- P-GES-005/17-
POLÍTICA DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (POSIC)

EMITENTE:	COMITÊ DE SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (CSICOM)
COLABORADOR:	GT-Segurança da Informação (POR/PRES/0140/2016)
APROVADOR:	CONSELHO DE ADMINISTRAÇÃO

Histórico das revisões

Rev. Nº	Data	Descrição
00	24/04/17	Estabelece princípios e diretrizes pertinentes aos aspectos de Segurança da Informação e Comunicações na FINEP.

Sumário

1. Definições

Dimensão Humana:

1.1 Colaborador: Toda pessoa física que:

a. 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);

b. 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

c. Atue como consultor da Finep.

Dimensão Técnica:

1.2 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.

1.3 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.

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

1.5 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.

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

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

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

1.9 **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.

1.10 **Informação restrita** - aquela sujeita à classificação, sobre a qual recai imposição legal de sigilo ou que possui conteúdo relacionado à pessoa natural identificada ou identificável. Gênero da qual são espécies informação pessoal e informação sigilosa.

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

1.12 **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.

1.13 **Política de Segurança da Informação e Comunicações (POSIC)** – documento aprovado pela autoridade responsável pelo órgão ou entidade da Administração Pública Federal, direta e indireta, com o objetivo de fornecer diretrizes, critérios e suporte administrativo suficientes à implementação da segurança da informação e comunicações.

1.14 **Processo crítico -** processo cuja interrupção ou descontinuidade possa comprometer a imagem da instituição e gerar impacto financeiro, legal ou operacional.

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

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

1.17 **Termo de Responsabilidade**: termo firmado pelos colaboradores concordando em contribuir com a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações que tiverem acesso, bem como em assumir responsabilidades decorrentes de tal acesso (Anexo I).

1.18 **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.

1.19 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.

2. Conteúdo específico

2.1. Objetivo

2.1.1. 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.

2.2. Abrangência

2.2.1. Toda e qualquer pessoa que tenha acesso às informações e/ou instalações da Finep sujeitam-se aos princípios, diretrizes e normas de segurança da informação de que trata esta Política e são responsáveis pelo seu cumprimento.

2.3. Princípios e Diretrizes Gerais

2.3.1. A Segurança da Informação e Comunicações da Finep, que abrange 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; e

d. defesa de auditabilidade dos processos.

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

a. A gestão da Segurança da Informação e Comunicações deve observar o alinhamento com os referenciais estratégicos organizacionais e a conformidade com a legislação e regulamentação em vigor;

b. A gestão da Segurança da Informação e Comunicações deve orientar a tomada de decisão e otimizar os investimentos proporcionando a eficácia, eficiência e efetividade dos processos organizacionais;

c. 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;

d. 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;

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 de seus colaboradores sobre a Segurança da informação e das Comunicações deve ser promovida;

h. 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.

i. O estabelecimento de normativos internos derivados de Segurança da Informação e Comunicação para processos, sistemas e procedimentos deve observar estreita conformidade com os princípios e diretrizes definidos nesta política.

j. 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.

2.4. Tratamento à Informação

2.4.1. O tratamento da informação deve observar os princípios e as diretrizes de segurança estabelecidos por esta Política durante todo o seu ciclo de vida, que compreende a produção, recepção, classificação, utilização, acesso, reprodução, transporte, transmissão, distribuição, arquivamento, armazenamento, eliminação, avaliação, destinação e controle da informação, assim como devem ser estabelecidas as regras em normativos internos derivados.

2.5. Tratamento de Incidentes de Rede - ETIR

2.5.1. A Finep deve instituir e nomear Equipe de Tratamento e Resposta a Incidentes em Redes Computacionais (ETIR) para executar o serviço de tratamento de incidentes de segurança, em

conformidade com a legislação vigente e com os normativos internos, assegurando os recursos necessários à realização das atividades. A ETIR também é responsável pela proposta de normativos internos derivados desta Política.

2.6. Auditoria e Conformidade

2.6.1. A Finep deve estabelecer processo periódico de Auditoria e de Avaliação de Conformidade em Segurança da Informação e Comunicações, a ser executado por unidade administrativa que detenha tal atribuição.

2.6.2. As não-conformidades relativas ao descumprimento de legislações, normativos e procedimentos de Segurança de Informação e Comunicações são considerados riscos, devendo ser comunicados ao GSICOM, que por sua vez deverá adotar as providências para comunicação às autoridades competentes para apuração e providências.

2.7. Gestão de Continuidade

2.7.1. A Finep deve elaborar e atualizar periodicamente um Plano de Gestão de Continuidade de Negócios (PGCN), definindo escopo, abrangência, medidas de continuidade operacional e recuperação de informação, procedimentos e periodicidade de execução de simulações e testes, considerando-se a magnitude dos riscos associados à interrupção de processos críticos, ocorrência de incidentes e acidentes e danos ao patrimônio. As medidas, procedimentos e responsabilidades estabelecidos no PGCN devem ser disseminados por meio de ações de comunicação e treinamento.

