CENTRO DE TECNOLOGIA DA INFORMAÇÃO RENATO ARCHER

PORTARIA CTI Nº 164, DE 18 DE NOVEMBRO DE 2021

Institui a Política de Segurança da Informação - POSIN do CTI.

O DIRETOR DO CENTRO DE TECNOLOGIA DA INFORMAÇÃO RENATO ARCHER SUBSTITUTO, Unidade de Pesquisa do Ministério da Ciência, Tecnologia e Inovações (MCTI), nomeado por meio da Portaria nº 3.843, de 7 de outubro de 2020, publicada no Diário Oficial da União (DOU) de 14 de outubro de 2020, seção 2, página 9, em conformidade com as competências delegadas pela Portaria MCT nº 407, de 29 de junho de 2006, publicada no DOU de 30 de junho de 2006, e CONSIDERANDO

A Portaria nº 4.711, de 18 de agosto de 2017, que aprova a Política de Segurança da Informação e Comunicações do Ministério da Ciência, Tecnologia, Inovações e Comunicações (Posic/MCTIC);

O Decreto nº 9.637, de 26 de dezembro de 2018, que institui a Política Nacional de Segurança da Informação e dá outras providências;

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

A Instrução Normativa GSI nº 01, de 27 de maio de 2020 (alterada pela Instrução Normativa GSI nº 02, de 24 de julho de 2020), que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

A Portaria GSI nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação;

A Portaria MCTI nº 3.426, de 10 de setembro de 2020, que aprova o Regimento Interno do CTI,

RESOLVE:

Art. 1º Instituir a Política de Segurança da Informação – POSIN do Centro de Tecnologia da Informação Renato Archer - CTI, na forma do Anexo I.

Art. 2º Esta Portaria entra em vigor em 01 de dezembro de 2021.

ANEXO I DA PORTARIA CTI Nº 164, DE 18 DE NOVEMBRO DE 2021

CAPÍTULO I – DO ESCOPO

Art. 1º A Política de Segurança da Informação do Centro de Tecnologia da Informação Renato Archer alinha-se às estratégias estabelecidas pelo Plano Diretor do CTI e objetiva garantir a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações produzidas ou custodiadas pelo

CTI.

Art. 2º Esta POSIN deve obedecer aos princípios constitucionais, administrativos e do arcabouço legal que rege a Administração Pública Federal.

Art. 3º A Gestão de Segurança da Informação no CTI deve apoiar e orientar a tomada de decisões institucionais para otimizar investimentos em segurança que visem à eficiência, à eficácia e à efetividade das ações de Segurança da Informação.

Art. 4º Integram esta POSIN as normas e os procedimentos complementares destinados à proteção da informação e à disciplina de sua utilização, já existentes no âmbito da Administração Pública Federal ou a serem criadas em texto complementar.

Art. 5º Esta POSIN deve ser observada por todo agente público que execute atividades no CTI.

§ 1º O conceito de agente público é o constante do Glossário de Segurança da Informação, aprovado pela Portaria GSI nº 93/2019.

§ 2º Todos os agentes públicos em atividade no CTI são solidariamente responsáveis e devem estar comprometidos com a Segurança da Informação no âmbito da instituição.

Art. 6º Esta POSIN também se aplica, no que couber, ao relacionamento institucional do CTI com terceiros e aos contratos, convênios, acordos e outros instrumentos congêneres celebrados pelo CTI e que envolvam quaisquer dos aspectos associados à Segurança da Informação.

§ 1º Os contratos, convênios, acordos e instrumentos congêneres devem conter a previsão de termo específico de responsabilidade e sigilo, quando a natureza de seu objeto ou condições específicas assim o exigirem.

§ 2º Os contratos, convênios, acordos e instrumentos congêneres devem prever a obrigação de divulgação desta POSIN e suas normas complementares aos empregados envolvidos em atividades do instrumento celebrado, por meio da assinatura de termo de ciência, quando a natureza de seu objeto ou condições específicas assim o exigirem.

