- 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.
02	02/09/2025	Revisão apreciada pela Diretoria Executiva na RD nº 31/25, de 12/08/2025, e aprovada pelo Conselho de Administração em 29/08/2025, por meio da DEL/CA/037/2025. Altera definições, objetivo, abrangência, princípios, diretrizes e responsabilidades.

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** - meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização.

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. **Conformidade em segurança da informação** - cumprimento das legislações, normas e procedimentos relacionados à segurança da informação da organização.

1.10. **Disponibilidade** - propriedade de que a informação esteja acessível e utilizável, sob demanda, por uma pessoa física ou determinado sistema, órgão ou entidade devidamente autorizados.

1.11. **Incidente cibernético** - ocorrência que pode comprometer, real ou potencialmente, a disponibilidade, a integridade, a confidencialidade ou a autenticidade de sistema de informação ou das informações processadas, armazenadas ou transmitidas por esse sistema. Poderá também ser caracterizada pela tentativa de exploração de vulnerabilidade de sistema de informação que caracterize violação de norma, política de segurança, procedimento de segurança ou política de uso. De maneira geral, os tipos de atividade comumente reconhecidas como incidentes cibernéticos são: a) tentativas de obter acesso não-autorizado a um sistema ou a dados armazenados; b) tentativa de utilização não-autorizada de sistemas para a realização de atividades de processamento ou armazenamento de dados; c) mudanças não-autorizadas de *firmware, hardware* ou *software* em um ambiente computacional; d) ataques de negação de serviço (DoS); e e) demais ações que visem afetar a disponibilidade ou integridade dos dados. Um incidente de segurança cibernética não significa necessariamente que as informações já estão comprometidas; significa apenas que a informação está ameaçada.

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

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

1.14. **Informação pessoal** - informação relacionada à pessoa natural identificada ou identificável, relativa à intimidade, vida privada, honra e imagem.

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

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

1.17. **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.

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

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

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

1.21. **Risco de segurança da informação** - risco potencial associado à exploração de uma ou mais vulnerabilidades de um ou mais ativos de informação, por parte de uma ou mais ameaças, com impacto negativo no negócio da organização.

1.22. **Resiliência** - capacidade de uma organização ou de uma infraestrutura de resistir aos efeitos de um incidente, ataque ou desastre, e retornar à normalidade das operações.

1.23. **Segurança cibernética** - ações voltadas para a segurança de operações, visando garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético, capazes de comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.

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

1.25. **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.

1.26. **Tratamento de incidentes cibernéticos** - consiste nas ações e procedimentos tomados imediatamente após a identificação do incidente, visando garantir a continuidade de operações, preservar evidências e emitir as notificações necessárias.

2. Objetivo

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

3. Conteúdo específico

3.1. Disposições iniciais

3.1.1. 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 e cibernética.

3.2. Abrangência

3.2.1. A segurança da informação e cibernética na Finep abrange os seguintes temas:

a. ações voltadas para a segurança de operações, visando garantir que os sistemas de informação não tenham a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos comprometidos, nem que os serviços que esses sistemas ofereçam se tornem inacessíveis;

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.

3.2.2. Todos os colaboradores são responsáveis pela segurança das informações tratadas na Finep.

3.2.3. 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.

3.3. Princípios e diretrizes gerais

3.3.1. A segurança da informação e cibernética na 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. a garantia dos direitos 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 e cibernética;

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 e de ataques cibernéticos;

k. resiliência a incidentes e ataques cibernéticos;

l. desenvolvimento e uso seguro, ético e responsável de inteligência artificial.

3.3.2. São diretrizes gerais da Política de Segurança da Informação da 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 ao tratamento 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 e cibernética, bem como devem ser assegurados os recursos necessários à 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 cibernéticos, 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.

m. A gestão de riscos e a adoção de medidas de proteção cibernética devem ser estimuladas para prevenir, evitar, mitigar, diminuir e neutralizar vulnerabilidades, incidentes e ataques cibernéticos e seus impactos.

n. A resiliência a incidentes e ataques cibernéticos deve ser incrementada.

