FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO - FNDE
DIRETORIA DE ADMINISTRAÇÃO - DIRAD
COORDENAÇÃO-GERAL DE RECURSOS LOGÍSTICOS - CGLOG
COORDENAÇÃO DE DOCUMENTAÇÃO INFORMAÇÃO E LOGÍSTICA - CODIL
DIVISÃO DE DOCUMENTAÇÃO E PUBLICAÇÃO - DIDOP
SERVIÇO DE BIBLIOTECA E PUBLICAÇÃO OFICIAL - SEBIP

BOLETIM DE PESSOAL E SERVIÇO

Brasília-DF, terça-feira, 27 de novembro de 2018

SUMÁRIO

ATOS ADMINISTRATIVOS

PRESIDÊNCIA

FICHA TÉCNICA

Fundo Nacional de Desenvolvimento da Educação - FNDE
PRESIDENTE: SILVIO DE SOUSA PINHEIRO
DIRETORA DE ADMINISTRAÇÃO: MANUEL DERNIVAL SANTOS NETO

Boletim de pessoal e serviço / Fundo Nacional de Desenvolvimento da Educação. - N. 127(jul.2010)- .— Brasília: FNDE, 1993- .

Diário
Continuação de: Boletim de Pessoal e Serviço - Extra

1. Atos oficiais das autoridades administrativas - Periódicos. I. Fundo Nacional de Desenvolvimento da Educação

CDU 35.077.2(05)

SBS - Quadra 02 - Bloco 'I' - Ed. Elcy Meireles - Térreo
Brasília/DF - CEP: 70.070-929
Telefone: (061) 2022-4018 / 4020

BPS N° 352/2018

PORTARIA Nº 671, DE 16 DE NOVEMBRO DE 2018

Aprova as Normas de Segurança da Informação e Comunicação do Fundo Nacional de Desenvolvimento da Educação - FNDE.

O PRESIDENTE DO FUNDO NACIONAL DE DESENVOLVIMENTO DA EDUCAÇÃO, no uso de suas atribuições legais e tendo em vista o disposto no art. 15, inciso II, Anexo I, do Decreto n. º 9.007, de 20 de março de 2017, no Decreto nº 8.638, de 15 de janeiro de 2016 e no inciso VII, do art. 176, Anexo, da Portaria nº 629, de 3 de agosto de 2017 do Fundo Nacional de Desenvolvimento da Educação, **resolve**:

Art. 1º Aprovar a norma de Segurança da Informação e Comunicação NS 002/CGD/FNDE, que trata do Uso de Redes Sociais, conforme anexo I desta Portaria.

Art. 2º Aprovar a norma de Segurança da Informação e Comunicação NS 006/CGD/FNDE, que trata da Sensibilização, Conscientização e Capacitação em Segurança da Informação e Comunicação, conforme anexo II desta Portaria.

Art. 3º Aprovar a norma de Segurança da Informação e Comunicação NS 010/CGD/FNDE, que trata dos Procedimentos e Responsabilidades Operacionais, conforme anexo III desta Portaria.

Art. 4º Aprovar a norma de Segurança da Informação e Comunicação NS 014/CGD/FNDE, que trata da Aquisição, Desenvolvimento, Manutenção e Testes de Sistemas de Informação, conforme anexo IV desta Portaria.

Art. 5º Aprovar a norma de Segurança da Informação e Comunicação NS 016/CGD/FNDE, que trata das Responsabilidades dos Usuários, conforme anexo V desta Portaria.

Art. 6º Aprovar a norma de Segurança da Informação e Comunicação NS 019/CGD/FNDE, que trata do Uso de Dispositivos Móveis Dentro do FNDE, conforme anexo VI desta Portaria.

Art. 7º Aprovar a norma de Segurança da Informação e Comunicação NS 022/CGD/FNDE, que trata do Trabalho Remoto, conforme anexo VII desta Portaria.

Art. 8º Aprovar a norma de Segurança da Informação e Comunicação NS 023/CGD/FNDE, que trata da Segregação de Funções, conforme anexo VIII desta Portaria.

Art. 9º Aprovar a norma de Segurança da Informação e Comunicação NS 024/CGD/FNDE, que trata da Instalação e Configuração Segura de Sistemas Operacionais e Aplicações, conforme anexo IX desta Portaria.

Art. 10 Esta Portaria entra em vigor na data de sua publicação no Boletim de Pessoal e Serviço do FNDE.

Parágrafo único. O início da vigência das Normas de Segurança da Informação e Comunicação anexas está estabelecido no item sobre vigência e atualização de cada norma.

SILVIO DE SOUSA PINHEIRO

ANEXO I

USO DE REDES SOCIAIS

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2018-CGD: Diretrizes de Segurança.

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

Norma Complementar nº 04/IN01/DSIC/GSIPR – Diretrizes para o processo de Gestão de Riscos de Segurança da Informação e Comunicação – GRSIC nos órgãos e entidades da Administração Pública Federal.

Norma Complementar nº 07/IN01/DSIC/GSIPR – Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicação, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 08/IN01/DSIC/GSIPR – Estabelece as Diretrizes para Gerenciamento de Incidentes em Redes Computacionais nos órgãos e entidades da Administração Pública Federal.

Norma Complementar nº 15/IN01/DSIC/GSIPR – Estabelece diretrizes de Segurança da Informação e Comunicação para o uso de redes sociais, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

Manual de Orientação para Atuação em Mídias Sociais - Identidade padrão de comunicação digital do poder executivo federal.

US-CERT - Security Tip (ST06-003) - Staying Safe on Social Networking Sites

US-CERT - Security Tip (ST04-014) - Avoiding Social Engineering and Phishing Attacks

US-CERT - Security Tip (ST04-011) - Using Instant Messaging and Chat Rooms Safely

CAMPO DE APLICAÇÃO

Esta norma se aplica no âmbito do Fundo Nacional de Desenvolvimento da Educação.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

Silvio de Sousa Pinheiro
Presidente do FNDE

1. OBJETIVO

Estabelecer diretrizes de Segurança da Informação e Comunicação para o uso e gestão das redes sociais.

2. DESCRIÇÃO E ESCOPO

Estabelecer diretrizes, critérios, limitações e responsabilidades na gestão do uso seguro das redes sociais por parte de usuários que tenham permissão para administrar perfis institucionais, ou que possuam credencial de acesso a qualquer rede social, a partir da infraestrutura de rede do FNDE.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores que tenham permissão para administrar perfis institucionais ou acessar qualquer rede social, a partir da infraestrutura tecnológica do FNDE.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicação localizam-se no "Dicionário dos termos técnicos".

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicação está fundamentada nos princípios da disponibilidade, da integridade, da confidencialidade, da autenticidade e da legalidade, visando à proteção e a preservação das informações necessárias à execução das atividades da Autarquia.

6. PERFIL INSTITUCIONAL

6.1 O perfil institucional do FNDE deve ser protegido por meio das seguintes ações preventivas:

a) Não divulgar informações que possam tornar o perfil vulnerável;

b) Publicar apenas informações demandadas pelo FNDE;

c) Publicar apenas informações públicas, nos termos da Lei nº 12.527 de 2011;

d) Alterar as configurações padrões de privacidade, para que sejam acessíveis as informações somente aos interessados.

e) Utilizar senhas fortes que possam garantir segurança de acordo com o item 09 – Uso de Senhas da Norma de Segurança NS016 "Responsabilidades dos usuários";

f) Verificar as políticas de privacidade dos sites visitados; e

g) Manter os softwares de proteção e privacidade, principalmente o navegador da Web, atualizados.

6.2 Perfis institucionais mantidos nas redes sociais devem ser administrados e gerenciados por equipes integradas exclusivamente por servidores públicos. Quando não for possível, a equipe poderá ser mista, desde que sob a coordenação e responsabilidade de um servidor público.

6.2.1 No caso de equipe mista, as responsabilidades de gestão e administração por atuação nas redes sociais são exclusivas da coordenação da equipe, nos termos descritos no item 6.2, isentando destas responsabilidades os colaboradores terceirizados que compõem a equipe.

6.2.2 É vedada a terceirização completa da administração e da gestão de perfis institucionais mantidos nas redes sociais, conforme disposto no item anterior.

6.3 Se possível, nomear um servidor público, ocupante de cargo efetivo, para a função de proprietário do ativo de informação responsável pela gestão do uso seguro de cada perfil institucional nas redes sociais.

6.3.1 As responsabilidades de gestão e administração são exclusivas do proprietário do ativo de informação responsável pela gestão do uso seguro dos perfis institucionais nas redes sociais, isentando destas responsabilidades os colaboradores terceirizados envolvidos nas atividades operacionais da equipe.

6.4 O proprietário do ativo da informação deverá gerenciar, acompanhar e analisar, de forma contínua, a gestão do uso seguro de perfis institucionais nas redes sociais.

7. PERFIL PARTICULAR

7.1 O perfil particular que possua credencial de acesso a qualquer rede social, a partir da infraestrutura de rede do FNDE, deve ser protegido por meio das seguintes ações preventivas:

a) Não divulgar informações que possam tornar o perfil vulnerável;

b) Utilizar senhas fortes que possam garantir segurança de acordo com o item 09 - Uso de Senhas da Norma de Segurança, da norma NS016 “Responsabilidades dos usuários”;

c) Verificar as políticas de privacidade dos sites visitados; e

d) Manter os softwares de proteção e privacidade, principalmente o navegador da Web, atualizados.

7.2 Utilizar as redes sociais de forma segura, a fim de evitar:

a) Contato com pessoas mal-intencionadas;

b) Furto de identidade;

c) Invasão de perfil;

d) Uso indevido de informações;

e) Invasão de privacidade;

f) Recebimento de mensagens maliciosas;

g) Acesso a conteúdos impróprios ou ofensivos; e

h) Danos à imagem e à reputação.

8. **MIDIAS SOCIAIS**

8.1 Orientação das características comuns entre as mídias sociais:

a) Observar que, via de regra, a criação do perfil ou página de uma marca ou instituição e as respectivas configurações são gratuitas;

b) Observar que as redes aceitam a utilização de *hashtags* (ou marcadores);

c) Criar a montagem da base de seguidores e postagens sem limitações de caracteres;

d) Observar que há possibilidade de inserir fotos, vídeos e de utilizar aplicações diversas;

e) Observar que é permitido para o usuário curtir a página (botões chamados "curtir"); e

f) As interações dos usuários - cliques, comentários e postagens - devem ficar registrados em sua própria página, alimentando-a com conteúdo referente a tudo o que o usuário fez, gostou ou não gostou desde que passou a utilizar essa página.

NOTA: Ao aceitar utilização da plataforma de mídias sociais como uma ferramenta de comunicação pública com o cidadão, o FNDE deverá concordar com os termos impostos pela empresa criadora da mídia, caso a plataforma seja fornecida por terceiros.

8.2 Orientação para tomar conhecimento que a empresa criadora da mídia social poderá:

a) Alterar as regras de funcionamento a qualquer momento;

b) Eliminar ou restringir as possibilidades e funcionalidades do disponibilizado, mediante alteração das Políticas de Uso;

c) Personalizar os perfis e as páginas através de publicação de histórias, promoção de eventos, adição de aplicativos, entre diversas outras funcionalidades; e.

d) Atribuir funções administrativas a outras pessoas para que possam colaborar no gerenciamento;

NOTA: Somente servidores e colaboradores do setor responsável estão autorizados a criar páginas do FNDE.

8.3 Utilizar as melhores práticas na criação da página e observar algumas informações importantes desta plataforma:

- **Nomes das páginas:** Usar corretamente maiúsculas e minúsculas, não é permitida a utilização de sinais (! ou *, por exemplo);
- **Gerenciamento da página:** O responsável pela página pode definir vários gestores (perfis de pessoas reais) para cuidar da página do FNDE, com níveis de acesso e publicação definidos para cada um deles;

Ações	Administradores	Editor	Moderador	Anunciante	Analista
Gerenciar as funções e					

configurações da Página	✓				
Editar a Página e adicionar aplicativos	✓	✓			
Criar e excluir publicações em nome da Página	✓	✓			
Responder e excluir comentários e publicações na Página	✓	✓	✓		
Enviar mensagens como a Página	✓	✓	✓		
Criar anúncios	✓	✓	✓	✓	
Exibir informações	✓	✓	✓	✓	✓
Ver quem publicou como a Página	✓	✓	✓	✓	✓

- **Interação:** Ao administrador da página de mídia social é permitido, apenas, responder às demandas válidas endereçadas ao FNDE;
- **Promoções (Institucional):** O responsável pela manutenção da página na mídia social do FNDE pode realizar campanhas na página da Autarquia, desde que autorizado pela área de tecnologia da informação, após motivação do setor demandante; e
- **Fotos de capa:** Utilizar conteúdo e imagem exclusiva que represente a página do FNDE.

8.4 O FNDE deverá realizar ações preventivas contra situações de ataque e distorção informacional originada de uma base anônima, de cidadãos plugados à rede, tais como:

a) Monitorar as mídias sociais para se evitar o dano à segurança da informação do FNDE;

b) Implementar ações que fortaleçam a credibilidade desse veículo de comunicação;

c) Ter plano de resposta a crises em mídias sociais;

d) Controlar os canais de comunicação corporativos;

e) Manter redundância nos canais de comunicação corporativos; e

f) Realizar controle de autenticação e acesso às mídias sociais corporativas.

8.5 A gestão de perfis oficiais de Ministros ou de autoridades da administração pública não é permitida.

NOTA: Aplicar o estabelecido na Lei de Acesso à Informação (Lei nº 12.527, de 2011) às redes sociais.