CAPÍTULO II – DOS CONCEITOS E DEFINIÇÕES

Art. 7º Para os fins desta POSIN devem ser adotados os conceitos insertos na Portaria GSI nº 93, de 26 de setembro de 2019, que aprova o Glossário de Segurança da Informação, observadas as atualizações constantes do art. 9º desta Política.

Art. 8º Em conformidade com o disposto na Instrução Normativa GSI nº 01, de 27 de maio de 2020, o conceito de Segurança da Informação abrange:

I - a segurança cibernética;

II - a defesa cibernética;

III - a segurança física;

IV - a proteção de dados organizacionais; e

V - as ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade da informação.

Art. 9º No âmbito desta POSIN, destacam-se os seguintes conceitos e definições basilares, com fundamento no Glossário de Segurança da Informação aprovado pela Portaria GSI nº 93/2019:

I – Ativos de informação: meios de produção, armazenamento, transmissão ou processamento da informação, sistemas ou equipamentos utilizados para esses fins, os locais onde se encontram esses meios, e os recursos humanos que a eles têm acesso.

II – Autenticidade: propriedade que assegura que a informação foi produzida, expedida, modificada ou

destruída por determinado indivíduo, entidade, equipamento ou sistema.

III – CGTIC, Comitê de Governança de Tecnologia da Informação e Comunicação: estrutura colegiada com a incumbência de orientar e amparar o processo decisório associado à governança de tecnologia da informação e comunicação.

IV – Confidencialidade (ou Sigilo): propriedade que assegura que a informação não está acessível e não pode ser revelada a pessoas, entidades ou sistemas não autorizados nem credenciados.

V – CSIN, Comitê de Segurança da Informação: grupo de pessoas com a responsabilidade de assessorar o CGTIC no que tange à implementação das ações de segurança da informação.

VI – DICSI, Divisão de Infraestrutura Computacional e Sistemas de Informação: unidade interna responsável pela gestão da tecnologia da informação e comunicação no âmbito do CTI.

VII – DIGEP, Divisão de Gestão de Pessoas: unidade organizacional do CTI responsável pelas ações institucionais na área de gestão de recursos humanos.

VIII – Disponibilidade: propriedade que assegura que a informação está acessível e utilizável por determinada pessoa, entidade, equipamento ou sistema, devidamente autorizados.

IX – ETIR, Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e eventos relacionados a incidentes de segurança cibernética que envolvam ou tenham impacto sobre os recursos de tecnologia da informação e comunicação do CTI.

X – Gestor de Segurança da Informação: servidor responsável pela coordenação do CSIN e pelo assessoramento da alta administração na implementação desta POSIN.

XI – Integridade: propriedade que assegura que a informação não foi alterada, modificada ou destruída, de maneira não autorizada ou acidental.

XII – Segurança da Informação: conjunto de ações que visam assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

XIII – TIC: acrônimo de Tecnologia da Informação e Comunicação.

XIV – VPN (*Virtual Private Network* ou Rede Privada Virtual): canal privado de comunicação implementado com o uso da infraestrutura de uma rede pública, como a Internet, por exemplo. O acesso a uma VPN é restrito a usuários autorizados e técnicas criptográficas são empregadas para garantir atributos de segurança – como sigilo, integridade e autenticidade – das informações em trânsito.

CAPÍTULO III – DOS PRINCÍPIOS

Art. 10. Constituem princípios desta POSIN:

I - respeito e promoção dos direitos humanos e das garantias fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação;

II - visão abrangente e sistêmica da segurança da informação;

III - intercâmbio científico e tecnológico relacionado à segurança da informação entre os órgãos e as entidades da administração pública federal;

IV - desenvolvimento econômico e tecnológico e promoção da inovação;

V - preservação do acervo, dos processos e dos ativos do CTI;

VI – capacitação para o fomento da cultura em segurança da informação;

VII - orientação à gestão de riscos e à gestão da segurança da informação;

VIII - prevenção e tratamento de incidentes de segurança da informação;

IX - articulação entre as ações de segurança cibernética, de defesa cibernética e de proteção de dados e ativos da informação;

X - dever de garantir o sigilo das informações imprescindíveis à segurança da sociedade e do Estado e a inviolabilidade da intimidade da vida privada, da honra e da imagem das pessoas;

XI – aderência à missão regimental do CTI e sua estrutura organizacional, seus objetivos estratégicos, processos, requisitos legais e demais normas atinentes ao seu funcionamento.

