- P-GES-005/17-

POLÍTICA DE SEGURANÇA DA INFORMAÇÃO (POSIN)

EMITENTE:	COMITÊ DE SEGURANÇA DA INFORMAÇÃO (CSI)
COLABORADOR:	----------
APROVADOR:	CONSELHO DE ADMINISTRAÇÃO

Histórico das revisões

Rev. Nº	Data	Descrição
00	24/04/2017	Estabelece princípios e diretrizes pertinentes aos aspectos de Segurança da Informação na Finep.
01	27/08/2021	Revisão apreciada pela Diretoria Executiva na RD nº 31/21, de 08/07/2021, e aprovada pelo Conselho de Administração em 27/08/2021, por meio da DEL/CA/040/2021. Altera título da norma, definições, objetivos, abrangência, princípios, diretrizes, responsabilidades e atribuições em Segurança da Informação na Finep.

Sumário

1. Definições

1.1. **Acesso** - ato de ingressar, transitar, conhecer ou consultar a informação, bem como a possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique.

1.2. **Alta Administração** - pessoa ou grupo de pessoas que dirige e controla a Finep no mais alto nível (membros da Diretoria Executiva e do Conselho de Administração).

1.3. **Ativos de informação** - dados e informações gerados ou manipulados, os meios de armazenamento, transmissão e processamento, os sistemas de informação, bem como os locais onde se encontram esses meios, processos, equipamentos e as pessoas que a eles têm acesso.

1.4. **Auditabilidade** - atributo que garante a possibilidade de rastrear os diversos passos de um processo.

1.5. **Autenticidade** - propriedade de que a informação foi produzida, expedida, modificada ou destruída por uma determinada pessoa física, equipamento, sistema, órgão ou entidade.

1.6. **Ciclo da vida da informação** - ciclo formado pelas fases da produção e recepção, organização, uso e disseminação, e destinação da informação.

1.7. **Colaborador** - pessoa física que tenha vínculo celetista, estatutário ou administrativo com a Finep (empregado do quadro efetivo; membros da Diretoria Executiva e colegiados; ocupantes de cargos em comissão não pertencentes ao quadro de empregados efetivos da Finep); que preste serviços, nas dependências físicas da Finep ou fora dela, mediante contrato firmado com empresa interposta (serviços terceirizados, temporários, consultoria jurídica e outros); que atue como estagiário ou jovem aprendiz ou que atue como consultor ad hoc da Finep.

1.8. **Confidencialidade** - propriedade de que a informação não esteja disponível ou revelada a pessoa, a sistema, a órgão ou a entidade não autorizados, nem credenciados.

1.9. **Disponibilidade** - propriedade de que a informação esteja acessível e utilizável sob

demanda por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

1.10. Incidente de segurança - qualquer evento adverso, confirmado ou sob suspeita, relacionado à segurança dos sistemas de computação ou das redes de computadores.

1.11. Informação - dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato.

1.12. Informação restrita - informação confidencial protegida por sigilo previsto em lei ou em contrato ou segredo de justiça.

1.13. Integridade - propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

1.14. Irretratabilidade ou não repúdio - propriedade da informação que não permite ter seu envio ou conteúdo contestados, rejeitados ou repudiados por seu emissor ou por seu receptor.

1.15. Necessidade de conhecer - condição segundo a qual o conhecimento da informação com restrição de acesso é indispensável para o adequado exercício de cargo, função, emprego ou atividade.

1.16. Processo crítico - processo cuja interrupção ou descontinuidade possa comprometer a imagem da instituição e/ou gerar impacto relevante no atingimento dos objetivos estratégicos.

1.17. Quebra de segurança - ação ou omissão, intencional ou acidental, que resulta no comprometimento da segurança da informação.

1.18. Segurança da informação - ações que objetivam viabilizar e assegurar a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações.

1.19. Tratamento da informação - conjunto de ações referentes à produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação ou controle da informação.

1.20. Tratamento de Incidentes de Segurança em Redes Computacionais - serviço que consiste em receber, filtrar, classificar e responder às solicitações e aos alertas e realizar as análises dos incidentes de segurança, procurando extrair informações que permitam impedir a continuidade da ação maliciosa e também a identificação de tendências.

2. Conteúdo específico

2.1. Disposições iniciais

2.1.1. O objetivo da presente política é estabelecer princípios, diretrizes, competências e subsídios para a gestão da segurança da informação na Finep.