9. DIRETRIZES GERAIS

9.1 Publicar textos, preferencialmente, com conteúdo simples, fácil, resumido, direto e com a menor extensão possível.

9.2 Padronização visual:

a) A composição dos elementos visuais deve representar a proposta ou a essência do perfil, tendo que representar graficamente o FNDE;

b) A linguagem visual deve ser integrada e coesa, independentemente do canal, para facilitar a relação direta com o público. É importante manter a mesma imagem de avatar (imagem do perfil), e as fotos de capa do usuário (cover) em todas as plataformas sociais.

9.3 Diretrizes editoriais

9.3.1 Dividir o padrão de produção de informação e divulgação da seguinte forma:

a) **Conteúdo Institucional:** São informações básicas de governo, em geral mais perenes e atemporais;

b) **Conteúdo Vivo ou Noticioso:** Trata-se do conteúdo de caráter factual, importante para o dia a dia da população.

c) **Conteúdo de Utilidade Pública:** São aquelas informações que o cidadão procura sobre serviços e processos governamentais.

10. PENALIDADES

Os servidores e colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicação, e têm o dever de observar integralmente o disposto nesta norma. A inobservância dessas regras acarretará em penalidades previstas no âmbito penal, civil e administrativo, na forma da legislação vigente.

11. RESPONSABILIZAÇÃO

11.1 Não é dado ao servidor e colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicação, devendo seguir rigorosamente o proposto nas normas de segurança. O desconhecimento dessa norma por parte do usuário não o isenta das responsabilidades e penalidades previstas.

11.2 **Disposições Gerais**

11.3 Os casos omissos e não amparados pelas orientações emanadas desta norma serão resolvidos pelo:

a) Comitê responsável pela Segurança da Informação e Comunicação, com apoio, se necessário, das áreas técnicas do FNDE; e

b) Presidente do FNDE, em decisão final, caso o Comitê responsável pela Segurança da Informação e Comunicação não tenha autonomia para tomar as providências cabíveis.

12. VIGÊNCIA E ATUALIZAÇÃO

12.1 **Este documento entra em vigor em 60 (sessenta) dias a partir da data de sua publicação e pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:**

a) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma;

b) Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

12.2 **A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração.**

12.3 **Condições obrigatórias de atualização do documento**

a) Surgimento ou alteração de leis e/ou regulamentações vigentes;

b) Mudança estratégica da instituição que tenha impacto nesta Norma;

c) Mudança de tecnologia no FNDE que tenha impacto nesta Norma; ou

d) 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).

12.4 **Responsável pela atualização**

12.4.1 Conforme Mapa de Responsabilidades.

ANEXO II

SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2018-CGD: **Diretrizes de Segurança.**

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

Norma Complementar nº 17/IN01/DSIC/GSIPR – Atuação e Adequações para Profissionais da área de Segurança da Informação e Comunicações nos Órgãos e Entidades da Administração Pública Federal.

Norma Complementar nº 18/IN01/DSIC/GSIPR – Estabelece diretrizes para as atividades de ensino em segurança da informação e comunicações nos órgãos e entidades da Administração Pública Federal.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Fundo Nacional de Desenvolvimento da Educação.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-005-2002-SEXEC: Norma para conscientização de usuários em segurança da informação*, publicada em 10 de dezembro de 2002.

APROVAÇÃO

_____

Silvio de Sousa Pinheiro
Presidente do FNDE

1. OBJETIVO

Assegurar que os servidores e colaboradores sejam sensibilizados e capacitados em Segurança da Informação e Comunicação, segundo suas atribuições, a fim de reduzir o risco de quebra de segurança.

2. DESCRIÇÃO E ESCOPO

Estabelecer regras para a sensibilização, conscientização e capacitação dos usuários quanto à Política de Segurança da Informação e Comunicação (POSIC).

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores responsáveis pelo processo de sensibilização, conscientização e capacitação em Segurança da Informação e Comunicação.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações localizam-se no "Dicionário dos Termos Técnicos".

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, da integridade, da confidencialidade, da transparência e da autenticidade, visando a proteção e a preservação das informações necessárias às atividades da organização.

6. SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO

6.1 A área responsável pela capacitação de servidores e colaboradores do FNDE deverá produzir programa de sensibilização, conscientização e capacitação relativo ao conteúdo de segurança da informação e comunicação (SIC) alinhado às políticas e procedimentos dessa POSIC e com o apoio da área de Segurança da Informação e Comunicação do FNDE bem como do Gestor de SIC.

6.2 O programa de SIC deverá atender as seguintes orientações:

a) Conter atividades de conscientização e capacitação;

b) Produzir campanhas como o Dia da Segurança da Informação;

c) Produzir informação simples e constante ao usuário por meio de boletins, folhetos e dicas de segurança;

d) Desenvolver conteúdos pertinentes aos perfis profissionais de cada área da casa. Levar em consideração conteúdos específicos que atendam ao usuário comum, ao profissional de tecnologia da Informação e a alta administração da casa;

e) Manter ciclos regulares de ações de conscientização e capacitação por meio de calendário, conforme o exemplo apresentado no exemplo do anexo A;

f) Acompanhar a atualização da POSIC e implementar alterações no programa conforme necessário;

g) Coletar informações e alertas da área de tratamento e resposta a incidentes computacionais para inclusão em suas atividades de ensino;

h) Desenvolver formas eficientes de ensino por meio de educação à distância (treinamento pela Internet);

i) Privilegiar educação presencial para assuntos que envolvam debate e conteúdo mais complexo de acordo com avaliação pedagógica da área de capacitação do FNDE;

j) Desenvolver métricas para avaliar a retenção da informação disponibilizada ao usuário tanto na capacitação quanto na conscientização regular. Privilegiar treinamentos baseados em incidentes publicamente divulgados na mídia televisiva e jornalística;

k) Desenvolver conteúdos de SIC com apoio pedagógico e tomando por exemplo o anexo B; e

l) Desenvolver conteúdo inicial de SIC para novos servidores e colaboradores.

6.3 O programa de SIC deverá ter orçamento anual a fim de garantir ações contínuas de segurança da informação e comunicação para toda a casa.

7. PENALIDADES

Os servidores e colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicação e têm o dever de observar integralmente o disposto nesta norma. A inobservância dessas regras acarretará em penalidades previstas no âmbito penal, civil e administrativo, na forma da legislação vigente.

8. RESPONSABILIZAÇÃO

8.1 Não é dado ao servidor ou colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicações, devendo este seguir rigorosamente o proposto nesta norma de segurança. O desconhecimento desta norma por parte do usuário não o isenta das responsabilidades e penalidades previstas.

8.2 **Disposições Gerais**

8.3 Os casos omissos e não amparados pelas orientações emanadas desta norma serão resolvidos pelo:

a) Comitê responsável pela Segurança da Informação e Comunicação, com apoio, se necessário, das áreas técnicas do FNDE; e

b) Presidente do FNDE, em decisão final, caso o Comitê responsável pela Segurança da Informação e Comunicação não tenha autonomia para tomar as providências cabíveis.

9. VIGÊNCIA E ATUALIZAÇÃO

9.1 **Este documento entra em vigor em 120 (cento e vinte) dias a partir da data de sua publicação e pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:**

a) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma;

b) Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

9.2 **A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração.**

9.3 **Condições obrigatórias de atualização do documento**

a) Surgimento ou alteração de leis e/ou regulamentações vigentes;

b) Mudança estratégica da instituição que tenha impacto nesta Norma;

c) Mudança de tecnologia no FNDE que tenha impacto nesta Norma; ou

d) 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).

9.4 **Responsável pela atualização**

9.4.1 Conforme Mapa de Responsabilidades.

10. ANEXOS

Anexo A - Calendário anual de eventos (exemplo).
Anexo B - Atividades de ensino em segurança da informação e comunicações (exemplo).

ANEXO A

CALENDÁRIO ANUAL DE PALESTRAS (EXEMPLO)

Evento	Sumário	Período
PROPRIEDADE INTELECTUAL E MARKETING LEGAL	Uma sociedade baseada em conhecimento e ativos intangíveis, proteger a propriedade intelectual, a marca e a marca, mesmo em ambientes digitais, tem uma importância ainda maior do que antes. Essa proteção pode ser obtida com o registro nos escritórios competentes de Propriedade Intelectual (como o Instituto Nacional da Propriedade Industrial - INPI), registradores e mídias sociais.	Janeiro
SEGURANÇA DA INFORMAÇÃO E COMBATE À FRAUDE	Na atual realidade, onde os dados são a base da economia digital, os procedimentos e regras de Segurança da Informação são indispensáveis para uma boa gestão dos negócios, pois sua implementação protege o valor de uma empresa. São medidas extremamente relevantes para a blindagem das empresas e envolvem todos os setores, abrangendo três níveis: Tecnologia, Processos e Pessoas.	Março
PRIVACIDADE, PROTEÇÃO DE DADOS E CONFORMIDADE	Em uma sociedade cada vez mais complexa, conectada e definida por seus ativos intangíveis, a tecnologia se estabeleceu como base e diferencial competitivo para todos os negócios.	Maio
CONTRATOS DE TI	A maioria dos processos críticos das empresas depende da qualidade, regularidade e disponibilidade dos serviços de tecnologia. Somente quando os riscos envolvidos são devidamente compreendidos, é possível estabelecer acordos que possam proteger os interesses de ambas as partes sem atrapalhar o equilíbrio econômico do contrato.	Julho
PERÍCIA DIGITAL, CONTENCIOSO CÍVEL E CRIMINAL	Resolução de conflitos extrajudiciais e judiciais, coleta de evidências eletrônicas por meio de perícia digital.	Setembro
Dia da Segurança da Informação	Divulgação da POSIC. Distribuição de Folhetos. Distribuição de Panfletos. Filmes. Teatro CIA-Toque de Areia - Tema SIC	Novembro

Fonte: www.ppadvogados.com.br – Patrícia Peck Pinheiro – Direito Digital

ANEXO B

ATIVIDADES DE ENSINO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES (EXEMPLO)

Atividades de ensino	Modelo da atividade de ensino	Duração mínima
Sensibilização	Ambientação em SIC	1 h
Conscientização	Seminário de noções básicas em SIC	8 h
	Noções de SIC nos cursos de formação	6 h
Capacitação	Curso de gestão em SIC – presencial	40 h
	Curso de gestão em SIC - EAD	120 h
Especialização	Curso de especialização em SIC	360 h

Fonte: Norma Complementar nº 18/IN01/DSIC/GSIPR, Anexo A.

A Norma Complementar nº 03, de 30 de junho de 2009 – Diretrizes para Elaboração de Política de Segurança da Informação e Comunicações, recomenda aos órgãos e entidades da APF, promover a cultura de segurança da informação e comunicações, por meio de atividades de sensibilização, conscientização, capacitação e especialização.

Sensibilização e Conscientização			
Calendário de eventos	**Temas alinhadas com a POSIC**	**Objetivo**	**Eventos**
1º mês	Contas e senhas NS016-RESPONSABILIDADES DOS USUÁRIOS	O uso de contas com privilégios administrativos para a realização de operações ordinárias.	Treinamento
1º mês	Classificação da informação NS020-CLASSIFICAÇÃO DA INFORMAÇÃO	A classificação, o tratamento, e a gestão da informação	Treinamento
2º mês	Ambiente de trabalho NS016-RESPONSABILIDADES DOS USUÁRIOS	O uso dos computadores dos usuários.	Treinamento
2º mês	Código malicioso NS008-PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS	Orientação sobre vírus, "trojans", "worms", "spyware" e outras pragas virtuais.	Treinamento
3º mês	Controle de acesso NS017-CONTROLE DE ACESSO AO SISTEMA OPERACIONAL	Garantir que tais prestadores acessem áreas estritamente relacionadas às suas funções	Treinamento

3º mês	Funções e responsabilidades NS003-ORGANIZAÇÃO INTERNA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES	Orientar sobre as regras que regem a infraestrutura de segurança da informação	Treinamento
4º mês	Transporte físico NS019-SEGURANÇA DE EQUIPAMENTOS	Orientar sobre o transporte de Equipamentos portáteis, como os "laptops" e PDAs etc.	Treinamento
4º mês	Criptografia NS022-CONFORMIDADE LEGAL	Orientar sobre a utilização de certificados digitais na assinatura de mensagens garantindo que o conteúdo da mesma não foi alterado, e que o usuário que enviou é realmente aquele que aparece no corpo da mensagem	Treinamento
5º mês	Infraestrutura de Segurança NS003-ORGANIZAÇÃO INTERNA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES	Orientar sobre Infraestrutura de Segurança da Informação	Treinamento
5º mês	Incidente de segurança NS003-ORGANIZAÇÃO INTERNA DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES	Orientar sobre a resposta adequada e oportuna aos incidentes de segurança.	Treinamento
6º mês	Recursos humanos e prestação de serviços NS006-SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES	Orientar sobre o cumprimento voluntário, consciente e maduro do Código de Ética	Treinamento
6º mês	Direitos de privacidade NS022-CONFORMIDADE LEGAL	Orientar sobre a preservação da privacidade das informações próprias ou custodiadas pelo FNDE	Treinamento
7º mês	Integridade de sistemas e dados NS009-MONITORAMENTO DE SISTEMAS	Orientar sobre Integridade de sistemas e dados	Treinamento
7º mês	Conformidade NS022-CONFORMIDADE LEGAL	Orientar sobre regras de verificação de conformidade com requisitos legais..	Treinamento

8º mês	Comunicação de dados/voz NS014-AQUISIÇÃO, DESENVOLVIMENTO E MANUTENÇÃO DE SISTEMAS DE INFORMAÇÃO	Orientar sobre Comunicação de dados/voz	Treinamento
9º mês	Direitos de propriedade intelectual NS022-CONFORMIDADE LEGAL	Orientar sobre ações criminais pela negligência ou pelo uso impróprio de informações de terceiros, protegidas pelo direito de propriedade intelectual, tais como a apropriação ou reprodução indevida de informações sem citação da fonte, a reprodução ilegal de software protegido, etc.	Treinamento
10º mês	Utilização adequada de recursos NS011-ADMINISTRAÇÃO DO CORREIO ELETRÔNICO	Orientação sobre a utilização do correio eletrônico que deve ser usado para fins do negócio por exemplo.	Treinamento
11º mês	Identificação e autenticação NS017-CONTROLE DE ACESSO AO SISTEMA OPERACIONAL	Orientar sobre o compartilhamento de contas e outros mecanismos de autenticação.	Treinamento
12º mês	Educação e conscientização NS006-SENSIBILIZAÇÃO, CONSCIENTIZAÇÃO E CAPACITAÇÃO EM SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÕES	Orientar sobre as regras que regem a segurança na contratação dos recursos humanos do FNDE, a fim de prevenir e reduzir os riscos de erro humano, roubo, fraude ou uso indevido das instalações e informações.	Treinamento

Fonte: Norma Complementar nº 18/IN01/DSIC/GSIPR.

