Diário Oficial
Imprensa Nacional

REPÚBLICA FEDERATIVA DO BRASIL
BRASÍLIA - DF

Nº 167 - DOU – 01/09/22 - Seção 1 – p.18

MINISTÉRIO DA CIÊNCIA, TECNOLOGIA E INOVAÇÕES
CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO

PORTARIA CNPQ Nº 1.019, DE 30 DE AGOSTO DE 2022

O Presidente do CONSELHO NACIONAL DE DESENVOLVIMENTO CIENTÍFICO E TECNOLÓGICO - CNPq, no uso da atribuição que lhe confere o Decreto nº 8.866, de 3 de outubro de 2016, em conformidade com a legislação aplicável e demais atos normativos pertinentes [1], e considerando a decisão do Comitê de Segurança da Informação e Comunicações do CNPq, em sua 42ª (quadragésima segunda) reunião, em 29 de julho de 2022, e nos termos constantes dos autos do Processo nº 01300.003475/2022-50, resolve:

Art. 1º Aprovar e homologar a Política de Segurança da Informação - PoSIN do Conselho Nacional de Desenvolvimento Científico e Tecnológico.

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

Escopo

Art. 2º A Política de Segurança da Informação - PoSIN tem a finalidade de estabelecer princípios e diretrizes para a implementação de ações de segurança da informação e, no que couber, no relacionamento com outros órgãos públicos ou entidades privadas.

§ 1º Todos os instrumentos normativos complementares e procedimentos elaborados a partir da PoSIN do CNPq são partes integrantes da mesma e emanam de princípios e diretrizes nela estabelecidos.

§ 2º Os documentos que comporão a estrutura normativa de Segurança da Informação serão divididos em três categorias:

I - Política - nível estratégico: define as regras de alto nível que representam os princípios básicos que o CNPq decidiu incorporar à sua gestão de acordo com a visão estratégica da alta direção, serve como base para que as normas e procedimentos sejam elaborados e detalhados;

II - normas complementares - nível tático: especificam as escolhas tecnológicas e os controles que deverão ser implementados para alcançar o cenário definido estrategicamente nos princípios e diretrizes da Política; e

III - procedimentos - nível operacional: instrumentalizam o disposto nas normas complementares e na Política, permitindo sua aplicação direta nas atividades cotidianas do CNPq.

§ 3º As diretrizes previstas nesta PoSIN e nas demais normas e procedimentos específicos de segurança da informação do órgão são aplicadas a todos os colaboradores do CNPq, conforme definição dada no art. 4º, que tenham acesso a informações e a recursos de Tecnologia da Informação do CNPq.

§ 4º Os documentos integrantes da estrutura normativa de Governança de Segurança da Informação deverão ser divulgados a todos os colaboradores do CNPq quando da admissão e também, publicados em repositório eletrônico de documentos de maneira que seu conteúdo possa ser consultado a qualquer tempo.

§ 5º Todos são responsáveis e estarão comprometidos com a segurança da informação.

Art. 3º A Gestão de Segurança da Informação deve apoiar e orientar a tomada de decisões institucionais e otimizar investimentos em segurança que visem à eficiência, eficácia e efetividade das atividades de segurança da informação.

Conceitos e definições

Art. 4º No âmbito da PoSIN, considera-se:

I - ativo de informação: o patrimônio composto por todos os dados e informações geradas, custodiadas, manipuladas, utilizadas ou armazenada no CNPq, bem assim todos os elementos de pessoal, inclusive colaboradores que manuseiam os ativos, infraestrutura, tecnologia, hardware e software necessários à execução dos processos da organização;

II - autenticidade: propriedade pela qual se assegura que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade;

III - colaborador: todas as pessoas envolvidas com o desenvolvimento de atividades no CNPq de caráter permanente, continuado ou eventual, incluindo autoridades, servidores, prestadores de serviço, consultores e estagiários;

IV - confidencialidade: propriedade pela qual se assegura que a informação não esteja disponível ou não seja revelada a pessoa, a sistema, a entidade ou órgão não autorizado e nem credenciado;

V - diretrizes de segurança da informação: ações que definem a Política de Segurança da Informação do CNPq, visando a preservar a disponibilidade, integridade, confiabilidade e autenticidade das informações da Instituição;

VI - disponibilidade: propriedade pela qual se assegura que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados;

