado com o objetivo de garantir a segurança dos agentes públicos e a proteção dos seus ativos.

CAPÍTULO VI
DAS PENALIDADES

ART. 30 - Ações que violem a política de segurança da informação e comunicação poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

CAPÍTULO VII
DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 31 - É dever do agente público do Instituto conhecer e zelar pelo cumprimento desta norma.
Art. 32 - Os agentes públicos são responsáveis pela segurança dos ativos e processos que estejam sob sua custódia e por todos os atos executados com suas identificações, tais como: crachá, login, senha eletrônica, certificado digital, cópia de segurança dos arquivos pessoais e endereço de correio eletrônico.
Parágrafo único - A identificação do usuário deve ser pessoal e intransferível, qualquer que seja a forma, permitindo de maneira clara e irrefutável o seu reconhecimento.
Art. 33 - Independentemente da adoção de outras medidas, o titular da unidade administrativa deverá, de imediato, comunicar todo incidente de segurança que ocorra no âmbito de suas atividades ao gestor de segurança da informação e comunicações.
Art. 34 - No caso de incidente na rede corporativa a ETIR deve ser comunicada.
Art. 35 - Sempre que necessário, o gestor da informação providenciará autorização relativa à cessão de direitos sobre as informações de terceiros, antes de utilizá-las.
Art. 36 - A cessão de informações do Instituto a terceiros deverá ser submetida previamente à autorização do gestor da informação.
Art. 37 - O gestor de segurança da informação, com apoio da área de tecnologia, tem total autonomia para atuar sobre os recursos de TI do instituto, sem prévio aviso, para:
I - realizar auditoria (local ou remota);
II - redefinir perfis de usuários cujos privilégios possam levar à prática de atividades tidas como nocivas à rede ou ao ambiente computacional;
III - instalar softwares de monitoramento;
IV - desinstalar quaisquer softwares não homologados ou considerados nocivos à integridade da rede ou ao ambiente computacional;
V - credenciar/descredenciar usuários.

CAPÍTULO VIII
DA DIVULGAÇÃO

Art. 38 - Após a publicação desta POSIC, ela deverá ser divulgada amplamente a todos os agentes públicos do Instituto, inclusive de forma permanente na página da intranet do Instituto.

CAPÍTULO IX
DA ATUALIZAÇÃO E VIGÊNCIA

Art. 39 - Esta POSIC deverá ser revisada e atualizada quando identificada necessidade ou a cada 12 (doze) meses, a contar da data de sua publicação.