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, segunda-feira, 24 de setembro de 2018

SUMÁRIO

ATOS ADMINISTRATIVOS

PRESIDÊNCIA

PORTARIA Nº 564, DE 17 DE SETEMBRO DE 2018 2
ANEXO 3

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° 270/2018

PORTARIA Nº 564, DE 17 DE SETEMBRO 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 008/CGD/FNDE, que trata da Proteção Contra Códigos Maliciosos, conforme anexo I desta Portaria.

Art. 2º Aprovar a norma de Segurança da Informação e Comunicação NS 011/CGD/FNDE, que trata da Administração do Correio Eletrônico, conforme anexo II desta Portaria.

Art. 3º Aprovar a norma de Segurança da Informação e Comunicação NS 012/CGD/FNDE, que trata da Administração da Internet, conforme anexo III desta Portaria.

Art. 4º Aprovar a norma de Segurança da Informação e Comunicação NS 017/CGD/FNDE, que trata do Controle de Acesso ao Sistema Operacional, conforme anexo IV desta Portaria.

Art. 5º Aprovar a norma de Segurança da Informação e Comunicação NS 025/CGD/FNDE, que trata da Instalação e Configuração Segura de Dispositivo de Roteamento Computacional, conforme anexo V desta Portaria.

Art. 6º Aprovar a norma de Segurança da Informação e Comunicação NS 026/CGD/FNDE, que trata da Instalação e Configuração Segura de Dispositivo de Segurança da Informação do FNDE, conforme anexo VI desta Portaria.

Art. 7º Esta Portaria entra em vigor na data de sua publicação no Boletim de Pessoal e Serviço do FNDE.

SILVIO DE SOUSA PINHEIRO

ANEXO I

PROTEÇÃO CONTRA CÓDIGOS MALICIOSOS

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.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

1. **Objetivo** **3**
2. **Descrição e Escopo** **3**
3. **Público-Alvo** **3**
4. **Conceitos e Definições** **3**
5. **Princípios** **3**
6. **Administração da Solução Contra Códigos Maliciosos** **3**
7. **Instalação e Configuração da Solução Contra Códigos Maliciosos** **7**
8. **Uso e Manutenção da Solução Contra Códigos Maliciosos** **5**
9. **Controles Contra Códigos Móveis** **6**
10. **Penalidades** **9**
11. **Competências e Responsabilidades** **9**
12. **Vigência e Atualização** **9**

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-008-2002-SEXEC: Norma de Segurança sobre proteção contra software malicioso*, publicada em 10 de dezembro de 2002.

APROVAÇÃO

_____

SILVIO DE SOUSA PINHEIRO
Presidente do FNDE

1. OBJETIVO

Assegurar a proteção das informações e dos recursos de tecnologia da informação contra códigos maliciosos.

2. DESCRIÇÃO E ESCOPO

Estabelecer controles de detecção, prevenção e recuperação contra códigos maliciosos em recursos de tecnologia da informação e demais equipamentos do FNDE, com a utilização de um programa adequado de capacitação e conscientização, com o objetivo de reduzir a probabilidade da ocorrência de incidentes.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação, doravante chamados simplesmente de administradores, sendo ainda responsabilidade dos usuários a observância desta norma.

4. CONCEITOS E DEFINIÇÕES

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

5. PRINCÍPIOS

A presente 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 do FNDE.

6. ADMINISTRAÇÃO DA SOLUÇÃO CONTRA CÓDIGOS MALICIOSOS

6.1 Os recursos de Tecnologia da Informação do FNDE devem conter soluções de detecção e bloqueio de programas contra códigos maliciosos, tais como: *antispyware*, antivírus, filtros de análise de conteúdo de correio eletrônico e tráfego de *Internet* a fim de evitar as vulnerabilidades aos códigos maliciosos ou qualquer tentativa de acesso não autorizado.

6.2 As soluções de prevenção, detecção e bloqueio de programas contendo códigos maliciosos devem ser especificadas e homologadas, considerando-se as seguintes características:

a) Possuir console de administração centralizada;
b) Permitir atualização automática e programável;
c) Permitir bloqueio de alteração das configurações por meio de senha de administração;
d) Prover serviço de atualização por parte do fabricante;
e) Possuir mecanismo de varredura em tempo real;
f) Possuir mecanismo de controle estatístico e emissão de relatórios;
g) Possuir mecanismo de controle centralizado com emissão de alertas de problemas;
h) Possuir bloqueio de execução de aplicações não homologadas;
i) Possuir bloqueio de conteúdos web; e
j) Possuir *personal firewall.*

6.3 Deve ser realizada verificação periódica, junto ao fabricante, de todas as atualizações da solução de prevenção, detecção e bloqueio de programas maliciosos.

6.4 Todas as atualizações e correções de versão das soluções de prevenção, detecção e bloqueio de programas maliciosos devem ser homologadas antes de serem aplicadas no ambiente de produção.

6.5 Deve ser elaborada e mantida atualizada toda documentação com a descrição dos procedimentos de instalação e configuração das soluções de prevenção, detecção e bloqueio de programas contra códigos maliciosos.

6.5.1 A documentação deve ser armazenada em local seguro, com acesso controlado e restrito.

6.6 As análises regulares de softwares e dos dados dos sistemas que manipulam informações do FNDE devem ser realizadas pela área de Tecnologia da Informação.

6.7 Os arquivos em meio magnético devem passar por verificação de existência de programas maliciosos, antes do uso e leitura.

6.8 A Central de Atendimento ao Usuário (CAU) deve ser imediatamente informada sobre qualquer suspeita por infecção de programa malicioso em equipamentos do ambiente computacional do FNDE.

6.8.1 O (s) equipamento (s) suspeito (s) deve (m) ser desligado (s) imediatamente.

7. INSTALAÇÃO E CONFIGURAÇÃO DA SOLUÇÃO CONTRA CÓDIGOS MALICIOSOS

7.1 A instalação e a configuração da solução de prevenção, detecção e bloqueio de programas maliciosos devem ser autorizadas pela área de segurança pertinente.

7.2 A solução de prevenção, detecção e bloqueio de programas maliciosos deve ser configurada para execução periódica e tempestiva de varredura completa nos recursos de tecnologia da informação, com a finalidade de identificar potenciais programas contendo códigos maliciosos.

7.3 A solução de prevenção, detecção e bloqueio de programas maliciosos deve ser configurada para verificação das mensagens por correio eletrônico e arquivos anexos quanto à contaminação por códigos maliciosos.

8. USO E MANUTENÇÃO DA SOLUÇÃO CONTRA CÓDIGOS MALICIOSOS

8.1 Todos os softwares utilizados pela Autarquia devem estar devidamente licenciados, em atendimento aos direitos autorais, contratuais e legais vigentes.

8.2 É obrigatório o uso de software de prevenção, detecção e bloqueio de programas maliciosos nos recursos de tecnologia da informação disponibilizados aos usuários.

8.2.1 A solução de prevenção, detecção e bloqueio de programas maliciosos deve ser mantida sempre ativada e atualizada.

8.2.2 Deve ser configurado o envio de alertas aos administradores de recursos de tecnologia da informação, a fim de que eles sejam notificados, de forma automática, sobre os eventos que identificaram a existência de códigos maliciosos nos recursos de tecnologia da informação.

8.3 Os softwares que compõem a solução de prevenção, detecção e bloqueio de programas maliciosos devem estar configurados para operar de forma transparente para o usuário.

8.3.1 Esses softwares devem ser configurados de forma a impedir que o usuário consiga desabilitar ou interromper o seu correto funcionamento.

8.4 Quando da detecção de mensagens de correio eletrônico e de arquivos contaminados com códigos maliciosos, devem ser adotados, no mínimo, os seguintes procedimentos:

a) Colocar as mensagens de correio eletrônico e os arquivos suspeitos em uma área de acesso restrito (quarentena), por tempo determinado pelo administrador de rede para o tratamento adequado;
b) Enviar ao usuário uma notificação quando do recebimento de uma mensagem de correio eletrônico ou arquivo contaminado, informando o prazo da quarentena; e
c) O usuário deverá desligar imediatamente os recursos de tecnologia da informação suspeitos, a fim de evitar a propagação do código malicioso na rede corporativa do FNDE.

8.5 Devem ser previstos, em planos de contingência, procedimentos necessários para salvar e recuperar o software e informação infectados e danificados por programas maliciosos.

8.6 Será instaurado processo para apuração de responsabilidade contra o usuário que transmitir de forma dolosa, a partir da rede corporativa do FNDE, qualquer arquivo infectado para usuário externo ou interno.

8.6.1 A Área de Tecnologia da Informação deve apurar os fatos relativos à transmissão realizada, para subsidiar a decisão do Comitê responsável pela Segurança da Informação e Comunicação, que adotará as medidas legais cabíveis.

9. CONTROLES CONTRA CÓDIGOS MÓVEIS

9.1 Permitir a execução de programas Java e de *JavaScripts* utilizando complementos, como por exemplo o *NoScript* (disponível para alguns navegadores), conforme necessário e apenas em sites confiáveis;

9.2 Permitir que os componentes *ActiveX* sejam executados apenas quando vierem de sites conhecidos e confiáveis;

9.3 Usar de cautela ao permitir a instalação de componentes não assinados.

10. 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.

11. COMPETÊNCIAS E RESPONSABILIDADES

11.1 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.

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**

Conforme Mapa de Responsabilidades.

ANEXO II

ADMINISTRAÇÃO DO CORREIO ELETRÔNICO

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.

Lei 8.112, de 11 de dezembro de 1990 – dispõe sobre o regime jurídico dos servidores públicos Civil da União das Autarquias e das Fundações Públicas Federais.

Lei 9.296, de 24 de julho de 1996 – regulamenta o inciso XII, parte final do art. 5º da Constituição Federal.

Constituição Federal - 1988 - Art. 37 - dispõe que a administração pública direta e indireta de qualquer dos Poderes da União, dos Estados, do Distrito Federal e dos Municípios obedecerá aos princípios de legalidade, impessoalidade, moralidade, publicidade e eficiência.

Lei nº 7.716, de 5 de janeiro de 1989 - define os crimes resultantes de preconceito de raça e cor;

Lei nº 8.027, de 12 de abril de 1990 - dispõe sobre normas de conduta dos servidores públicos civis da União, das Autarquias e das Fundações Públicas, e dá outras providências;

Lei nº 8.069, de 13 de julho de 1990 - dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências;

Lei nº 8.159, de 8 de janeiro de 1991 - dispõe sobre a Política Nacional de Arquivos Públicos e Privados e dá outras providências;

Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil Brasileiro - Art. 186 - dispõe que "Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar danos a outrem, ainda que exclusivamente moral, comete ato ilícito";

Decreto Lei nº 2.848, de 07 dezembro de 1940 - Código Penal:

1. Arts. 153 e 154 - definem os crimes de divulgação de segredo e de violação do segredo profissional;

2. Arts. 312 ao 327 - definem os crimes praticados por funcionário público contra a Administração em Geral;

3. Arts. 297, 305 e 307 - define os crimes de falsificação de documento público, supressão de documento e falsa identidade.