2.1.2. Esta política deve nortear outras políticas, normativos, metodologias, processos e procedimentos da Finep em conformidade com a legislação vigente e as boas práticas de segurança da informação.

2.2. Abrangência

2.2.1. A segurança da informação na Finep abrange os seguintes temas:

a. segurança cibernética;

b. segurança física e proteção de dados organizacionais e pessoais; e

c. ações destinadas a assegurar a disponibilidade, a integridade, a confidencialidade e a

autenticidade da informação.

2.2.2. Toda e qualquer pessoa que tenha acesso às informações e/ou instalações da Finep sujeitam-se aos princípios, diretrizes e regras de segurança da informação de que trata esta Política e normas derivadas e são responsáveis pelo seu cumprimento, assim como as empresas e demais organizações com que a Finep se relaciona.

2.3. Princípios e diretrizes gerais

2.3.1. A segurança da informação da Finep, que aborda aspectos físicos, tecnológicos e humanos, deve obedecer aos seguintes princípios:

a. preservação da integridade, autenticidade e irretratabilidade das informações produzidas e recebidas;

b. transparência das informações públicas;

c. garantia da disponibilidade das informações custodiadas e da confidencialidade das informações que necessitam de restrição de acesso;

d. defesa da auditabilidade dos processos;

e. visão abrangente e sistêmica da segurança da informação;

f. 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;

g. educação como base para a segurança da informação;

h. orientação à gestão de riscos e à gestão da segurança da informação;

i. necessidade de conhecer para o acesso à informação restrita, nos termos da legislação;

j. prevenção de incidentes de segurança da informação.

2.3.2. São diretrizes gerais da Política de Segurança da Informação na Finep:

a. A gestão da segurança da informação deve observar o alinhamento com os referenciais estratégicos organizacionais e a conformidade com a legislação e regulamentação em vigor.

b. A segurança da informação dever ser considerada no processo de tomada de decisão e na execução das ações estratégicas e operacionais.

c. O planejamento das ações de segurança da informação deve ser realizado por meio de metodologia baseada em processo de melhoria contínua, considerando a natureza e a finalidade da Finep e o gerenciamento de riscos corporativos.

d. Os ativos de informação da Finep devem ser inventariados e protegidos de acordo com os riscos a eles associados.

e. As instalações de infraestrutura e recursos tecnológicos destinados à produção, distribuição, arquivamento e preservação de dados e informações devem ser adequadamente protegidos contra indisponibilidade, comprometimento de integridade e confidencialidade, alterações não autorizadas ou acesso indevido, falhas ou interrupções não programadas.

f. As informações produzidas por colaboradores da Finep, no exercício de suas atribuições, são patrimônio intelectual da Finep e não cabe a seus criadores qualquer forma de direito autoral, salvo aqueles assegurados por legislação específica.

g. A conscientização e capacitação sobre a segurança da informação deve ser promovida permanentemente para fortalecer a cultura da segurança da informação dos

colaboradores e das partes interessadas.

h. O fomento à formação e à qualificação dos recursos humanos necessários às atividades de segurança da informação deve ser promovido.

i. Os contratos de fornecimento e prestação de serviços, convênios e instrumentos congêneres firmados pela Finep e que abranjam a gestão de ativos de informação, documentos, instalações de infraestrutura e recursos tecnológicos devem observar, no que couber, as disposições estabelecidas nesta Política e normativos internos.

j. O Comitê de Segurança da Informação (CSI) deve estar em funcionamento, o Gestor de Segurança da Informação (GSIn) e as demais estruturas organizacionais devem estar trabalhando para garantir a implementação desta Política e das normas internas relativas à Segurança da Informação, bem como devem ser assegurados os recursos necessários a sua operacionalização.

k. A Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR) deve estar em funcionamento para executar o serviço de prevenção e tratamento de incidentes de segurança, em conformidade com a legislação vigente e com os normativos internos, tendo os recursos necessários à realização de suas atividades assegurados pela Finep.

l. A segurança da informação deve contribuir para a preservação do acervo histórico e da memória da Finep.

2.4. Tratamento da informação

2.4.1. O tratamento da informação deve observar, durante todo o seu ciclo de vida, os princípios e as diretrizes de segurança da informação estabelecidos por esta Política, sem prejuízo do estabelecimento de regras específicas em normativos internos.

2.5. Gestão de incidentes em segurança da informação

2.5.1. A Finep deve estabelecer em normativos internos as diretrizes, os requisitos e o processo de gestão de incidentes de segurança relacionados ao ambiente de tecnologia da informação da Finep.