2.8. Gestão de Risco

2.8.1. Os riscos de quebra de segurança associados aos ativos da informação devem ser identificados por meio de um processo permanente estabelecido para medição do impacto e probabilidade dos eventos para que seja implantado processo de gerenciamento de riscos.

2.8.2. O processo de Gerenciamento de Riscos de Segurança da Informação e Comunicações deve estar alinhado com a Política Integrada de Gestão de Riscos da FINEP e demais normativos internos aplicáveis.

2.9. Controle de Acesso

2.9.1. A Finep deve estabelecer regras e procedimentos de controle de acesso aos ativos de informação em normativo interno, a fim de garantir que o acesso físico e lógico às informações restritas seja franqueado exclusivamente a pessoas autorizadas, com base nos requisitos de negócio e nos riscos de Segurança da Informação e Comunicações.

2.10. Uso de e-mail

2.10.1. A Finep deve estabelecer em normativos internos as regras para o uso eficiente do serviço de correio eletrônico, como ferramenta de trabalho.

2.11. Acesso à Internet

2.11.1. A Finep deve estabelecer regras para o uso eficiente da Internet na empresa de acordo com a legislação brasileira e com normativos internos.

2.12. Responsabilidades e Atribuições

2.12.1. O Comitê de Segurança da Informação e Comunicações tem as seguintes responsabilidades e atribuições:

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

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

c. Propor alterações e executar revisões periódicas na política de Segurança da Informação e Comunicações, em conformidade com a legislação existente sobre o tema; e

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

2.12.2. O Gestor de Segurança da Informação e Comunicações tem as seguintes responsabilidades e atribuições:

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

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

c. 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;

d. Propor normativos internos relativos à Segurança da Informação e Comunicações;

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

f. Coordenar o CSICOM e a ETIR;

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

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

2.12.3. A ETIR tem as seguintes responsabilidades e atribuições:

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 GSICOM;

e. cooperar com outras equipes internas e externas;

f. participar de fóruns e redes nacionais e internacionais

2.12.4. Ao Conselho de Administração da Finep compete a deliberação desta política e dos demais normativos relacionados à Segurança da Informação e Comunicações, que forem de sua alçada de aprovação.

2.12.5. À Diretoria Executiva da Finep compete:

a. deliberar e encaminhar esta política para aprovação do Conselho de Administração;

b. deliberar sobre normativos derivados desta política, que forem de sua alçada, com o devido encaminhamento para ciência ou aprovação do Conselho de Administração, conforme o caso.

2.12.6. Os colaboradores da Finep têm as seguintes responsabilidades e atribuições:

a. conhecer e cumprir todos os princípios e diretrizes estabelecidos nesta política;

b. adotar os requisitos de controle de segurança especificados em normativos;

c. comunicar tempestivamente ao GSICOM os incidentes que afetam a Segurança da Informação e Comunicações; e

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

2.12.7. 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.

2.13. Medidas Disciplinares

2.13.1. O descumprimento ou inobservância de quaisquer princípios ou diretrizes definidos neste instrumento e de responsabilidades e procedimentos estabelecidos em seus normativos internos derivados está sujeito à aplicação de medidas disciplinares adequadas e proporcionais previstas nos normativos internos da Finep, bem como à aplicação de medidas judiciais e administrativas

cabíveis, conforme previsto no Termo de Responsabilidade - Segurança da Informação e Comunicações – FINEP (Anexo I).

2.14. Atualização

2.14.1. A presente política e os normativos complementares devem ser objeto de revisão, em prazo não superior a três anos.

2.15. Divulgação

2.15.1. A presente política e os normativos internos 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.

2.16. Conscientização

2.16.1. 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.

2.17. Disposições Gerais

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

2.17.2. A Finep deve prever em seus documentos normativos a aplicabilidade de termos de sigilo e confidencialidade no que tange a informações restritas.

3. Referências

3.1. Instrução Normativa GSI/PR Nº 1, de 13 de junho de 2008, que disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências, e suas respectivas Normas Complementares publicadas no DOU pelo DSIC/GSIPR.

3.2. 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.

3.3. Manual de Boas práticas em segurança da informação, do Tribunal de Contas da União. – 4. ed. – Brasília; Secretaria de Fiscalização de Tecnologia da Informação, 2012.

3.4. Resolução CGPAR 11, de 10 de maio de 2016.

4. Anexos

ANEXO I - Termo de Responsabilidade - Segurança da Informação e Comunicações – FINEP