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

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

Instrução Normativa nº 01 do DSIC/GSI/PR, de 13 de junho de 2008, disciplina a Gestão de Segurança da Informação e Comunicações na Administração Pública Federal, direta e indireta, e dá outras providências.

Norma técnica internacional, *Request for comments* - RFC, número 1912 (*DNS*), padroniza protocolo para Correio Eletrônico e assuntos afins;

05/CGD/FNDE Responsabilidade pelos ativos

20/CGD/FNDE Classificação da Informação

SP 800-177 - Trustworthy Email

SP 1800-6 - Domain Name System-Based Electronic Mail Security

SP 800-45 Version 2 - Guidelines on Electronic Mail Security

CAMPO DE APLICAÇÃO

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

SUMÁRIO

1. **Objetivo** **14**
2. **Descrição e Escopo** **12**
3. **Público-Alvo** **12**
4. **Conceitos e Definições** **12**
5. **Princípios** **12**
6. **Disposições Iniciais** **12**
7. **Direito de Acesso** **12**
8. **Dos Procedimentos para Criação de Contas** **13**
9. **Dos Limites de Cota, Destinatários e Mensagens das Caixas Postais** **14**
10. **Dos Administradores do Serviço de Correio Eletrônico** **15**
11. **Da Auditoria e do Monitoramento das Mensagens** **16**
12. **Medidas de Segurança** **16**
13. **Penalidades** **17**
14. **Competências e Responsabilidades** **17**
15. **Disposições Gerais** **17**
16. **Vigência e Atualização** **20**

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-011-2002-SEXEC: Norma de Segurança sobre o Correio Eletrônico do FNDE*, publicada em 14 de março de 2003.

APROVAÇÃO

SILVIO DE SOUSA PINHEIRO
Presidente do FNDE

1. OBJETIVO

Disciplinar e regulamentar a utilização do serviço de correio eletrônico corporativo no âmbito do FNDE.

2. DESCRIÇÃO E ESCOPO

Esta norma visa estabelecer critérios para envio e recebimento de mensagens eletrônicas, de forma a minimizar os riscos de segurança da informação nos ativos de rede internos e móveis.

3. PÚBLICO-ALVO

Esta norma destina-se apenas aos servidores e colaboradores que exercem função de administração dos recursos de correio eletrônico.

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, da legalidade, visando à proteção e à preservação das informações necessárias à execução das atividades da Autarquia.

6. DISPOSIÇÕES INICIAIS

6.1 O servidor de correio eletrônico corporativo é uma ferramenta para identificar o envio e recebimento de mensagens para apoio exclusivo às atividades desenvolvidas em âmbito institucional do FNDE.

6.2 Os clientes de correio eletrônico devem usar esquemas de autenticação, como nomes de usuário e senhas ou autenticação baseada em *PKI*, utilizando-se sempre uma conexão protegida com protocolo *TLS*.

7. DIREITO DE ACESSO

7.1 A área de tecnologia da informação deve realizar o monitoramento do correio eletrônico, sem violação de conteúdo, avaliando periodicamente a quantidade de mensagens e o volume das informações.

7.2 O serviço deve ser cancelado ou bloqueado quando for constatada de acordo com item 11 a utilização indevida.

7.3 Havendo necessidade de utilização de informação provenientes do e-mail privado do colaborador, para fins apuratórios, a disponibilização desses dados dependerá de autorização judicial, conforme previsão legal.

7.4 A administração do sistema de correio eletrônico é de responsabilidade da área de tecnologia da informação.

7.4.1 É terminantemente proibido, aos técnicos responsáveis pela administração do correio eletrônico, violar o conteúdo das mensagens de qualquer usuário, mesmo em serviços de manutenção e suporte.

7.5 As contas de correio eletrônico são de responsabilidade pessoal e intransferíveis, exceto em caso de contas corporativas, pela sua função colaborativa institucional. Sendo proibido o acesso ao conteúdo das mensagens transmitidas, salvo nas hipóteses previstas no item 11.

7.5.1 A identificação das contas de e-mail deve ser formada pela combinação do nome e sobrenome do usuário, exceto em caso de contas corporativas onde serão formadas pelos dados que identificam o setor demandante.

7.5.2 A criação de contas individuais deve preceder da assinatura, pelo usuário, do Termo de Ciência pertinente.

7.5.3 A criação de contas institucionais deverá ser solicitada formalmente pelos gestores à área de tecnologia da informação.

7.6 As informações de grupos, funções ou listas são acessadas apenas por usuários autorizados pelos administradores das contas criadas, chamados de moderadores, os quais também são responsáveis pela remoção dos usuários.

7.7 As mensagens do correio eletrônico são restritas aos seus remetentes e destinatários, sendo proibida a sua leitura por outros usuários, mesmo quando impressas ou disponibilizadas na tela.

8. DOS PROCEDIMENTOS PARA CRIAÇÃO DE CONTAS

8.1 O usuário possuirá um único e exclusivo endereço de correio eletrônico. Situações excepcionais serão tratadas pela área de tecnologia da informação.

8.2 Para criar uma nova conta, considerar o seguinte:

a) Cadastrar o nome completo do usuário para visualização na lista de endereços;

b) O endereço de correio eletrônico deve ser único e seguir sequencialmente os critérios de composição, de acordo com o nome do servidor e do colaborador. Deverá ser formado com o prenome seguido de um PONTO (.) e seguido do último sobrenome;

Exemplo de composição para um servidor ou colaborador de nome **José Carlos Beltrano**:

Nome e sobrenome: jose.beltrano@fnde.gov.br

8.3 A identificação do usuário e o endereço de correio eletrônico deverão possuir o mesmo nome antes do símbolo arroba (@).

8.4 No caso de ocorrência de um usuário homônimo previamente cadastrado na Autarquia, o endereço de correio eletrônico será definido pela área de tecnologia da informação.

NOTA - O usuário que solicitar a troca do endereçamento, devidamente motivada, deverá adotar os critérios descritos no item 8.2.

9. DOS LIMITES DE COTA, DESTINATÁRIOS E MENSAGENS DAS CAIXAS POSTAIS

9.1 Limite de Cota:

9.1.1 A cota das caixas postais mantidas no servidor de Correio Eletrônico do FNDE será definida de acordo com o cargo/função ocupado pelo servidor ou colaborador, conforme tabela abaixo:

CARGO/FUNÇÃO	COTA
Caixas Corporativas	2048 MB
Presidente, Diretores.	2048 MB
Coordenadores, Chefes e afins.	1024 MB
Usuários de TI	512 MB
Usuário Comum	300 MB
Estagiários	200 MB

9.1.2 Quando a caixa de correio alcançar 100% (cem por cento) do limite estabelecido pela cota da caixa postal, em um primeiro momento o correio deverá bloquear apenas o envio de novos e-mails. Caso nenhuma ação seja realizada, pelo usuário, para diminuir o tamanho da caixa postal, será bloqueado o envio e recebimento de novos e-mails.

9.1.3 Se houver necessidade de maior espaço para o armazenamento de mensagens de Correio Eletrônico, o aumento de cota deverá ser solicitado à área de tecnologia da informação, que analisará a viabilidade do ajuste, por meio de correio eletrônico ou documento oficial motivado, aprovado pela chefia imediata ou superior,

9.2 Limite de Destinatários:

9.2.1 Será permitido ao usuário o envio de mensagem para até 50 (cinquenta) destinatários internos ou externos;

9.3 Limite do Tamanho de Mensagens:

9.3.1 O tamanho máximo por mensagens de correio eletrônico permitido é de 25 MB para envio e recebimento

9.3.2 Recomenda-se compactar sempre os arquivos a serem anexados nas mensagens.

9.3.3 Quando o usuário necessitar enviar arquivos que excedam o tamanho permitido, deverá entrar em contato com a CAU - Central de Atendimento ao Usuário para obter informações sobre os procedimentos para realização do envio.

9.4 Será bloqueada automaticamente pelo sistema de correio eletrônico qualquer tentativa de envio ou recebimento de mensagem acima dos limites estabelecidos.

10. DOS ADMINISTRADORES DO SERVIÇO DE CORREIO ELETRÔNICO

10.1 É dever dos Administradores do Sistema:

a) Minimizar a interrupção das atividades do FNDE ocasionadas pelo uso indevido do serviço de Correio Eletrônico;

b) Cumprir as políticas e procedimentos relativos aos serviços de Correio Eletrônico e auxiliar na apuração formal do descumprimento de leis ou normas especificas, com auxílio de ferramentas quando demandados pela chefia;

c) Manter o sigilo profissional no trato de informações veiculadas por meio de mensageria eletrônica, observando, sempre, as normas de segurança da informação e comunicação do FNDE.

d) Observar as orientações técnicas para garantir a disponibilidade do serviço, monitorando, permanentemente, o desempenho e a integridade do sistema de Correio Eletrônico;

e) Informar à área de Tecnologia da Informação sobre eventuais descumprimentos desta norma;

f) Estabelecer e manter um processo sistemático para gravação e retenção de arquivos de *log* de mensagens de Correio Eletrônico por um prazo máximo de 06 (seis) meses e o conteúdo de caixas postais por um período de 45 (quarenta e cinco) dias, observando a NS020 – Classificação da Informação.

g) Proporcionar o redirecionamento de mensagens em caso de mudança de endereço eletrônico destinadas ao endereço anterior para o novo endereço, desde que pertencente ao FNDE, por um prazo máximo de 30 (trinta) dias;

h) Observar as orientações técnicas para garantir a recuperação de mensagens em caso de danos ao ambiente computacional, sempre que for necessário;

NOTA - Se houver indícios de que mensagens veiculadas pelo correio eletrônico possam ocasionar quebra de segurança ou violação de quaisquer vedações constante desta norma, a administração do Correio Eletrônico adotará, imediatamente, medidas para a sua apuração, utilizando-se, para tanto, dos meios e procedimentos legalmente previstos.