VII - Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais: grupo de pessoas com a responsabilidade de receber, analisar e responder às notificações e atividades relacionadas a incidentes de segurança em redes de computadores;

VIII - Gestor de Segurança da Informação: servidor público efetivo responsável pelas ações de segurança da informação do CNPq;

IX - incidente: evento, ação ou omissão, que tenha permitido, ou possa vir a permitir, acesso não autorizado, interrupção ou mudança nas operações (inclusive pela tomada de controle), destruição, dano, deleção ou mudança da informação protegida, remoção ou limitação de uso da informação protegida ou ainda a apropriação, disseminação e publicação indevida de informação protegida de algum ativo de informação crítico ou de alguma atividade crítica por um período de tempo inferior ao tempo objetivo de recuperação;

X - incidente de segurança: qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores;

XI - integridade: propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental;

XII - recursos de Tecnologia da Informação: conjunto formado pelos bens e serviços de tecnologia da informação que constituem a infraestrutura utilizada na produção, coleta, tratamento, armazenamento, transmissão, recepção, comunicação e disseminação da informação;

XIII - responsável pelo ativo de informação: servidor público responsável pela salvaguarda do ativo de informação;

XIV - risco: possibilidade de ocorrência de um evento que venha a ter impacto no cumprimento dos objetivos, sendo mensurado em termos de impacto e de probabilidade;

XV - risco de segurança da informação: potencial associado à exploração de uma ou mais vulnerabilidades de um ativo de informação ou de um conjunto de tais ativos, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização;

XVI - segurança da informação: ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações;

XVII - servidor público: toda pessoa legalmente investida em cargo público;

XVIII - sistema de Gestão de Segurança da Informação: é um conjunto de pessoas, processos e procedimentos, baseado em normas e na legislação vigente, que uma organização deve implementar para prover segurança no uso de seus ativos de informação de modo a preservá-los quanto aos aspectos de disponibilidade, integridade, confidencialidade e autenticidade, independentemente do meio em que se encontram; e

XIX - vulnerabilidades: fatores internos ou causa potencial de incidente indesejado, que podem resultar em risco para um sistema ou organização, e podem ser corrigidas ou evitadas por uma ação interna de segurança da informação.

XX - Custodiante da informação - Qualquer indivíduo ou estrutura de órgão ou entidade da Administração Pública Federal direta e indireta que tenha responsabilidade formal de proteger a informação e aplicar os níveis de controle de segurança, em conformidade com as exigências de Segurança da Informação comunicadas pelo proprietário da informação; e

XXI - Gestor de ativo de informação: pessoa responsável pela proteção dos ativos de informação.

CAPÍTULO II

DO OBJETIVO E PRINCÍPIOS

Art. 5º São objetivos da Política de Segurança da Informação do CNPq:

I - estabelecer diretrizes para a disponibilização e utilização de recursos de informação, serviços de redes de dados, estações de trabalho, internet, telecomunicações e correio eletrônico institucional;

II - designar, definir ou alterar papéis e responsabilidades do grupo responsável pela Segurança da Informação;

III - apoiar a implantação das iniciativas relativas à Segurança da Informação; e

IV - possibilitar a criação de controles e promover a otimização dos recursos e investimentos em tecnologia da informação, contribuindo com a minimização dos riscos associados.

Art. 6º A PoSIN deve orientar-se pelos seguintes princípios da Segurança da Informação: confidencialidade, disponibilidade, integridade e autenticidade.

Art. 7º Toda informação produzida ou recebida pelos colaboradores, em resultado da função exercida e/ou atividade profissional contratada, pertence ao CNPq.

Parágrafo único. As exceções devem ser explícitas e formalizadas entre as partes.

Art. 8º Todos os recursos de informação do CNPq devem ser projetados para que seu uso seja consciente e responsável.

Parágrafo único. Os recursos comunicacionais e computacionais da instituição devem ser utilizados para a consecução de seus objetivos finalísticos.

Art. 9º Deverão ser criados e instituídos controles apropriados, trilhas de auditoria ou registros de atividades, em todos os pontos e sistemas em que a instituição julgar necessário, com vistas à redução dos riscos dos seus ativos de informação.

Art. 10. Os gestores, administradores e operadores dos sistemas computacionais poderão, pela característica de suas credenciais como usuários - privilégios diferenciados associados a cada perfil -, acessar arquivos e dados de outros usuários, mediante regulamentação específica.