CAPÍTULO IV – DAS DIRETRIZES GERAIS

Seção I
DO TRATAMENTO DA INFORMAÇÃO

Art. 11. As diretrizes de segurança da informação descritas nesta POSIN devem ser observadas por todos os usuários que executem atividades no CTI, durante todas as etapas do tratamento da informação, a saber: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transferência, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, modificação, comunicação, difusão, extração, avaliação ou controle da informação.

Art. 12. As informações geradas, adquiridas ou custodiadas sob a responsabilidade do CTI são consideradas parte do seu patrimônio intelectual não cabendo a seus criadores qualquer forma de direito patrimonial, salvo aqueles direitos garantidos no âmbito da Lei de Inovação (Lei nº 10.973/2004) e outros dispositivos legais, e devem ser protegidas segundo as diretrizes descritas nesta Política, em seus documentos complementares e nas demais regulamentações em vigor.

Art. 13. É vedada a utilização de informações produzidas por terceiros para uso exclusivo do CTI em quaisquer projetos ou atividades de uso diverso do originalmente estabelecido, salvo autorização específica emitida pelo proprietário da informação, nos processos e documentos de sua competência, observada a legislação em vigor.

Parágrafo único. Nos casos de obtenção de informações de terceiros, o gestor da área na qual a informação será utilizada deve, se necessário, providenciar junto ao cedente a documentação formal relativa à cessão de direitos sobre essas informações, antes de seu uso.

Art. 14. Nos termos da Lei de Acesso à Informação (Lei n° 12.527/2011), é vedada a divulgação e uso por terceiros de informações restritas ou classificadas por grau de sigilo, produzidas ou custodiadas pelo CTI, salvo nos casos de autorização específica.

Art. 15. Informações geradas, adquiridas ou custodiadas pelo CTI podem ser classificadas segundo seu grau de relevância, prioridade, necessidade, criticidade, confidencialidade ou sensibilidade, para indicar o nível de proteção requerido para seu tratamento, observada a legislação em vigor.

§ 1º Quando classificadas, deverão ser observadas as exigências das atividades da instituição, considerando as implicações que determinado grau de classificação trará para os seus objetivos institucionais, observada a legislação em vigor.

§ 2º Cópias de documentos que contenham informações classificadas deverão sofrer o mesmo processo de classificação de seu original.

§ 3º A classificação da informação será regulamentada por norma específica.

Art. 16. O tratamento de informações que contenham dados pessoais deverá observar estritamente as determinações da Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018).

Seção II
DA SEGURANÇA FÍSICA E DO AMBIENTE

Art. 17. O Comitê de Segurança da Informação (CSIN) do CTI, em conjunto com a DICSI, deve promover mecanismos de proteção às instalações físicas e áreas de processamento de informações críticas ou sensíveis contra acesso indevido, danos e interferências, em resposta aos riscos identificados.

Parágrafo único. Os mecanismos de proteção estabelecidos devem estar alinhados aos riscos identificados.

Seção III
DA GESTÃO DE INCIDENTES EM SEGURANÇA DA INFORMAÇÃO

Art. 18. O Gestor de Segurança da Informação deverá acompanhar os trabalhos da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) do CTI, cuja atuação será orientada por normas, padrões e procedimentos técnicos exarados pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo (CTIR Gov), sem prejuízo das demais metodologias e padrões conhecidos ou que vierem a ser adotados pelo CTI na forma dos regulamentos.

Art. 19. A ETIR do CTI integrará a rede constituída pelas equipes congêneres dos órgãos e entidades da administração pública federal, coordenada pelo Centro de Tratamento e Resposta a Incidentes Cibernéticos de Governo, do Gabinete de Segurança Institucional da Presidência da República.