10.2 Gerenciamento corporativo.

10.2.1 Para garantir a segurança de um servidor de *e-mail* e a infraestrutura de rede de suporte, o FNDE deve implementar serviços de:

a) Configuração / Controle de Mudanças e Gerenciamento;

b) Avaliação e gerenciamento de riscos;

c) Configurações padronizadas;

d) Conscientização e treinamento em segurança;

e) Contingência, continuidade de operações e planejamento de recuperação de desastres;

f) Certificação e Credenciamento.

Obs.: A auditoria de acreditação para os recursos de tecnologia da informação poderá ser solicitada após a avaliação e aplicação de boas práticas técnicas.

11. DA AUDITORIA DAS MENSAGENS

O FNDE poderá auditar o conteúdo das caixas postais dos usuários do sistema de mensagens da Autarquia nas seguintes circunstâncias:

a) Em processo administrativo disciplinar ou sindicância;

b) Por determinação judicial competente, conforme previsão do subitem 7.4;

c) Por solicitação da Comissão de Ética do FNDE.

12. MEDIDAS DE SEGURANÇA

12.1 O acesso externo aos serviços de correio eletrônico deve ser provido pela área de Tecnologia da Informação mediante conexão segura, com autenticação forte do usuário e com recursos de criptografia.

12.2 **Segurança na Camada de Transporte (*TLS*)**

12.2.1 Utilizar o *TLS* para proteger a confidencialidade das mensagens de e-mail trocadas entre os servidores de e-mail.

12.2.2 Utilizar chaves públicas dos certificados digitais X.509 para autenticar a identidade (servidor, domínio ou organização) do proprietário do certificado.

12.3 **Extensões de Segurança do Sistema de Nomes de Domínio (*DNSSEC*)**

12.3.1 Utilizar a tecnologia DNSSEC para proteger a integridade dos dados do DNS, a qual utiliza assinaturas digitais nos dados do DNS para impedir que um invasor adultere ou falsifique as respostas do DNS.

12.4 **Solução de Prevenção, Detecção e Bloqueio de Programas Maliciosos**

12.4.1 A solução de prevenção, detecção e bloqueio de programas maliciosos deve enviar ao usuário uma notificação quando do recebimento de uma mensagem de correio eletrônico (08-CGD-FNDE – PROTEÇÃO DE CÓDIGOS MALICIOSOS) ou arquivo contaminado (casos específicos).

12.4.2 Deve ser executado, no mínimo, o seguinte procedimento quando da detecção de mensagens de correio eletrônico (08-CGD-FNDE – PROTEÇÃO DE CÓDIGOS MALICIOSOS) e arquivos contaminados com códigos maliciosos:

a) As mensagens de correio eletrônico (08-CGD-FNDE – PROTEÇÃO DE CÓDIGOS MALICIOSOS) e os arquivos suspeitos deverão permanecer em uma área de acesso restrito (quarentena), por tempo determinado pelo administrador de rede, para tratamento adequado.

13. **PENALIDADES**

13.1 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.

NOTAS:

- O Código Civil Brasileiro estabelece a incidência da Responsabilidade objetiva, ou seja, também são responsáveis pela reparação civil o empregador ou comitente, por seus empregados, serviçal e prepostos, no exercício do trabalho que lhes competir, ou em razão dele.
- A Súmula 341 do STF traz o entendimento de que "É presumida a culpa do patrão ou comitente pelo ato culposo do empregador ou preposto".

14. **COMPETÊNCIAS E RESPONSABILIDADES**

Não é dado ao servidor e nem ao 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.

15. **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 do órgão, 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 do órgão não tenha autonomia para tomar as providências cabíveis.

16. VIGÊNCIA E ATUALIZAÇÃO

16.1 **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.

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

16.3 **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).

16.4 **Responsável pela atualização**

Conforme Mapa de Responsabilidades.

ANEXO III

ADMINISTRAÇÃO DA INTERNET

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 Controle de Acesso Relativo à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 21/IN01/DSIC/GSIPR – Diretrizes para o Registro de Eventos, Coleta e Preservação de Evidências de Incidentes de Segurança em Redes.

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

Resolução nº 7, de 29 de julho de 2002 - Estabelece regras e diretrizes para os sítios na internet da Administração Pública Federal.

Lei nº 12.965, de 23 de abril de 2014 - Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

SP 800-92 Guide to Computer Security Log Management

SP 800-44 Version 2 Guidelines on Securing Public Web Servers

CAMPO DE APLICAÇÃO

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

SUMÁRIO

1. **Objetivo** 21
2. **Descrição e Escopo** 21
3. **Público-Alvo** 21
4. **Conceitos e Definições** 21
5. **Princípios** 21
6. **Administração de Contas** 21
7. **Rede Corporativa** 22
8. **Dos Requisitos para Adequação dos Ativos de Informação** 22
9. **Orientações de Segurança da Informação nos Ambientes Físico e Virtual** 23
10. **Destinação** 25
11. **Gestão de *Log* de Segurança** 26
12. **Gerenciamento de Segurança ao Manter um Servidor *Web* Seguro** 27
13. **Da Utilização** 27
14. **Direito de Acesso** 30
15. **Administração do Serviço de Internet** 30
16. **Sistemas Públicos** 30
17. **Das Recomendações** 29
18. **Disposições Finais** 29
19. **Penalidades** 30
20. **Competências e Responsabilidades** 30
21. **Disposições Gerais** 30
22. **Vigência e Atualização** 30

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-012-2002-SEXEC: Norma de Segurança sobre a utilização da Internet*, publicada em 14 de março de 2003.

APROVAÇÃO

SILVIO DE SOUSA PINHEIRO
Presidente do FNDE

1. OBJETIVO

Disciplinar as regras e condições de uso da Internet, por meio da infraestrutura computacional do FNDE.

2. DESCRIÇÃO E ESCOPO

Descrever as atividades para a administração da internet, de forma a minimizar os riscos de segurança da informação nos ativos de rede internos e móveis.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação, doravante chamados simplesmente de administradores, sendo ainda responsabilidade dos usuários a observância desta norma.

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. ADMINISTRAÇÃO DE CONTAS

6.1.1 A criação de contas de acesso à rede corporativa requer procedimentos prévios de credenciamento de qualquer usuário.

6.1.2 Somente usuários cadastrados poderão utilizar conta de acesso no perfil de administrador para executar tarefas específicas na administração.

6.1.3 Não usar senhas administrativas para atividades comuns e pertinentes a perfis sem privilégios administrativos.

6.1.4 A criação de contas de serviço deve estar atrelada à Política de Privilégio mínimo que possibilite executar esse serviço.

6.1.5 Estabelecer regras para credenciamento, bloqueio e exclusão de contas administrativas de acesso.

7. REDE CORPORATIVA

7.1.1 Conceder credenciais de acesso à rede corporativa de computadores após a data de admissão ou de entrada em exercício do usuário.

7.1.2 Registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido pela área de Tecnologia da Informação.

7.1.3 Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem na rede corporativa de computadores.

7.1.4 Manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

7.1.5 Gravar o acesso remoto à rede corporativa em *logs*, pelo período mínimo de 06 meses, para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada.

7.1.6 Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.

7.1.7 Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação.

7.1.8 Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia.

7.1.9 Registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas.

7.1.10 Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

8. DOS REQUISITOS PARA ADEQUAÇÃO DOS ATIVOS DE INFORMAÇÃO

8.1 O horário dos ativos de informação deve ser ajustado por meio de mecanismos de sincronização de tempo, de forma a garantir que as configurações de data, hora e fuso horário do relógio interno estejam sincronizados com a "Hora Legal Brasileira (HLB) – GMT3 - Brasília", de acordo com o serviço oferecido e assegurado pelo Observatório Nacional (ON).

8.1.1 Os ativos de informação devem ser configurados de forma a registrar todos os eventos relevantes de SIC, e os seguintes:

a) Autenticação, tanto os bem-sucedidos quanto os malsucedidos;

b) Acesso a recursos e dados privilegiados; e

c) Acesso e alteração nos registros de auditoria.

8.1.2 Os registros dos eventos previstos no item anterior devem incluir as seguintes informações:

a) Identificação inequívoca do usuário que acessou o recurso;

b) Natureza do evento, como por exemplo, sucesso ou falha de autenticação, tentativa de troca de senha, etc;

c) Data, hora e fuso horário, observando o previsto no item 9.1; e

d) Endereço IP (Internet Protocol), identificador do ativo de informação, coordenadas geográficas, se disponíveis, e outras informações que possam identificar a possível origem do evento.

8.1.3 Os ativos de informação que não permitirem os registros de eventos acima listados devem ser mapeados e documentados quanto ao tipo e formato de registros de auditoria que o sistema permita armazenar;

8.1.4 Deve haver o acompanhamento dos sistemas e redes de comunicação de dados, registrando-se os eventos de segurança elencados abaixo, sem prejuízo de outros considerados relevantes:

a) Utilização de usuários, perfis e grupos privilegiados;

b) Inicialização, suspensão e reinicialização de serviços;

c) Modificações de política de senhas, como por exemplo, tamanho, expiração, bloqueio automático após exceder determinado número de tentativas de autenticação, histórico, etc.

d) Acesso ou modificação de arquivos ou sistemas considerados críticos; e

e) Eventos obtidos de quaisquer mecanismos de segurança existentes.

8.1.5 Os servidores de hospedagem de página eletrônica, ou qualquer outro ativo de informação que permita hospedagem, devem ser configurados de maneira que armazene registros históricos de eventos (*Logs*) em formato que permita a completa identificação dos fluxos de dados.

8.1.6 Os registros devem ser armazenados pelo período mínimo de 06 (seis) meses, sem prejuízo de outros prazos previstos em normativos específicos.

8.1.7 Recomenda-se que os ativos de informação sejam configurados de forma a armazenar seus registros de auditoria não apenas local, mas também remotamente, por meio do uso de tecnologia recomendável.

9. ORIENTAÇÕES DE SEGURANÇA DA INFORMAÇÃO NOS AMBIENTES FÍSICO E VIRTUAL

9.1 Orientações Gerenciais

9.1.1 As informações e os recursos de TI para acesso à rede do FNDE devem ser disponibilizados, única e exclusivamente, àqueles que os utilizam para o exercício de suas funções;

9.1.2 FNDE deve implementar mecanismos de proteção que impeçam o acesso indevido aos ativos de informação e às áreas em que se encontram, como por exemplo, estações de trabalho com identificação de usuário e senha, os quais são pessoais e intransferíveis;

9.1.3 Os acessos aos dados e às informações devem ser registrados, de modo que as informações sobre acesso ou tentativas de acesso, frustradas ou não, estejam sempre disponíveis;

9.1.4 Toda informação deve ser protegida para que não haja alteração, acesso ou eliminação indevida;

9.1.5 Todos os dispositivos utilizados para a proteção, manutenção da integridade, disponibilidade e confidencialidade das informações devem ser considerados sigilosos, sendo, portanto, proibida a sua divulgação a pessoas não autorizadas ou a terceiros;

9.1.6 É de responsabilidade do FNDE promover a filtragem de acessos indevidos, provenientes de sua rede com destino à outra (s) rede (s) de outro (s) órgão (s), ou para a Internet. Esses acessos indevidos podem ser gerados por ataques direcionados, códigos maliciosos (*malware*) e ataques de negação de serviço (*DDoS*), dentre outros;

9.1.7 É obrigação dos servidores e colaboradores notificar imediatamente à administração da rede qualquer ponto de vulnerabilidade, irregularidade ou descumprimento dos requisitos de segurança estabelecidos pelo órgão.

