ANEXO I

RESOLUÇÃO Nº 9/CEGOV/INSS, DE 31 DE AGOSTO DE 2020

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO DO INSTITUTO NACIONAL DO SEGURO SOCIAL – POSIN–INSS.

Art. 1º A POSIN-INSS tem por objetivo estabelecer e difundir diretrizes e princípios de Segurança da Informação – SI, com vistas à orientação para uso e proteção adequados das informações produzidas e custodiadas pelo Instituto, preservando sua disponibilidade, integridade, confidencialidade e autenticidade.

Parágrafo único. A Política de que trata o **caput** e suas normas complementares aplicam-se a todos os agentes públicos que têm vínculo direto e/ou indireto com o Instituto.

Art. 2º Para os efeitos da POSIN-INSS, entende-se:

I - agente público: todo aquele que exerce, ainda que transitoriamente ou sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função nos órgãos e entidades da Administração Pública Federal, direta e indireta;

II - atividades críticas: atividades que devem ser executadas de forma a garantir a consecução dos produtos e serviços fundamentais do órgão ou entidade, de tal forma que permitam atingir os seus objetivos mais importantes e sensíveis ao tempo;

III - ativos de informação: meios de armazenamento, transmissão e processamento, sistemas de informação, bem como os locais onde se encontram esses meios e as pessoas que a eles têm acesso;

IV - dados processados: dados submetidos a qualquer operação ou tratamento, por meio de processamento eletrônico ou automatizado, com o emprego de tecnologia da informação;

V - gestor de Segurança da Informação: é o responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal;

VI - informação: dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

VII - informação custodiada: informações pessoais e de terceiros obtidas pelo Instituto em razão de suas atribuições;

VIII - necessidade de conhecer: condição segundo a qual o conhecimento da informação classificada é indispensável para o adequado exercício de cargo, função, emprego ou atividade reservada. O termo "necessidade de conhecer" descreve a restrição de dados que sejam considerados extremamente sigilosos. Sob restrições do tipo necessidade de conhecer, mesmo que um indivíduo tenha as credenciais necessárias para acessar uma determinada informação, ele só terá acesso a essa informação caso ela seja estritamente necessária para a condução de suas atividades oficiais;

IX - riscos de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades nos ativos de informação, em razão de ameaças, com impacto negativo às atividades do Instituto;

X - Segurança da Informação – SI: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e autenticidades das informações;

XI - vínculo direto: agentes públicos contratados diretamente pelo INSS; e

XII - vínculo indireto: agentes privados ou públicos pertencentes a órgãos ou unidades da Administração Pública Federal, Estadual ou Municipal que mantenham contrato, convênio, acordo de cooperação técnica ou instrumento congênere com o INSS.

Art. 3º Esta POSIN-INSS foi elaborada com base nos seguintes normativos:

I - Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados;

II - Lei nº 12.527, de 18 de novembro de 2011, que regula o acesso a informações previsto na Constituição Federal;

III - Lei nº 12.965, de 23 de abril de 2014, que estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil;

IV - Lei nº 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais;

V - Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

VI - Decreto nº 7.724, de 16 de maio de 2012, regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

VII - Decreto nº 7.845, de 14 de novembro de 2012, que 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;

VIII - Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação;

IX - Decreto nº 10.222, de 5 de fevereiro de 2020, que aprova a Estratégia Nacional de Segurança Cibernética;

X - Instrução Normativa GSI/PR nº 01, de 27 de maio de 2020, que disciplina a gestão de segurança da informação na Administração Pública Federal, direta e indireta, e dá outras providências;

XI - instruções normativas relacionadas à segurança da informação, publicadas pelo Gabinete de Segurança Institucional da Presidência da República;

XII - Portaria GSI/PR nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação; e

XIII - NBR ISO/IEC 27002:2013, que institui código de melhores práticas para a Gestão de Segurança da Informação.

