PORTARIA Nº 250, DE 24 DE ABRIL DE 2018

Dispõe sobre a Política de Segurança da Informação e Comunicações do Fundo Nacional de Desenvolvimento da Educação - FNDE.

O PRESIDENTE DO FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO-FNDE, no uso de suas atribuições legais e tendo em vista o disposto no art. 15, inciso V, Anexo I, do Decreto nº 9.007, de 20 de março de 2017, e

Considerando as diretrizes do Governo Federal, representado pelo Gabinete de Segurança Institucional da Presidência da República, que recomenda a implantação, no âmbito de cada órgão da Administração Pública Federal (APF), de processos e de metodologias de segurança da informação e comunicações, conforme preconiza a Norma Complementar nº 02/IN01/DSIC/GSI/PR, de 13 de outubro de 2008;

Considerando o advento da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação-LAI), que regula 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;

Considerando as boas práticas em segurança preconizadas pelas normas ABNT NBR ISO/IEC 27001:2013, 27002:2013 e 27005:2011;

Considerando a necessidade de estabelecer os direcionamentos e os valores adotados para a gestão de segurança da informação e comunicações no âmbito do Fundo Nacional de Desenvolvimento da Educação;

Considerando a importância que deve ser dada à garantia da integridade, à disponibilidade, à confidencialidade e à autenticidade dos dados e das informações nos mais diversos suportes utilizados pelo Fundo Nacional de Desenvolvimento da Educação; e

Considerando o Acórdão nº 1.233-TCU/2012, que trata da adoção dos normativos de Segurança da Informação e Comunicações (SIC), não facultativos, mas obrigação da alta administração, e o Acórdão nº 3.051-TCU/2014, que prevê a estratégia geral de Segurança da Informação, **resolve**:

Art. 1º Instituir, no âmbito Fundo Nacional de Desenvolvimento da Educação (FNDE), a Política de Segurança da Informação e Comunicações (POSIC) do FNDE, regida pelos objetivos e diretrizes estabelecidos nesta Portaria.

CAPÍTULO I

DAS DISPOSIÇÕES PRELIMINARES

Art. 2º A POSIC tem como finalidade definir as diretrizes de segurança da informação e comunicações do FNDE, que demonstram os princípios considerados adequados para o manuseio, o controle e a proteção das informações contra a destruição, a modificação, a violação, a divulgação indevida e os acessos não autorizados, sejam acidentalmente ou intencionalmente, visando preservar a integridade, a confidencialidade, a disponibilidade e a autenticidade das informações, comumente indicada pela sigla C.I.D.A.

CAPÍTULO II

DOS OBJETIVOS

Art. 3º Constituem objetivos da POSIC:

I. Estabelecer direcionamentos, regras, objetivos e valores a serem adotados para a gestão de segurança da informação e comunicações em âmbito do FNDE, de acordo com sua missão e com as leis e regulamentações relevantes ao caso. Para tanto, deve atender às seguintes orientações:

a. Estabelecer uma política clara e alinhada com a missão da casa.

b. Obter apoio e comprometimento com a segurança da informação por meio da publicação, atualização e manutenção de uma política de segurança da informação para o FNDE.

c. Revisar as diretrizes de segurança da informação a intervalos planejados ou quando mudanças significativas ocorrerem, para assegurar a sua contínua pertinência, adequação e eficácia.

CAPÍTULO III

DA ABRANGÊNCIA

Art. 4º Esta Política aplica-se aos recursos de Tecnologia da Informação e Comunicações (TIC), ambientes e processos de trabalho, estabelecendo responsabilidades e obrigações a todos os servidores, terceirizados, prestadores de serviços, fornecedores e estagiários, doravante chamados simplesmente de colaboradores, sendo de responsabilidade de cada um o seu cumprimento.

CAPÍTULO IV

CONCEITOS E DEFINIÇÕES

Art. 5º Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações localizam-se no documento “Dicionário dos Termos Técnicos”.