Parágrafo único. Tal operação só será permitida quando necessária para a execução de atividades operacionais sob sua responsabilidade.

Art. 11. Todo o acesso a redes e sistemas do órgão deverá ser feito por meio de login de acesso único, pessoal e intransferível.

Art. 12. O CNPq pode utilizar tecnologias e ferramentas para monitorar e controlar o conteúdo e o acesso a quaisquer tipos de informação alocada na infraestrutura provida pela instituição, mediante regulamentação específica.

Art. 13. Cada usuário é responsável pela segurança das informações dentro do CNPq, principalmente daquelas que estão sob sua responsabilidade.

Art. 14. Todos os requisitos de segurança da informação, incluindo a necessidade de planos de contingência, devem ser identificados na fase de levantamento de escopo de um projeto ou sistema, e justificados, acordados, documentados, implantados e testados durante a fase de execução.

Art. 15. A governança da segurança da informação no CNPq será realizada por comitê multidisciplinar, ora designado Comitê de Segurança da Informação - CSI.

Art. 16. Deverá constar em todos os contratos do CNPq, quando o objeto for pertinente, cláusula de confidencialidade e de obediência às normas de segurança da informação a ser observada por empresas fornecedoras e por todos os profissionais que desempenham suas atividades no CNPq, inclusive provenientes de organismos internacionais; deverá estar prevista, por parte das empresas e profissionais prestadores de serviço, entrega de declaração expressa de compromisso em relação à confidencialidade e de termo de ciência das normas vigentes, como condição imprescindível para que possa ser concedido acesso aos ativos de informação disponibilizados pela instituição.

CAPÍTULO III

DOS PAPÉIS E RESPONSABILIDADES

Art. 17. Os papéis são os seguintes:

PAPEL	PERFIL	ASSOCIADO DESCRIÇÃO
Usuário Interno	Colaboradores, conforme definição disposta no art. 4º	Todos os servidores, gestores, técnicos, estagiários, bolsistas de programas, consultores e colaboradores terceirizados, que fazem uso dos recursos informacionais e computacionais do CNPq.
Usuário Externo	Prestadores de serviço e demais colaboradores externos.	Prestadores de serviços contratados direta ou indiretamente pelo CNPq e demais colaboradores externos (clientes dos serviços do CNPq) que fazem uso de seus recursos informacionais e computacionais.
Gestores	Presidente, Diretores, Chefe de	Todos aqueles que exercem funções de gerência no

	Gabinete, Coordenadores Gerais, Coordenadores e Chefes de Serviço.	âmbito da organização, administrando pessoas e/ou processos.
Área de TI	Coordenação Geral de Tecnologia da Informação (CGETI)	Unidade organizacional responsável pela gestão e operação dos recursos de TI na organização e Custodiante da informação.
Gestor de Segurança da - GSI	Gestão técnica	Responsável pelas ações de segurança da informação no âmbito do órgão ou entidade da Administração Pública Federal - APF.
Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR	Equipe técnica	Grupo de pessoas com a responsabilidade de receber, analisar e responder a notificações e atividades relacionadas a incidentes de segurança em redes de computadores.
Comitê de Segurança da Informação - CSI	Alta Administração	Grupo de pessoas com a responsabilidade de assessorar a implementação das ações de segurança da informação no âmbito do órgão ou entidade da APF.

Responsabilidades gerais e comuns

Art. 18. São responsabilidades gerais e comuns a todos os usuários e gestores de serviços de rede de dados, internet, telecomunicações, estações de trabalho, correio eletrônico e demais recursos de informação e comunicação do CNPq:

I - respeitar a propriedade intelectual, não copiando, modificando, usando ou divulgando, no todo ou em parte, textos, artigos, programas ou qualquer outro material, sem a permissão expressa, por escrito, do detentor destes direitos;

II - zelar pelos equipamentos de TI que utiliza, não sendo permitida qualquer remoção, movimentação, desconexão de partes, substituição ou qualquer alteração em suas características físicas ou técnicas;

III - zelar pela segurança de seu usuário corporativo, departamental ou de rede local, bem como de seus respectivos dados e credenciais de acesso;