9.2 Orientações Técnicas

a) No sítio do FNDE, todas as páginas que gerenciam dados sensíveis devem trafegar em páginas conhecidas como "conexão segura", ou seja, as que usam o protocolo *HTTPS – SSL* (*Secure Sockets Layer*);

b) Nunca permitir que a aplicação receba dados de usuários e senhas em texto claro. Utilize sempre o protocolo *SSL(acessar sites com segurança) e TLS(segurança de comunicação)*;

c) Não enviar a senha por e-mail nos casos em que o usuário execute a função "esqueci minha senha". Procurar usar mecanismos como o de pergunta secreta;

d) Não armazenar cookies com o login e a senha do usuário, mesmo que criptografados, na estação de trabalho;

e) Certificar-se de que a função de "*logout*" da aplicação realmente encerra completamente a sessão;

f) Conceder ao usuário de serviço de sua aplicação somente os acessos mínimos para o seu funcionamento. Nunca o definir como "root", "administrador" ou "sa";

g) Desenvolver permissões de acesso de acordo com cada funcionalidade da aplicação e não por menus;

h) Implementar mecanismos de validação da entrada de dados na aplicação impossibilitando a inserção de dados de um tamanho ou tipo (numérico, alfanumérico, data/hora, etc.) que contrarie a regra de negócio estabelecida no sistema;

i) Realizar o tratamento de erros impedindo a ocorrência de mensagens de erro com origem no sistema de banco de dados ou no *webserver*;

j) Estabelecer procedimentos, com periodicidade no mínimo anual, de teste de intrusão com foco na tentativa de exploração de vulnerabilidades em aplicações web;

k) Eliminar as vulnerabilidades reportadas com a maior brevidade possível;

l) Concentrar os servidores de banco de dados em uma rede segregada. Nunca os deixar expostos às conexões provenientes da internet;

m) Estabelecer e documentar as portas permitidas para a comunicação entre os dispositivos, tendo como objetivo aumentar o controle e tornar formal o tipo de comunicação que é permitida em cada ambiente computacional;

n) Evitar o uso de portas de comunicação reconhecidas como vulneráveis, tais como: *TELNET* e *FTP*;

o) Optar por soluções com criptografia como *SFTP* e *SSH*;

p) Proibir qualquer acesso originado da *Internet* que tenha como destino algum equipamento da rede interna;

q) Utilizar o mascaramento de *IP* (*Network Address Translation - NAT*) para todo o tráfego de saída para a Internet;

r) Utilizar, obrigatoriamente, a criptografia *SSL V3*, impedindo a conexão por meio do uso de versões antigas do *SSL*. Isso é aplicado por meio da alteração da configuração de seu *Webserver*;

s) Utilizar certificados digitais de autoridades certificadoras válidas;

t) Administrar dispositivos utilizando protocolos com criptografia forte como *SSH*;

u) Realizar a troca de arquivos entre dispositivos utilizando protocolos com criptografia forte como *SFTP*.

10. DESTINAÇÃO

A destinação da informação contida em sítios eletrônicos institucionais e repositórios internos deve observar o disposto nas legislações vigentes sobre o tema e, nos casos necessários, ser objeto de normatização complementar pelos órgãos e entidades da Administração Pública Federal, com o intuito de garantir a preservação de conteúdos relevantes para o exercício de suas competências e a preservação da memória institucional.

11. GESTÃO DE *LOG* DE SEGURANÇA

11.1 O FNDE estabelecerá políticas e procedimentos para o gerenciamento de *logs* para determinar e manter atividades de gerenciamento de registros bem-sucedidas.

11.2 O FNDE desenvolverá procedimentos para executar o gerenciamento de *log* como parte do processo de planejamento e definirá os requisitos e metas de registro.

11.3 O FNDE deverá criar e manter uma infraestrutura de gerenciamento de *logs* que atenda as seguintes características:

a) Manusear *logs* em *hardware*, *software*, redes e mídia capazes de gerar, transmitir, armazenar, analisar e descartar dados de *log*;

b) Executar funções que suportam a análise e segurança de dados de *log*;

c) Estabelecer política de gerenciamento de registros e identificação de encargos e responsabilidades;

d) Estabelecer gerenciamento de *log* que incluam servidores de log centralizados e armazenamento de dados de *log*; e

e) Considerar o volume de dados de *log* a serem processados, a largura de banda da rede, armazenamento de dados online e off-line, os requisitos de segurança para os dados e o tempo e os recursos necessários para o pessoal analisar os *logs*.

11.4 Os administradores de sistemas receberão apoio adequado por meio de:

a) Divulgação de informações;

b) Fornecimento de treinamento;

c) Designação de pontos de contato para responder os questionamentos, fornecer orientação técnica específica e disponibilizar ferramentas e documentação.

NOTA: Os administradores dos recursos de tecnologia da informação têm, ainda, as seguintes responsabilidades:

a) Acompanhar o *status* de registro de todas as fontes de *log*;

b) Rotacionar, monitorar e armazenar corretamente os arquivos de *logs*;

c) Alinhar a política de *logs* à política de segurança da informação do FNDE.

d) Manter relatórios contendo avaliação de quebra de segurança em tecnologia da informação.

11.5 Implementar mecanismos de geração de logs, sobretudo para as transações críticas;

11.6 Armazenar os logs em arquivos ou bancos de dados com acesso disponível somente às equipes de infraestrutura;

11.7 Configurar os dispositivos de rede para gerar logs de todos os eventos realizados com privilégios administrativos;

11.8 Configurar os dispositivos de rede para gerar logs de todos os eventos cuja tentativa de acesso resultar em falha;

11.9 Configurar os logs para manter os dados de data/hora do evento, identificação do usuário, tipo de evento, indicação de sucesso ou falha e a indicação do componente alterado ou que sofreu tentativa de alteração;

12. GERENCIAMENTO DE SEGURANÇA AO MANTER UM SERVIDOR *WEB* SEGURO

Os administradores deverão observar as práticas elencadas abaixo, para aumentar a segurança do servidor *Web* e da infraestrutura de rede de suporte:

a) Política de Segurança;

b) Configuração / controle e gestão da mudança;

c) Avaliação e gestão do risco;

d) Configurações de *software* padronizadas que satisfaçam a política de segurança da informação;

e) Conscientização e treinamento em segurança da informação; e

f) Planejamento de contingência, continuidade das operações e planejamento de recuperação de desastres.

13. DA UTILIZAÇÃO

Os serviços de *INTERNET* e *INTRANET*, no âmbito do FNDE, têm por finalidade permitir a pesquisa e a troca de informações necessárias ao desempenho das atividades inerentes à Autarquia:

a) A autorização de serviços da *INTERNET* e *INTRANET* dependem de prévia verificação das condições técnicas de atendimento, ou seja, segurança, infraestrutura de equipamentos, software e de comunicação instaladas na rede do FNDE.

b) O desenvolvimento e a inserção de páginas na *INTERNET* e *INTRANET* deverá ser feito mediante solicitação à área de Tecnologia da Informação.

c) A atualização e a qualidade das informações das páginas são de responsabilidade das respectivas Áreas que as produziram.

d) A critério da área de Tecnologia da Informação poderá ser restringido o acesso a determinadas seções ou páginas, mediante solicitação por escrito da área responsável.

14. DIREITO DE ACESSO

14.1 O acesso à *INTERNET* somente será feito por meio da infraestrutura de tecnologia da informação do FNDE.

Antes da habilitação do usuário para acesso à *Internet*, a área de tecnologia da informação deverá:

a) Providenciar o pacote inicial de privilégios de usuário conforme padrão do Gerenciador de Identidade Digital – GID; e

b) Observar as regras da política de *proxy* em vigor.

14.2 O serviço deve ser cancelado ou bloqueado no momento em que for constatada a utilização indevida.

É facultado o acesso ao Correio Eletrônico Pessoal, respeitadas as regulamentações específicas (11-CGD-FNDE – Adm. Correio Eletrônico) para esse fim.

15. ADMINISTRAÇÃO DO SERVIÇO DE INTERNET

15.1 A administração do serviço *Internet* é de responsabilidade da Área de Tecnologia da Informação.

15.1.1 A Área de Tecnologia da Informação realizará o monitoramento sistemático do uso da *Internet*, objetivando a avaliação contínua e o atendimento de demandas específicas.

15.1.1.1 A Área de Tecnologia da Informação deverá elaborar e disponibilizar para o Comitê responsável pela Segurança da Informação e Comunicação e Gestores do primeiro nível hierárquico do FNDE, relatórios periódicos sobre a utilização da *Internet*.

15.1.1.2 É terminantemente proibido aos técnicos responsáveis pela administração do serviço *Internet* divulgar as informações resultantes do monitoramento.

15.1.2 A Área de Informática deve realizar avaliação contínua para determinar quais arquivos não são passíveis de *download* (baixa).

15.1.3 Somente os técnicos da Central de Atendimento ao Usuário podem alterar a configuração padrão de segurança definida para o *browser*.

15.1.4 No uso da *internet* deve-se ter proteção dos dados pessoais.

16. SISTEMAS PÚBLICOS

16.1 Arquivos de programas, dados e outras informações expostas em sistemas públicos devem estar em conformidade com legislações vigentes.

16.1.1 A guarda, a disponibilização dos registros de conexão e de acesso a aplicações de *internet*, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

16.1.2 A exposição de dados, arquivos de programas e informações na *Internet* deve ser, formalmente, autorizado pelos Gestores da Informação à Área de Comunicação Social da Autarquia, de acordo com a classificação da informação.

16.1.3 Os sistemas de publicação eletrônica, especialmente aqueles que permitam retorno (*feedback*) e entrada direta de informações devem ser cuidadosamente controlados, de forma que:

a) A informação seja obtida em conformidade com a legislação relacionada à proteção de dados;
b) A entrada e o processamento de dados sejam feitos de forma completa e no devido tempo;
c) As informações sensíveis sejam protegidas durante o processo de coleta e quando armazenadas, e
d) A forma de acesso a sistemas que divulguem informações não permita o acesso casual às redes nas quais esses sistemas estejam conectados.