Art. 20. A gestão de incidentes de segurança da informação do CTI será regulamentada por norma específica.

Seção IV
DA GESTÃO DE ATIVOS DA INFORMAÇÃO

Art. 21. Os ativos de informação do CTI devem:

I - ser inventariados e protegidos;

II - ter identificados, formalmente, seus proprietários e custodiantes;

III - ter mapeadas suas ameaças, vulnerabilidades e interdependências;

IV - ter as suas entradas e saídas nas dependências do CTI autorizadas e registradas por autoridade competente;

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;

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

VII - ter sua gestão regulamentada por norma específica.

Art. 22. Os recursos de infraestrutura, físicos e tecnológicos, os sistemas de informação e as aplicações do CTI devem ser protegidos contra indisponibilidade, acessos indevidos, alterações, falhas, bem como perdas, danos, furtos, roubos e interrupções não programadas.

Art. 23. O acesso dos usuários aos ativos de informação do CTI e sua utilização, quando autorizados, devem ser condicionados ao aceite de Termo de Responsabilidade próprio, observada a legislação em vigor.

Seção V

DA GESTÃO DO USO DOS RECURSOS OPERACIONAIS E DE COMUNICAÇÕES

Art. 24. A Divisão de Infraestrutura Computacional e Sistemas de Informação – DICSI do CTI deve estabelecer modelos e arquiteturas de referência, que descrevam requisitos mínimos para a disponibilização de serviços, sistemas e infraestrutura, atendendo às necessidades operacionais e de segurança desta política.

Art. 25 Os ativos de informação e os recursos de TIC do CTI serão disponibilizados somente para usuários cadastrados, mediante a utilização de credenciais individuais e intransferíveis fornecidas pela DICSI.

Art. 26. Nas atividades institucionais do CTI, deverão ser utilizados somente ativos de informação e recursos de TIC que tenham sido:

I – adquiridos e patrimoniados pelo CTI; ou

II – registrados no CTI como bens de terceiros sob a guarda da instituição; ou

III – devidamente autorizados pela DICSI, que manterá sistemas próprios de controle sobre esses ativos.

Parágrafo único. Para a utilização de equipamentos pessoais em atividades institucionais do CTI, seus proprietários deverão autorizar a DICSI a aplicar nesses equipamentos os padrões corporativos de segurança da informação.

Art. 27. Os ativos de informação e os recursos de TIC disponibilizados pelo CTI – que incluem equipamentos, sistemas, aplicações, redes de comunicação, correio eletrônico, acesso à internet, mídias sociais, recursos de computação em nuvem, entre outros – deverão ser utilizados exclusivamente para a execução de atividades institucionais.

Art. 28. Toda a informação que trafega pelos ativos de informação e demais recursos de TIC do CTI poderá ser monitorada de acordo com as necessidades de segurança da informação estabelecidas pelo CSIN e aprovadas pelo CGTIC do CTI, respeitada a legislação vigente.

Art. 29. Em caso de desligamento ou impedimento de um agente público que tenha executado atividades no CTI, sua chefia imediata poderá requisitar autorização formal do CGTIC para que a DICSI recupere informações armazenadas em ativos de informação do CTI, ou de terceiros que estejam sob a guarda da instituição, utilizados por esse agente.

Art. 30. Serão estabelecidos processos permanentes de conscientização, capacitação e sensibilização em segurança da informação, que alcancem todos os agentes públicos que executem atividades no CTI, de acordo com suas competências funcionais.

Seção VI
DOS CONTROLES DE ACESSO ÀS INFORMAÇÕES

Art. 31. Eventos relevantes, previamente definidos, devem ser registrados para a segurança e o rastreamento de acesso às informações.

Parágrafo único. Devem ser criados mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

Art. 32. A autorização, o acesso e o uso da informação e dos recursos de TIC devem ser controlados e limitados ao necessário para o cumprimento das atribuições de cada usuário, e qualquer outra forma de uso ou acesso além do necessário depende de autorização do responsável pelo ativo de informação, observando-se a legislação em vigor.