As diretrizes nos contextos de atuação e adequações para profissionais da área de TIC na APF com vistas a prover diretrizes estratégicas, responsabilidades, competências e o apoio para implementar a Gestão de SIC no FNDE, bem como a ampliação do conhecimento de seus profissionais, a troca de experiências, a capacitação e consequente evolução da SIC no FNDE.

Capacitação - Linhas e Temas	
Gestão da Segurança da Informação e Comunicações	Gestão da Segurança da Informação e Comunicações
	Governança e Riscos
	Leis, Regulação e Conformidade
	Segurança em Redes
	Controle de Acesso Físico e Lógico
	Gestão de Continuidade de Negócios
	Criptografia e Infraestrutura de Chaves Públicas (ICP)
	Desenvolvimento Seguro
	Gerencia de Projetos
	Gestão de Processos
	Prospecção de oportunidades, tecnologias e inovação em SIC
Segurança de Redes	Firewall
	IDS/IPS
	Arquiteturas e Escopo de Segurança
	Segmentação
	Tunelamento de Tráfego e VPN
	Segurança de Perímetro
	Segurança de Aplicações e Serviços
	Segurança Redes Wireless e Serviços Móveis
	Segurança dos Dispositivos de Rede
Tratamento de Incidentes de Segurança Computacional	Aspectos Normativos: criação de CSIRTS, CSIRTS de Governo; CSIRTS na Rede Mundial de Computadores
	Processos de Monitoramento e Detecção de Intrusão
	Processos de Análise e Resposta a Incidentes
	Processos de Divulgação e Comunicação com Entidades Externas
Forense Computacional	Aspectos Normativos
	Técnicas de Cópia e Preservação de Evidências
	Técnicas de Análise Forense
Segurança no Desenvolvimento de Software	Vulnerabilidades de Software
	Testes de Vulnerabilidade
	Arquitetura de Software Seguro
	Codificação de Software Seguro
	Firewall de Aplicações Web
Gestão de Continuidade de Negócios	Gestão de Continuidade de Negócios e Recuperação de Desastres
	Estratégias de Gestão de Continuidade de Negócios
	Implementação, Manutenção e Testes
	Cultura da Gestão de Continuidade de Negócios
Gestão de Riscos	Planejamento de Gestão de Riscos
	Metodologias de Gestão de Riscos
	Identificação de Riscos
	Análise/Avaliação de Riscos
	Tratamento de Riscos
Auditoria/Conformidade	Planejamento
	Análise dos Riscos
	Execução
	Relatório Final
Certificação Digital	Conceitos e Recursos
	Convenções, Políticas e Formatos
	Aplicações em uso
Computação em Nuvem	Conceitos Básicos
	Modelos de Computação em Nuvem
	Riscos da Computação em Nuvem
	Proteção dos Dados
	Responsabilidades dos Usuários
	Responsabilidades do Provedor de Serviço
Mobilidade	Conceito e Evolução
	Riscos de Segurança associados com os Dispositivos Móveis
	Segurança para Dispositivos Móveis
	Gerenciamento de Dispositivos Móveis
	Responsabilidades dos Usuários
Redes Sociais	Conceito e Evolução

	Riscos de Segurança associados com o uso das Redes Sociais
	Privacidade, Exposição e Comportamento do Usuário
	Principais Controles de Segurança

Fonte: Norma Complementar nº 18/IN01/DSIC/GSIPR, Anexo B

Certificações Recomendadas para Profissionais de SIC	
Gestão da Segurança da Informação	CISM - Certified Information Security Manager
	CISSP - Certified Information Systems Security Professional
	CISSP (ISSAP) - Information Systems Security Architecture Professional
	CISSP (ISSEP) - Information Systems Security Engineering Professional
	CISSP (ISSMP) - Information Systems Security Management Professional
	ISFS - Information Security Foundation based on ISO/IEC 27002
	ISMAS - Information Security Management Advanced based on ISO/IEC 27002
	ISMES - Information Security Management Expert based on ISO/IEC 27002
	MCSO - Modulo Certified Security Officer
Segurança de Redes	CompTIA Security+
	ECSA - Ec-Council Security Analyst
	GAWN -GIAC Assessing Wireless Networks
	GCIA - GIAC Certified Intrusion Analyst
	GPEN - GIAC Penetration Tester
	SSCP - Sustems Security Certified Practitioner
Segurança de Redes/Gestão da Segurança da Informação	CASP - CompTIA Advanced Security Practitioner
Segurança de Redes/Segurança no Desenvolvimento de Software	CEH - Certified Ethical Hacker
	GWAPT - GIAC Certified Web Application Penetration Tester
	LPT - Licensed Penetration Tester
Tratamento de Incidentes de Segurança Computacional	CHFI - Certified Hacking Forensic Investigator
	GCFA - GIAC Certified Forensic Analyst
	GCFE - GIAC Cetified Forensic Examiner
	GREM - GIAC Certified Reverse Engineering Malware
Forense Computacional	CHFI - Certified Hacking Forensic Investigator
	GCFA - GIAC Certified Forensic Analyst
	GCFE - GIAC Certified Forensic Examiner
	GREM - GIAC Certified Reverse Engineering Malware
Segurança no Desenvolvimento de Software	CSSLP - Certified Secure Software Lifecycle Professional
Gestão de Continuidade de Negócios	ABCP - Associate Business Continuity Professional
	AMBCI - Associate Member Business Continuity Institute
	CBCI - Certified Business Continuity Institute
	CBCP - Certified Business Contitnuity Professional
	CFCP - Certified Functional Continuity Professional
	MBCP - Master Business Continuity Professional
	SBCI - Specialist Business Continuity Institute
Auditoria/Conformidade	Auditor Lider ISO 27001
	CISA - Certified Information Systems Auditor
Gestão/Auditoria/Conformidade	Cobit - Certified Objectives for Information and related Technology
	CRISC - Risk and Information Systems Control
	ITIL - Information Technology Infrastructure Library

Fonte: Norma Complementar nº 18/IN01/DSIC/GSIPR, Anexo A

ANEXO III

PROCEDIMENTOS E RESPONSABILIDADES OPERACIONAIS

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2018-CGD: **Diretrizes de Segurança.**

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

ABNT NBR ISO/IEC 20000-1:2013 - Tecnologia da informação - Gestão de serviços - Parte 1: Requisitos do sistema de gestão de serviços

ABNT NBR ISO/IEC 20000-2:2013 - Gerenciamento de serviços - Parte 2: Guia de aplicação do sistema de gestão de serviços

Norma Complementar nº 20/IN01/DSIC/GSIPR, (Revisão 01) Estabelece as Diretrizes de Segurança da informação e Comunicações para Instituição do Processo de Tratamento da Informação nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Fundo Nacional de Desenvolvimento da Educação.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-010-2002-SEXEC: Norma sobre os procedimentos e responsabilidades operacionais*, publicada em 10 de dezembro de 2002.

APROVAÇÃO

_____

Silvio de Sousa Pinheiro
Presidente do FNDE

1. OBJETIVO

Garantir uma operação segura e correta dos recursos de processamento, armazenamento e movimentação da informação.

2. DESCRIÇÃO E ESCOPO

Esta norma tem por escopo a segurança na gestão de serviços de tecnologia da informação e comunicação (TIC) bem como na segmentação de ambientes computacionais.

3. PÚBLICO-ALVO

Esta norma destina-se à direção e às equipes técnicas envolvidas com a gestão de serviços de tecnologia da informação e comunicação (TIC) bem como na segmentação de ambientes computacionais.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da informação e Comunicação localizam-se no "Dicionário dos Termos Técnicos".

5. PRINCÍPIOS

Além dos princípios que regem a Política de Segurança da Informação e Comunicação do FNDE, esta Norma está fundamentada no princípio da Divulgação, segundo o qual, os procedimentos e responsabilidades em relação à gestão e operação de todos os recursos de processamento da informação quando divulgados no âmbito da organização evitam diversos problemas no ambiente.

6. RESPONSABILIDADES

6.1 A área de tecnologia da informação deverá prover mecanismos de segurança para garantir a proteção das informações sob sua custódia, em especial nos quesitos confidencialidade, integridade, disponibilidade e autenticidade.

6.2 Qualquer alteração/deleção no conteúdo da informação custodiada somente será permitida mediante autorização formal da área fornecedora da informação, do proprietário do ativo da informação.

7. ACESSO LÓGICO

7.1 As áreas produtoras das informações e seus proprietários são responsáveis por determinar o nível de autorização e acesso às suas informações sob custódia da área de tecnologia da informação.

7.2 Devem-se levar em consideração, na gestão da informação, os seguintes critérios:

a) Conceder o acesso apenas a quem deve conhecer a informação;

b) Cancelar o acesso após desligamento ou mudança de setor;

c) Autorizar o acesso apenas após formalização da demanda; e

d) Bloquear todo acesso de conta inativa ou sem atividade observada acima de 30 (trinta) dias corridos;

NOTA: A área de tecnologia da informação deverá manter constante auditoria sob toda autorização, autenticação e acesso às informações custodiadas em seu ambiente tecnológico, a fim de se cumprir as orientações dessa norma.

8. REGISTRO DOS PROCEDIMENTOS DE SERVIÇOS

8.1 As áreas responsáveis pela gestão de serviços de TIC, segmentação e execução de atividades em ambientes computacionais deverão, dentro de suas áreas de atuação:

a) Definir procedimentos e responsabilidades operacionais e atualizá-los conforme haja mudança em regras de negócio corporativas que afetem sua regular execução;

b) Definir e divulgar regras seguras para a execução de suas atividades; e

c) Definir regras de confidencialidade, integridade, disponibilidade e autenticidade em sua área de atuação, em especial que contemplem:

1. A instalação e configuração de sistemas;

2. A interdependência entre sistemas;

3. A necessidade e periodicidade de criação de cópias, testes de restauração de sistemas e ambientes de acordo com a norma de segurança NS018 - Cópia de Segurança;

4. A devida restrição para o uso de utilitários e softwares em soluções de tecnologia da informação e ambientes;

5. O momento e a forma de acionamento das equipes necessárias para intervenção em caso de falhas inesperadas ou dificuldades técnicas enfrentadas nas Soluções de Tecnologia da Informação;

6. A necessidade de criação de trilhas e informações/registros de transações (*logs) para* auditoria das Soluções de Tecnologia da Informação e ambientes;

7. A periodicidade e a forma de descarte de resultados e registros de transações (*logs*) de falhas inesperadas;

8. O monitoramento eficaz e efetivo de ações executadas em sistemas e ambientes; e

9. A gestão de mudanças, de capacidade, de problemas, de configuração, de liberação, de implantação, de acordo com as boas práticas elencadas pela família de produtos ITIL em sua versão mais atual. Em especial:

a. Na gestão de mudanças:

i. A avaliação de impactos da mudança que comprometam a Segurança da Informação e Comunicação;

ii. A aprovação formal das mudanças propostas e considerar os riscos e impactos potenciais no serviço e no FNDE;

iii. Os procedimentos de recuperação e estabilização de sistemas e ambientes;

iv. As ações autorizadas em situações emergenciais;

v. Os testes necessários para evitar o comprometimento da Segurança da Informação e Comunicação; e

vi. O registro, monitoramento e auditoria das mudanças implementadas.

b. Na gestão de capacidade:

i. A correta gestão da capacidade para atender às necessidades de crescimento futuro, de acordo com a criticidade do negócio e com as regras de Segurança da Informação e Comunicação.

c. Na gestão de problemas:

i. Os procedimentos mapeados para a correta identificação de problemas e minimização de impactos na infraestrutura computacional;

ii. As ações preventivas para minimização de problemas; e

iii. Os registros de erros em bases de conhecimento divulgados para as áreas responsáveis.

d. Na gestão de configuração:

i. A correta e única identificação de cada Item de Configuração (IC);

ii. A aplicação de regras de segurança nos procedimentos de configuração da cada IC;

iii. O monitoramento, auditoria e eficaz recuperação dos ICs, em especial dos ativos que auxiliam na Segurança da Informação e Comunicação da TIC; e

iv. O armazenamento seguro das configurações dos ICs.

e. Na Gestão de liberação e implantação:

i. O alinhamento entre os gerentes de mudança e o de liberação/implementação para que haja a manutenção da Segurança da Informação e Comunicação nos ICs afetados, em especial nos casos emergenciais;

ii. A devida reversão de uma implantação dentro das regras de Segurança da Informação e Comunicação; e

iii. As trilhas de auditoria e monitoramento das implantações efetuadas.

8.2 Todos os procedimentos de serviços que contenham regras de segurança deverão ser formalizados e submetidos à direção da área de tecnologia da informação para aprovação.