17. **DAS RECOMENDAÇÕES**

Quanto à elaboração das páginas:

a) Zelar pela correção gramatical e ortográfica;

b) Normas internas do FNDE (NI) e Manuais de Procedimentos (MP) - Serão divulgados via *INTRANET*, após assinatura. Para divulgação externa, somente com autorização expressa da área de Tecnologia da Informação.

c) Evitar informações que possam ser caracterizadas como autopromoção pessoal, devendo citar, preferencialmente, a unidade administrativa;

18. **DISPOSIÇÕES FINAIS**

18.1 A Área de Tecnologia da Informação deve promover a elaboração e difusão:

18.1.1 Da política de uso de *internet*, disciplinando o seguinte:

a) Condições de uso de correio eletrônico pessoal;

b) Condições de navegação, otimização, manutenção periódica e uso da ferramenta browser pelo usuário.

18.1.2 O recadastramento de usuários para utilização da Internet será realizado de acordo com o disposto nesta norma.

19. **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.

20. **COMPETÊNCIAS E RESPONSABILIDADES**

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

21. **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.

22. **VIGÊNCIA E ATUALIZAÇÃO**

22.1 **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.

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

22.3 **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).

22.5 **Responsável pela atualização**

22.5.1 Conforme Mapa de Responsabilidades.

ANEXO IV

CONTROLE DE ACESSO AO SISTEMA OPERACIONAL

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 o Uso de Dispositivos Móveis nos Aspectos relativos à Segurança da Informação e Comunicações nos órgãos e entidades da Administração Pública Federal.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

1. **Objetivo** **34**
2. **Descrição e Escopo** **34**
3. **Público-Alvo** **34**
4. **Conceitos e Definições** **34**
5. **Princípios** **34**
6. **Ambiente de Sistema Operacional Corporativo** **34**
7. **Administração e Controle de Acesso Lógico** **35**
8. **Instalação, Configuração e Manutenção** **35**
9. **Procedimentos Seguros de Entrada no Sistema (*log-on*)** **36**
10. **Identificação e Autenticação de Usuário** **37**
11. **Sistema de Gerenciamento de Senha** **38**
12. **Uso de Utilitários de Sistema** **39**
13. **Limitação de Horário de Conexão** **39**
14. **Penalidades** **40**
15. **Competências e Responsabilidades** **40**
16. **Disposições Gerais** **40**
17. **Vigência e Atualização** **40**

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-017-2002-SEXEC: Norma de Segurança sobre acesso aos sistemas operacionais*, publicada em 14 de março de 2003.

APROVAÇÃO

SILVIO DE SOUSA PINHEIRO
Presidente do FNDE

1. OBJETIVO

Disciplinar as condições de acesso aos sistemas operacionais do FNDE, visando contribuir para a garantia da integridade, disponibilidade, confidencialidade e autenticidade das informações da Autarquia.

2. DESCRIÇÃO E ESCOPO

Definir requisitos de segurança para instalação, configuração e administração dos sistemas operacionais em uso na rede corporativa.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação, doravante chamados simplesmente de administradores, sendo ainda responsabilidade dos usuários a observância desta norma.

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

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

6. AMBIENTE DE SISTEMA OPERACIONAL CORPORATIVO

6.1 Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.

6.2 Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos ativos de informação.

6.3 Ser homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia.

6.4 Registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas.

6.5 Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

7. ADMINISTRAÇÃO E CONTROLE DE ACESSO LÓGICO

A administração de sistemas operacionais e aplicações na rede corporativa são de responsabilidade da área de tecnologia da informação, que tem a competência para:

a) Conceder credenciais de acesso à rede corporativa de computadores após a data de admissão ou de entrada em exercício do usuário;

b) Excluir credenciais de acesso à rede corporativa de computadores quando da demissão ou exoneração do usuário;

c) Registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do servidor ou do colaborador por período mínimo de 06 (seis) meses;

d) Utilizar mecanismos automáticos para inibir que equipamentos externos não autorizados se conectem à rede do FNDE;

e) Gravar o acesso remoto à rede corporativa em *logs* para posterior auditoria, contendo informações específicas que facilitem o rastreamento da ação tomada;

f) Acompanhar a instalação, a configuração e a manutenção dos sistemas operacionais e das aplicações nos recursos de tecnologia da informação. Considerar sempre a segurança da informação nesses procedimentos;

g) Avaliar e autorizar os casos, nos quais haja necessidade de utilização de outro sistema operacional e sistemas distintos, após justificativa formal da área demandante;

h) Homologar a instalação das atualizações dos sistemas operacionais e das aplicações nos recursos de tecnologia da informação. Considerar sempre a segurança da informação nesses procedimentos;

i) Documentar todos os procedimentos de instalação e configuração dos sistemas operacionais e aplicações em uso, utilizando as orientações fornecidas pelos fabricantes dos sistemas operacionais e das aplicações. Observar melhores práticas de segurança da informação; e

j) Utilizar autenticação multifatores para o controle de acesso lógico a fim de aumentar a segurança alocada ao acesso aos ativos de informação.

8. INSTALAÇÃO, CONFIGURAÇÃO E MANUTENÇÃO

8.1 Os sistemas operacionais e aplicações utilizadas devem estar devidamente licenciados, respeitando a legislação sobre direitos autorais e os contratos dos fornecedores.

8.2 Devem ter desabilitados ou desinstalados os serviços e protocolos desnecessários para o funcionamento normal dos recursos de tecnologia da informação.

8.3 Todos os recursos de tecnologia da informação utilizados pelos usuários devem ser homologados para uso pela área de tecnologia da informação.

8.4 Os sistemas operacionais e aplicações utilizadas devem ser configurados para manterem a sincronização de data e hora de acordo com o servidor da rede corporativa responsável por este serviço e de acordo com a política de segurança da informação do FNDE.

8.4.1 Devem ser observadas, anualmente, as definições de horário de verão de forma a ajustar as configurações de data e hora dos recursos de tecnologia da informação.

8.5 Os pacotes de atualização, tais como "*service packs"* e "*hotfixes"*, disponibilizados pelos fabricantes dos sistemas operacionais e das aplicações, apenas devem ser instalados nos recursos de tecnologia da informação que operam em produção após previamente homologados em ambiente de teste. Todas as alterações, inclusões e exclusões que objetivem aplicação em ambiente de produção devem passar, primeiro, por ambiente de teste, onde serão examinadas a estabilidade e pertinência dessas ações.

8.5.1 Deverão ser utilizadas soluções automáticas que permitam verificações de atualizações aplicáveis aos sistemas operacionais e de aplicações.

8.5.2 As imagens de instalação dos sistemas operacionais dos recursos de tecnologia da informação devem ser atualizadas sempre que forem identificadas alterações de padronização ou em regras de segurança da informação.

8.5.3 Quando da atualização de sistemas operacionais, devem ser observadas a seguinte precaução:

a) antes de qualquer atualização na partição do sistema operacional dos servidores da rede corporativa, deverá ser feito cópia de segurança dessa partição;

8.6 As falhas de autenticação nos sistemas operacionais e aplicações devem ser registradas em sistemas de *logs* indicando o número de tentativas realizadas.

8.7 Os sistemas operacionais dos servidores da rede corporativa devem ser configurados para:

a) emitir um alerta, nos casos de ocorrência de corrompimento do sistema; e

b) não reiniciar automaticamente após ocorrência de corrompimento do sistema.

8.8 Devem ser documentadas as rotinas de recuperação das credenciais ou contas de acesso do sistema operacional e aplicações, em caso de perda desse sistema.

8.9 A recuperação de sistemas operacionais e aplicações, bem como a realização de cópias de segurança devem observar as orientações descritas na norma de cópias de segurança.

9. PROCEDIMENTOS SEGUROS DE ENTRADA NO SISTEMA (*LOG-ON*)

9.1 O processo de *log-on* nos computadores / servidores de rede e sistemas de informação deve ser configurado de forma a:

a) Mostrar aviso geral e legal, informando que o computador só deve ser acessado por pessoa autorizada;

b) Validar a informação do usuário apenas quando todos os dados de entrada estiverem completos;

c) Limitar em 3 (três) o número de tentativas de acesso sem sucesso, sendo este registrados em arquivo de *logs*;

d) Registrar as tentativas inválidas de acesso;

e) Implementar o espaço de tempo antes de permitir novas tentativas de acesso; e

f) Limitar o tempo máximo e mínimo para o procedimento de acesso. Se excedido, o sistema deve encerrar a conexão.

9.2 Os sistemas operacionais e aplicações disponibilizadas devem ser configurados de maneira que os usuários tenham permissão para alterar as suas próprias senhas de entrada no sistema (log-on), principalmente no primeiro acesso.

10. **IDENTIFICAÇÃO E AUTENTICAÇÃO DE USUÁRIO**

10.1 Os sistemas operacionais utilizados devem ser configurados para liberarem o acesso mediante a utilização de um mecanismo de autenticação de segurança, considerando a seguinte orientação:

a) Criar perfis de acesso nos sistemas operacionais e nas aplicações em uso conforme a política de segurança da informação;

b) A utilização da conta com perfil "*convidado"* no sistema operacional deve ser desabilitada; e

c) O *log-on* automático no sistema operacional deve ser desabilitado. Casos excepcionais deverão ser documentados e validados pela área de Tecnologia da Informação.

10.2 Disponibilizar ao usuário que não exerce funções de administração da rede corporativa somente uma única conta de acesso, pessoal e intransferível. A área de tecnologia da informação é responsável pela disponibilização do serviço.

10.2.1 Utilizar conta de acesso com perfil de administrador somente para usuários cadastrados e para execução de tarefas específicas que requeiram essa credencial para administração de ativos de informação. Não utilizar esta conta para serviços rotineiros os quais não demandem esta credencial.

10.2.2 Casos excepcionais deverão ser documentados e validados pela área de tecnologia da informação.

11. SISTEMA DE GERENCIAMENTO DE SENHA

11.1 Os computadores / servidores de rede e os sistemas de informação devem estar configurados de forma que não aceitem senhas óbvias. Observar a norma de segurança NS016 - Responsabilidades dos Usuários.

11.2 Os computadores / servidores de rede e equipamentos de conectividade devem ter as contas e senhas padrão dos fabricantes renomeadas e devidamente documentadas pela área de tecnologia da informação antes de sua utilização no ambiente de produção.