2.6. Auditoria e conformidade

2.6.1. A Finep deve estabelecer processos periódicos de auditoria e de avaliação de conformidade em segurança da informação, a serem executados pelas unidades administrativas que detenham tais atribuições.

2.6.2. As não-conformidades relativas ao descumprimento de legislações, normativos e procedimentos de segurança de informação deverão ser comunicados ao GSIn, que por sua vez deverá adotar as providências internas cabíveis.

2.7. Gestão de continuidade

2.7.1. A Finep deve elaborar e atualizar periodicamente planos de contingência, considerando a magnitude dos riscos associados à interrupção de processos críticos, ocorrência de incidentes e acidentes e danos ao patrimônio.

a. As medidas, procedimentos e responsabilidades estabelecidos nos planos devem ser desdobrados em medidas voltadas à segurança da informação com a definição clara das unidades da empresa envolvidas e a periodicidade de simulações e testes.

2.8. Gestão de riscos

2.8.1. A Finep deve estabelecer processo de gerenciamento de riscos de segurança da informação, a fim de que os riscos de ameaças, incidentes, quebras de segurança e vulnerabilidades associados aos ativos de informação possam ser identificados, medidos seus impacto e

probabilidade e definidos planos de ação.

2.8.2. O processo de gerenciamento de riscos de segurança da informação deve estar alinhado com a Política Integrada de Gestão de Riscos da Finep e demais normativos internos aplicáveis.

2.9. Controles de acesso

2.9.1. A Finep deve estabelecer em normativos internos critérios e procedimentos gerais para o controle de acesso aos ativos de tecnologia da informação e às informações, a fim de garantir que o acesso físico e lógico às informações restritas e pessoais seja franqueado exclusivamente a pessoas autorizadas ou com necessidade de conhecer, com base nos requisitos de negócio e na tipificação das informações.

2.10. Gestão do uso de recursos operacionais e de comunicações

2.10.1. A Finep deve estabelecer em normativo interno as regras para o uso eficiente de:

a. serviço de correio eletrônico, como ferramenta de trabalho;

b. internet na empresa de acordo com a legislação brasileira e com normativos existentes;

c. computação em nuvem de acordo com as normas legais e regulatórias existentes.

2.11. Gestão de ativos de informação

2.11.1. A Finep deve estabelecer critérios e procedimentos para inventariar, mapear e atualizar a base de ativos de informação da empresa em normativo interno, a fim de permitir a proteção e manutenção destes ativos em conformidade com os requisitos legais e do negócio, além de auxiliar na gestão de segurança da informação e nos aspectos relacionados à gestão de riscos de segurança da informação e gestão de continuidade de negócios.

2.12. Segurança física e do ambiente

2.12.1. A Finep deve estabelecer critérios e procedimentos para o controle de acesso e circulação de pessoas e de movimentação de bens nas dependências da empresa em normativo interno.

2.13. Responsabilidades e atribuições

2.13.1. Compete ao Comitê de Segurança da Informação (CSI), sem prejuízo de outras previstas em regulamento próprio:

a. Assessorar e atuar na implementação das ações de segurança da informação.

b. Propor grupos de trabalho para tratar de temas e propor soluções específicas sobre segurança da informação.

c. Propor alterações e executar revisões periódicas na POSIN, em conformidade com a legislação existente sobre o tema.

d. Propor e elaborar normativos internos relativos à segurança da informação.

2.13.2. Compete ao Gestor de Segurança da Informação (GSIn):

a. Promover a cultura de segurança da informação na Finep.

b. Monitorar a implementação da legislação aplicável e pertinente ao domínio da segurança da informação na Finep.

c. Acompanhar as investigações e as avaliações dos danos decorrentes de eventual quebra de segurança da informação, assim como realizar reporte de ação para correção de eventuais problemas estruturais ou pontuais identificados à instância superior.

d. Propor a elaboração ou atualização de normativos internos relativos à segurança da informação.

e. Propor recursos necessários às ações de segurança da informação.

f. Coordenar o CSI e a ETIR.

g. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na Segurança da Informação.

h. Manter contato direto com o Departamento de Segurança da Informação (DSI), órgão vinculado ao Gabinete de Segurança Institucional (GSI) da Presidência da República.

2.13.3. Compete à Equipe de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos (ETIR), sem prejuízo de outras responsabilidades e atribuições previstas em regulamento próprio:

a. Facilitar e coordenar as atividades de tratamento e resposta a incidentes em redes computacionais.

b. Auxiliar na recuperação de sistemas.

c. Analisar ataques, intrusões e incidentes.

d. Comunicar formalmente o resultado de seus trabalhos ao GSIn.

e. Cooperar com outras equipes internas e externas.

f. Participar de fóruns e redes nacionais e internacionais.