IV - não executar programas, instalar equipamentos ou executar ações que tenham como finalidade a decodificação de senhas, a monitoração da rede do CNPq, a leitura de dados de terceiros, a facilitação do acesso à rede do CNPq de usuários não autorizados, a propagação de vírus de computador, enganar programas e sistemas de segurança, a destruição parcial ou total de arquivos ou causar a indisponibilidade de serviços;

V - não utilizar os direitos especiais de acesso ou de qualquer outro privilégio já extintos com o término do período de ocupação de cargo ou função que tenha exercido no CNPq;

VI - não utilizar a rede do CNPq ou permissões de acesso concedidas para divulgar informações a terceiros que são sigilosas ou de interesse apenas do CNPq;

VII - não compartilhar credenciais de acesso e conexões com outras pessoas;

VIII - manter a confidencialidade, memorizar e não registrar a senha em lugar algum;

IX - alterar a senha sempre que existir qualquer suspeita do seu comprometimento;

X - comunicar imediatamente à área de Tecnologia da Informação suspeita de comprometimento de senha;

XI - seguir, de forma colaborativa, as orientações fornecidas pelos setores competentes em relação ao uso dos recursos corporativos de informação, utilizando-os sempre de forma ética, legal e consciente; e

XII - manter-se atualizado em relação a esta PoSIN, às suas normas complementares e aos procedimentos relacionados, buscando informação junto ao GSI sempre que não estiver absolutamente seguro quanto à obtenção, tratamento, uso e/ou descarte de informações.

Responsabilidades dos usuários internos e externos

Art. 19. Cabe aos usuários internos e externos:

I - conhecer e cumprir todos os princípios, diretrizes, normas complementares e procedimentos desta PoSIN, bem como os demais normativos e resoluções relacionados à segurança da informação;

II - obedecer aos requisitos de controle especificados pelos gestores e custodiantes da informação;

III - comunicar imediatamente à ETIR os incidentes que afetam a segurança dos ativos de informação;

IV - não permitir ou colaborar com o acesso aos recursos computacionais por parte de pessoas não autorizadas. Os usuários são responsáveis por qualquer atividade desenvolvida através de suas contas e pelos eventuais custos dela decorrentes em atividades não autorizadas;

V - zelar pelo uso adequado dos recursos de TI a eles disponibilizados; e

VI - cooperar na aplicação e no cumprimento desta PoSIN, bem como das normas complementares e procedimentos relacionados.

Responsabilidades dos gestores

Art. 20. Cabe aos Gestores - titular ou substituto - da unidade administrativa:

I - corresponsabilizar-se pelas ações realizadas por aqueles que estão sob sua responsabilidade;

II - conscientizar os usuários sob sua supervisão em relação aos conceitos e às práticas de segurança da informação;

III - incorporar aos processos de trabalho de sua unidade, ou de sua área, práticas inerentes à segurança da informação;

IV - tomar as medidas administrativas necessárias para que sejam aplicadas ações corretivas nos casos de comprometimento da segurança da informação por parte dos usuários sob sua supervisão;

V - informar à área de Recursos Humanos ou à área de Gestão de Contratos, conforme a condição do colaborador, por meio de formulário específico, a movimentação de pessoal de sua unidade;

VI - autorizar, de acordo com a legislação vigente, a divulgação das informações produzidas na sua unidade administrativa;

VII - comunicar à ETIR os casos de quebra de segurança; e

VIII - defender os direitos autorais (copyright), as leis que regulamentam o acesso e o uso das informações, e as regras e normas específicas de uso de recursos de TI.

Responsabilidades da área da TI

Art. 21. Cabe à área de Tecnologia da Informação:

I - garantir a segurança dos ativos de informação sob sua responsabilidade;

II - definir e gerir os requisitos de segurança para os ativos de informação, em conformidade com esta PoSIN;

III - manter os recursos de TI do Data Center, ou de estrutura similar, do CNPq sob sua gestão;

IV - preservar a disponibilidade, integridade, confidencialidade e autenticidade dos dados e informações sob sua custódia;

V - configurar os recursos informacionais e computacionais concedidos aos usuários com os controles necessários para cumprir os requerimentos de segurança da informação estabelecidos nesta PoSIN, bem como pelas normas complementares e procedimentos de segurança da informação;

VI - gerar e manter trilhas para auditoria com nível de detalhe suficiente para rastrear possíveis falhas e fraudes;