11.3 Os computadores / servidores de rede e equipamentos de conectividade devem ser configurados de forma a mascararem suas respectivas senhas.

11.4 Para fins de utilização dos dispositivos móveis no FNDE, os usuários são classificados em três grupos:

11.4.1 Agentes públicos com dispositivos móveis corporativos – servidores ou colaboradores do FNDE, que utilizam dispositivos móveis de computação de propriedade da Autarquia;

11.4.1.1 Os dispositivos móveis de computação fornecidos pelo FNDE devem ser cadastrados, garantindo sua identificação única, bem como a do usuário responsável pelo uso;

11.4.1.2 Os equipamentos devem ser utilizados única e exclusivamente por aqueles agentes que assumiram a responsabilidade pelo seu uso;

11.4.1.3 Os servidores e os colaboradores não devem instalar aplicativos ou recursos não disponibilizados pelo setor responsável sem permissão;

11.4.1.4 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;

11.4.1.5 É recomendada a adoção de mecanismos que garantam a proteção e sigilo dos dados armazenados nos dispositivos em casos de extravio;

11.4.1.6 Os servidores e os colaboradores devem ser orientados a respeito dos procedimentos de segurança acerca dos dispositivos que lhes forem disponibilizados, mediante a assinatura de Termo de Uso e Responsabilidade do FNDE, não sendo admitida a alegação de seu desconhecimento nos casos de uso indevido.

11.4.2 Agentes públicos com dispositivos móveis particulares – servidores e colaboradores do FNDE que utilizam dispositivos móveis de computação de sua propriedade. Os dispositivos particulares que se submetem aos padrões corporativos de software e controles de segurança, e que são incorporados à rede de dados do FNDE, são considerados como dispositivos corporativos.

11.4.2.1 O servidor e o colaborador proprietário de dispositivo móvel particular, deve solicitar autorização ao Gestor de Segurança da Informação e Comunicações ou Agente Responsável para tais atribuições, o acesso aos recursos corporativos;

11.4.2.2 Cabe ao FNDE definir as quais recursos ou dados corporativos o dispositivo móvel particular terá acesso;

11.4.2.3 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;

11.4.2.4 É recomendada a adoção de mecanismos que garantam a proteção e sigilo dos dados corporativos armazenados nos dispositivos móveis em casos de extravio; e

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

11.4.3 Usuários visitantes com dispositivos móveis – servidor de outro órgão, colaboradores ou não que utilizam dispositivos móveis de sua propriedade, ou do FNDE ou entidade a que pertencem, dentro dos ambientes físicos e virtuais do FNDE.

11.4.3.1 Devem ser estabelecidos procedimentos de controle e concessão de acesso a visitantes que durante a permanência em instalações do FNDE, necessitem conectar seus dispositivos móveis à rede da Autarquia;

11.4.3.2 A concessão de uso deve estar vinculada à conscientização do usuário sobre as normas internas de uso da rede, podendo o FNDE estabelecer critérios próprios.

12. **USO DE UTILITÁRIOS DE SISTEMA**

12.1 O acesso aos utilitários de sistema deve ser controlado e registrado.

12.2 O uso dos utilitários de sistema deve ser limitado a usuários autorizados e capacitados.

12.3 As mídias dos utilitários de sistema devem ser guardadas em local de acesso restrito e sob a responsabilidade da área de Tecnologia da Informação.

13. **LIMITAÇÃO DE HORÁRIO DE CONEXÃO**

Para os serviços e sistemas de informação considerados críticos deve haver mecanismos que limitem o horário e a origem da sua utilização.

14. 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 administrativo, na forma da legislação vigente.

15. COMPETÊNCIAS E RESPONSABILIDADES

Não é dado ao servidor e colaborador o direito de alegar 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 previstas.

16. DISPOSIÇÕES GERAIS

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

a) Comitê responsável pela Segurança da Informação e Comunicação da Autarquia, 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 da Autarquia 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.

ANEXO V

INSTALAÇÃO E CONFIGURAÇÃO SEGURA DE DISPOSITIVOS DE ROTEAMENTO COMPUTACIONAL

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 Controle de Acesso Relativos à Segurança da Informação e Comunicações, nos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

Norma Complementar nº 19/IN01/DSIC/GSIPR – Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes da Administração Pública Federal (APF), direta e indireta.

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

SP 800-147B - Diretrizes de proteção do *BIOS* para servidores.

SP 800-137 - Monitoramento Contínuo de Segurança da Informação (*ISCM*).

SP 800-123 - Guia para Segurança Geral do Servidor.

SP 800-92 - Guia para Gerenciamento de *Log* de Segurança do Computador.

SP 800-70 Rev. 4 - Programa Nacional de Lista de Verificação para Produtos de TI: Diretrizes para Usuários e Desenvolvedores de Lista de Verificação.

SP 800-54 - Segurança do protocolo *Border Gateway*.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

1. **Objetivo** **44**
2. **Descrição e Escopo** **44**
3. **Público-Alvo** **44**
4. **Conceitos e Definições** **44**
5. **Princípios** **44**
6. **Administração de Contas de Dispositivos Computacionais** **44**
7. **Rede Corporativa - Orientações** **45**
8. **Dispositivos de Roteamento Computacional** **45**
9. **Planejamento, Concepção e Manutenção de Solução de Roteamento** **45**
10. **Segurança para Solução de Roteamento** **46**
11. **Segurança do Protocolo *Border Gateway*** **46**
12. **As Diretrizes de Segurança do *BIOS* do Sistema** **47**
13. **Administração de *Switches* e Roteadores** **47**
14. **Penalidades** **50**
15. **Competências e Responsabilidades** **50**
16. **Disposições Gerais** **50**
17. **Vigência e Atualização** **50**

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

SILVIO DE SOUSA PINHEIRO
Presidente do FNDE

1. OBJETIVO

Estabelecer regras de configuração segura para instalação e administração de dispositivos de conexão de redes.

2. DESCRIÇÃO E ESCOPO

Estabelecer procedimentos a serem seguidos pelos administradores da rede para proteção dos recursos de tecnologia da informação e para instalação e gerenciamento dos roteadores e switches.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação, doravante chamados simplesmente de administradores, sendo ainda responsabilidade dos usuários a observância desta norma.

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 a proteção e a preservação das informações necessárias à execução das atividades do FNDE.

6. ADMINISTRAÇÃO DE CONTAS DE DISPOSITIVOS COMPUTACIONAIS

6.1 A criação de contas de acesso requer procedimentos prévios de credenciamento para qualquer usuário.

6.2 A utilização da conta de acesso no perfil de administrador será somente por usuários cadastrados para execução de tarefas específicas na administração. Não usar senhas administrativas para atividades comuns e pertinentes a perfis sem privilégios administrativos.

6.3 O usuário será responsabilizado pela quebra de segurança ocorrida com a utilização de sua respectiva conta de acesso, conforme as disposições contidas na Norma de Segurança nº 16 – Responsabilidades dos Usuários.

6.4 A criação de contas de serviço deve estar atrelada à política do mínimo privilégio que possibilite a execução do serviço.

6.5 Devem ser estabelecidas regras para credenciamento, bloqueio e exclusão de contas administrativas de acesso aos dispositivos.

7. REDE CORPORATIVA - ORIENTAÇÕES

7.1 Conceder credenciais de acesso à rede corporativa de computadores após a data de admissão ou de entrada em exercício do usuário.

7.2 Registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido pela área de Tecnologia da Informação.

7.3 Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem à rede corporativa de computadores da Autarquia.

7.4 Manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

7.5 Gravar o acesso remoto (três meses) à rede corporativa em *logs* para posterior auditoria, sem prejuízo de outros prazos previstos em normativos, contendo informações específicas que facilitem o rastreamento da ação tomada.

8. DISPOSITIVOS DE ROTEAMENTO COMPUTACIONAL

8.1 Conter ferramentas de proteção contra acesso não autorizado aos ativos de informação, que favoreça, preferencialmente, a administração de forma centralizada.

8.2 Respeitar o princípio do menor privilégio para configurar as credenciais ou contas de acesso dos usuários aos dispositivos.

8.3 Utilizar ativo de informação homologado nas aplicações de controle de acesso, de tratamento das informações sigilosas e de criptografia.

8.4 Registrar eventos relevantes, previamente definidos, para a segurança e rastreamento de acesso às informações sigilosas.

8.5 Criar mecanismos para garantir a exatidão dos registros de auditoria nos ativos de informação.

9. PLANEJAMENTO, CONCEPÇÃO E MANUTENÇÃO DE SOLUÇÃO DE ROTEAMENTO

9.1 As demandas de planejamento, concepção e manutenção de sistemas estruturantes deverão seguir processo formal de Gestão de Riscos de Segurança da Informação e Comunicação.

9.2 As demandas de planejamento que resultem em sistemas estruturantes deverão seguir as diretrizes para a gestão de continuidade de negócios, nos aspectos relacionados à Segurança da Informação e Comunicações.

9.3 Os sistemas estruturantes deverão atender aos padrões de interoperabilidade estabelecidos pela e-PING/SLTI/MP, caso tenha pertinência.

10. **SEGURANÇA PARA SOLUÇÃO DE ROTEAMENTO**

Para garantir a segurança de um servidor e a infraestrutura de rede de suporte, as seguintes práticas devem ser implementadas:

a) Configurar / controlar alterações e gerenciar mudanças;

b) Avaliar e gerir riscos;

c) Planejar contingências, continuidade de operações e recuperação de desastres;

d) Certificar e acreditar (acreditação).

Obs.: Através da gestão de riscos será avaliado os controles que serão implementados no servidor para se conseguir a certificação.

11. **SEGURANÇA DO PROTOCOLO *BORDER GATEWAY***

Melhorar a segurança dos roteadores de acordo com as listas abaixo:

a) Estabelecer e usar listas de controle de acesso;

b) Usar autenticação de *peer BGP* para impedir atividades maliciosas *IPSEC* (segurança) ou *BGP MD5* (criptografia);

c) Usar limites de prefixo para evitar o preenchimento de tabelas do roteador:

- Os roteadores devem ser configurados para desabilitar ou encerrar uma sessão de emparelhamento do *BGP*;
- Emitir mensagens de aviso para os administradores quando um vizinho enviar um número pré-definido de prefixos.

d) Permitir que apenas *peers* se conectem à porta 179;

e) Configurar o BGP para permitir o anúncio apenas de *detblocks* designados;

f) Sempre que possível, os roteadores devem filtrar ingresso em *peers*;

g) Não permitir prefixos específicos em excesso;

h) Desativar o *failover* externo rápido para evitar grandes mudanças de rota devido a falhas transitórias de *peers* para enviar *keepalive*;

12. AS DIRETRIZES DE SEGURANÇA DO *BIOS* DO SISTEMA

12.1 Realizar atualização de *BIOS* localmente e em um ambiente seguro.

12.2 Verificar assinatura da aplicação antes de realizar a atualização.

12.3 Proteger a integridade de firmware para impedir a modificação não intencional ou maliciosa do *BIOS* fora do processo de atualização normal do *BIOS*.