8.3 As áreas responsáveis pela gestão de serviços de TIC, bem como pela segmentação e execução de atividades em ambientes computacionais deverão, dentro de suas áreas de atuação, aplicar as melhores práticas da família de produtos COBIT 5, em especial aquelas afetas à Segurança da Informação.

9. SEGREGAÇÃO DOS AMBIENTES DE DESENVOLVIMENTO, HOMOLOGAÇÃO, SUSTENTAÇÃO E PRODUÇÃO

9.1 Os responsáveis pelas áreas de desenvolvimento, homologação, sustentação e produção deverão observar e atender as seguintes regras de segurança:

9.1.1 Segregar os ambientes de desenvolvimento, homologação, sustentação e produção.

9.1.2 Implementar camada de segurança que garanta o manuseio e estabilidade dos ambientes em questão.

9.1.3 Gerar perfis distintos para acesso a cada ambiente operacional, com níveis de segurança pertinentes à importância dos dados trafegados em cada um deles.

9.1.4 Implementar perfil de segurança mais rígido e restritivo para o manuseio de informações no ambiente de produção.

9.1.5 Observar e reproduzir as seguintes regras de segurança:

a) Utilizar diferentes senhas de acesso para cada um dos ambientes;

b) Controlar os perfis e senhas de acesso por meio de autorização oficial fornecida pela área responsável pela gestão do ambiente;

c) Controlar todas as mudanças realizadas em aplicações e sistemas operacionais;

d) Migrar as modificações realizadas em ambientes de desenvolvimento, homologação e sustentação para ambiente de produção somente após averiguar a estabilidade;

e) Não utilizar compiladores, editores e outras ferramentas de desenvolvimento ou utilitários de sistemas em ambiente de produção;

f) Não utilizar o ambiente de produção para testes;

g) Não utilizar dados reais em ambientes de desenvolvimento e homologação.

h) Apagar todas as massas de dados usadas em ambientes de desenvolvimento e homologação após regular teste e aprovação das aplicações executadas com carga desses dados fictícios;

i) Manter, de forma centralizada e por um tempo mínimo de 6 (seis) meses, trilhas de auditoria das ações executadas em todos os ambientes tratados nesta norma.

10. DOCUMENTAÇÃO DOS AMBIENTES

10.1 Todo ambiente lógico custodiado pela área de tecnologia da informação deverá observar as seguintes orientações:

a) Manter documentação sempre atualizada. Essa documentação deverá refletir o ambiente real implantado/gerenciado/modificado; e

b) Comunicar a área gestora das informações custodiadas sob alterações de ambientes que impactem o funcionamento, acesso e disponibilização de suas bases de dados.

NOTA: A área de tecnologia da informação é responsável por garantir a adequada segurança e controle de acesso à documentação gerada pelos ambientes custodiados.

11. MANUTENÇÃO DOS AMBIENTES

11.1 Toda manutenção de ambientes lógicos custodiados pela área de tecnologia da informação deverá:

a) Solicitar a prévia autorização da área gestora da informação impactada pela manutenção preventiva; e

b) Comunicar, com urgência, a área impactada com relação a manutenção corretiva necessária.

12. PENALIDADES

Os servidores e colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicação, e têm o dever de observar integralmente o disposto nesta norma. A inobservância dessas regras acarretará em penalidades previstas no âmbito penal, civil e administrativa, na forma da legislação vigente.

13. RESPONSABILIZAÇÃO

Não é dado ao servidor ou colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicação, devendo seguir rigorosamente o proposto nesta norma. O desconhecimento desta norma por parte do usuário não o isenta das responsabilidades e penalidades previstas.

14. DISPOSIÇÕES GERAIS

Os casos omissos e não amparados pelas orientações emanadas desta norma serão resolvidos pelo:

a) Comitê responsável pela Segurança da informação e comunicação – CGD, com apoio, se necessário, das áreas técnicas do FNDE; e

b) Presidente do FNDE, em decisão final, caso o Comitê responsável pela Segurança da Informação e Comunicação não tenha autonomia para tomar as providências cabíveis.

15. VIGÊNCIA E ATUALIZAÇÃO

15.1 **Este documento entra em vigor em 90 (noventa) dias a partir da data de sua publicação e pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:**

a) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma;

b) Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

15.2 **A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração.**

15.3 **Condições obrigatórias de atualização do documento**

a) Surgimento ou alteração de leis e/ou regulamentações vigentes;

b) Mudança estratégica da instituição que tenha impacto nesta Norma;

c) Mudanças de tecnologia no FNDE que tenha impacto nesta Norma; ou

d) A partir dos resultados das análises de riscos realizadas no FNDE que venham a impactar/provocar a necessária mudança do normativo de segurança para readequação da Autarquia aos riscos encontrados (mitigação).

15.4 **Responsável pela atualização**

15.4.1 Conforme Mapa de Responsabilidades.

ANEXO IV

AQUISIÇÃO, DESENVOLVIMENTO, MANUTENÇÃO E TESTES DE SISTEMAS DE INFORMAÇÃO

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2018-CGD: Diretrizes de Segurança.

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

ABNT NBR ISO/IEC 12207:2009 – Tecnologia da informação – Processos de ciclo de vida de software.

Norma Complementar nº 16/IN01/DSIC/GSIPR – Estabelece diretrizes para desenvolvimento e obtenção de software seguro nos órgãos e entidades da administração pública federal.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Fundo Nacional de Desenvolvimento da Educação.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-014-2002-SEXEC: Norma de Segurança para o desenvolvimento e aquisição de sistemas*, publicada em 14 de março de 2003.

APROVAÇÃO

_____

Silvio de Sousa Pinheiro
Presidente do FNDE

1. OBJETIVO

Definir requisitos de segurança da informação para a aquisição, desenvolvimento, manutenção e testes de sistemas de informação.

2. DESCRIÇÃO E ESCOPO

Estabelecer regras que envolvam todo o ciclo de vida dos sistemas de informação adquiridos, desenvolvidos, mantidos e testados pelo FNDE, a fim de garantir a segurança.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores responsáveis pela aquisição, desenvolvimento, manutenção e testes dos sistemas de informação.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações localizam-se no "Dicionário dos Termos Técnicos".

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, da integridade, da confidencialidade e da autenticidade, visando a proteção e a preservação das informações necessárias às atividades da organização.

6. AQUISIÇÃO DE APLICAÇÕES

Na aquisição de aplicações a área de tecnologia da informação ou a área adquirente, com o apoio da área de TI, deverá:

a) Estabelecer exigências acerca da segurança afeta as aplicações adquiridas. É fundamental que toda aplicação possua ferramentas de correção de falhas para mitigar problemas de segurança;

b) Solicitar e receber todos os códigos-fontes e direitos de propriedade intelectual das aplicações adquiridas. Apenas em situações as quais estes códigos são fechados ou a transferência de propriedade intelectual é vedada legalmente (licença e propriedade sob domínio exclusivo da empresa, a exemplo de empresas como Microsoft, Oracle, etc.) não será exigida a transferência contratual para o FNDE;

c) Cobrar da empresa fornecedora das aplicações demandadas:

   1) A transferência de conhecimento sobre o completo funcionamento dessas aplicações;

   2) O funcionamento apenas de protocolos seguros para a comunicação entre os componentes dessa solução e entre essa solução e os demais sistemas "acoplados/conectados";

3) Segurança necessária para autenticação, autorização e acesso a suas bases de dados; e

4) A garantia de que suas aplicações atendam aos seguintes fundamentos de segurança: integridade, confidencialidade e autenticidade quanto ao manuseio das informações geradas/fornecidas por estas soluções.

d) Apenas implantar aplicações estáveis (já testadas e certificadas quanto a sua estabilidade e confiança).

7. DESENVOLVIMENTO DE APLICAÇÕES

7.1 Requisitos de Segurança no Desenvolvimento de Aplicações

7.1.1 Toda aplicação deverá obedecer às regras seguras durante o seu desenvolvimento, considerando os seguintes requisitos:

a) Segurança pelo *design*: toda metodologia de desenvolvimento de *software* deverá trazer mecanismos de segurança a fim de se atender a segurança pelo *design;*

b) Linguagem de programação segura: apenas utilizar linguagem de programação comprovadamente segura segundo indicação técnica do mercado;

c) Código seguro: obedecer a regras de segurança na produção do código da solução;

d) Repositório seguro: manter os códigos da solução em repositórios seguros e controlados;

e) Controlar versionamento: proteger os versionamentos das aplicações a fim de coibir acesso e uso indevido;

f) Checagem periódica: realizar checagens periódicas nas aplicações em desenvolvimento a fim de se evitar ou corrigir - em tempo - falhas, erros e vulnerabilidades; e

g) Reciclagem de desenvolvedor: realizar reciclagem dos desenvolvedores acerca de técnicas de programação seguras. Apresentar resultados dessa reciclagem por meio de documentação comprobatória.

7.2 Desenvolvimento de Aplicações de forma terceirizada

A Área de Tecnologia da Informação deve supervisionar as atividades de desenvolvimento de sistemas considerando, ao longo de todo o ciclo de vida das aplicações fornecidas por terceiros, os seguintes requisitos:

a) A necessária transferência do código-fonte e da de propriedade intelectual da solução demandada;

b) A garantia e a comprovação de que as aplicações foram desenvolvidas obedecendo a boas práticas de segurança. Comprovar que erros, falhas e vulnerabilidades foram considerados e mitigados adequadamente; e

c) A garantia de que os quesitos integridade, confidencialidade, autenticidade e disponibilidade foram levados em consideração na arquitetura da solução. Comprovar, tecnicamente e documentalmente, o atendimento dessa garantia.

8. MANUTENÇÃO E TESTE DE APLICAÇÕES

8.1 Critérios para manutenção e teste seguro de aplicações

8.1.1 Toda manutenção realizada em aplicações deverá:

a) Solicitar prévia aprovação técnica e conter regras de segurança a fim de se manter protegida as informações veiculadas por essas soluções;

b) Evitar instabilidades no ambiente de produção;

c) Privilegiar a segurança nos perfis de acesso às aplicações, concedendo permissão apenas aos módulos em efetiva manutenção no ambiente de produção;

d) Obedecer a procedimento formal de manutenção já documentado;

e) Evitar quebra de integridade do ambiente de produção;

f) Registrar trilha de auditoria para futuras checagens; e

g) Ocorrer apenas em horários fora do expediente. Exceções deverão ser motivadas e registradas para futura auditoria.

8.1.2 Implementar testes para aplicações a fim de se comprovar que erros, falhas e vulnerabilidade foram, efetivamente, evitados dentro de ciclo de desenvolvimento dessas soluções;

8.1.3 Realizar, no mínimo, os seguintes testes nas soluções:

a) Testes de recuperação;

b) Testes de autorização, autenticação e acesso seguro;

c) Testes de stress ou volumetria;

d) Testes de desempenho a fim de se verificar se as soluções atendem aos quesitos de confiabilidade e integridade de dados.

NOTA: Todos os testes deverão ser documentados e armazenados em local seguro para futura checagem ou auditoria.

NOTA FINAL: Toda aplicação deverá ser projetada, desenvolvida, mantida e testada observando princípios e boas práticas de segurança da informação durante todo o ciclo de vida da solução.

9. PENALIDADES

Os servidores e colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicação e têm o dever de observar integralmente o disposto nesta norma. A inobservância dessas regras acarretará em penalidades previstas no âmbito penal, civil e administrativo, na forma da legislação vigente.

10. RESPONSABILIZAÇÃO

10.1 Não é dado ao servidor ou colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicações, devendo este seguir rigorosamente o proposto nesta norma de segurança. O desconhecimento desta norma por parte do usuário não o isenta das responsabilidades e penalidades previstas.

10.2 **Disposições Gerais**

10.3 Os casos omissos e não amparados pelas orientações emanadas desta norma serão resolvidos pelo:

a) Comitê responsável pela Segurança da Informação e Comunicação, com apoio, se necessário, das áreas técnicas do FNDE; e

b) Presidente do FNDE, em decisão final, caso o Comitê responsável pela Segurança da Informação e Comunicação não tenha autonomia para tomar as providências cabíveis.

11. VIGÊNCIA E ATUALIZAÇÃO

11.1 **Este documento entra em vigor em 120 (cento e vinte) dias a partir da data de sua publicação e pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:**

a) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma;

b) Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

11.2 **A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração.**

11.3 **Condições obrigatórias de atualização do documento**

a) Surgimento ou alteração de leis e/ou regulamentações vigentes;

b) Mudança estratégica da instituição que tenha impacto nesta Norma;

c) Mudança de tecnologia no FNDE que tenha impacto nesta Norma; ou

d) 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).

11.4 **Responsável pela atualização**

11.4.1 Conforme Mapa de Responsabilidades.

ANEXO V

RESPONSABILIDADES DOS USUÁRIOS

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2018-CGD: **Diretrizes de Segurança.**

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

Norma Complementar nº 07/IN01/DSIC/GSIPR - Estabelece Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

Lei Nº 12.527, de 18 de Novembro de 2011 - Regula o acesso a informações previsto no inciso XXXIII do art. 5.

CAMPO DE APLICAÇÃO

Esta norma se aplica no âmbito do Fundo Nacional de Desenvolvimento da Educação.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-016-2002-SEXEC: Norma de Segurança sobre as responsabilidades dos usuários*, publicada em 14 de março de 2003.

APROVAÇÃO

_____

Silvio de Sousa Pinheiro
Presidente do FNDE

1. OBJETIVO

Orientar os usuários sobre responsabilidades associadas ao acesso seguro e sobre a prevenção contra acesso não autorizado aos recursos de tecnologia da informação.

