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, quarta-feira, 15 de maio de 2019

SUMÁRIO

ATOS ADMINISTRATIVOS

PRESIDÊNCIA

FICHA TÉCNICA

Fundo Nacional de Desenvolvimento da Educação - FNDE
PRESIDENTE: CARLOS ALBERTO DECOTELLI DA SILVA
DIRETOR DE ADMINISTRAÇÃO: LUIS CLÁUDIO DA FONSECA BRAGANÇA PINHEIRO

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 Serviï¿½o - 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° 150/2019

PORTARIA Nº 244, DE 7 DE MAIO DE 2019

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 003/CGD/FNDE, que trata da Implementação, Operacionalização e Acesso às Redes Sem Fio do FNDE, conforme anexo I desta Portaria.

Art. 2º Aprovar a norma de Segurança da Informação e Comunicação NS 004/CGD/FNDE, que trata da Identificação da Segurança da Informação e Comunicação nos Contratos com Terceiros, conforme anexo II desta Portaria.

Art. 3º Aprovar a norma de Segurança da Informação e Comunicação NS 005/CGD/FNDE, que trata da Gestão de Ativos de Informação, conforme anexo III desta Portaria.

Art. 4º Aprovar a norma de Segurança da Informação e Comunicação NS 007/CGD/FNDE, que trata do Gerenciamento da Segurança em Redes, conforme anexo IV desta Portaria.

Art. 5º Aprovar a norma de Segurança da Informação e Comunicação NS 009/CGD/FNDE, que trata do Monitoramento de Sistemas, conforme anexo V desta Portaria.

Art. 6º Aprovar a norma de Segurança da Informação e Comunicação NS 013/CGD/FNDE, que trata da Classificação e Tratamento de Incidentes Computacionais, conforme anexo VI desta Portaria.

Art. 7º Aprovar a norma de Segurança da Informação e Comunicação NS 015/CGD/FNDE, que trata da Troca de Informações, conforme anexo VII desta Portaria.

Art. 8º Aprovar a norma de Segurança da Informação e Comunicação NS 018/CGD/FNDE, que trata da Garantia da Integridade e da Disponibilidade das Informações, conforme anexo VIII desta Portaria.

Art. 9º Aprovar a norma de Segurança da Informação e Comunicação NS 021/CGD/FNDE, que trata de Áreas Seguras, conforme anexo IX desta Portaria.

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

CARLOS ALBERTO DECOTELLI DA SILVA

ANEXO I

IMPLEMENTAÇÃO, OPERACIONALIZAÇÃO E ACESSO ÀS REDES SEM FIO 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.

ISO/IEC 27033-6 - Information technology - Security techniques - Network security - Securing wireless IP network access

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.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Não há.

APROVAÇÃO

Carlos Alberto Decotelli da Silva
Presidente do FNDE

1. OBJETIVO

Assegurar a proteção dos ativos de segurança da informação quanto à implementação, operacionalização e acesso à rede sem fio do FNDE.

2. DESCRIÇÃO E ESCOPO

Estabelecer regras (controles) e orientar as ações e procedimentos para a implementação, operacionalização e acesso a rede sem fio de forma segura.

3. PÚBLICO-ALVO

Esta norma destina-se aos responsáveis pela implementação, operacionalização e acesso da rede sem fio do FNDE.

4. CONCEITOS E DEFINIÇÕES

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

5. PRINCÍPIOS

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

6. DA IMPLEMENTAÇÃO

6.1 Da Topologia

6.1.1 Definir a topologia das redes sem fio, observar as seguintes orientações:

a) A potência de sinal do Ponto de Acesso (PA) não poderá ultrapassar o perímetro interno do FNDE; e

b) Os Pontos de Acesso deverão ser conectados por meio de *Switches*, nunca *Hubs*.

6.2 Rede Visitante

6.2.1 A rede visitante sem fio deverá ser implementada de forma isolada das demais redes corporativas do FNDE. Não será permitida a comunicação entre as redes, exceto quanto ao compartilhamento da infraestrutura necessária para possibilitar o correto funcionamento dessas redes.

6.3 Rede Corporativa

6.3.1 A rede corporativa sem fio deverá ser implementada de forma isolada das demais redes do FNDE. Deverão ser adotados mecanismos de autenticação centralizada, controles de acesso e periodicamente realizada análise de vulnerabilidade na infraestrutura que suporta este ambiente mitigando eventuais riscos.