12.4 Habilitar recursos de segurança para garantir que não haja mecanismos que permitam que o processador principal ou qualquer outro componente do sistema ignore as proteções do *BIOS*.

13. ADMINISTRAÇÃO DE *SWITCHES* E ROTEADORES

13.1 Os *switches* e roteadores devem ter as senhas padrões dos fabricantes substituídas antes de serem instalados na rede corporativa.

13.2 Os *switches* e roteadores devem ser configurados para solicitar usuário e senha de autenticação do domínio para realização das atividades de administração.

NOTA: Os roteadores de borda, quando possível, devem aplicar autenticação local para acesso administrativo aos equipamentos.

13.3 Os *switches* e roteadores devem estar configurados de maneira que os administradores de rede autorizados, ao se autenticarem, possuam uma credencial ou conta de acesso associada e centralizada.

13.4 Um Plano de Continuidade de Negócios deve ser elaborado e mantido em casos de perda das senhas de acesso administrativo dos *switches* e roteadores.

13.5 Os *switches* e roteadores devem ser instalados em locais apropriados, tais como *racks*, e seu acesso físico e lógico restrito aos administradores de rede, conforme orientações da norma 24-CGD-FNDE - Segurança para Equipe Técnica de TI do FNDE.

13.6 Devem ser realizadas verificações periódicas junto aos fabricantes dos *switches* e roteadores sobre a disponibilidade de atualizações e *patches* dos respectivos sistemas operacionais e aplicações para que os recursos de tecnologia da informação estejam atualizados.

13.7 Os pacotes de instalações, de atualizações e *patches* para os *switches* e roteadores devem ser homologados antes de serem aplicadas no ambiente de produção.

13.8 Devem ser implementados mecanismos de tolerância à falha para os *switches* e roteadores, considerados fundamentais para o funcionamento da rede corporativa.

13.9 Os serviços e portas não utilizados nos *switches* e roteadores devem ser desativados ou desinstalados.

13.10 As configurações abaixo devem ser seguidas para manter a segurança satisfatória nos *switches* e roteadores:

a) Número máximo de 05 (cinco) tentativas com falhas no processo de identificação e autenticação (*log-on*);

b) Período de inatividade de 10 (dez) minutos para *switches* e 5 (cinco) minutos para roteadores (*timeout*);

c) Alterar, sempre que possível, as portas padrões dos serviços *HTTP*, *TELNET* e *SSH*;

d) Utilizar a versão 3.x ou a mais recente do protocolo *SNMP* e solicitar a autenticação do usuário, quando possível;

e) Quando não houver um *SNMP* versão 3 ou superior implementada, o acesso de escrita (*write*) ao agente *SNMP* deve ser removido;

f) O agente *SNMP* deve ser configurado para enviar *traps* somente para equipamentos de gerenciamento autorizados;

g) Quando o *switch* e/ou roteador suportar o protocolo *SSH*, o serviço *TELNET* deve ser desabilitado;

h) O gerenciamento dos *switches* e roteadores deve ser feito por meio de *VLANs* dedicadas e diferentes das demais *VLANs* utilizadas;

i) A sincronização de data e hora dos equipamentos deve estar alinhada com o servidor da rede corporativa responsável por este serviço;

j) Recursos de detecção de erros (*RMON*) devem ser habilitados, quando possível;

k) Deve haver uma segregação de *VLAN*s para o tráfego de rede, considerando as diferenças relativas a serviços, produtos e criticidade ofertados pela rede corporativa;

l) O mecanismo de autenticação que utilize uma função de *hash* irreversível deve ser configurado nos protocolos de gerenciamento, quando possível;

m) Quando possível, a autenticação 802.1x deve ser habilitada para interfaces nas quais se conectam dispositivos que a suportem, exceto para portas que se conectam aos servidores da rede corporativa;

n) Nas interfaces do *switch* conectadas às estações de trabalho deve ser bloqueado todo o tráfego de *Spanning Tree Protocol* (*STP*);

13.11 Deve ser criada *ACL's* (*Access Control List* – Lista de Controle de Acesso) para proteção da rede corporativa, bloqueando, no mínimo:

a) ICMP desnecessários;

b) Mapeamento de rede;

c) Ataques do tipo *Land*, *Smurf*, *Syn-Flood*;

d) Entradas de IP indevidos;

e) Ações de negação de serviços (*DDOS*);

f) Mecanismos *anti-spoofing*;

g) Encaminhamento de pacotes de *Broadcast*;

h) Respostas a pacotes *Address Mark Request*;

i) ICMP *Redirect* e ICMP *Unreachable*;

j) *Proxy* ARP; e

k) IP *Source Routing*.

13.12 Devem ser implementados processos periódicos de cópias de segurança das configurações e sistemas operacionais dos *switches* e roteadores, para dispositivos protegidos contra acessos não autorizados.

13.13 Devem ser realizadas cópias de segurança dos sistemas operacionais e das configurações lógicas dos *switches* e roteadores antes de manutenção ou atualização.

13.14 As restaurações de uma cópia de segurança das configurações lógicas e dos sistemas operacionais dos *switches* e roteadores condicionam-se à ocorrência de anormalidades no funcionamento ou grave quebra de segurança.

13.15 O acesso remoto aos *switches* e roteadores deve ser realizado por canais e meios seguros, conforme descrito na norma 17-CGD-FNDE - Controle de acesso ao sistema operacional.

13.16 Deve ser mantido um monitoramento diário dos *switches* e roteadores, verificando-se seu funcionamento e desempenho.

13.17 Devem ser implementados mecanismos que permitam a emissão de alertas, quando ocorrerem problemas no funcionamento, desempenho e segurança dos *switches* e roteadores.

13.18 Os *switches* e roteadores devem ter seus registros de auditoria (*logs*) habilitados de maneira a verificar, no mínimo:

a) Desempenho do equipamento;

b) Tráfego de rede em cada interface;

c) Falhas no processo de identificação e autenticação (*log-on*), indicando o número de tentativas de acesso, endereço de origem, identificação do usuário, data e hora de acesso e serviço solicitado; e

d) Alteração nas contas e senhas de acesso.

13.19 Os registros de auditoria dos *switches* e roteadores devem ser redirecionados para um servidor / aplicação de registro centralizado e seguro, possibilitando o armazenamento e a rastreabilidade para verificação periódica.

13.20 Deve ser implementado um período de retenção mínimo de *logs*, com previsão de capacidade para atender necessidades de segurança, auditoria e rastreabilidade de dados.

14. PENALIDADES

14.1 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 administrativo, na forma da legislação vigente.

15. COMPETÊNCIAS E RESPONSABILIDADES

Com base no disposto no art. 3º do Decreto-Lei nº 4.657, de 4 de setembro de 1942, não é dado ao servidor e colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicações, devendo seguir rigorosamente o proposto nas normas de segurança. O desconhecimento dessa norma por parte do usuário não o isente das responsabilidades e penalidades previstas.

16. DISPOSIÇÕES GERAIS

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

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

b) Presidente do FNDE, em decisão final, casa o Comitê responsável pela Segurança da Informação e Comunicação da Autarquia 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.

ANEXO VI

INSTALAÇÃO E CONFIGURAÇÃO SEGURA DE DISPOSITIVOS DE SEGURANÇA DA INFORMAÇÃO 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.

Norma Complementar nº 19/IN01/DSIC/GSIPR – Estabelece Padrões Mínimos de Segurança da Informação e Comunicações para os Sistemas Estruturantes.

Norma Complementar nº 20/IN01/DSIC/GSIPR – Estabelece as Diretrizes de Segurança da Informação e Comunicações para Instituição do Processo de Tratamento da Informação.

CSIRT-Handbook - Computer Security Incident Response Teams (CSIRTs)

SP 800-147 - BIOS Protection Guidelines

SP 800-92 - Guide to Computer Security Log Management

SP 800-70 Rev. 4 - National Checklist Program for IT Products: Guidelines for Checklist Users and Developers

SP 800-41 Rev. 1 - Guidelines on Firewalls and Firewall Policy

CAMPO DE APLICAÇÃO

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

SUMÁRIO

1. Objetivo 54
2. Descrição e Escopo 54
3. Público-Alvo 54
4. Conceitos e Definições 54
5. Princípios 54
8. As Diretrizes de Segurança do *BIOS* do Sistema 55
9. Listas de Verificação - Checklists de Segurança 55
10. Administração de Firewalls 55
11. Instalação e Configuração 57
12. Operação 58
13. Manutenção 59
14. Documentação 59
15. Penalidades 59
16. Competências e Responsabilidades 60
17. Disposições Gerais 60
18. Vigência e Atualização 60

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

SILVIO DE SOUSA PINHEIRO
Presidente do FNDE

1. OBJETIVO

Definir as regras de instalação, configuração e administração segura dos dispositivos de segurança, chamados firewalls.

2. DESCRIÇÃO E ESCOPO

Estabelecer procedimentos a serem seguidos na instalação, configuração e administração segura dos dispositivos de segurança chamados firewalls.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação, doravante chamados simplesmente de administradores, sendo ainda responsabilidade dos usuários a observância desta norma.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações constam 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 do FNDE.

6. ADMINISTRAÇÃO DE CONTAS DE DISPOSITIVOS DE SEGURANÇA DA INFORMAÇÃO

6.1 A criação de contas de acesso requer procedimentos prévios de credenciamento de qualquer usuário.

6.2 Somente usuários cadastrados poderão utilizar conta de acesso no perfil de administrador para executar tarefas específicas na administração. Não usar senhas administrativas para atividades comuns e pertinentes a perfis sem privilégios administrativos.

6.3 A criação de contas de serviço deve estar atrelada à Política de Privilégio mínimo que possibilite executar esse serviço.

6.4 Estabelecer regras para credenciamento, bloqueio e exclusão de contas de acesso dos usuários, bem como para o ambiente de desenvolvimento.

7. REDE CORPORATIVA – ORIENTAÇÕES

7.1 Conceder credenciais de acesso à rede corporativa de computadores após a data de admissão ou de entrada em exercício do usuário.

7.2 Registrar os acessos à rede corporativa de computadores de forma a permitir a rastreabilidade e a identificação do usuário por período mínimo a ser definido pela Tecnologia da Informação.

