**POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES**

**(P-GES-005/17)**

Aprovada pelo Conselho de Administração da FINEP, através da deliberação DEL/CA/020/2017 DE 24/04/2017.

**DESTAQUES**

**1 INTRODUÇÃO**

Referenciando-se na Instrução Normativa GSI/PR n° 01/2008[[1]](#footnote-1); na Resolução CGPAR n° 11/2016[[2]](#footnote-2); na lei n° 12.527/2011[[3]](#footnote-3) e nas melhores práticas de mercado, a Finep aprovou POLÍTICA de Segurança da Informação e Comunicações.

**2 OBJETIVO E ABRANGÊNCIA**

A política tem o objetivo de estabelecer princípios e diretrizes relativos ao uso, compartilhamento e trâmite das informações em conformidade com a legislação vigente, as boas práticas e os normativos internos, de modo a garantir a Segurança da Informação e Comunicações e a transparência das informações públicas.

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 dela derivados e por comunicar, formalmente, ao GSICOM qualquer irregularidade ou ameaça à Segurança da informação e Comunicações na Finep.

**3 DEFINIÇÕES**

**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.

**Ativo 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.

**Auditabilidade -** atributo que garante a rastreabilidade dos diversos passos de um processo.

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

**Colaborador -** Toda pessoa física que:

1. 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);
2. Preste serviços, nas dependências físicas da Finep ou fora dela, mediante contrato firmado com empresa interposta (serviços terceirizados, temporários, estagiários/jovens aprendizes, consultoria jurídica e outros); ou
3. Atue como consultor da Finep.

**Confidencialidade** - propriedade de que a informação não esteja disponível ou revelada a pessoa física, sistema, órgão ou entidade não autorizado e credenciado.

**Conformidade -** Se refere ao conjunto de disciplinas para fazer cumprir as normas legais e regulamentares, as políticas e as diretrizes estabelecidas para o negócio e para as atividades da Finep, bem como evitar, detectar e tratar qualquer desvio ou inconformidade que possa ocorrer.

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

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

**Integridade** - propriedade de que a informação não foi modificada ou destruída de maneira não autorizada ou acidental.

**Irretratabilidade ou Não repúdio –** propriedade da informação que não possa ter seu envio ou conteúdo contestados, rejeitados ou repudiados por seu emissor ou por seu receptor.

**Quebra de Segurança -** comprometimento da segurança da informação e das comunicações, resultante de ação ou omissão, intencional ou acidental.

**Risco -** possibilidade de ocorrência de eventos que venham a ter impacto no cumprimento dos objetivos estratégicos da Finep. O risco é medido em termos de probabilidade de ocorrência e de impacto.

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

**Tratamento de Incidentes de Segurança em Redes Computacionais -** serviço que consiste em receber, filtrar, classificar e responder às solicitações e 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.

**4 PRINCÍPIOS**

🡺 Preservação da integridade, autenticidade e irretratabilidade das informações produzidas e recebidas;

🡺 Transparência das informações públicas;

🡺 Garantia da disponibilidade das informações custodiadas e da confidencialidade das informações que necessitam de restrição de acesso; e

🡺 Defesa de auditabilidade dos processos.

**5 DIRETRIZES GERAIS**

🡺 Observar o alinhamento com os referenciais estratégicos organizacionais e a conformidade com a legislação e regulamentação em vigor;

🡺 Orientar a tomada de decisão e otimizar os investimentos proporcionando a eficácia, eficiência e efetividade dos processos organizacionais;

🡺 O planejamento das ações de Segurança da Informação e Comunicações deve ser realizada por meio de metodologia baseada em processo de melhoria contínua, considerando o gerenciamento de riscos corporativos;

🡺 Os ativos de informação da Finep devem ser inventariados e protegidos, assim como devem ter identificados os seus gestores e custodiantes e mapeados os riscos a eles associados;

🡺 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;

🡺 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;

🡺 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 derivados.

🡺 O Comitê de Segurança da Informação e Comunicações (CSICOM) deve ser instituído e seus membros nomeados, o Gestor de Segurança da Informação e Comunicações (GSICOM) deve ser nomeado e as demais estruturas organizacionais aptas a garantir a implementação desta Política e das normas complementares relativas à Segurança da Informação e Comunicações devem ser criadas, bem como assegurados os recursos necessários a sua operacionalização.

**6 RESPONSABILIDADES**

**Comitê de Segurança da Informação e Comunicações**

🡺 Assessorar e atuar na implementação das ações de Segurança da Informação e Comunicações previstas nesta Política;

🡺 Constituir grupos de trabalho para tratar de temas e propor soluções específicas sobre Segurança da Informação e Comunicações;

🡺 Propor normativos internos relativos à Segurança da Informação e Comunicações.

**Gestor de Segurança da Informação e Comunicações**

🡺 Promover a cultura de Segurança da Informação e Comunicação na FINEP;

🡺 Monitorar a implementação da legislação aplicável e pertinente ao domínio da Segurança da Informação e Comunicação na FINEP;

🡺 Acompanhar as investigações e as avaliações dos danos decorrentes de eventual quebra de segurança da informação, assim como realizar reporte periódico de ação para correção de eventuais problemas estruturais ou pontuais identificados;

🡺 Propor normativos internos relativos à Segurança da Informação e Comunicações;

🡺 Propor recursos necessários às ações de Segurança da Informação e Comunicações;

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

**Equipe de Tratamento de Incidentes de Redes Computacionais**

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

🡺 Auxiliar na recuperação de sistemas;

🡺 Analisar ataques, intrusões e incidentes;

**Todos os colaboradores da FINEP**

🡺 Conhecer e cumprir todos os princípios e diretrizes estabelecidos nesta política;

🡺 Adotar os requisitos de controle de segurança especificados em normativos;

🡺 Comunicar tempestivamente ao GSICOM os incidentes que afetam a Segurança da Informação e Comunicações;

🡺 Manter os processos sob sua responsabilidade aderentes às políticas e normativos internos derivados e específicos de Segurança da Informação e Comunicações.

**7 CONSCIENTIZAÇÃO**

🡺 A Finep deve adotar ações permanentes de caráter preventivo e educativo para comunicação e treinamento de seus colaboradores com o objetivo de desenvolver a cultura de Segurança da Informação e Comunicações.

1. Disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências. [↑](#footnote-ref-1)
2. Trata das empresas estatais que deverão planejar, implementar e manter práticas de governança de Tecnologia da Informação (TI) que atendam de forma adequada os padrões usualmente reconhecidos nesta área. [↑](#footnote-ref-2)
3. 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. [↑](#footnote-ref-3)