2. DESCRIÇÃO E ESCOPO

Estabelecer requisitos de segurança para acesso seguro dos usuários autorizados e prevenir acesso não autorizado aos recursos de tecnologia da informação, de forma a garantir a proteção das informações e dos ativos de informação.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores,

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações localizam-se no "Dicionário dos Termos Técnicos".

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, da integridade, da confidencialidade, da autenticidade e da legalidade, visando à proteção e a preservação das informações necessárias à execução das atividades da Autarquia.

6. RESPONSABILIDADES DO USUÁRIO

6.1 O usuário deve:

a) Manter todo seu trabalho institucional na rede corporativa do FNDE.

b) Comunicar os problemas e incidentes relativos à segurança da informação à área de segurança da informação.

c) Prestar atenção a URL - Uniform Resource Locator de um site, para garantir que o site acessado seja legítimo e não um site malicioso;

d) Aproveitar os recursos antiphishing (protetor contra páginas/sites falsos) oferecidos pelo cliente de e-mail e pelo navegador;

e) Utilizar apenas aplicações homologadas pelo FNDE.

f) O usuário deve bloquear qualquer dispositivo eletrônico que faça uso da rede corporativa, ao afastar-se dele, para evitar o uso indevido por pessoas não autorizadas.

NOTA: Caberá à área de Tecnologia da Informação definir os recursos ou dados corporativos que o dispositivo móvel particular terá acesso.

6.2 O usuário não deve:

a) Divulgar informações sigilosas a que teve acesso por causa de sua função;

b) Enviar informações confidenciais pela Internet antes de verificar a segurança do canal de comunicação;

7. USO DE SENHAS

7.1 Ao receber uma nova senha de *login*, fornecida pelo administrador do serviço, o usuário deverá trocá-la por uma senha que seja de seu exclusivo conhecimento, no prazo máximo de 24 (vinte e quatro) horas.

NOTA: Após este período a conta será bloqueada, permanecendo assim até que haja uma solicitação formal da chefia imediata para o desbloqueio deste usuário;

7.2 Devem ser observados os seguintes cuidados ao usar a senha:

c) Certificar-se de que não está sendo observado. Caso sua senha seja capturada desta forma, poderá ser utilizada para cometer ações em seu nome (sob sua total responsabilidade);

d) NÃO compartilhar sua senha com outra pessoa (sua senha é pessoal e intransferível). Pelos mesmos motivos, não use senhas que não estejam designadas para você;

e) Alterar a senha nas seguintes situações:

- Após o primeiro acesso (trocar a senha padrão);
- Quando o sistema solicitar uma nova senha;
- Suspeita de descoberta de senha por terceiros; e
- Mesma senha durante 90 dias.

7.3 De acordo com os critérios de segurança, as senhas devem ser criadas observando as seguintes regras:

f) Não utilizar como elementos na elaboração das senhas:

- Caracteres repetidos consecutivamente (aaaaa, 222222, aabbcc etc.);
- Caracteres em ordem numérica ou alfabética (12345, abcde, aeiou etc.);
- Caracteres em ordem do teclado (qwert, asdfg, zxcvb, poiuy etc.);
- Qualquer tipo de dado pessoal, como: nome, sobrenome, *username*, nomes de parentes (esposa, filhos, etc.), número de telefone, datas importantes (aniversário, casamento, etc.) ou qualquer variação (por exemplo, de trás para frente). Todos esses exemplos são alternativos muito fáceis de serem descobertas;
- Palavras da língua portuguesa ou inglesa, pois são opções fracas;
- Nomes próprios em geral (pessoas, empresas, estados, cidades etc.);
- Apelidos, abreviações, iniciais dos nomes etc.; e
- Termos óbvios: Brasil, senha, usuário, *password*, system, sistema etc.

g) Utilizar, obrigatoriamente, como elementos na elaboração das senhas a combinação de letras, números e caracteres especiais (# & % $! * / + [ ]).

7.4 Os meios de identificação de cada administrador de recursos de tecnologia da informação, como senhas são únicos, pessoais e intransferíveis, não devendo ser compartilhados.

8. POLÍTICA DE MESA LIMPA E TELA PROTEGIDA

8.1 Deve-se adotar as políticas de "mesa limpa" e de "tela protegida" que são formas eficazes para reduzir os riscos de acesso não autorizado, perda e dano à informação, durante e fora do horário de trabalho.

NOTA: A não adoção da prática de "mesa limpa" e de "tela protegida" permite que pessoas mal-intencionadas possam acessar divulgar, modificar ou furtar informações restritas.

8.2 Deve-se adotar a política de "mesa limpa" para que nenhuma informação confidencial seja deixada à vista, seja em papel, mídias magnéticas ou qualquer outro dispositivo eletrônico.

8.3 Considerar sempre a classificação das informações (a ser divulgada oportunamente), os riscos correspondentes e os aspectos culturais, observando-se as seguintes regras:

h) Papéis e mídias de computador devem ser armazenados, quando não estiverem sendo utilizados, em lugares adequados, com fechaduras ou outras formas seguras de mobiliário, especialmente fora do horário normal de trabalho;
i) Informações sensíveis ou críticas ao negócio, quando não requeridas, devem ser guardadas em local distante da área de trabalho, de forma segura e fechada, de preferência em um cofre ou arquivo resistente a fogo, especialmente quando não houver expediente;
j) Pontos de recepção e envio de correspondências e máquinas de fax devem ser protegidas;
k) Equipamentos de reprodução corporativos (fotocopiadoras, scanners e máquinas fotográficas digitais) devem ser protegidos contra o uso não autorizado; e
l) Informações sensíveis e classificadas, quando impressas, devem ser imediatamente retiradas da impressora e fax.

8.4 A política de "tela protegida" para recursos de tecnologia da informação deve considerar a classificação das informações (a ser divulgada oportunamente), os riscos correspondentes e os aspectos culturais, contendo regras que incluam os seguintes pontos:

m) Os computadores e impressoras devem ser desligados quando não estiverem em uso (caso seja possível seu desligamento sem causar prejuízos ao serviço); e
n) Os equipamentos devem ser protegidos por mecanismos de bloqueio automático quando não estiverem em uso.

9. USO DO CORREIO ELETRÔNICO

9.1 O usuário deverá gerenciar seu Correio Eletrônico observando as seguintes regras:

a) Evitar bloqueio de sua conta por excesso de mensagens;

b) Eliminar periodicamente as mensagens cujo valor legal, administrativo ou corporativo não tenha mais utilidade ou pertinência;

c) Transmitir mensagens por Correio Eletrônico de forma consciente e responsável;

d) Utilizar o serviço de Correio Eletrônico apenas para atividades inerentes ao trato de informações corporativas;

NOTA: O manuseio da conta pessoal de correio eletrônico corporativo, disponibilizada ao usuário, é pessoal e intransferível, sendo seu titular o único responsável pelas ações e danos que venham a ser ocasionados por mau uso do serviço.

9.2 Deve ser vetada a utilização do serviço de correio eletrônico corporativo para enviar/encaminhar, receber e armazenar mensagens contendo:

o) Códigos maliciosos (vírus, Cavalos de Tróia, entre outros);
p) Materiais com conteúdo pornográfico, antiético, atentatórios à moral e aos bons costumes, ofensivos ou que incentivem a violência ou descriminação de raça ou credo ou qualquer outro tipo de discriminação previsto na Constituição Federal;
q) Conteúdo criminoso ou ilegal, ou que façam sua apologia;
r) Conteúdo que não respeite os direitos autorais ou comerciais pertinentes;
s) Mensagens em cadeia ou "pirâmides", independentemente da vontade do destinatário de receber tais mensagens;
t) Transmissão de conteúdo potencialmente perigoso, tais como arquivos executáveis ou outros que possam conter vírus ou outras ameaças;
u) Grande quantidade de mensagens de correio eletrônico (*junk mail* ou *spam*, incluindo qualquer tipo de mala direta, publicidade, comercial ou não, anúncios e informativos ou propaganda política) que afete a capacidade técnica da rede corporativa, ou seja, prejudicial ao trabalho de terceiros; e
v) Listas de endereços institucionais ao público externo em geral não afetos às atividades da Autarquia.

9.3 O correio eletrônico particular do usuário (ex. Gmail, Yahoo, etc.) não deve ser utilizado para tráfego de informações de interesse ou posse da Autarquia.

9.4 O usuário deve utilizar os serviços de correio eletrônico, tanto corporativo quanto particular, no ambiente da Autarquia, de forma a não prejudicar o trabalho de terceiros, causar tráfego desnecessário na rede de dados ou sobrecarregar os sistemas de informação ou outras organizações.

9.5 Mensagens de correio eletrônico que contenham informações classificadas como Ultrassecretas, Secretas e Reservadas, (segundo a Lei de Acesso à Informação – LAI nº 12.527/2011), utilizar, obrigatoriamente, criptografia, para garantir a segurança das informações trafegadas.

9.6 Para preservação e um bom funcionamento do serviço de correio eletrônico, o usuário deve atentar-se aos seguintes itens:

w) Manter o sigilo de sua senha de acesso a este serviço;

x) Excluir e-mails que contenham links de internet ou arquivos anexos de origem desconhecida ou duvidosa, a fim de evitar execução/instalação de softwares que contenham códigos maliciosos;
y) Não divulgar o endereço de correio eletrônico corporativo em sites ou listas de discussão na Internet cujo tema não está ligado às atividades corporativas; e
z) Evitar sobrecarregar o correio eletrônico com anexos (arquivos) facilmente localizáveis nessa rede.

9.7 O acesso à conta corporativa de correio eletrônico, do servidor ou colaborador deve ser realizado por pessoal designado mediante solicitação formal e justificada ao Gestor de Segurança da Informação, observando-se as seguintes situações:

aa) Desligamento do colaborador;
bb) Término do contrato de trabalho;
cc) Afastamento do usuário por motivos de licenças;
dd) Falecimento do usuário;
ee) Suspeita de infração à Política de Segurança da Informação e Comunicações em vigor; e
ff) Outros casos legais.

NOTA: Os serviços disponibilizados ao colaborador são de propriedade da Autarquia. Assim, o colaborador não pode recusar o compartilhamento das informações veiculadas por meio desses serviços alegando proteção à sua privacidade, intimidade, vida privada ou inviolabilidade das suas comunicações. Desta forma, é possível ao órgão monitorar as atividades de correio eletrônico, inclusive mensagens e conteúdos que trafegam dentro de seu portal de mensageria.

Fonte: Recurso de Revista nº TST-RR-613/2000-013-10-00.7

9.8 A caixa postal individual de correio eletrônico poderá, entre outras medidas, ser cancelada ou bloqueada quando for constatada utilização indevida, segundo avaliação prévia do Comitê responsável pela Segurança da Informação e Comunicação.

9.9 Toda mensagem de e-mail deve seguir a padronização estabelecida pelo órgão.

NOTA: Recomenda-se ser mantido o mesmo "Título" em uma cadeia de respostas sobre o mesmo assunto.

10. USO DA INTERNET

10.1 Todo usuário pode utilizar o serviço de Internet após a liberação da concessão de acesso à rede corporativa e segundo o perfil de acesso autorizado.

10.2 O usuário não deve disponibilizar informações, que não sejam públicas, custodiadas ou de propriedade do FNDE na Internet sem prévia autorização do respectivo proprietário.

10.3 A utilização da Internet deverá ser realizada dentro dos princípios da administração pública, em especial dos princípios da legalidade, da moralidade, da razoabilidade, da ética entre outros.

10.4 Caso seja necessário ao desempenho das funções institucionais do usuário, poderá ser autorizado *download* de arquivos da Internet, desde que sejam respeitados os termos de licença de cópia, de uso e contratuais pertinentes.

10.4.1 Os arquivos que eventualmente forem bloqueados poderão ter o *download* liberado temporariamente desde que previamente autorizados após adequada justificativa.

10.5 Quando o usuário utilizar o acesso à Internet para a realização de transações que envolvam informações classificadas como Reservadas, Secretas e Ultrassecretas (conforme a LAI nº 12.527/2011), adotar, pelo menos, as seguintes regras de segurança:

gg) Digitar o endereço do site diretamente no navegador (browser);
hh) Não clicar em links indicados nas páginas de Internet ou mensagens de correio eletrônico;
ii) Ao acessar sites de instituições bancárias, verificar a existência de certificado digital (cadeado indicado na janela do navegador); e
jj) Quando da transmissão de informações, verificar se o endereço do site (URL) inicia-se por "HTTPS".

10.6 A Internet não deve ser utilizada para:

kk) Transmitir em benefício próprio ou para terceiros, softwares ou informações custodiadas ou de propriedade do FNDE sem prévia autorização;
ll) Acessar sites de pornografia, pedofilia, que façam incitação à violência e outros contrários à legislação e regulamentação em vigor, mesmo que alguns desses sites não estejam bloqueados pelos mecanismos de segurança implementados na rede corporativa;
mm) Acessar sites com conteúdo que viola as leis de proteção da propriedade intelectual, industrial e de direitos autorias (pirataria, rateio ou que divulguem número de série para registro de softwares), sites ofensivos ou que façam apologia a racismo, xenofobia ou a qualquer outro tipo de discurso de ódio;
nn) Executar atividades relacionadas a jogos eletrônicos; e
oo) Acessar conteúdo multimídia, exceto nos casos em que tais ações sejam condizentes com as atividades desempenhadas no FNDE.

11. **PENALIDADES**

Os servidores e colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicações e têm o dever de observar integralmente o disposto nesta norma. A inobservância dessas regras acarretará em penalidades previstas no âmbito penal, civil e administrativo, na forma da legislação vigente.

12. **RESPONSABILIZAÇÃO**

12.1 Não é dado ao servidor ou colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicações, devendo este seguir rigorosamente o proposto nesta norma de segurança. O desconhecimento desta norma por parte do usuário não o isenta das responsabilidades e penalidades previstas.