VII - zelar pela segregação de funções gerenciais e operacionais, a fim de restringir ao mínimo necessário os privilégios de cada indivíduo;

VIII - nas movimentações internas dos ativos de TI, assegurar-se de que as informações de determinado usuário sejam removidas antes de disponibilizar o ativo para outro usuário;

IX - gerir o armazenamento, processamento e transmissão de dados de forma a garantir os níveis de segurança requeridos;

X - atribuir cada conta de acesso a computadores, sistemas, bases de dados e qualquer outro ativo de informação a um responsável identificável como pessoa física, responsável pelo uso da conta;

XI - proteger continuamente todos os ativos de informação contra ameaças de segurança, buscando assegurar que novos ativos apenas sejam integrados ao ambiente de produção após cumprirem os requisitos de segurança da informação definidos;

XII - zelar pela não introdução de vulnerabilidades ou fragilidades indesejadas nos ativos de informação ou nos ambientes informacionais do CNPq durante sua operação ou de eventos de mudança de ambiente, como de desenvolvimento para teste, homologação ou produção, dentre outros;

XIII - definir regras para instalação de softwares e hardwares no ambiente corporativo e demais ambientes vinculados; e

XIV - definir metodologia e realizar auditorias periódicas de configurações técnicas e análise de riscos.

Responsabilidades da área de logística e patrimônio

Art. 22. Cabe à área de Logística e Patrimônio:

I - proteger os ativos de informação contra perdas, danos, furtos, roubos e interrupções não programadas, inclusive quanto ao fornecimento de energia e controle climático;

II - inventariar e proteger:

a) identificação e classificação de ativos de informação;

b) identificação de potenciais ameaças e vulnerabilidades quanto ao acesso físico ao ambiente do CNPq; e

c) avaliação de riscos aos ativos de informação.

III - identificar os proprietários e custodiantes;

IV - mapear ameaças, vulnerabilidades e interdependências aos ativos de informação e tomar ações visando evitá-las;

V - autorizar e registrar a entrada e saída nas dependências do CNPq de ativos de informação; e

VI - gerenciar os proprietários dos ativos de informação, realizando o registro das seguintes atividades:

a) descrever o ativo de informação;

b) definir as exigências de segurança da informação do ativo de informação;

c) comunicar as exigências de segurança da informação do ativo de informação a todos os custodiantes e usuários;

d) buscar assegurar-se de que as exigências de segurança da informação estejam cumpridas por meio de monitoramento; e

e) indicar os riscos que podem afetar os ativos de informação.

Responsabilidades do GSI

Art. 23. Cabe ao Gestor de Segurança da Informação - GSI:

I - promover cultura de Segurança da Informação;

II - acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;

III - elaborar plano de investimentos com a correspondente proposta orçamentária para as ações de Segurança da Informação;

IV - coordenar a ETIR;

V - comunicar ao CSI os resultados e outras informações pertinentes;

VI - realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação;

VII - manter contato direto com o DSIC/GSI/PR para o trato de assuntos relativos à segurança da informação; e

VIII - propor normas relativas à segurança da informação.

Responsabilidades da ETIR

Art. 24. Cabe à ETIR:

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

II - agir proativamente com o objetivo de evitar que ocorram incidentes de segurança, divulgando práticas e recomendações de segurança da informação e avaliando condições de segurança de redes por meio de verificações de conformidade;

III - realizar ações reativas que incluem recebimento de notificações de incidentes, orientação de equipes no reparo a danos e análise de sistemas comprometidos buscando causas, danos e responsáveis;

IV - analisar ataques e intrusões na rede do CNPq;

V - executar as ações necessárias para tratar quebras de segurança;

VI - obter informações quantitativas acerca dos incidentes ocorridos que descrevam sua natureza, causas, data de ocorrência, frequência e custos resultantes;

VII - cooperar com outras equipes de Tratamento e Resposta a Incidentes; e

VIII - participar em fóruns, redes nacionais e internacionais relativas à segurança da informação.