§ 1º A identificação do usuário, qualquer que seja o meio e a forma adotados, deve ser pessoal e

intransferível, e deve permitir o seu reconhecimento de maneira clara, inequívoca e irrefutável.

§ 2º Sempre que houver mudança nas atribuições de determinado usuário, os seus privilégios de acesso às informações e aos recursos computacionais devem ser imediatamente readequados, devendo ser cancelados em caso de seu desligamento do CTI.

§ 3º Todos os sistemas de informação do CTI, automatizados ou não, devem ter um custodiante do ativo da informação, formalmente designado pela autoridade competente, que deve definir os privilégios de acesso às informações, observando-se a legislação em vigor.

Art. 33 O usuário é responsável por todos os atos praticados com suas identificações pessoais, bem como pela segurança dos ativos de informação que estejam sob sua responsabilidade, salvo em situações que comprovadamente ocorram sem o seu conhecimento ou seu consentimento.

Art. 34. O acesso remoto, quando autorizado pela autoridade competente, deve ser implementado por meio de uma VPN (*Virtual Private Network* ou Rede Privada Virtual) e utilizar somente recursos devidamente autorizados pela Divisão de Infraestrutura Computacional e Sistemas de Informação – DICSI do CTI.

Seção VII
DA GESTÃO DE RISCOS

Art. 35. As áreas responsáveis por ativos de informação devem implantar processos contínuos de gestão de riscos, os quais serão aplicados na implementação e operação da gestão da segurança da informação.

§ 1º Os processos de gestão de riscos devem permitir a identificação de ameaças potenciais aos ativos de informação e a implementação das medidas de proteção necessárias para eliminar ou reduzir as vulnerabilidades desses ativos e os impactos negativos provocados por essas ameaças sobre sua operação.

§ 2º A gestão de riscos de Tecnologia da Informação deve avaliar os riscos relativos à segurança dos ativos de informação e a conformidade com exigências regulatórias ou legais.

Art. 36. A gestão de riscos de segurança da informação será regulamentada por norma específica.

Seção VIII
DA GESTÃO DE CONTINUIDADE

Art. 37. O Comitê de Segurança da Informação (CSIN) do CTI poderá instituir, formalmente, grupo de trabalho com o objetivo de propor, manter e periodicamente testar medidas de gestão da continuidade de negócio e de recuperação da informação, visando reduzir para um nível aceitável e previamente definido a possibilidade de interrupção ou o impacto na operação, causados por falhas ou desastres, dos ativos de informação que suportam os processos críticos do CTI, até que se retorne à normalidade.

Art. 38. A gestão de continuidade de negócio será regulamentada por norma específica.

Seção IX
DA AUDITORIA E CONFORMIDADE

Art. 39. A verificação de conformidade das práticas de segurança da informação do CTI deverá ser realizada sempre que necessária, não excedendo o período máximo de 3 (três) anos.

§ 1º A verificação da conformidade será realizada de forma planejada, mediante calendário de ações aprovado pelo CSIN.

§ 2º A verificação de conformidade de que trata o caput deverá tomar como referências esta POSIN, as normas e procedimentos complementares, bem como a legislação aplicável referente ao tema.

§ 3º A verificação de conformidade deverá ser realizada também nos contratos, convênios, acordos de cooperação e outros instrumentos congêneres celebrados pelo CTI.

Art. 40. A verificação de conformidade será executada por grupo de trabalho formalmente instituído pelo Comitê de Segurança da Informação (CSIN) do CTI, podendo, com a prévia aprovação deste, ser subcontratada no todo ou em parte.

§ 1º A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise documental, análise de registros (*logs*), análise de código-fonte, entrevistas e testes de invasão.

§ 2º É vedado ao prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 41. Os resultados de cada ação de verificação de conformidade serão documentados em relatório específico, que deverá ser encaminhado ao Gestor de Segurança da Informação do CTI para ciência e tomada das medidas cabíveis.

Seção X
DA AQUISIÇÃO, DO DESENVOLVIMENTO E DA MANUTENÇÃO DE SISTEMAS

Art. 42. O CSIN deverá estabelecer e submeter à aprovação do CGTIC do CTI critérios de segurança para desenvolvimento, manutenção e aquisição de sistemas e aplicações.

