SUPERINTENDÊNCIA NACIONAL DE PREVIDÊNCIA COMPLEMENTAR

PORTARIA PREVIC Nº 295, DE 04 DE ABRIL DE 2023

Dispõe sobre a Política de Segurança da Informação (Posin), no âmbito da Superintendência Nacional de Previdência Complementar (Previc).

A DIRETORIA COLEGIADA DA SUPERINTENDÊNCIA NACIONAL DE PREVIDÊNCIA COMPLEMENTAR (PREVIC), no uso das competências que lhe conferem o inciso VIII do art. 12 do Decreto nº 11.241, de 18 de outubro de 2022, e em atenção ao disposto no inciso II do art. 15 da Instrução Normativa nº 01, de 27 de maio de 2020, editada pelo Gabinete de Segurança Institucional da Presidência da República, **RESOLVE**:

CAPÍTULO I

DO ESCOPO

Art. 1º A Política de Segurança da Informação (Posin/Previc) da Superintendência Nacional de Previdência Complementar (Previc) deve alinhar-se às estratégias da Previc e ter como objetivo estabelecer em seu âmbito as diretrizes, as responsabilidades, as competências e os subsídios para a gestão da segurança da informação.

Parágrafo único. A Segurança da Informação (SI) compreende ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Art. 2º Integram também a Posin/Previc as normas, as metodologias e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização.

Art. 3º A Posin/Previc aplica-se:

I - às áreas de negócio, em todas as suas localidades;

II - à área de Tecnologia da Informação (TI);

III - às áreas de apoio;

IV - aos projetos, às ações e atividades de trabalho exercidos dentro ou fora das suas instalações;

V - ao relacionamento com outros órgãos e entidades públicas ou privadas, no que couber; e

VI - aos seus servidores, aos prestadores de serviço, aos estagiários, aos consultores externos e a outros usuários que, de alguma forma, tenha acesso às informações geradas, adquiridas ou custodiadas sob a sua responsabilidade.

Parágrafo único. A não observância do disposto na Posin/Previc, bem como em suas normas correlatas, por parte de quaisquer dos agentes públicos de que trata o inciso VI do *caput*, pode implicar a aplicação de sanções previstas na legislação vigente.

Art. 4º Os convênios, os acordos e outros instrumentos congêneres celebrados pela Previc devem atender a esta Posin/Previc.

CAPÍTULO II

DOS CONCEITOS E DEFINIÇÕES

Art. 5º Para os fins da Posin/Previc, considera-se:

I - agentes de tratamento: o controlador e o operador;

II - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

III - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; e

IV - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador.

Parágrafo único. Os demais conceitos relacionados à Posin/Previc podem ser consultados no Glossário de Segurança da Informação, aprovado pelo Gabinete de Segurança Institucional da Presidência da República.

Art. 6º As informações geradas, adquiridas ou custodiadas sob a responsabilidade da Previc são consideradas parte do seu patrimônio intelectual, não cabendo a seus criadores qualquer forma de direito autoral, salvo aqueles direitos garantidos no âmbito da Lei nº 10.973, de 2 de dezembro de 2004 (Lei de incentivos à inovação e à pesquisa científica e tecnológica no ambiente produtivo), e outros dispositivos legais e devem ser protegidas segundo as diretrizes descritas nesta Posin/Previc, em seus documentos complementares e demais regulamentações em vigor.

Art. 7º É vedado comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações geradas, adquiridas ou custodiadas sob a responsabilidade da Previc.

Art. 8º Todas as pessoas que tenham acesso às informações da Previc são responsáveis pela sua segurança.

CAPÍTULO III

DOS PRINCÍPIOS

Art. 9º A Posin/Previc tem como princípios:

I - alinhamento estratégico: alinhamento das ações de SI com as suas estratégias de planejamento organizacional;

II - engajamento da alta administração: comprometimento da alta direção na coordenação de esforços e no estabelecimento de políticas, de estratégias e de diretrizes relacionadas à SI;

III - publicidade: transparência das informações públicas, observados os critérios legais;

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

V - sigilo: garantia ao sigilo das informações imprescindíveis à segurança da sociedade e do Estado e à inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

VI - proteção permanente: preservação do acervo e dos seus ativos de informação;

VII - capacitação contínua: educação como alicerce fundamental para o fomento da cultura em SI; e

VIII - economicidade: o custo das ações de SI não deve ser maior do que o valor do ativo da informação a ser protegido, salvo os casos formalmente analisados e justificados durante o processo de Gestão de Riscos.