12.2 **Disposições Gerais**

12.3 Os casos omissos e não amparados pelas orientações emanadas desta norma serão resolvidos pelo:

pp) Comitê responsável pela Segurança da Informação e Comunicação, com apoio, se necessário, das áreas técnicas do FNDE; e

qq) Presidente do FNDE, em decisão final, caso o Comitê responsável pela Segurança da Informação e Comunicação não tenha autonomia para tomar as providências cabíveis.

13. VIGÊNCIA E ATUALIZAÇÃO

13.1 **Este documento entra em vigor em 60 (sessenta) dias a partir da data de sua publicação e pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:**

a) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma;

b) Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

13.2 **A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração.**

13.3 **Condições obrigatórias de atualização do documento**

e) Surgimento ou alteração de leis e/ou regulamentações vigentes;

f) Mudança estratégica da instituição que tenha impacto nesta Norma;

g) Mudança de tecnologia no FNDE que tenha impacto nesta Norma; ou

h) 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).

13.4 **Responsável pela atualização**

13.4.1 Conforme Mapa de Responsabilidades.

ANEXO VI

USO DE DISPOSITIVOS MÓVEIS DENTRO DO FNDE

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2018-CGD: Diretrizes de Segurança.

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

Norma Complementar nº 07/IN01/DSIC/GSIPR – Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 12/IN01/DSIC/GSIPR – Estabelece as Diretrizes e Orientações Básicas para o Uso de Dispositivos Móveis nos aspectos referentes à Segurança da Informação e Comunicações (SIC) nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta - APF.

CAMPO DE APLICAÇÃO

Esta norma se aplica no âmbito do Fundo Nacional de Desenvolvimento da Educação.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

Silvio de Sousa Pinheiro
Presidente do FNDE

1. OBJETIVO

Estabelecer diretrizes e orientações básicas para o uso de dispositivos móveis, no âmbito do FNDE, referentes à Segurança da Informação e Comunicação.

2. DESCRIÇÃO E ESCOPO

Estabelecer procedimentos relativos à utilização de dispositivos móveis particulares e corporativos, de forma a garantir que as informações e ativos de informação do FNDE sejam devidamente protegidos.

3. PÚBLICO-ALVO

Esta norma destina-se aos servidores, colaboradores e visitantes que tenham acesso à rede do FNDE a partir de dispositivos móveis particulares ou corporativos.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicação localizam-se no "Dicionário dos Termos Técnicos".

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicação está fundamentada nos princípios da disponibilidade, da integridade, da confidencialidade, da autenticidade, da legalidade, visando à proteção e a preservação das informações necessárias à execução das atividades da Autarquia.

6. DIRETRIZES

6.1 Para o uso de dispositivos móveis corporativos nos ambientes do FNDE os seguintes pontos devem ser verificados:

a) Registros dos dispositivos móveis;

b) Restrições para conexão aos serviços de informação;

c) Controle de acesso;

d) Técnicas criptográficas;

e) Proteção contra *malware*;

f) Desativação, bloqueio e exclusão de forma remota;

g) *Backups*;

h) Uso dos serviços *web* e aplicações *web*.

6.2 Estabelecer procedimentos para evitar o acesso não autorizado ou a divulgação de informações armazenadas e processadas nos dispositivos (item 6.1).

6.3 Os dispositivos móveis corporativos devem ser protegidos fisicamente contra furto, roubo ou perda, especialmente quando deixados em carros ou em outros meios de transporte, quartos de hotéis, centros de conferência e locais de reunião.

6.4 Estabelecer procedimento específico de acordo com as exigências legais, securitárias e outros requisitos de segurança do FNDE em caso de furto, roubo ou perda de dispositivos móveis corporativos.

6.5 Os usuários de dispositivos móveis deverão cumprir as regras de segurança adotadas pelo órgão para manuseio de informação organizacional.

6.6 Programar treinamento aos servidores e colaboradores que utilizam dispositivos móveis corporativos como forma de aumentar a conscientização quanto aos riscos adicionais decorrentes desta forma de trabalho, e quanto aos controles implementáveis.

7. GERENCIAMENTO DA INFORMAÇÃO DE AUTENTICAÇÃO SECRETA

7.1 A concessão de informação de autenticação secreta deve ser controlada por meio de um processo de gerenciamento formal com os seguintes requisitos:

a) Os usuários deverão assinar o Termo de Uso de Responsabilidade (Anexo A) -, instrumento que estabelece as condições para a manutenção da confidencialidade da informação de autenticação secreta e a preservação das senhas de grupos de trabalho;

b) Garantir aos usuários, caso necessitem manter suas informações de autenticação secreta, que lhes seja fornecida uma informação de autenticação secreta temporária, sendo obrigatória a alteração no primeiro uso;

c) Estabelecer procedimentos para verificar a identidade do usuário antes de fornecer a informação de autenticação secreta temporária, de substituição ou nova;

d) Fornecer informação de autenticação secreta temporária aos usuários de maneira segura;

e) Informação de autenticação secreta temporária deve ser única para cada usuário e não deve ser fácil de ser descoberta; e

f) As informações de autenticações secretas padronizadas deverão ser alteradas logo após a instalação de sistemas ou *softwares.*

8. REGRAS GERAIS

8.1 Para fim de utilização dos dispositivos móveis, esta norma classifica os usuários em três grupos:

a) Servidores e colaboradores com dispositivos móveis corporativos: são aqueles que utilizam dispositivos móveis de computação e de comunicação de propriedade do FNDE;

b) Servidores e colaboradores com dispositivos móveis particulares: são aqueles que utilizam dispositivos móveis de computação e de comunicação de sua propriedade. Para fins desta Norma, os dispositivos particulares que se submetem aos padrões corporativos de software e controles de segurança; e

c) Usuários visitantes com dispositivos móveis particulares: terceiros que utilizam dispositivos móveis de computação e de comunicação de sua propriedade, ou do órgão ou entidade a que pertencem dentro do ambiente físico e virtual do FNDE.

8.2 Observar, no mínimo, os seguintes requisitos e procedimentos para autorização de acesso dos dispositivos móveis à rede corporativa do FNDE:

a) Configuração e utilização conforme os interesses da Autarquia; e

b) Adoção das medidas de segurança necessárias, como limitar o acesso às informações e aos recursos de tecnologia da informação, conforme os graus de segurança.

8.3 Os usuários descritos no subitem 8.1 "a" e "b" são responsáveis pelo transporte, guarda e proteção das informações armazenadas nos dispositivos móveis utilizados corporativamente, devendo zelar pela sua segurança.

8.3.1 Ao utilizar os dispositivos móveis fora da Autarquia, os usuários devem seguir o mesmo padrão de segurança utilizado dentro do perímetro do FNDE.

8.3.2 Quando não estiverem em uso, os dispositivos móveis devem ser desligados e armazenados em local que salvaguarde sua integridade física e lógica.

8.3.3 O uso dos dispositivos móveis corporativos deverá observar os princípios da ética, razoabilidade e legalidade.

8.3.4 Não será permitido armazenar, transportar, acessar ou distribuir conteúdo ilícito ou que fira a legislação nos dispositivos móveis utilizados corporativamente.

8.3.5 O usuário deverá bloquear o dispositivo móvel corporativo ao afastar-se dele, ainda que temporariamente, a fim de evitar que outras pessoas tenham acesso às informações armazenadas.

8.4 Poderão ser realizadas vistorias, a qualquer tempo, com o objetivo de avaliar a integridade física e lógica dos dispositivos móveis em uso corporativo, bem como para verificação acerca de armazenamento de conteúdo ilegal.

8.5 Devem ser divulgados, corporativamente, os requisitos mínimos de segurança aplicados aos dispositivos móveis, assim como o manuseio e guarda de informações.

9. COMPUTAÇÃO MÓVEL

9.1 Para fins de utilização dos dispositivos móveis, esta norma classifica os usuários em três grupos:

a) Servidores e colaboradores com dispositivos móveis corporativos: usuários que utilizam dispositivos móveis de computação e de comunicação de propriedade do FNDE;

b) Servidores e colaboradores com dispositivos móveis particulares: usuários que utilizam dispositivos móveis de computação e de comunicação de sua propriedade. Os dispositivos particulares que se submetem aos padrões corporativos de software e aos controles de segurança, e incorporados à rede de dados do FNDE, são considerados como dispositivos corporativos; e

c) Usuários visitantes com dispositivos móveis: usuários que utilizam dispositivos móveis de computação e de comunicação de sua propriedade, do órgão ou da entidade que representam, dentro do ambiente físico e virtual da Autarquia.

10. AGENTES PÚBLICOS COM DISPOSITIVOS MÓVEIS CORPORATIVOS

10.1 Os dispositivos móveis devem ser identificados e inventariados conforme os requisitos de segurança definidos na norma 05/CGD-FNDE – Responsabilidade pelos Ativos.

10.2 Os servidores e colaboradores não devem instalar aplicativos ou recursos não disponibilizados pelo setor responsável sem a devida permissão.

10.2.1 É vedada a modificação de *hardware* e *software* dos dispositivos móveis por parte do usuário. *Hardwares* e *softwares* não homologados serão removidos.

10.2.2 Havendo necessidade de instalação de *hardware* e/ou *software* específico, o usuário deve registrar uma solicitação à área de Tecnologia da Informação, que avaliará a demanda e sua justificativa.

10.3 É necessária a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, bem como do dispositivo às conexões de rede e recursos disponíveis.

10.4 É recomendada a adoção de mecanismos que garantam a proteção e sigilo dos dados armazenados nos dispositivos em caso de extravio.

10.4.1 Os dispositivos móveis devem ser classificados e protegidos conforme os requisitos de segurança.

10.5 Os servidores e colaboradores serão orientados a respeito dos procedimentos de segurança dos dispositivos que lhes forem disponibilizados, mediante a assinatura de Termo de Uso e Responsabilidade da Autarquia, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido.

10.6 O usuário deverá efetuar o ressarcimento quando da ocorrência de perda ou danos causados aos dispositivos móveis corporativos, ocasionados por mau uso ou utilização indevida, estando sujeito à aplicação das sanções cabíveis.

10.7 Quando da devolução dos dispositivos móveis corporativos:

a) As informações deverão ser transferidas em definitivo para o servidor de arquivos do FNDE;

b) O usuário deverá apagar todas as informações de cunho particular que por ventura estejam armazenadas nos dispositivos móveis; e

c) Os dispositivos móveis, bem como seus acessórios, devem ser devolvidos nas mesmas condições em que foram cedidos.

10.8 O FNDE não se responsabiliza por quaisquer informações de cunho particular que o usuário tenha deixado nos dispositivos móveis após sua devolução. Após a devolução dos dispositivos, o FNDE providenciará a sua sanitização (limpeza completa) para novo empréstimo.

11. AGENTES PÚBLICOS COM DISPOSITIVOS MÓVEIS PARTICULARES

11.1 Caberá à área de Tecnologia da Informação definir os recursos ou dados corporativos que o dispositivo móvel particular terá acesso.

11.2 É necessária a implementação de mecanismos de autenticação, autorização e registro de acesso do usuário, bem como do dispositivo às conexões de rede e recursos disponíveis.

11.3 Os servidores e colaboradores deverão adotar mecanismos que garantam a proteção e sigilo dos dados corporativos armazenados nos dispositivos móveis em caso de extravio.

11.4 Os servidores e colaboradores devem ser orientados a respeito dos procedimentos de segurança dos dispositivos móveis e dos recursos disponibilizados, mediante a assinatura do Termo de Uso e Responsabilidade, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido.

11.5 O dispositivo móvel particular do agente público somente poderá acessar a rede corporativa depois de atendidas as seguintes condições:

a) Instalação do Certificado de Segurança; e

b) Autenticação no portal.

12. USUÁRIOS VISITANTES COM DISPOSITIVOS MÓVEIS

12.1 Serão estabelecidos procedimentos de controle e concessão de acesso à rede visitante aos usuários não corporativos, durante sua permanência no FNDE.

12.2 A concessão de uso deve estar vinculada do aviso ao usuário sobre as normas internas de uso da rede.

13. DISPOSITIVOS MÓVEIS REMOVÍVEIS DE ARMAZENAMENTO

13.1 Informações classificadas somente podem ser armazenadas em dispositivos móveis removíveis que possibilitem a aplicação de controles compatíveis com seu nível de classificação.

13.2 Os dispositivos móveis removíveis devem ser utilizados considerando as soluções de segurança, de acordo com a Política de Segurança da Informação e Comunicações.

14. PENALIDADES

Os servidores e colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicação, e têm o dever de observar integralmente o disposto nesta norma. A inobservância dessas regras acarretará em penalidades previstas no âmbito penal, civil e administrativo, na forma da legislação vigente.

15. RESPONSABILIZAÇÃO

Não é dado ao servidor e ao colaborador o direito de alegar o desconhecimento da Política de Segurança da Informação e Comunicação, devendo seguir rigorosamente o proposto nas normas de segurança. O desconhecimento dessa norma por parte do usuário não o isenta das responsabilidades e penalidades.

16. DISPOSIÇÕES GERAIS

Os casos omissos e não amparados pelas orientações emanadas desta norma serão resolvidos pelo:

a) Comitê responsável pela Segurança da Informação e Comunicação, com apoio, se necessário, das áreas técnicas do FNDE; e

b) Presidente do FNDE, em decisão final, caso o Comitê responsável pela Segurança da Informação e Comunicação não tenha autonomia para tomar as providências cabíveis.

17. VIGÊNCIA E ATUALIZAÇÃO

17.1 **Este documento entra em vigor em 60 (sessenta) dias a partir da data de sua publicação e pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:**

a) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma;

b) Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

17.2 **A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração.**

17.3 **Condições obrigatórias de atualização do documento**

a) Surgimento ou alteração de leis e/ou regulamentações vigentes;

b) Mudança estratégica da instituição que tenha impacto nesta Norma;

c) Mudança de tecnologia no FNDE que tenha impacto nesta Norma; ou

d) 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).