CAPÍTULO V – DAS COMPETÊNCIAS E RESPONSABILIDADES

Art. 43. As competências do Comitê de Segurança da Informação do CTI – CSIN, da Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos – ETIR, bem como as do Gestor de Segurança da Informação do CTI, estão definidas em Portaria própria do CTI, que trata da Política de Governança de Tecnologia da Informação e Comunicação do CTI.

Art. 44. Compete à Divisão de Infraestrutura Computacional e Sistemas de Informação – DICSI a gestão da tecnologia da informação e comunicação no âmbito do CTI, na forma do disposto no Regimento Interno da instituição.

Art. 45. Constituem responsabilidades da DICSI, no âmbito desta POSIN:

I – fornecer aos usuários cadastrados, as credenciais individuais e intransferíveis para acesso aos ativos de informação e demais recursos de TIC disponibilizados pelo CTI;

II – determinar os ativos de informação e demais recursos de TIC autorizados para uso nas atividades institucionais do CTI;

III – recuperar, mediante autorização do CGTIC, informações armazenadas em ativos de informação utilizados anteriormente por agentes públicos que tenham executado atividades no CTI, nos casos de desligamento ou impedimento desses agentes;

IV – comunicar ao Gestor de Segurança da Informação do CTI qualquer indício de violação desta POSIN ou de quebra de controles de segurança da informação;

V – suspender ou cancelar o acesso de usuários aos ativos de informação e demais recursos de TIC disponibilizados pelo CTI, nos casos identificados de violação desta POSIN ou de quebra de controles

de segurança da informação;

VI – designar, quando necessário, os responsáveis pela custódia dos ativos de informação disponibilizados pelo CTI;

VII – garantir que todo usuário com acesso autorizado aos ativos de informação e aos demais recursos de TIC disponibilizados pelo CTI assine previamente o "Termo de Responsabilidade pelo Uso de Recursos de TIC", estabelecido em norma interna específica;

VIII – realizar regularmente e manter cópias de segurança (*backup*) das informações armazenadas nos ativos de informação sob sua responsabilidade;

IX – zelar pelo cumprimento das medidas de gestão da continuidade de negócio e de recuperação da informação de que trata o art. 37;

X – zelar pelo cumprimento desta Política, na sua esfera de competência.

Art. 46. Constituem responsabilidades da Divisão de Gestão de Pessoas – DIGEP do CTI, no âmbito desta POSIN:

I – realizar, com emprego de sistema próprio, o cadastramento e o descadastramento dos agentes públicos que executam atividades no CTI, observando os normativos vigentes;

II – zelar pelo cumprimento desta Política, na sua esfera de competência.

Art. 47. Compete aos usuários dos ativos de informação e dos recursos de TIC disponibilizados pelo CTI:

I – assinar o "Termo de Responsabilidade pelo Uso de Recursos de TIC" antes de ter acesso aos ativos de informação e aos recursos de TIC que lhe forem disponibilizados pelo CTI;

II – zelar pelo sigilo de suas credenciais de acesso – tais como nome de usuário, senhas, crachá, endereço de correio eletrônico, certificado digital, *tokens* e chaves criptográficas – aos ativos de informação e demais recursos de TIC disponibilizados pelo CTI, que são pessoais e intransferíveis;

III – zelar pela integridade e segurança física de todos os ativos de informação e recursos de TIC que lhe forem disponibilizados pelo CTI;

IV – nas atividades institucionais, utilizar somente ativos de informação e recursos de TIC:

a) adquiridos e patrimoniados pelo CTI; ou

b) registrados no CTI como bens de terceiros sob a guarda da instituição; ou

c) devidamente autorizados pela DICSI.