Art. 4º Esta POSIN-INSS foi elaborada com base nos seguintes princípios:

I - a preservação da imagem do Instituto e de seus agentes públicos;

II - a salvaguarda das informações do cidadão;

III - ações de segurança orientadas pela gestão de riscos;

IV - continuidade assegurada dos serviços ao cidadão;

V - o alinhamento com a missão institucional e seu planejamento estratégico; e

VI - respeito à natureza e finalidade de cada área do Instituto.

Art. 5º São diretrizes gerais da POSIN-INSS:

I - tratamento da informação:

a) toda informação produzida pelos agentes públicos, no exercício de suas atividades, é de propriedade do INSS e deve ser protegida;

b) informações produzidas, armazenadas e tratadas pelo Instituto, especialmente as informações pessoais e custodiadas, devem receber o devido tratamento para assegurar sua proteção durante todo o ciclo de vida; e

c) somente os canais de comunicação disponibilizados pelo INSS devem ser utilizados para trafegar informações institucionais;

II - tratamento de incidentes de SI: todo incidente de segurança da informação deve ser imediatamente relatado à área responsável pela gestão de segurança da informação de Tecnologia da Informação – TI, observando-se a apropriada coleta de evidências;

III - gestão de riscos de segurança:

a) os riscos de segurança da informação devem ser identificados e tratados; e

b) os critérios para a gestão de risco devem ser definidos e comunicados à toda Instituição;

IV - gestão de continuidade:

a) os ativos de informação que suportam as atividades críticas do Instituto devem ser suportados por ambiente de alta disponibilidade e ter capacidade de recuperação em prazos e condições previamente definidos para situações de contingência, em conformidade com o processo de continuidade; e

b) a continuidade das operações e serviços de TI deve estar prevista nos contratos, assim como os prazos e condições devem estar formalmente estabelecidos;

V - controles de acesso:

a) todo acesso à informação deve ser motivado pela necessidade de conhecer;

b) os sistemas de informação e as instalações físicas devem ter capacidade de controlar os acessos, com fins de responsabilização pelo seu uso; e

c) as autorizações de acesso às informações, sistemas e instalações físicas devem ter critérios de acesso definidos e divulgados a todos da Instituição;

VI - recursos computacionais:

a) correio eletrônico:

1. o correio eletrônico, e-mail, é uma forma de comunicação oficial e deve ser utilizado exclusivamente no desempenho das atividades funcionais; e

2. ao produzir, responder ou encaminhar mensagem em caixa de correio eletrônico institucional, o servidor deverá se identificar, subscrevendo, ao menos, seu nome, cargo e telefone de contato institucional;

b) acesso à Internet:

1. o acesso à Internet, por meio da rede de dados do INSS, é uma concessão e deve ter seu uso orientado para a execução das atividades do Instituto; e

2. os acessos serão liberados de acordo com perfis previamente definidos pelo órgão responsável pelos serviços de TI;

c) gestão de mudanças de TI:

1. toda mudança nos sistemas de informação do INSS deve ser previamente e formalmente autorizada; e

2. a gestão de mudanças deve prever, no mínimo, a guarda dos registros, realização de testes e a possibilidade de recuperação do ambiente;

d) computação em nuvem:

1. o ambiente de computação em nuvem, sua infraestrutura e canal de comunicação devem estar aderentes às diretrizes e normas de SI, estabelecidas pelo Instituto, e às legislações vigentes; e

2. o contrato de prestação de serviço, quando for o caso, deverá conter cláusulas que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço;

VII - educação e conscientização:

a) esta Política e seus normativos complementares devem ser periodicamente divulgados a todos os agentes públicos do Instituto;

b) o Instituto deve manter programa contínuo de conscientização dos agentes públicos em SI; e

c) deve ser mantido plano de capacitação especializado aos profissionais que atuam na gestão de SI;