3.4. Tratamento da informação

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

3.5. Gestão de incidentes cibernéticos

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

3.6. Auditoria e conformidade

3.6.1. 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.

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

3.7. Gestão de continuidade

3.7.1. 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 e cibernética com a definição clara das unidades da empresa envolvidas e a periodicidade de simulações e testes.

3.8. Gestão de riscos

3.8.1. 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.

3.8.2. 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.

3.9. Controles de acesso

3.9.1. A Finep deve estabelecer em normativos internos critérios e procedimentos gerais para o gerenciamento de credenciais de acesso e 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.

3.10. Gestão do uso de recursos operacionais e de comunicações

3.10.1. 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.

3.11. Gestão de ativos de informação

3.11.1. 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 cibernética e nos aspectos relacionados à gestão de riscos de segurança da informação e gestão de continuidade de negócios.

3.12. Gestão de mudanças

3.12.1. A Finep deve estabelecer critérios e procedimentos para a gestão de mudanças nos aspectos de segurança da informação e cibernética, de maneira a se preparar para as alterações decorrentes da evolução dos processos de negócios e das soluções tecnológicas, visando a garantia da segurança das informações relacionadas a essas mudanças, à mitigação de possíveis riscos de segurança da informação e à resiliência cibernética.

3.13. Segurança física e do ambiente

3.13.1. 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.

3.14. Responsabilidades e atribuições

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

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

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

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 e cibernética.

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

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

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

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

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

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

f. Acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e cibernética.

g. Manter contato com a Secretaria de Segurança da Informação e Cibernética (SSIC), órgão vinculado ao Gabinete de Segurança Institucional (GSI) da Presidência da República.

3.14.3. 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 cibernéticos.

b. Auxiliar na recuperação de sistemas.

c. Analisar ataques, intrusões e outros incidentes cibernéticos.

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.

3.14.4. Compete à Alta Administração da Finep:

a. Estabelecer segurança da informação e cibernética como tema estratégico para a continuidade dos processos de negócios da Finep.

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

3.14.5. Compete aos colaboradores da Finep:

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

b. Adotar os controles de segurança especificados em normativos internos e em outros documentos orientativos em suas atividades.

c. Comunicar tempestivamente à ETIR os incidentes que afetam a segurança da informação e cibernética.

d. Manter os processos sob sua responsabilidade aderentes às políticas e normativos internos de segurança da informação e cibernética.

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

3.14.6. 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.

3.15. Disposições gerais

3.15.1. No caso de descumprimento ou inobservância desta política devem ser seguidos, no que couber, as disposições estabelecidas em normativos específicos, incluindo o de infrações disciplinares.

3.15.2. 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.

3.15.3. A Finep deve prever em seus normativos a aplicabilidade de termos de confidencialidade no que tange a informações restritas e pessoais.

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

3.15.5. 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.

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

3.16. Tratamento de omissões e exceções

3.16.1. Os casos omissos e as exceções serão deliberados pelo Conselho de Administração.

4. Referências

4.1. 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;

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

4.3. Decreto nº 11.856, de 26 de dezembro de 2023, institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança;

4.4. 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;

4.5. 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;

4.6. Instrução Normativa GSI/PR Nº 3, de 28 de maio de 2021, dispõe sobre os processos relacionados à gestão de segurança da informação nos órgãos e nas entidades da administração pública federal;

4.7. IT-GES-009/20 - Instrução de Trabalho de Gerenciamento de Credenciais de Acesso;

4.8. 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;

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

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

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

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

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

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

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

4.16. N-SIS-007/24 - Norma de Uso dos Ativos de Tecnologia da Informação;

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

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

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

5. Anexos

Não se aplica.