CAPÍTULO IV

GESTÃO DA SEGURANÇA DA INFORMAÇÃO

Art. 10. A Gestão da Segurança da Informação (GSI) tem como objetivo prover segurança às informações geradas, adquiridas ou custodiadas sob a responsabilidade da Previc, sendo composta pelas seguintes atividades:

I - Gestão de Ativos de Informação;

II - Tratamento da Informação, Segurança e Privacidade dos Dados;

III - Segurança Física e do Ambiente;

IV - Gestão de Incidentes em Segurança da Informação;

V - Gestão de Mudanças em Segurança da Informação;

VI - Gestão dos Recursos de Tecnologia da Informação;

VII - Controles de Acesso à Informação;

VIII - Gestão de Riscos de Segurança da Informação;

IX - Gestão de Continuidade de Negócios;

X - Conscientização, Capacitação e Sensibilização em Segurança da Informação; e

XI - Auditoria e Conformidade.

§ 1º As atividades da GSI podem ser alteradas conforme necessidade e conveniência da Previc.

§ 2º As atividades da GSI da Previc são interdependentes e devem ser estruturadas e monitoradas de forma a permitir sua melhoria contínua.

§ 3º O método PDCA (Plan-Do-Check-Act) deve ser utilizado na estruturação do ciclo de ações das atividades da GSI.

§ 4º As atividades da GSI devem ser desenvolvidas em sintonia com os normativos vigentes e as boas práticas.

Art. 11. A GSI deve compreender ações e métodos que visem a estabelecer parâmetros adequados, relacionados à SI, para a disponibilização dos serviços, sistemas e infraestrutura que os apoiam, de forma que atendam aos

requisitos mínimos de qualidade e reflitam as necessidades operacionais da Previc.

Art. 12. A GSI deve ser dinâmica e deve evoluir em conjunto com os objetivos estratégicos de segurança da Previc.

Art. 13. Para cada uma das atividades constantes das seções deste capítulo deve ser observada a pertinência de elaboração de políticas, de procedimentos, de normas, de orientações e/ou de manuais que disciplinem ou facilitem o seu entendimento.

Art. 14. A Estrutura para a GSI da Previc tem a seguinte composição:

I - Comitê de Segurança da Informação (CSI);

II - Gestor de Segurança da Informação; e

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

Parágrafo único. A finalidade, as competências, a composição e o regimento de cada um dos componentes referidos no *caput* devem ser definidos em portarias específicas propostas pelo CSI.

CAPÍTULO V

DAS DIRETRIZES

Seção I

Da Gestão de Ativos de Informação

Art. 15. Os ativos de informação da Previc devem:

I - ser inventariados e protegidos;

II - ter identificados, formalmente, o proprietário do ativo de informação e o custodiante do ativo de informação;

III - ter mapeadas as suas ameaças, vulnerabilidades e interdependências;

IV - ter a entrada e a saída das dependências e unidades referidas nos incisos I a III do art. 3º autorizadas e registradas pelo proprietário do ativo de informação;

V - ser passíveis de monitoramento e ter seu uso investigado quando houver indícios de quebra de segurança, por meio de mecanismos que permitam a rastreabilidade do uso desses ativos; e

VI - 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. 16. O custodiante do ativo de informação deve ser formalmente designado pelo proprietário do ativo de informação.

Parágrafo único. A não designação pressupõe que o proprietário do ativo de informação é o próprio custodiante.

Art. 17. Os gestores dos ativos de informação devem estabelecer regras e mecanismos que visem à manutenção de uma base de conhecimento sobre a

realização de atividades na Previc, observadas as normas de segurança da informação.

Seção II

Do Tratamento da Informação, da Segurança e da Privacidade dos Dados

Art. 18. A Previc deve criar, gerir e avaliar critérios de tratamento da informação, de acordo com o sigilo requerido e a respectiva relevância, criticidade e sensibilidade, observando a legislação em vigor.