17.4 **Responsável pela atualização**

17.4.1 Conforme Mapa de Responsabilidades.

18. ANEXOS

Anexo A – Termo de Uso e Responsabilidade (Modelo).

ANEXO A

TERMO DE USO E RESPONSABILIDADE (MODELO)

Especificações do dispositivo móvel

Nome do dispositivo:			
Marca/modelo:			
Área responsável pelo empréstimo:		Data de retirada:	_____/_____/_____
Nº. de Série:		Data prevista de devolução:	_____/_____/_____
Nº. de Patrimônio:		Data efetiva da devolução:	_____/_____/_____

	Processador (tipo/modelo/velocidade):_____		Disco rígido Capacidade (Gbytes):_____
	Memória RAM Quantidade (Mbytes):_____		Sistema Operacional Instalado:_____
	Placa de *Fax/Modem* Velocidade: _____		Cabo de conexão da placa *Fax/Modem*
	Placa de Rede		Cabo de conexão da placa de Rede
	Dispositivo *Wireless* Marca: _____		Mouse Tipo: _____
	Dispositivo *Bluetooth* Marca: _____		Teclado Número de série_____
	Dispositivo IrDA (infravermelho)		Dispositivos USB
	Unidade de CD-ROM interna Tipo: _____		Outros:
	Unidade de CD-ROM externa. Tipo: _____		
	Fonte de alimentação e cabo de força		

Recibo de Empréstimo de dispositivos móveis

Confirmo o recebimento deste Termo de Uso e Responsabilidade e do dispositivo especificado.

Comprometo-me a cumprir as regras descritas na Política de Segurança da Informação e Comunicações e a devolver o dispositivo com os respectivos acessórios nas mesmas condições que me foi entregue, bem como respeitar o prazo ora acordado deste empréstimo.

Usuário solicitante	**Responsável da área responsável pelo empréstimo**
Nome:	Nome:
Telefone:	Telefone:
Assinatura:	Assinatura:

========== recortar aqui ==========

Recibo de Devolução de dispositivos móveis

Confirmamos o recebimento do dispositivo descrito abaixo com os acessórios que o acompanharam, sem danos aparentes. Testes de funcionamento e eventual notificação ao usuário serão realizados no prazo máximo de 5 (cinco) dias úteis. Caso seja identificado qualquer problema com o dispositivo ou seus acessórios, o usuário será contatado para regularização da situação.

Marca/modelo:			
Área responsável pelo empréstimo:		Data de devolução:	
Nº. de Série:		Nº. de Patrimônio:	

Responsável da área responsável pelo empréstimo:	
Nome:	Assinatura:

ANEXO VII

TRABALHO REMOTO

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2018-CGD: Diretrizes de Segurança.

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

ABNT NBR ISO/IEC 27033-5 – Securing Comunication Across Networks Using Virtual Private Network (VPNs)

Norma Complementar nº 07/IN01/DSIC/GSIPR – Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 20/IN01/DSIC/GSIPR - Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação nos Órgãos e Entidades da Administração Pública Federal.

Requisitos Mínimos de Segurança da Informação aos Órgãos da Administração Pública Federal.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Fundo Nacional de Desenvolvimento da Educação.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

_____

Silvio de Sousa Pinheiro
Presidente do FNDE

1. OBJETIVO

Estabelecer diretrizes para implementação de controles no acesso remoto relativos a Segurança da Informação e Comunicação do FNDE.

2. DESCRIÇÃO E ESCOPO

Estabelecer procedimentos a serem seguidos na utilização de acesso remoto externo, através de recursos de tecnologia da informação, de forma a garantir a proteção dos ativos de informação do FNDE.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores que gerenciam soluções de acesso remoto.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicação localizam-se no "Dicionário dos Termos Técnicos".

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações 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.

6. ORIENTAÇÕES DE SEGURANÇA DA INFORMAÇÃO NO AMBIENTE VIRTUAL

6.1 Todo acesso remoto deverá:

a) Ser disponibilizado somente para pessoal autorizado;

b) Fornecer apenas o perfil de acesso necessário para o atendimento das atribuições inerentes às atividades desenvolvidas pelo usuário;

c) Ser monitorado, registrado e armazenado nos termos da norma 09-CGD-FNDE - Monitoramento de Sistemas;

d) Utilizar segurança necessária para se evitar quebra de proteção dos dados em trânsito;

e) Conter informações de segurança a serem repassadas ao usuário do serviço a fim de conscientizá-lo acerca dessa ferramenta de trabalho; e

f) Toda solução de acesso remoto deverá prover mecanismos de desconexão após 5 minutos de inatividade do usuário. Esse tempo deverá ser configurado pela área de tecnologia da informação segundo boas práticas de segurança.

6.1.1 A solução de acesso remoto deverá:

a) Ser liberada através de regras de firewall permitindo somente as portas necessárias para suportar o serviço;

b) Implementar segurança baseada em certificados digitais fornecidos apenas por autoridades certificadoras ligadas à ICP-Brasil;

c) Ser administrada por pessoal autorizado e por meio de acesso seguro; e

d) Proibir tráfego de informações de forma clara (textos sem criptografia) ou por meio de protocolos inseguros.

7. RESPONSABILIDADES

7.1 A área de tecnologia da informação é responsável:

a) Pela concessão de todos os acessos remotos disponibilizados pelo FNDE;

b) Pela recepção e conferência de toda a documentação que solicita o acesso remoto;

c) Pela administração da solução de acesso remoto;

d) Pelo descredenciamento de usuários após desligamento do órgão pela Coordenação-Geral de Gestão de Pessoas e Organizações – CGPEO;

e) Pela desconexão e auditoria de equipamentos estranhos à infraestrutura de tecnologia da informação do órgão;

f) Pela orientação dos usuários do serviço, em especial, quanto a procedimentos advindos da Norma 016-CGD-FNDE - Responsabilidades dos usuários;

g) Pelo fornecimento de solução de segurança que mitigue os riscos inerentes ao acesso remoto;

h) A sessão de acesso remoto deverá ser isolada das demais atividades/processos executados pela máquina do cliente. Não deverá haver ameaça independentemente do status da máquina cliente (máquina protegida/segura ou não), para o ambiente corporativo; e

i) Pelo fornecimento de Termo (s) a ser (em) assinado (s) pelo usuário antes de qualquer autorização de acesso remoto.

8. REDE PRIVADA VIRTUAL – DETERMINAÇÕES TÉCNICAS ENTRE REDES PARCEIRAS

8.1 A equipe técnica de segurança da área de Tecnologia da Informação deverá observar os seguintes aspectos para a operacionalização segura de rede privada virtual:

a) Proteção de endpoints;

b) Proteção contra *software* malicioso;

c) Autenticação, autorização e acesso controlado;

d) Sistema de detecção e prevenção de intrusão;

e) Recursos de segurança (incluindo firewalls);

f) Design seguro de rede;

g) Segregação de tunelamento;

h) Auditoria e monitoramento de rede;

i) Gerenciamento de vulnerabilidades; e

j) Criptografia de rotas da rede pública.

8.2 Todo dado trafegado via VPN deve, obrigatoriamente, ser criptografado.

8.3 Os mecanismos utilizados para implementar o túnel VPN (fim a fim) devem suportar verificação de integridade do dado por meio de:

a) Código de verificação;

b) Código de autenticação; e

c) Mecanismos de proteção *Anti-Replay*.

8.4 O processo de estabelecimento da VPN deve suportar controles de autorização e incluir ACLs - Acess Control List.

8.5 Controles de segurança devem ser implementados como contramedida a ataques de negação de serviço.

8.6 Autenticação para uso da VPN com consulta em base centralizada e com os devidos controles de política de senha.

8.7 Implementar tecnologia IPS (*Intrusion Prevention System*).

8.8 Selecionar tecnologia de gateway de segurança (incluindo firewall) apropriada para dar suporte seguro a uma implantação de VPN.

8.9 Evitar o tunelamento dividido.

NOTA: Os servidores e os colaboradores devem utilizar o portal remoto disponibilizado pela área de tecnologia da informação do FNDE.

9. **PENALIDADES**

Os servidores e colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicação, e têm o dever de observar integralmente o disposto nesta norma. A inobservância dessas regras acarretará em penalidades cabíveis, previstas no âmbito penal, civil e administrativa, na forma da legislação vigente.

10. RESPONSABILIZAÇÃO

10.1 Não é dado ao servidor ou colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicação, devendo seguir rigorosamente o proposto nas normas de segurança. O desconhecimento desta norma por parte do usuário não o isenta das responsabilidades e penalidades previstas.

10.2 **Disposições Gerais**

10.3 Os casos omissos e não amparados pelas orientações emanadas desta norma serão resolvidos pelo:

a) Comitê responsável pela Segurança da Informação e Comunicação, com apoio, se necessário, das áreas técnicas do FNDE; e

b) Presidente do FNDE, em decisão final, caso o Comitê responsável pela Segurança da Informação e Comunicação não tenha autonomia para tomar as providências cabíveis.

11. VIGÊNCIA E ATUALIZAÇÃO

11.1 **Este documento entra em vigor em 120 (cento e vinte) dias a partir da data de sua publicação e pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:**

a) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma; e

b) Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

11.2 **A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração.**

11.3 **Condições obrigatórias de atualização do documento**

a) Surgimento ou alteração de leis e/ou regulamentações vigentes;

b) Mudança estratégica da instituição que tenha impacto nesta Norma;

c) Mudança de tecnologia no FNDE que tenha impacto nesta Norma; ou

d) 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).

11.4 **Responsável pela atualização**

11.4.1 Conforme Mapa de Responsabilidades.

12. ANEXOS

Anexo A – Modelo de Termo de Responsabilidade.

ANEXO A

MODELO DE TERMO DE RESPONSABILIDADE

Declaro ter conhecimento da Política de Segurança da Informação e Comunicações (POSIC) do FNDE e estou ciente dos princípios de conduta ética e moral que regem todas as relações de trabalho e atividades exercidas.

Comprometo-me, sob as possíveis penalidades previstas nessa POSIC, a realizar meu trabalho de forma íntegra, respeitando os preceitos fundamentais que pautam a missão, a visão e os valores do FNDE.

Afirmo que as normas constantes na POSIC, os princípios éticos e demais parâmetros de conduta, orientarão o meu comportamento em todas as futuras iniciativas e decisões profissionais, como usuário de ativos de informação.

Obrigo-me a informar, imediatamente, qualquer violação das regras da POSIC, por minha parte ou de quaisquer outras pessoas, que possam prejudicar a confidencialidade, a disponibilidade, a integridade e a autenticidade das informações.

[Local], ___ de _____ de _____.

_____
Nome e unidade organizacional: [Agente Público]
Matrícula

_____
Nome e unidade organizacional: [Responsável pela área ou departamento]

Testemunhas:

_____

_____

ANEXO VIII

Fundo Nacional de Desenvolvimento da Educação

SEGREGAÇÃO DE FUNÇÕES

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2018-CGD: **Diretrizes de Segurança.**

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

Norma Complementar nº 07/IN01/DSIC/GSIPR (Revisão 01) - Estabelece as Diretrizes para Implementação de Controles de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal (APF), direta e indireta.

CAMPO DE APLICAÇÃO

Esta norma se aplica no âmbito do Fundo Nacional de Desenvolvimento da Educação.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Notas acerca da segregação de funções:

a) INTOSAI (2007, p. 51) - entendimento acerca da segregação de funções: as políticas, procedimentos e a estrutura organizacional [devem ser] estabelecidos para prevenir que uma pessoa controle todos os aspectos importantes relacionados às operações informatizadas e possa, desse modo, realizar ações não autorizadas ou obter acesso não autorizado aos bens ou aos registros;

b) Acórdão 1382/2009 Plenário 9.2. (...) envide esforços para que sejam estabelecidos procedimentos com vistas a implementar a segregação de funções e assegurar sua efetividade na execução das atividades de tecnologia de informação, com base nas orientações contidas na NBR ISO/IEC 17799:2005, item 10.1.3 - Segregação de funções e no Cobit 4.1, item PO4.11 - Segregação de funções;

c) Acórdão 309/2009 Plenário 9.1.37. segregue as funções e responsabilidades dos envolvidos com desenvolvimento e produção, em conformidade com o disposto no item 10.1.3 da NBR ISO/IEC 17799:2005;

APROVAÇÃO

Silvio de Sousa Pinheiro
Presidente do FNDE

1. OBJETIVO

Estabelecer parâmetros para definição da segregação de funções pelas autoridades competentes, a fim de reduzir as modificações não autorizadas ou não intencionais dos ativos de informação do FNDE, bem como o seu uso indevido.

2. DESCRIÇÃO E ESCOPO

Esta norma tem por escopo atividades, funções e atribuições empenhadas pelos servidores e colaboradores do FNDE.

3. PÚBLICO-ALVO

Esta norma destina-se aos servidores e colaboradores do FNDE.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações localizam-se no "Dicionário dos termos técnicos".

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, da integridade, da confidencialidade, da autenticidade e da legalidade, impessoalidade, moralidade, supremacia do interesse público e probidade administrativa visando à proteção e a preservação das informações necessárias à execução das atividades da Autarquia.

6. RESPONSABILIDADES DA DIREÇÃO

6.1 É responsabilidade da Direção assegurar que os servidores, colaboradores e fornecedores sejam instruídos para cumprirem, adequadamente, a Política de Segurança da Informação do FNDE.

6.2 A área de Segurança da Informação disponibilizará um canal seguro e anônimo de notificação para receber denúncias de violações às políticas e procedimentos de segurança da informação.