Responsabilidades do CSI

Art. 25. Cabe ao Comitê de Segurança da Informação - CSI:

I - estabelecer, regulamentar e rever, quando necessário, os princípios e diretrizes desta Política, promover e supervisionar a implementação das ações preventivas e corretivas de segurança da informação, de forma sistêmica e integrada aos negócios, e respaldar a realização de auditorias, dentre outras competências previstas em seu regimento;

II - aprovar o plano de investimentos em segurança da informação;

III - solicitar apuração de suspeitas de ocorrência de quebra de segurança da informação; e

IV - estabelecer normas e procedimentos destinados a disciplinar e proteger o uso da informação no âmbito do CNPq, complementando a Política de Segurança da Informação do Órgão, sobre, dentre outros que julgar pertinente, os seguintes temas julgados relevantes para a sua atuação:

a) tratamento da informação;

b) tratamento de incidentes de rede;

c) gestão de riscos;

d) gestão de continuidade;

e) auditoria e conformidade;

f) controles de acesso;

g) uso do correio eletrônico corporativo;

h) acesso à internet;

h) gestão de ativos de informação;

i) segurança física e do ambiente;

j) segurança em recursos humanos;

h) gestão de operações e comunicações;

i) criptografia; e

j) desenvolvimento seguro de software.

Art. 26. A alegação de desconhecimento das regras contidas nesta PoSIN não exime o usuário de suas responsabilidades por atos praticados em sua desconformidade.

CAPÍTULO IV

DAS DIRETRIZES GERAIS

Art. 27. O cumprimento desta PoSIN e de suas normas complementares e procedimentos deverá ser avaliado periodicamente por meio de verificações de conformidade, realizadas por grupo de trabalho formalmente constituído pelo CSI, buscando a certificação do cumprimento dos requisitos de segurança da informação e garantia de cláusula de responsabilidade e sigilo.

Art. 28. As normas complementares, procedimentos, manuais e metodologias de segurança da informação do CNPq devem considerar as melhores práticas no tema, além das referências legais e normativas citadas nesta Portaria.

Art. 29. Toda e qualquer informação gerada, custodiada, manipulada, utilizada ou armazenada no CNPq compõe o seu ativo da informação e deve ser protegida conforme a PoSIN, normas complementares e procedimentos em vigor, incluídas as referências legais e normativas citadas nesta Portaria

Art. 30. Cabe à Autoridade máxima de Tecnologia da Informação, com o apoio da área de Tecnologia da Informação, da Comunicação Social, da área de Recursos Humanos e demais unidades pertinentes, instituir programas permanentes e regulares de conscientização, sensibilização e capacitação em segurança da informação, buscando parcerias com outros órgãos e entidades sempre que possível e desejável.

Art. 31. Fica instituída a Estrutura de Segurança da Informação do CNPq, composta pelo Gestor de Segurança da Informação - GSI, pelo Comitê de Segurança da Informação - CSI e pela Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais - ETIR, os quais serão solidariamente responsáveis pelas seguintes atividades:

I - executar os processos de segurança da informação;

II - desenvolver, implementar e monitorar estratégias de segurança da informação que atendam aos objetivos estratégicos do CNPq;

III - avaliar, selecionar, administrar e monitorar controles apropriados de proteção dos ativos de informação e desenvolver ações de conscientização dos usuários a respeito da implementação desses controles;

IV - fornecer subsídios visando à verificação de conformidade de segurança da informação; e

V - promover a melhoria contínua nos processos e controles de Segurança da Informação.

Art. 32. A Estrutura de Segurança da Informação do CNPq deve possuir um sistema para o registro de incidentes sobre o tema.

Art. 33. Os membros da Estrutura de Segurança da Informação devem receber, regularmente, capacitação especializada nas disciplinas relacionadas à segurança da informação de acordo com suas funções.

Art. 34. A Estrutura de Segurança da Informação do CNPq deve auxiliar a Alta Administração na priorização de ações e investimentos com vistas à correta aplicação de mecanismos de proteção, tendo como base as exigências estratégicas e necessidades operacionais prioritárias da instituição e as implicações que o nível de segurança poderá trazer ao cumprimento dessas exigências.

Art. 35. A Estrutura de Segurança da Informação deve planejar medidas de proteção e balancear os custos na aplicação de controles, de acordo com os danos potenciais de falhas de segurança.

Art. 36. É vetado comprometer a integridade, a confidencialidade ou a disponibilidade das informações criadas, manuseadas, armazenadas, transportadas, descartadas ou custodiadas pelo CNPq.

Art. 37. O custodiante do ativo de informação deve ser formalmente designado pelo gestor do ativo de informação.

Parágrafo único. A não designação pressupõe que o gestor é o próprio custodiante.