Art. 19. A Previc deve estabelecer critérios, procedimentos e responsabilidades para a classificação da informação segundo o grau de proteção requerido e criar os controles voltados a assegurar que o grau de proteção atribuído à informação seja efetivamente observado ao longo de seu ciclo de vida.

§ 1º A informação deve ser classificada em termos de valor, de requisitos legais aplicáveis, de sensibilidade e de criticidade para a Previc.

§ 2º A classificação da informação deve alinhar-se ao disposto na Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), e nas leis que definem os sigilos fiscal, bancário, comercial e aqueles relativos a denúncias.

§ 3º Compete à Previc classificar a informação por ela produzida.

§ 4º Cabe à Previc respeitar a classificação atribuída na origem da informação recebida de terceiros.

§ 5º Todas as pessoas referidas no inciso VI do art. 3º devem ser capazes de identificar a classificação atribuída a um ativo de informação.

§ 6º As cópias de documentos classificados devem sofrer o mesmo processo de classificação de seu original.

Art. 20. Os agentes de tratamento de dados pessoais devem adotar medidas de segurança, técnicas e administrativas, aptas a proteger os dados pessoais de incidentes que possam representar não conformidade com os princípios gerais previstos na Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais - LGPD), bem como suas normas regulamentares.

Seção III

Da Gestão da Segurança Física e do Ambiente

Art. 21. Os ativos de informação da Previc devem ser protegidos contra incidentes que possam torná-los indisponíveis, com efeitos adversos à realização dos seus negócios.

Art. 22. Os recursos tecnológicos, de infraestrutura e os ambientes físicos utilizados para suportar os sistemas de informação devem:

I – ter controle de acesso físico;

II – ter condições ambientais adequadas; e

III - ser protegidos contra situações de indisponibilidade causadas por incidentes em SI.

Seção IV

Da Gestão de Incidentes em Segurança da Informação

Art. 23. O processo de Gestão de Incidentes em Segurança da Informação deve implantar normas, políticas e procedimentos que definam a responsabilidade e estabeleçam respostas rápidas, efetivas e ordenadas a incidentes de SI.

Parágrafo único. São incidentes em SI quaisquer ameaças internas ou externas, representadas por:

I - ataques, intrusões ou acessos não autorizados ou indevidos;

II - falhas, perdas, furtos ou roubos;

III - interrupções não programadas, desastres, contingências ou situações de destruição;

IV - alteração indevida ou equivocada;

V - comunicação inapropriada, deficiente ou incorreta; ou

VI - qualquer outra forma de tratamento inadequado ou ilícito que possa ter causado ou vir a causar dano à disponibilidade no acesso aos ativos de informação da Previc.

Art. 24. Os incidentes de SI devem ser identificados, monitorados, comunicados, analisados e devidamente tratados pelas áreas responsáveis pelos respectivos ativos de informação impactados, de forma a assegurar a continuidade das atividades e o não comprometimento do alcance dos objetivos estratégicos da Previc.

Seção V

Da Gestão de Mudanças em Segurança da Informação

Art. 25. As mudanças nos processos de negócio e nos ambientes tecnológicos da Previc que possam afetar a SI devem ser controladas e formalmente autorizadas.

Art. 26. O processo de gestão de mudanças nos aspectos de SI deve ser respaldado pelas informações levantadas no relatório de identificação, análise e avaliação de riscos de SI e no relatório de tratamento de riscos de SI.

Art. 27. O processo mencionado no art. 26 deve promover o controle das mudanças planejadas e considerar a análise crítica das consequências de mudanças não previstas, atuando em ações para amenizar os efeitos adversos.

Seção VI

Da Gestão dos Recursos de Tecnologia da Informação

Art. 28. Os recursos de TI da Previc têm como objetivo atender aos propósitos de negócios da Autarquia.

Parágrafo único. Para fins do disposto nesta Posin/Previc, são

considerados recursos de TI os equipamentos, os sistemas, as aplicações, as redes de comunicação, o correio eletrônico institucional, os meios de acesso à internet, as mídias sociais institucionais, os recursos de computação em nuvem, entre outros.