V – utilizar os ativos de informação e os recursos de TIC disponibilizados pelo CTI – que incluem equipamentos, sistemas, aplicações, redes de comunicação, correio eletrônico, acesso à internet, mídias sociais, recursos de computação em nuvem, entre outros – exclusivamente para a execução de atividades institucionais;

VI – responsabilizar-se pelas atividades que executar com o uso dos ativos de informação e dos recursos de TIC disponibilizados pelo CTI, bem como responder, administrativa ou judicialmente, por danos, materiais ou a pessoas, que porventura provocar, na forma das normas e regulamentos aplicáveis;

VII – responsabilizar-se pelo conteúdo das informações que gerar, transferir, disponibilizar ou armazenar com o uso dos ativos de informação e dos recursos de TIC disponibilizados pelo CTI;

VIII – participar, quando solicitado, de treinamentos relacionados à segurança da informação;

IX – comunicar imediatamente à DICSI qualquer indício de que tiver ciência de violação desta POSIN ou de uso indevido dos ativos de informação e dos recursos de TIC disponibilizados pelo CTI;

X – armazenar todas as informações geradas no desempenho de suas funções institucionais em pasta de rede disponibilizada pela DICSI, cujo conteúdo é protegido por cópia de segurança regular (*backup*);

XI – cumprir fielmente as determinações desta POSIN, de suas normas e procedimentos complementares, bem como as políticas, normas, procedimentos e orientações de segurança da informação do Ministério da Ciência, Tecnologia e Inovações.

Art. 48. Para os fins desta POSIN, compete aos Coordenadores e Chefes de Divisão em exercício no CTI:

I – cumprir fielmente as determinações desta POSIN, de suas normas e procedimentos complementares, bem como as políticas, normas, procedimentos e orientações de segurança da informação do Ministério da Ciência, Tecnologia e Inovações e de outros órgãos competentes;

II – dar amplo conhecimento desta Política aos colaboradores alocados na unidade organizacional sob sua responsabilidade;

III – comunicar imediatamente à DICSI qualquer indício de que tiver ciência de violação desta POSIN ou de uso indevido dos ativos de informação e dos recursos de TIC disponibilizados pelo CTI;

IV – solicitar à DIGEP o cadastramento de colaboradores que serão alocados na unidade organizacional sob sua responsabilidade e comunicar imediatamente à DIGEP o desligamento de colaboradores;

V – responsabilizar-se pela custódia dos ativos de informação e dos recursos de TIC disponibilizados pelo CTI para uso comum em sua respectiva unidade organizacional;

VI – sugerir, e submeter à apreciação do CGTIC, a classificação da informação gerada como resultado das atividades da unidade organizacional sob sua responsabilidade;

VII – zelar pelo cumprimento desta Política, na sua esfera de competência.

CAPÍTULO VI – DAS PENALIDADES

Art. 49. A não observância desta Política ou de suas normas e procedimentos complementares, bem como a quebra de controles de segurança da informação, poderá 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. Casos notificados de descumprimento desta POSIN deverão ser registrados e encaminhados ao Gestor de Segurança da Informação do CTI para ciência e tomada das providências cabíveis.

CAPÍTULO VII – DA POLÍTICA DE ATUALIZAÇÃO

Art. 50. Esta Política, bem como o conjunto de normas e procedimentos complementares dela derivado, serão revisados em períodos não superiores a 3 (três) anos, ou sempre que se fizer necessário, por recomendação do CSIN aprovada pelo CGTIC do CTI, ou ainda quando determinado pelos órgãos legais competentes.

CAPÍTULO VIII – DISPOSIÇÕES FINAIS

Art. 51. As situações não previstas nesta Política e os casos omissos serão tratados individualmente pelo CGTIC, apoiado pelo CSIN, na forma dos regulamentos internos em vigor.

Documento assinado eletronicamente por **Fernando Ely**, **Diretor do Centro de Tecnologia da Informação Renato Archer, Substituto**, em 18/11/2021, às 16:57 (horário oficial de Brasília), com fundamento no § 3º do art. 4º do Decreto nº 10.543, de 13 de novembro de 2020.

A autenticidade deste documento pode ser conferida no site http://sei.mctic.gov.br/verifica.html, informando o código verificador **8570778** e o código CRC **AB7D2246**.

Referência: Processo nº 01241.000002/2021-61 SEI nº 8570778