6.3 A direção deve demonstrar seu apoio às políticas, procedimentos e controles, e agir de forma exemplar.

7. SEGREGAÇÃO DE FUNÇÕES

7.1 A segregação de funções é um método para reduzir o risco de mau uso, acidental ou deliberado, dos ativos do FNDE. Para tanto, devem ser atendidas as seguintes determinações:

7.2 Separar as atribuições ou responsabilidades entre diferentes servidores e colaboradores, especialmente as funções ou atividades-chave de autorização, execução, atesto/aprovação, registro e revisão ou auditoria.

7.2.1 Realizar a rotatividade de funções, de modo a implementar controle que complemente a segregação de função, impedindo que o mesmo colaborador seja responsável pelas mesmas atividades por período indeterminado.

7.3 A segregação de funções em atividades críticas deverá ser realizada de acordo com a análise de risco corporativo.

7.4 O responsável pela diretoria deve definir o nível de acesso de cada servidor e colaborador dentro da sua área de atuação, bem como critérios de rodízio das atividades, processos e competências, a fim de impedir controle excessivo por uma única pessoa sobre diversos trabalhos do FNDE.

7.5 Designar substitutos para aqueles servidores e colaboradores que exerçam funções consideradas críticas.

8. PENALIDADES

Os servidores e colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicações, e têm o dever de observar integralmente o disposto nesta norma. A inobservância dessas regras acarretará em penalidades cabíveis, previstas no âmbito penal, civil e administrativa, na forma da legislação vigente.

9. RESPONSABILIZAÇÃO

Não é dado ao servidor ou colaborador o direito de alegar o desconhecimento da Política de Segurança da Informação e Comunicações, devendo seguir rigorosamente o proposto nas normas de segurança. O desconhecimento desta norma por parte do usuário não o isenta das responsabilidades e penalidades.

10. DISPOSIÇÕES GERAIS

Os casos omissos e não amparados pelas orientações emanadas desta norma serão resolvidos pelo:

c) Comitê responsável pela Segurança da Informação e Comunicação, com apoio, se necessário, das áreas técnicas do FNDE; e

d) Presidente do FNDE, em decisão final, caso o Comitê responsável pela Segurança da Informação e Comunicação não tenha autonomia para tomar as providências cabíveis.

11. VIGÊNCIA E ATUALIZAÇÃO

11.1 **Este documento entra em vigor em 60 (sessenta) dias a partir da data de sua publicação e pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:**

a) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma;

b) Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

11.2 **A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração.**

11.3 **Condições obrigatórias de atualização do documento**

i) Surgimento ou alteração de leis e/ou regulamentações vigentes;

j) Mudança estratégica da instituição que tenha impacto nesta Norma;

k) Mudança de tecnologia no FNDE que tenha impacto nesta Norma; ou

l) 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).

11.4 **Responsável pela atualização**

11.4.1 Conforme Mapa de Responsabilidades.

ANEXO IX

INSTALAÇÃO E CONFIGURAÇÃO SEGURA DE SISTEMAS OPERACIONAIS E APLICAÇÕES

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

***DS-001-2018-CGD:* Diretrizes de Segurança.**

ABNT ISO GUIA 73:2009 – Gestão de riscos – Vocabulário – Recomendações para uso em normas.

ABNT NBR ISO/IEC 27001:2013 – Tecnologia da informação – técnicas de segurança – sistemas de gestão de segurança da informação.

ABNT NBR ISO/IEC 27002:2013 – Tecnologia da informação – técnicas de segurança – código de prática para a gestão da segurança da informação.

ISO/IEC TR 19791 - Information technology - Security techniques - Security assessment of operational systems

ISO/IEC 15408-1 - Information technology - Security techniques - Evaluation criteria for IT security - Introduction and general model

ISO 27034-1:2011 Segurança da Informação em Aplicações – Parte 01

ISO 27034-2:2015 Segurança da Informação em Aplicações – Parte 02

ISO 27034-5:2017 Protocolos e estrutura de dados de Controle de Segurança de Aplicativos.

ISO 27034-6:2016 Guia de Segurança da Informação para Aplicações Específicas

Norma Complementar nº 16/IN01/DSIC/GSIPR – Diretrizes para Desenvolvimento e Obtenção de Software Seguro nos Órgãos e Entidades da Administração Pública Federal, direta e indireta – APF.

CAMPO DE APLICAÇÃO

Este documento se aplica no âmbito do Fundo Nacional de Desenvolvimento da Educação.

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

_____

Silvio de Sousa Pinheiro
Presidente do FNDE

1. OBJETIVO

Minimizar o risco de falhas de segurança em sistemas operacionais e aplicações.

2. DESCRIÇÃO E ESCOPO

Estabelecer requisitos de segurança da informação e comunicação na instalação e configuração de sistemas operacionais e aplicações.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores responsáveis pela instalação e configuração de sistemas operacionais e aplicações.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações localizam-se no "Dicionário dos Termos Técnicos".

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicações está fundamentada nos princípios da disponibilidade, da integridade, da confidencialidade e da autenticidade, visando a proteção e a preservação das informações necessárias às atividades da organização.

6. REQUISITOS PARA INSTALAÇÃO SEGURA DE SISTEMAS OPERACIONAIS

6.1 A instalação de sistemas operacionais deve ser feita de forma isolada do ambiente computacional disponibilizado para o FNDE

6.2 Toda instalação deverá observar os seguintes requisitos de segurança:

a) Disponibilizar em ambiente de produção apenas máquinas necessárias para o devido atendimento das funções institucionais da Autarquia, ou seja, apenas colocar em operação máquinas autorizadas a funcionar em ambiente corporativo;

b) Configurar os ambientes computacionais com os serviços, pacotes, componentes e protocolos mínimos para funcionamento e atendimento corporativo;

c) Prever plano de capacidade para toda instalação a fim de se evitar limitações de sistemas e erros por insuficiência de hardware;

d) Instalar o sistema operacional utilizando apenas manuais, mídias e arquivos autorizados/oficiais de fabricantes e fornecedores;

e) Instalar os sistemas a partir de dispositivos de armazenamento locais, desconectados da rede corporativa;

f) Aplicar todas as correções críticas e de segurança (*patches*, *fixes*, *service packs*) para tornar o sistema estável e seguro; e

g) Aplicar instalação personalizada a fim de se evitar a configuração de componentes cuja funcionalidade seja desconhecida.

6.3 **Desativação de Serviços não Necessários**

6.3.1 Deverão ser desativados os serviços (locais e de rede) que não forem necessários, a fim de se reduzir a exposição a vulnerabilidades.

6.3.2 Caso não seja possível desativar serviços individualmente, deverá ser utilizada solução para monitorar e bloquear portas ativas TCP/UDP fora do padrão de uso do FNDE, a fim de se impedir vulnerabilidades advindas de falhas em protocolos utilizados por estas portas.

NOTA1: Os serviços disponibilizados pelo ambiente computacional deverão ser distribuídos de forma a não se comprometer a disponibilidade, integridade e performance das soluções ofertadas corporativamente.

NOTA2: Um Plano de Riscos específico, contendo as etapas Identificação, Análise, Avaliação, Tratamento e Aceitação de riscos deverá ser apresentado pela área responsável pela inclusão de soluções/sistemas operacionais em ambiente computacional, a fim de se avaliar o impacto dessa inserção bem como medidas de segurança necessárias para contenção de riscos ao parque computacional do FNDE.

NOTA3: Devem ser documentadas todas as desativações de serviços e/ou a remoções de arquivos efetuadas e estas documentações deverão ser mantidas em local apropriado, seguro e de fácil recuperação.

NOTA4: Manter um repositório de todas as atualizações em rede corporativa a fim de se facilitar novas instalações de sistemas operacionais.

NOTA5: Inspecionar a configuração do sistema operacional, após instalação de uma correção, para se certificar que a correção não alterou eventuais modificações realizadas anteriormente (especialmente aquelas destinadas a desativar serviços).

7. CONTROLE DE SEGURANÇA NO CICLO DE VIDA DE SISTEMA OPERACIONAL

Durante todo o ciclo de vida de um sistema operacional, a área de tecnologia da informação do FNDE deverá observar e implementar os devidos controles de segurança, quer seja na fase de instalação, de desenvolvimento, de integração, de compra, de testes e de evolução de sistemas.

8. CONTROLES DE SEGURANÇA NA OPERACIONALIZAÇÃO DE SISTEMAS OPERACIONAIS

Controles de segurança deverão ser observados e implementados para se obter proteção adequada no parque tecnológico do FNDE. Observar, ainda, o pertinente e adequado gerenciamento dos seguintes itens:

a) Controles de acessos (Autenticação, Autorização e Auditoria);

b) Controles lógicos (Regras de Firewall, Atualizações do Sistema Operacional, Antivírus, entre outros);

c) Controles Físicos (acesso ao parque tecnológico, ambiente controlável para hardware [umidade, temperatura, estabilização de energia, entre outros]); e

d) Controle no acesso a dados Sigilosos.

9. DOCUMENTAÇÃO DA INSTALAÇÃO E CONFIGURAÇÃO DE SISTEMA OPERACIONAL

9.1 Toda documentação de instalação e configuração de sistemas operacionais deve:

a) Ser elaborada, mantida, atualizada e protegida contra acesso indevido;

b) Estar sempre disponível em caso de falha (acidental ou provocada) do sistema;

c) Conter informações suficientes para que, a partir delas, seja possível reconstruir a exata configuração que o sistema possuía antes da falha, sem que seja necessário recorrer a *backups;*

d) Ser consideradas informação sigilosa.

9.2 **Senhas de Administrador**

9.2.1 Definir a senha de administrador dos sistemas operacionais e de aplicações (*root* ou *Administrator*).

10. SEGURANÇA DAS APLICAÇÕES

10.1 Todas as aplicações deverão ter controles de segurança em seus processos, componentes, softwares, dados de configuração de usuário, dados de classificação e em todas as tecnologias envolvidas no ciclo de vida da aplicação.

10.2 Os mecanismos de segurança devem garantir autenticidade, disponibilidade, integridade e confidencialidade das aplicações.

10.3 A área responsável por gerenciar aplicações deverá produzir rotinas e procedimentos de proteção para o desenvolvimento seguro de soluções corporativas.

10.4 Auditorias regulares deverão ser realizadas com base nas rotinas e procedimentos de proteção definidos anteriormente.

10.5 **Aplicação Segura**

10.5.1 Deverão ser estabelecidos acordos de licenciamento, propriedade de códigos e direitos de propriedade intelectual necessário para o correto funcionamento das diversas soluções corporativas do FNDE.

10.5.2 Deverão ser definidos e documentados previamente todos os requisitos de segurança para a aplicação a ser adquirida pelo FNDE ou desenvolvida para a casa. Nenhuma aplicação poderá ser implementada em ambiente de operação sem o atendimento desses requisitos.

10.5.3 Todos os códigos-fontes escritos, em atendimento à demanda do FNDE, bem como todas as documentações que os acompanham deverão ser transferidos para a posse definitiva do órgão.

10.5.4 Aplicações desenvolvidas ou adquiridas deverão passar por testes de vulnerabilidade antes de sua entrega definitiva e colocação em operação. Documentação apropriada deverá ser apresentada provando a mitigação de todas as vulnerabilidades encontradas nestas aplicações.

NOTA: Para implementação de aplicações desenvolvidas interna, externamente ou adquiridas, estas devem ser homologadas e testadas quanto a sua estabilidade antes de serem disponibilizadas em ambiente de produção.

11. SEGURANÇA COMPLEMENTAR

Deve ser assegurada a proteção complementar das informações e recursos da Tecnologia da Informação contra códigos maliciosos, conforme disposto na norma NS 008/CGD/FNDE – Proteção contra códigos maliciosos.

12. PENALIDADES

Os servidores e colaboradores do FNDE estão sujeitos às regras da Política de Segurança da Informação e Comunicação e têm o dever de observar integralmente o disposto nesta norma. A inobservância dessas regras acarretará em penalidades cabíveis, previstas no âmbito penal, civil e administrativa, na forma da legislação vigente.

13. RESPONSABILIZAÇÃO

13.1 Não é dado ao servidor ou colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicação, devendo este seguir rigorosamente a proposta nesta norma de segurança. O desconhecimento desta norma por parte do usuário não o isenta das responsabilidades e penalidades previstas.

13.2 **Disposições Gerais**

13.3 Os casos omissos e não amparados pelas orientações emanadas por esta norma serão resolvidos pelo:

e) Comitê responsável pela Segurança da Informação e Comunicação, com apoio, se necessário, das áreas técnicas do FNDE; e

f) Presidente do FNDE, em decisão final, caso o Comitê responsável pela Segurança da Informação e Comunicação não tenha autonomia para tomar as providências cabíveis.

14. VIGÊNCIA E ATUALIZAÇÃO

14.1 **Este documento entra em vigor em 90 (noventa) dias a partir da data de sua publicação e pode ser atualizada ou cancelada pela ocorrência de alguma das seguintes situações:**

a) Alteração dos procedimentos vigentes ou adoção de novos que agreguem valor aos controles dessa norma; e

b) Acolhimento de sugestões dos usuários, visando ao seu aperfeiçoamento.

14.2 **A aprovação e divulgação da norma alterada seguirá o mesmo processo de elaboração.**

14.3 **Condições obrigatórias de atualização do documento**

a) Surgimento ou alteração de leis e/ou regulamentações vigentes;

b) Mudança estratégica da instituição que tenha impacto nesta Norma;

c) Mudança de tecnologia no FNDE que tenha impacto nesta Norma; ou

d) 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).

14.4 **Responsável pela atualização**

14.4.1 Conforme Mapa de Responsabilidades.