Art. 29. Os recursos de TI devem ser permanentemente protegidos contra incidentes.

Subseção I

Do Correio Eletrônico

Art. 30. As diretrizes específicas e procedimentos próprios ao serviço de correio eletrônico devem ser estabelecidas em norma complementar, considerando as seguintes diretrizes gerais:

I - o serviço de correio eletrônico será oferecido como um recurso institucional para apoiar os seus usuários no cumprimento das atividades; e

II - o correio eletrônico deverá ser utilizado somente para fins corporativos e relacionados às atividades do usuário no âmbito da Previc, sendo vedado o uso para fins pessoais.

Subseção II

Do Uso e do Acesso à Internet

Art. 31. As diretrizes específicas e os procedimentos próprios de controle de acesso e de uso de informações obtidas, recebidas, produzidas ou transmitidas por intermédio da internet, mediante a utilização de equipamentos, de tecnologias e de serviços de propriedade da Previc pelas pessoas referidas no inciso VI do art. 3º, devem ser estabelecidas em norma complementar, visando assegurar o cumprimento desta Posin/Previc.

Parágrafo único. As informações referidas no *caput* estão sujeitas, nos termos da legislação vigente:

I - a registro, a monitoramento e a auditoria; e

II - ao bloqueio de acesso ao arquivo, ao sítio, ao correio eletrônico e ao domínio ou aplicação em que estejam ou possam vir a estar armazenadas.

Subseção III

Do Uso Institucional das Redes Sociais

Art. 32. A utilização de perfis institucionais mantidos em redes sociais com o objetivo de prestar atendimento e serviços públicos, divulgar ou compartilhar informações da Previc, deve ser regida por normas internas específicas e estar em consonância com a Posin/Previc e com os seus objetivos estratégicos.

Art. 33. Os perfis institucionais mantidos nas redes sociais devem ser administrados pela Assessoria de Comunicação Social e Parlamentar.

Subseção IV

Do Uso de Computação em Nuvem

Art. 34. 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 internas, atendendo às determinações desta Posin/Previc e às demais orientações governamentais.

Art. 35. É vedado o uso de recurso de computação em nuvem não disponibilizado institucionalmente pela Previc para o armazenamento de informação institucional ou custodiada.

Seção VII

Do Controle de Acesso à Informação

Art. 36. O usuário deve ter acesso apenas aos ativos de informação necessários e indispensáveis à realização do seu trabalho, respeitando as recomendações de sigilo estabelecidas e a legislação específica de classificação de informação.

Art. 37. O acesso às informações que não sejam públicas deve ser restrito às pessoas que tenham necessidade de conhecê-las e estar submetido a controles compatíveis com a classificação quanto à confidencialidade.

Art. 38. O acesso aos ativos de informação e sua utilização, quando autorizados, devem ser condicionado à assinatura de Termo de Responsabilidade, observando a legislação em vigor.

Art. 39. A Política de Controle de Acesso deve ser estruturada com base nos requisitos de acesso das áreas de negócios da Previc.

Parágrafo único. O estabelecimento de perfis de acesso para usuário deve ser baseado nos requisitos dos negócios.

Art. 40. Todo acesso à informação realizado por usuário da Previc em ambiente de tecnologia deve ser registrado.

Seção VIII

Da Gestão de Riscos de Segurança da Informação

Art. 41. O processo de gestão de riscos de SI deve contemplar o contexto institucional, a identificação, a análise, a avaliação, o tratamento de riscos, a comunicação e consulta junto às partes interessadas, o monitoramento e a melhoria contínua.

Parágrafo único. Os riscos devem ser identificados, avaliados, priorizados e mitigados com base em critérios para a sua aceitação, considerando os objetivos estratégicos da Previc.

Art. 42. A Gestão de Riscos de Segurança da Informação deve avaliar os riscos relativos à segurança dos ativos de informação, em conformidade com as exigências regulatórias ou legais.

Seção IX

Da Gestão de Continuidade de Negócios

Art. 43. As ações de continuidade de negócios devem priorizar os processos críticos de negócios da Previc.

Art. 44. O Plano de Continuidade de Negócios da Previc deve incluir a análise de dependências externas aos negócios e de contratos existentes.