2.13.4. Compete à Alta Administração da Finep:

a. Estabelecer segurança da informação como tema estratégico para a continuidade das atividades da Finep.

b. Atender as atribuições definidas na Política Nacional de Segurança da Informação.

2.13.5. Compete aos colaboradores da Finep:

a. Conhecer e cumprir todos os princípios e diretrizes estabelecidos nesta política.

b. Adotar os requisitos de controle de segurança especificados em normativos internos e em outras orientações a suas atividades.

c. Comunicar tempestivamente à ETIR os incidentes que afetam a Segurança da Informação.

d. Manter os processos sob sua responsabilidade aderentes às políticas e normativos internos de Segurança da Informação.

e. Garantir o sigilo das informações restritas ou pessoais a que tenham acesso.

2.13.6. Toda e qualquer pessoa que tenha acesso às informações e/ou instalações da Finep é responsável por zelar pela estrita observância do disposto nesta Política e nos normativos internos e por comunicar, formalmente, ao GSIn qualquer irregularidade ou ameaça à segurança da informação na Finep.

2.14. Disposições gerais

2.14.1. No caso de descumprimento ou inobservância desta política devem ser seguidos, no que couber, as disposições estabelecidas em normativos específicos.

2.14.2. A violação da Política de Segurança da Informação ou a quebra de segurança por toda e qualquer pessoa que tenha acesso às informações e/ou instalações da Finep deve ser comunicada pelo GSIn às instâncias competentes para a apuração.

2.14.3. A Finep deve prever em seus documentos normativos a aplicabilidade de termos de

confidencialidade no que tange a informações restritas e pessoais.

2.14.4. A presente política deve ser objeto de revisão, em prazo não superior a quatro anos.

2.14.5. A presente política e os normativos derivados, assim como suas atualizações, devem ser divulgados pela Finep a toda e qualquer pessoa que tenha acesso a suas informações e/ou instalações e ter seu conteúdo integral disponibilizado para consulta interna.

2.14.6. Os conceitos e definições de segurança da informação a serem usados nos normativos da Finep devem se nortear pelo Glossário de Segurança da Informação mantido pelo DSI-GSI/PR.

2.15. Tratamento de omissões e exceções

2.15.1. Os casos omissos e as exceções serão deliberados pelo Diretoria Executiva.

3. Referências

3.1. Decreto nº 9.637, de 26 de dezembro de 2018, institui a Política Nacional de Segurança da Informação e dispõe sobre a governança da segurança da informação;

3.2. Decreto nº 10.641, de 2 de março de 2021, altera o Decreto nº 9.637, de 26 de dezembro de 2018;

3.3. Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020, dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

3.4. Instrução Normativa GSI/PR Nº 2, de 24 de julho de 2020, altera a Instrução Normativa GSI/PR Nº 1, de 27 de maio de 2020, que dispõe sobre a Estrutura de Gestão da Segurança da Informação nos órgãos e nas entidades da administração pública federal;

3.5. IT-GES-009/20 - Instrução de Trabalho de Uso de Credenciais de Acesso;

3.6. Lei nº 12.527, de 18 de novembro de 2011, dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal;

3.7. Lei nº 13.709/2018, de 14 de agosto de 2018, dispõe sobre a proteção de dados pessoais;

3.8. N-GES-020/20 - Norma de Controle de Acesso a Ativos de Tecnologia da Informação da Finep;

3.9. N-GES-018/19 - Norma de Controle de Acesso e Circulação nas Dependências da Finep;

3.10. N-GES-005/12 - Norma de Tipificação e Acesso à Informação;

3.11. N-GES-025/21 - Norma de Controle de Acesso à Informação na Finep;

3.12. N-GES-026/21 - Norma de Gestão de Incidentes Cibernéticos de Segurança da Informação;

3.13. N-RHM-014/11 - Norma de Infrações Disciplinares da Finep;

3.14. Portaria GSI/PR nº 93, de 26 de setembro de 2019, aprova o Glossário de Segurança da Informação;

3.15. R-GES-002/18 - Regulamento do Comitê de Segurança da Informação e Comunicações;

3.16. R-GES-004/18 - Regulamento da Equipe de Tratamento e Resposta a Incidentes.

4. Anexos

Não se aplica