7.3 Utilizar mecanismos automáticos para inibir que equipamentos externos se conectem à rede corporativa de computadores.

7.4 Manter, na rede corporativa, mecanismos que permitam identificar e rastrear os endereços de origem e destino, bem como os serviços utilizados.

7.5 Gravar o acesso remoto à rede corporativa em *logs*, por no mínimo 06 (seis) meses, para posterior auditoria, sem prejuízo de outros prazos previstos em normativos, contendo informações específicas que facilitem o rastreamento da ação tomada.

8. AS DIRETRIZES DE SEGURANÇA DO *BIOS* DO SISTEMA

8.1 Realizar atualização de *BIOS* local e dentro de um ambiente seguro.

8.2 Verificar assinatura da aplicação antes de realizar a atualização.

8.3 Proteger a integridade de firmware, para impedir a modificação não intencional ou maliciosa do *BIOS* fora do processo de atualização normal do *BIOS*.

8.4 Habilitar recursos de segurança para garantir que não haja mecanismos que permitam que o processador principal ou qualquer outro componente do sistema ignore as proteções do *BIOS*.

9. LISTAS DE VERIFICAÇÃO - CHECKLISTS DE SEGURANÇA

9.1 O FNDE deve aplicar listas de verificação a sistemas operacionais e aplicativos para reduzir o número de vulnerabilidades.

9.2 Utilizar listas de verificação que enfatizam a estabilização dos sistemas contra falhas de software (aplicando patches e eliminando funcionalidades desnecessárias) configurando sistemas com segurança que reduzirá o número de maneiras de atacar os sistemas.

9.3 A lista de verificação para o uso de configuração de segurança poderá ser encontrada no site *https://lists.nist.gov*

10. ADMINISTRAÇÃO DE FIREWALLS

10.1 São competências da área de Tecnologia da Informação:

a. Definir a política de operação do *firewall*, com apoio do Gestor de Segurança da Informação e Comunicação, quando pertinente; e

b. Implementar regras de filtragem do *firewall*.

10.2 Procedimentos de resposta às quebras de segurança detectadas pelo *firewall* devem ser implementados.

10.3 Qualquer alteração nas configurações do *firewall* deve ser registrada na documentação técnica desse dispositivo.

10.4 Análises de riscos devem ser realizadas periodicamente para identificar vulnerabilidades relacionadas ao sistema operacional que hospeda o *firewall* e o *software* do *firewall*.

10.5 Boletins de segurança com vulnerabilidades divulgadas pelos fabricantes devem ser consultados regularmente.

10.6 A versão do sistema operacional e softwares utilizados no *firewall* devem ser as mais atualizadas possível, considerando-se versões já estabilizadas e seguras pelo fornecedor.

10.7 Auditorias periódicas devem ser realizadas para verificar a aderência e a efetividade das regras de segurança implementadas no *firewall* com base na Política de Segurança da informação e Comunicações e normas correlatas.

10.8 Realizar checagens periódicas para análise dos registros de auditoria (*logs*) gerados pelo *firewall* quanto a irregularidades de segurança.

10.9 A política de licenciamento comercial de software de *firewall* deve ser monitorada e atendida.

10.10 Utilizar ferramentas que permitam o reconhecimento *on-line* de entradas de arquivos suspeitos e que auxiliem na análise de dados. Observando, ainda:

a) Questões de redundância na construção da rede local;

b) Componentes críticos como:

i. Arquivos de *"shadow copy";*

ii. Discos de *"shadow copy";*

iii. Estações de trabalho não monitoradas;

iv. Peças de reposição para os recursos de tecnologia da informação;

c) Interrupção no fornecimento de energia elétrica.

10.11 Realizar cópia de segurança e armazená-la em local distante das instalações do órgão, com o intuito de evitar perda de dados e de informações corporativas;

a) Cópias de segurança devem ser criptografadas.

10.12 Considerar o uso de sistemas de criptografia, como *Kerberos* ou algo baseado nesse sistema (como *AFS - Andrew File System*) na rede local ou, pelo menos, encriptação de dados sensíveis.

11. INSTALAÇÃO E CONFIGURAÇÃO

11.1 O *firewall* deve ser instalado em um hardware dedicado e adequadamente dimensionado para suportar a demanda de trabalho do FNDE.

11.2 A quantidade de aplicações executadas deve ser limitada para que o *firewall* realize apenas tarefas pertinentes à sua função. Todos os serviços ou softwares desnecessários devem ser desabilitados ou desinstalados.

11.3 O software de *firewall* utilizado na rede corporativa deve ser previamente homologado e aprovado pela área de Tecnologia da Informação.

11.4 O *firewall* deve estar instalado em local protegido por mecanismos de controle do acesso físico.

11.5 A configuração de endereçamento *IP* do *firewall* deve seguir o plano de endereçamento *IP* definido e recomendado pela área de Tecnologia da Informação.

11.6 As contas de acesso de administração, de gerenciamento e de manutenção do *firewall* devem ter as respectivas senhas padrão alteradas.

11.7 A senha com o privilégio de manutenção e de restauração do *firewall* deve permanecer em local seguro, em envelope lacrado e sob a guarda da área de Tecnologia da Informação.

11.8 A formação da senha das contas de acesso de administração, de gerenciamento e de manutenção do *firewall* deve estar em conformidade com as regras definidas pela área de Tecnologia da Informação e de acordo com a Política de Segurança da Informação do FNDE.

11.9 O acesso para administração, gerenciamento e manutenção do *firewall* deve ser restrito aos administradores de rede autorizados.

11.10 As regras configuradas no *firewall* devem seguir as orientações de cada fornecedor e estar de acordo com a Política de Segurança da informação e Comunicações existente.

11.11 Novas regras só poderão ser aplicadas no *firewall* após análise de segurança e aprovação da área de Tecnologia da Informação.

11.12 Regras desnecessárias ou redundantes devem ser eliminadas para assegurar que o *firewall* seja configurado apenas para as necessidades específicas.

11.13 Cópias de segurança das configurações e regras do software de *firewall* devem ser realizadas antes da aplicação de atualizações ou correções.

a) As atualizações devem ser instaladas tão logo sejam homologadas e aprovadas pela área de Tecnologia da Informação.

b) Os arquivos de atualização do software de *firewall* devem ser obtidos diretamente do fornecedor.

11.14 O tráfego de rede que não atenda às finalidades do FNDE deve ser bloqueado por uma política de negação no *firewall*. Se uma área necessitar de acessos diferenciados, deve solicitar e justificar formalmente à área de Tecnologia da Informação.

a) A área de Tecnologia da Informação deve analisar as solicitações e avaliar os possíveis riscos que os acessos diferenciados possam causar à segurança das informações na rede corporativa. De acordo com esta avaliação, o pedido poderá ser justificadamente negado. Neste caso, a área solicitante deverá ser informada a respeito.

11.15 Planos de recuperação da solução de *firewall* devem ser elaborados para a garantia da continuidade operacional.

11.16 O servidor *Web* deve ser colocado dentro de uma *DMZ* (zona desmilitarizada) protegida por *firewalls*;

11.17 Os dispositivos de *firewalls* devem ser configurados afim de garantir a autenticidade e integridade das informações;

11.18 Controles adicionais baseados em criptografia em criptografia (como *Tripwire* ou *MD5*) devem ser inseridos nos *firewalls*.

12. **OPERAÇÃO**

12.1 O dispositivo de *firewall* deverá permanecer ligado e ativo 24 horas por dia, 7 dias por semana.

12.2 O gerenciamento remoto do *firewall* deve ser permitido somente por canais seguros e para os administradores de recursos de tecnologia da informação responsáveis por este dispositivo.

a) Todo acesso interno ou remoto entre os administradores de recursos de tecnologia da informação e o *firewall* devem ser protegidos por criptografia e registros desses acessos devem ser mantidos para posteriores auditorias de *logs*.

12.3 A rede interna deve ser segmentada de acordo com as melhores práticas de segurança da informação. Observando, pelo menos, o seguinte:

a) Utilizar pelo menos dois segmentos;

b) Utilizar um segmento de produção, onde todas as atividades corporativas são executadas;

c) Utilizar um segmento para a realização de testes, validação de soluções, aplicação de softwares e *patches* de segurança, cuja finalidade é verificar a pertinência, a viabilidade e estabilidade das soluções de segurança apresentadas. Evitar aplicar em produção, ativos não homologados em ambiente de testes.

12.4 Os segmentos devem ser separados por meio de dispositivos de segurança, a exemplo de *firewalls*. A comunicação entre ambientes deve ser restrita ao necessário e o monitoramento constante deve ser aplicado ao caso.

13. **MANUTENÇÃO**

13.1 Áreas pertinentes devem ser acionadas para avaliação do motivo da mudança da documentação e da aprovação das alterações necessárias em ambiente de produção, além da definição de procedimentos de recuperação em caso de falhas.

13.2 A manutenção do *firewall* deve ser realizada somente pelos administradores de rede autorizados.

13.3 A manutenção preventiva deve ser realizada periodicamente, de acordo com o tipo, porte e recomendação do fornecedor, devendo ser realizada fora do horário normal de expediente e previamente comunicada às áreas envolvidas.

13.4 É recomendável que contratos de manutenção e suporte sejam firmados para a garantia da funcionalidade operacional do *firewall*.

14. **DOCUMENTAÇÃO**

14.1 Os manuais de instalação e configuração do *firewall* devem ser mantidos atualizados e armazenados em local restrito aos administradores de rede.

14.2 A documentação das identificações das conexões lógicas e físicas deve estar sempre atualizada e de acordo com a última alteração de sua configuração.

14.3 Um Plano de Continuidade de Negócios deverá ser elaborado e mantido em caso de perda das senhas de acesso administrativo.

14.4 A documentação técnica do *firewall* deve ser elaborada para contemplar a instalação, a configuração, as regras e os procedimentos de restauração.

15. **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.

16. COMPETÊNCIAS E RESPONSABILIDADES

Com base no disposto no art. 3º do Decreto-Lei nº 4.657, de 4 de setembro de 1942, não é dado ao servidor e colaborador o direito de alegar desconhecimento da Política de Segurança da Informação e Comunicações, devendo seguir rigorosamente o proposto nas normas de segurança. O desconhecimento dessa norma por parte do usuário não o isenta das responsabilidades e penalidades.

17. 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 da Autarquia, 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 da Autarquia não tenha autonomia para tomar as providências cabíveis.

18. VIGÊNCIA E ATUALIZAÇÃO

18.1 **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.

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

18.3 **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).

18.4 **Responsável pela atualização**

18.4.1 Conforme Mapa de Responsabilidades.