Art. 45. O CSI pode instituir, formalmente e de modo restrito à sua área de atuação, grupo de trabalho com objetivo de propor, manter e periodicamente testar medidas de gestão da continuidade e recuperação da informação, visando reduzir para um nível aceitável ou previamente definido a possibilidade de interrupção ou o impacto causado por incidentes nos recursos de TI que suportam os processos críticos da Previc, até que se retorne à normalidade.

Seção X

Da Conscientização, da Capacitação e da Sensibilização em Segurança da Informação

Art. 46. As pessoas que possuem acesso aos ativos de informação da Previc devem ser periodicamente conscientizadas, capacitadas e sensibilizadas em assuntos relacionados a SI.

Parágrafo único. A conscientização, a capacitação e a sensibilização em SI devem ser adequadas aos papéis e às responsabilidades das pessoas referidas no inciso VI do art. 3º.

Seção XI

Da Auditoria e da Conformidade

Art. 47. O cumprimento desta Posin/Previc, bem como dos normativos que a complementem, devem ser avaliados periodicamente por meio de verificações de conformidade, buscando a certificação do cumprimento dos requisitos de SI e da garantia de cláusula de responsabilidade e de sigilo, constantes de termos de responsabilidade, contratos, convênios, acordos e instrumentos congêneres.

Art. 48. Os resultados de cada ação de verificação de conformidade devem ser documentados em relatório de avaliação de conformidade.

Art. 49. As atividades, produtos e serviços desenvolvidos na Previc devem estar em conformidade com requisitos de SI presentes na legislação e nos contratos jurídicos vigentes, zelando pela proteção da privacidade das informações pessoais, profissionais e de terceiros.

Seção XII

Dos Contratos, dos Convênios, dos Acordos e dos Instrumentos Congêneres

Art. 50. Todos os contratos, os convênios, os acordos e os instrumentos congêneres devem:

I - conter cláusulas que estabeleçam a obrigatoriedade de observância desta Posin/Previc e de seus normativos complementares;

II - conter a previsão de termo específico de responsabilidade e de sigilo, quando a natureza de seu objeto ou condições específicas assim o exigirem;

III - prever a obrigação de divulgação desta Posin/Previc e suas normas complementares aos agentes externos envolvidos em atividades relacionadas ao instrumento celebrado, por meio da assinatura de termo de ciência, quando a natureza de seu objeto ou condições específicas assim o exigirem; e

IV - tratar os dados pessoais de acordo com as determinações da LGPD.

CAPÍTULO VI

DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 51. Compete ao CSI:

I - prover a orientação e o patrocínio necessários às ações de SI da Previc, de acordo com os objetivos estratégicos e com as leis e regulamentos pertinentes;

II - constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre SI na Previc;

III - participar da elaboração da Política de Segurança da Informação e das normas internas de SI da Previc;

IV - propor alterações à Política de Segurança da Informação e às normas internas de SI da Previc; e

V - deliberar sobre normas internas de SI da Previc.

Art. 52. Compete ao Gestor de Segurança da Informação (GSI):

I - coordenar o CSI;

II - coordenar a elaboração da Política de Segurança da Informação e das normas internas de SI da Previc, observadas as normas afins exaradas pelo Gabinete de Segurança Institucional da Presidência da República;

III - assessorar a Diretoria Colegiada da Previc na implementação da Política de Segurança da Informação;

IV - estimular ações de capacitação e de profissionalização de recursos humanos em temas relacionados à SI;

V - promover a divulgação da política e das normas internas de SI da Previc às pessoas referidas no inciso VI do art. 3º;

VI - incentivar estudos de novas tecnologias, bem como seus eventuais impactos relacionados à SI na Previc;

VII - propor os recursos necessários às ações de SI na Previc;

VIII - acompanhar os trabalhos da ETIR;

IX - verificar os resultados dos trabalhos de auditoria sobre a gestão da SI da Previc;

X - acompanhar a aplicação de ações corretivas e administrativas cabíveis nos casos de violação da SI da Previc; e

XI - manter contato direto com o Departamento de Segurança da Informação do Gabinete de Segurança Institucional da Presidência da República em assuntos relativos a SI.