CAPÍTULO V

DA CONFORMIDADE

Art. 38. Deve ser realizada, periodicamente, verificação de conformidade das práticas de segurança da informação do CNPq e de suas unidades administrativas com esta PoSIN e suas normas complementares e procedimentos, bem como com a legislação específica de segurança da informação.

Art. 39. A verificação de conformidade deve também ser realizada nos contratos, convênios, acordos de cooperação e outros instrumentos do mesmo gênero celebrados pelo CNPq.

Art. 40. A verificação da conformidade será realizada de forma planejada, mediante calendário de ações proposto pela Estrutura de Segurança da Informação e aprovado pelo CSI.

Art. 41. O calendário de ações de verificação de conformidade será elaborado com base na priorização dos riscos identificados ou percebidos.

Art. 42. A execução da verificação de conformidade será realizada pela Estrutura de Segurança da Informação, podendo, com a prévia aprovação do CSI, ser subcontratada no todo ou em parte.

Art. 43. É vedado a prestador de serviços executar a verificação da conformidade dos próprios serviços prestados.

Art. 44. A verificação de conformidade poderá combinar ampla variedade de técnicas, tais como análise de documentos, análise de registros (logs), análise de código-fonte, entrevistas e testes de invasão.

Art. 45. Os resultados de cada ação de verificação de conformidade serão documentados em relatório de avaliação de conformidade, o qual será encaminhado pelo GSI ao gestor da unidade administrativa verificada, para ciência e tomada das ações cabíveis.

CAPÍTULO VI

DO PLANO DE INVESTIMENTOS EM SEGURANÇA DA INFORMAÇÃO

Art. 46. O plano de investimentos será elaborado com base na priorização dos riscos a serem tratados e será obtido a partir da aplicação de método que considere, no mínimo, a probabilidade e o impacto do risco.

Art. 47. Caso haja limitação na execução orçamentária, caberá ao CSI realizar a correspondente revisão do plano de investimentos.

CAPÍTULO VII

DOS CONTRATOS, CONVÊNIOS, ACORDOS E INSTRUMENTOS CONGÊNERES

Art. 48. 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 informações de terceiros antes de seu uso.

Art. 49. Os acordos que concedam o acesso a terceiros podem incluir, quando necessário e justificado, permissão para designação de outras partes autorizadas e condições para os seus acessos desde que expressamente autorizadas pelo CNPq.

Art. 50. Todos os contratos, convênios, acordos e instrumentos congêneres devem conter cláusulas que estabeleçam a obrigatoriedade de observância desta PoSIN e de suas normas complementares.

Art. 51. O contrato, convênio, acordo ou instrumento congênere deverá prever a obrigação da outra parte de divulgar esta PoSIN e suas normas complementares aos seus empregados e prepostos envolvidos em atividades no CNPq.

Art. 52. Um plano de contingência deve ser elaborado no caso de uma das partes desejar encerrar a relação antes do final do acordo.

Art. 53. Deve ser definido um processo adequado/objetivo de gestão de mudanças que será detalhado em norma específica.

CAPÍTULO VIII

DAS PENALIDADES

Art. 54. Ações que violem a PoSIN do CNPq e suas normas complementares poderão acarretar, isolada ou cumulativamente, nos termos da legislação aplicável, sanções administrativas, civis e penais, assegurados aos envolvidos o direito ao contraditório e a ampla defesa.

CAPÍTULO IX

DA APROVAÇÃO E REVISÃO

Art. 55. De acordo com a Norma Complementar nº 03/IN01/DSIC/GSI/PR todos os instrumentos normativos gerados a partir da PoSIN, incluindo a própria PoSIN, devem ser revisados sempre que se fizer necessário, não excedendo o período máximo de 3 (três) anos.

Art. 56. Os documentos integrantes da estrutura normativa de governança de segurança da informação do CNPq deverão ser elaborados e aprovados pelas seguintes instâncias competentes: Presidente do CNPq e Comitê de Segurança da Informação - CSI do CNPq.

CAPÍTULO IX

DISPOSIÇÕES FINAIS

Art. 57. Fica revogada a Resolução Normativa nº 33, de 23 de outubro de 2012.

Art. 58. Esta Portaria entra em vigor no primeiro dia útil do mês seguinte ao da sua publicação.

EVALDO FERREIRA VILELA