CAPÍTULO V

REFERÊNCIAS LEGAIS E NORMATIVAS

Art. 6º As ações de Segurança da Informação e Comunicações do Fundo Nacional de Desenvolvimento da Educação deverão observar os seguintes requisitos legais e normativos:

I. Decreto nº 1.171, de 22 de junho de 1994, que aprova o Código de Ética Profissional do Servidor Público Civil do Poder Executivo Federal;

II. Decreto nº 3.505, de 13 de junho de 2000, que institui a Política de Segurança da Informação nos órgãos e entidades da Administração Pública Federal;

III. Lei nº 9.983, de 14 de julho de 2000, que altera o Decreto-Lei nº 2.848, de 7 de setembro de 1940 (Código Penal), que dispõe sobre a tipificação de crimes por computador contra a Previdência Social e a Administração Pública;

IV. Art. 1.016 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil), que dispõe que os administradores respondem solidariamente perante a sociedade e os terceiros prejudicados, por culpa no desempenho de suas funções;

V. Instrução Normativa nº 01, de 13 de junho de 2008, do Conselho de Defesa Nacional e suas respectivas Normas Complementares publicadas no Diário Oficial da União (DOU) pelo Departamento de Segurança da Informação e Comunicações do Gabinete de Segurança Institucional da Presidência da República (DSIC/GSIPR), que disciplina a gestão de segurança da informação e comunicações no âmbito da Administração Pública Federal;

VI. Portaria nº 763, de 30 de outubro de 2017, que institui o Comitê de Governança Digital (CGD) no âmbito do Fundo Nacional de Desenvolvimento da Educação;

VII. Lei nº 12.527, de 18 de novembro de 2011, que dispõe sobre os procedimentos a serem observados pela União, Estados, Distrito Federal e Municípios, com o fim de garantir o acesso a informações;

VIII. Decreto nº 7.724, de 16 de maio de 2012, que regulamenta a Lei nº 12.527, de 18 de novembro de 2011;

IX. Decreto nº 7.845, de 14 de novembro de 2012, que regulamenta procedimentos para credenciamento de segurança e tratamento de informação classificada em qualquer grau de sigilo, e dispõe sobre o Núcleo de Segurança e Credenciamento;

X. Norma NBR ISO/IEC 27002:2013-Código de Práticas para a Gestão da Segurança da Informação;

XI. Norma NBR ISO/IEC 27001:2013 – Sistemas de Gestão de Segurança da Informação; e

XII. Norma NBR ISO/IEC 27005:2001 – Gestão de Riscos de Segurança da Informação.

CAPÍTULO VI

PRINCÍPIOS

Art. 7º A Política de Segurança da Informação e Comunicação está fundamentada nos princípios da disponibilidade, da integridade, da confidencialidade e da autenticidade, visando a proteção e a preservação das informações necessárias às atividades do FNDE.

CAPÍTULO VII

DIRETRIZES GERAIS

Art. 8º É dever dos colaboradores do FNDE conhecer e cumprir a POSIC.

Art. 9º Todos colaboradores do FNDE são responsáveis pela segurança dos ativos de informação e comunicações que estejam sob a sua responsabilidade e por todos os atos executados com suas identificações, tais como: identificação de usuário da rede (Login), crachá, carimbo, endereço de correio eletrônico ou assinatura digital.

Art. 10 Os recursos de TIC disponibilizados pelo FNDE devem ser utilizados estritamente dentro do seu propósito.

Art. 11 Os contratos de prestação de serviços, firmados pelo FNDE conterão cláusula específica sobre a obrigatoriedade de atendimento às diretrizes desta POSIC, devendo ainda, exigir da entidade contratada, a assinatura de Termo de Compromisso.