Art. 53. A ETIR é responsável por:

I - coordenar as atividades de tratamento e resposta a incidentes de SI;

II - agir proativamente com o objetivo de evitar a ocorrência de incidentes de SI, divulgando práticas e recomendações e avaliando as condições de segurança de rede por meio de verificações de conformidade;

III - realizar ações reativas aos incidentes de SI, incluindo o recebimento de notificações, orientação de equipes para a realização de reparos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

IV - analisar os incidentes de SI ocorridos na rede da Previc;

V - gerar informações quantitativas acerca dos incidentes ocorridos, descrevendo, no que couber, sua natureza, seus impactos, as vulnerabilidades encontradas, a data de ocorrência, a frequência e os custos resultantes;

VI - comunicar imediatamente ao Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo a existência de vulnerabilidades ou incidentes de segurança cibernética que impactem ou que possam impactar os serviços prestados ou contratados pela Previc;

VII - notificar o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo quanto aos incidentes cibernéticos de maior impacto, com base nas informações obtidas pela ETIR no tratamento dos incidentes analisados;

VIII - comunicar de forma imediata ao Gestor de Segurança da Informação os incidentes referidos pelos incisos VI e VII do *caput*; e

IX - sanar, com urgência, as vulnerabilidades encontradas, em especial aquelas identificadas nos alertas e nas recomendações expedidos pelo Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos de Governo.

Parágrafo único. Os incidentes de maior impacto, a que se refere o inciso VII do *caput*, devem ser objeto de classificação de severidade com base no processo de gestão de riscos de SI da Previc.

Art. 54. As pessoas referidas no inciso VI do art. 3º, no uso dos ativos de informação da Previc, são responsáveis por:

I - observar o disposto nesta Posin/Previc e normativos decorrentes;

II - zelar pela integridade e segurança de todos os ativos de informação e recursos de TI que lhe forem disponibilizados pela Previc;

III - utilizar os ativos de informação e os recursos de TI disponibilizados pela Previc exclusivamente para a execução das atividades institucionais;

IV - comunicar os incidentes que afetem ou possam vir a afetar a segurança dos ativos de informação à ETIR;

V - informar ao Gestor de Segurança da Informação qualquer tipo de ação que implique em descumprimento desta Posin/Previc; e

VI - reportar imediatamente à ETIR qualquer caso de quebra de SI por

meios eletrônicos, para que sejam adotadas as providências cabíveis.

CAPÍTULO VII
DAS PENALIDADES

Art. 55. O descumprimento ou violação desta Posin/Previc ou de suas normas e procedimentos complementares, bem como realização de ações que infrinjam os controles de SI podem acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o contraditório e a ampla defesa.

Parágrafo único. Os casos de descumprimento ou violação desta Posin/Previc devem ser registrados e comunicados ao Gestor de Segurança da Informação da Previc, para ciência e adoção das providências cabíveis.

CAPÍTULO VIII
DAS DISPOSIÇÕES FINAIS

Art. 56. A Posin/Previc deve ser analisada criticamente a intervalos planejados ou quando mudanças significativas ocorrerem para assegurar a sua contínua pertinência, adequação e eficácia.

Art. 57. A periodicidade máxima para a revisão da Posin/Previc não deve exceder 4 (quatro) anos.

Art. 58. A Posin/Previc, as normas internas de SI e suas atualizações devem ser amplamente divulgadas a todos as pessoas referidas no inciso VI do art. 3º.

Art. 59. Os casos omissos e as dúvidas com relação a esta Política deverão ser submetidos ao CSI.

Art. 60. O Comitê Executivo de Tecnologia da Informação (Cexti), de que trata a Portaria Previc nº 973, de 12 de novembro de 2019, exercerá as competências do CSI enquanto esse último não for constituído.

Parágrafo único. O presidente do Cexti exercerá as competências do GSI enquanto não houver normativo específico de criação do CSI.

Art. 61º Esta Portaria entra em vigor na data de sua publicação.

Ricardo Pena Pinheiro

Diretor-Superintendente

Documento assinado eletronicamente por **Ricardo Pena Pinheiro**, **Diretor(a) Superintendente**, em 10/04/2023, às 11:31, conforme horário oficial de Brasília, com fundamento no §3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.