VIII - auditoria e conformidade:

a) o cumprimento desta Política e de suas normas complementares deve ser avaliado periodicamente, por meio de verificações de conformidade; e

b) o uso dos recursos de TI disponibilizados pelo Instituto é passível de monitoramento e auditoria;

IX - responsabilidade pela gestão das informações:

a) os responsáveis pela gestão dos ativos da informação e sistemas corporativos devem descrever os requisitos de segurança; e

b) os sistemas de informação devem se concebidos possibilitando a segregação de funções;

X - segurança física e do ambiente:

a) as instalações em que as informações críticas ou sensíveis serão processadas deverão ser mantidas em áreas seguras, com níveis e controles de acesso apropriados, incluindo proteção física; e

b) os ativos da organização devem ser protegidos contra acesso físico não autorizado, danos, perdas, furto e interferência. As proteções devem estar alinhadas aos riscos identificados;

XI - gestão de ativos da informação, os ativos de informação devem:

a) ser inventariados e protegidos;

b) ter identificados os seus proprietários e custodiantes;

c) ter a sua entrada e saída nas dependências do Instituto autorizadas e registradas por autoridade competente; e

d) ser utilizados estritamente dentro do seu propósito, sendo vedado seu uso para fins particulares ou de terceiros, entretenimento, veiculação de opiniões político-partidárias, religiosas, discriminatórias e afins.

Art. 6º A não observância dos preceitos desta Política implicará na aplicação de sanções administrativas, cíveis e penais, previstas na Lei nº 8.112, de 11 de dezembro de 1990 (Estatuto do Servidor Público Federal), no Código Penal, no Código Civil, e, ainda, em legislação que regule ou venha regular a matéria.

Art. 7º Competências e responsabilidades:

I - cabe ao Gestor de SI:

a) promover cultura de segurança da informação;

b) acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

c) propor os recursos necessários à implementação das ações de SI;

d) coordenar o Comitê de Segurança da Informação - CSI ou estrutura equivalente;

e) acompanhar os trabalhos e a Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR-INSS;

f) propor o detalhamento das diretrizes desta Política, por meio de normas e procedimentos, e acompanhar sua implementação;

g) assessorar a alta administração na implementação da Política de SI;

h) estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à SI;

i) promover a divulgação da política e das normas internas de SI do órgão a todos os servidores, usuários e prestadores de serviços que trabalham no INSS;

j) incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à SI;

k) verificar os resultados dos trabalhos de auditoria sobre a gestão da SI;

l) acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da SI; e

m) manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos à SI;

II - cabe ao Presidente do INSS nomear o Gestor de SI;

III - caso o Gestor de SI não seja nomeado, as atribuições relacionadas no inciso I do art. 7º serão desempenhadas pelo Diretor de Tecnologia da Informação e Inovação;

IV - a ETIR-INSS deve analisar e propor respostas a notificações e atividades relacionadas a incidentes de SI, no âmbito do Instituto;

V - é responsabilidade de todos os agentes públicos, diretos e indiretos, conhecer e cumprir as diretrizes desta Política e demais normas e procedimentos complementares de SI; e

VI - compete ao Comitê Estratégico de Governança - CEGOV deliberar sobre políticas e normas de segurança da informação, assessorado pelo Comitê Temático de Governança Digital, tendo em vista o Sistema de Governança do INSS, instituído pela Portaria nº 3.213/PRES/INSS, de 10 de dezembro de 2019.

Parágrafo único. O Comitê Temático de Gestão da Informação é responsável pela aprovação de procedimentos e de normas internas que orientem o compartilhamento de dados sob gestão do INSS e pela aprovação da categorização dos níveis de compartilhamento de dados com outras entidades públicas (federais ou de outras esferas e poderes) da sociedade civil, nos termos do art. 6º do anexo à Portaria nº 3.213/PRES/INSS, de 2019.

Art. 8º Esta Política e seus normativos devem ser revisados sempre que necessário, não excedendo o período máximo de 3 (três) anos.