CAPÍTULO VIII

DIRETRIZES ESPECÍFICAS

Art. 12 Estas diretrizes aplicam-se tanto no ambiente informatizado quanto nos meios convencionais de processamento, comunicação e armazenamento da informação e rege-se pelas seguintes diretrizes:

I. Informação é patrimônio

a. Toda e qualquer informação gerada, adquirida, utilizada ou armazenada pelo FNDE é considerada parte do seu patrimônio e deve ser protegida quanto aos aspectos de confidencialidade, autenticidade, integridade e disponibilidade.

II. Proteção compatível com riscos

a. O investimento necessário em medidas de segurança deve ser dimensionado segundo o valor do ativo que está sendo protegido e de acordo com o risco de potenciais prejuízos para o negócio, para a atividade fim e para os objetivos institucionais.

III. Tratamento conforme classificação

a. Todas as informações devem ter classificação de segurança, apostas de maneira a ser adequadamente protegidas quando da sua criação, utilização, custódia e descarte.

IV. Responsabilização baseada na credencial

a. A credencial de colaborador é pessoal e intransferível, qualificando-o como responsável por todas as atividades desenvolvidas por meio dela, sendo pré-requisito para a liberação do uso dos ativos de informação o preenchimento de um Termo de Ciência.

V. Utilização restrita às atividades

a. A autorização, o acesso e o uso da informação e dos ativos de informação são controlados e limitados às atribuições necessárias para cumprimento das atividades de cada colaborador. Qualquer outra forma de uso necessitará de prévia autorização do Proprietário do Ativo de Informação, entendido como aquele que gerou a informação.

VI. Utilização orientada à segurança

a. Somente é permitido o uso de ativos de informação homologados e autorizados pelo FNDE. Estes devem ser identificados de forma individual, protegidos, inventariados, com documentação atualizada e estarem de acordo com as cláusulas contratuais e a legislação em vigor. Segregação de funções

b. A administração e a execução de funções ou áreas de responsabilidade críticas para o negócio, definidas pelo FNDE, devem ser segregadas para que ninguém detenha controle de um processo na sua totalidade, visando à redução do risco de mau uso acidental ou deliberado.

VII. Conscientização contínua

a. Colaboradores devem ser continuamente capacitados e conscientizados nos procedimentos de segurança e no uso correto dos ativos de informação quando da realização de suas atividades, de forma a minimizar possíveis riscos à segurança.

VIII. Autorização definida pelo gestor

a. O gestor de um determinado perímetro do FNDE (definição no Dicionário de Termos Técnicos) é também responsável pela liberação e cancelamento do acesso aos recursos e aos locais restritos sob sua responsabilidade.

IX. Continuidade dos serviços

a. A disponibilidade de recursos, do uso, do acesso e da proteção das informações deverá ocorrer naturalmente, preservando a normalidade das atividades do FNDE, de modo a proteger os seus processos críticos contra falhas ou desastres significativos aos negócios da Autarquia que acarretem paradas das suas atividades administrativas.

X. Conformidade no uso

a. Os ativos disponibilizados para uso devem estar em conformidade com a legislação vigente, cláusulas contratuais pactuadas e os requisitos de segurança da informação.

XI. Auditoria permanente

a. O cumprimento da Política de Segurança da Informação e Comunicações será periodicamente monitorado. Auditorias, pelas áreas competentes, poderão ser realizadas, respeitando-se os princípios normativos e legais.

XII. Canal único de notificação

a. Todos os colaboradores, conhecendo qualquer desvio por quebra de segurança, devem notificar:

i. O Gestor de segurança da informação e comunicação.

XIII. Monitoramento do uso de recursos

a. O monitoramento do uso de recursos do FNDE é uma fase do ciclo de controle na qual as ações em Segurança da Informação e Comunicação devem ser checadas, após sua regular implementação.

XIV. Privilégio mínimo

a. Evitar permissões inadequadas que causem exposições desnecessárias à segurança do FNDE.

XV. Gestão de riscos de segurança da informação e comunicação

a. Mapear processos que permitam identificar e implementar medidas de proteção necessárias para minimizar os riscos a que estão sujeitos os ativos de informação do FNDE, e equilibrá-los com os custos operacionais e financeiros envolvidos (avaliar custo x benefício).

CAPITULO IX

COMPETÊNCIAS E RESPONSABILIDADES

Art. 13 Ao colaborador não é dado o direito de desconhecimento da Política de Segurança da Informação e Comunicações (POSIC), devendo seguir rigorosamente o proposto nas normas de segurança, desde que essa Política esteja regularmente publicada e divulgada.

Art. 14 Compete ao Comitê de Governança Digital – CGD aprovação das diretrizes da POSIC e suas regulamentações, que visam preservar a disponibilidade, a integridade e a confidencialidade das informações do FNDE.

Art. 15 O FNDE nomeará um servidor público que atuará como Gestor de Segurança da Informação e Comunicações com as seguintes competências:

I. Promover cultura de segurança da informação e comunicações;
II. Acompanhar as investigações e as avaliações dos danos decorrentes de quebras de segurança;
III. Propor recursos necessários às ações de segurança da informação e comunicações;
IV. Coordenar o Comitê de Governança Digital (CGD), quanto às atribuições relativas à segurança da informação e comunicação, e a equipe de tratamento e resposta a incidentes em redes computacionais;
V. Realizar e acompanhar estudos de novas tecnologias, quanto a possíveis impactos na segurança da informação e comunicações;
VI. Manter contato direto com o DSIC para o trato de assuntos relativos à segurança da informação e comunicações;
VII. Propor normas relativas à segurança da informação e comunicações.

CAPITULO X

DIVULGAÇÃO E CAPACITAÇÃO

Art. 16 O FNDE deverá promover ações permanentes de conscientização dos colaboradores visando à disseminação das diretrizes e normas estabelecidas nesta política.

Art. 17 A POSIC e as normas deverão ser divulgadas no boletim interno do FNDE e disponíveis na Intranet para todos os colaboradores.

CAPITULO XI

ATUALIZAÇÃO

Art. 18 Esta POSIC e todos os instrumentos normativos gerados a partir dela devem ser atualizadas ou canceladas pela ocorrência de alguma das seguintes situações:

I. Alteração dos procedimentos vigentes ou adoção de novos;
II. Estabelecimento de novos dispositivos legais ou regulamentares, bem como reformulação dos existentes;
III. Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento;
IV. Mudança estratégica da instituição;
V. Mudanças de tecnologia no FNDE; e
VI. A partir dos resultados das análises de riscos realizadas no FNDE que venham a impactar/provocar necessária mudança em normativo de segurança para readequação da Autarquia aos riscos encontrados (mitigação)

Parágrafo único-Os procedimentos para aprovação e divulgação das normas alteradas seguem a mesma tramitação de uma norma nova.

CAPITULO XII

PENALIDADES

Art. 19 As autoridades e todos os colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicações e devem observar integralmente o que dispõe este documento. A inobservância dessas regras acarretará a apuração das responsabilidades funcionais na forma da legislação em vigor, podendo haver responsabilização penal, civil e administrativa.

CAPÍTULO XIII

DAS DISPOSIÇÕES FINAIS

Art. 20 Os casos omissos e não cobertos pelas orientações emanadas por esta norma serão resolvidos pelas seguintes instâncias:

I. Comitê de Governança Digital-CGD, com apoio, se necessário, das áreas técnicas do FNDE; e
II. Presidência do FNDE, em decisão final, caso o CGD não tenha autonomia para tomar as providências cabíveis.

CAPITULO XIV

VIGÊNCIA

Art. 21 Esta Portaria entra em vigor na data de sua publicação.

Art. 22 Fica revogada a Norma DS-001-2002-SEXEC, aprovada pela Portaria nº 044, de 21 de março de 2003, constante do Boletim de Serviço – Edição Extra nº 09 de 21/03/2003.

SILVIO DE SOUSA PINHEIRO