6.4 Da Criptografia e Autenticação

6.4.1 Deverão ser utilizados mecanismos a fim de garantir a confidencialidade e integridade das informações trafegadas, assim como adotar mecanismos de autenticação utilizando base centralizada. Considerar, ainda:

a) Protocolo de criptografia, mais seguro disponível, entre o trafego do PA e usuário assim como PA e controladora; e

b) Acessos às aplicações a partir da rede sem fio devem ser realizados através de aplicações que suportem SSH e SSL.

6.4.2 Deverão ser implementados mecanismos de verificação de integridade das interfaces sem fio, a fim de proteger essas redes contra sequestro de sessão, ataques do tipo *man-in-the-midle* e ataques de repetição de mensagem;

6.5 Do Ponto de Acesso (PA)

6.5.1 Na seleção do modelo de PA, observar as seguintes características:

a) Conter recursos de criptografia e autenticação compatíveis com as orientações desta norma; e

b) Possiblidade de *upgrades* de *firmware*, permitindo incorporar novos padrões e eventuais correções lançadas pelo fabricante.

6.5.2 Nos procedimentos de configuração do PA adotar:

a) Acesso apenas pela rede cabeada ou ainda via conexão serial. Nunca realizar configuração pela própria rede sem fio; e

b) Utilizar exclusivamente protocolos seguros (SSH HTTPS).

6.5.3 Nas configurações originais de fábrica antes de colocar o PA em produção, modificar:

a) Senhas de administração;

b) SSID;

c) Chaves de criptografia; e

d) SNMP *communities.*

6.5.4 Nas ações de segurança dos PAs:

a) Desabilitar o acesso de escrita ("*read write*") ao agente SNMP. Evitar que suas configurações sejam alteradas remotamente;

b) Selecionar nome de difícil dedução para a comunidade SNMP de leitura ("*read only*") no agente SNMP. Evitar o uso do nome *default* PUBLIC;

c) Selecionar nome de difícil dedução para a comunidade SNMP de escrita ("*read write*") no agente SNMP. Evitar o uso do nome *default* PRIVATE;

d) Configurar o maior valor possível para o intervalo de envio de *broadcast* de *beacons.* Dificultar a descoberta da rede por atacantes que estejam pesquisando redes passivamente;

e) Configurar o PA para ignorar *probe-requests* sem SSID definido;

f) Configurar o PA para enviar *traps* somente para *hosts* de gerenciamento autorizados. Reduzir o risco de acesso não autorizado às informações de *status* dos agentes e outros alertas;

g) Configurar data e hora, assegurando o correto registro de trilhas de auditoria (*logs*);

h) Habilitar o recurso de MAC *Address Filtering* (filtragem por endereço MAC), limitando o acesso dos usuários ao PA em função do endereço MAC da placa em uso, caso possível; e

i) Usar frequência diferente daquelas utilizadas por outros aparelhos do FNDE. Evitar interferência entre aparelhos distintos.

6.5.5 Definir responsabilidade pela instalação, operacionalização e acesso aos PAs do FNDE;

6.5.6 O tráfego entre PAs deverá ser protegido usando protocolos baseados em IPsec.

6.6 Dos Controles de Acesso

Os controles de acesso devem ser implementados com base em:

a) Redes, endereços IP e protocolos;

b) Gerenciamento de vulnerabilidade que contemple avaliações periódicas de aplicativos e infraestrutura;

c) Taxa de transmissão limitada;

d) Controle RBAC;

e) Controle de acesso ao sistema de arquivos;

f) *Firewalls*; e

g) Detecção de intrusão.

7. DA OPERACIONALIZAÇÃO

7.1 Deverão ser definidos procedimentos de segurança em caso de roubo ou perda de equipamentos de redes sem fio;

7.2 Trocar as senhas de administração dos PAs de forma regular a cada 6 (seis) meses conforme norma 016-CGD-FNDE – Responsabilidades dos usuários;

7.3 Colocar PAs com opção de *reset* físico em locais com acesso controlado;

7.4 Desligar todo PA quando não utilizado;

7.5 Monitorar, constantemente, as redes sem fio, em especial:

a) Volume de tráfego gerado;

b) Conexão de usuários em horários improváveis;

c) Instalação de Pontos de Acesso não autorizados;

d) Servidores DHCP estranhos à rede corporativa;

e) Dispositivos que não estejam usando a criptografia requerida;

f) Ataques contra os usuários da rede sem fio;

g) Vulnerabilidades técnicas identificadas;

h) Acessos não autorizados;

i) Acesso a portas e serviços não autorizados;

j) Mudanças de endereços MAC sem autorização;

k) Mudanças de canal sem autorização;

l) Ruídos e interferências eletromagnéticas; e

m) Técnicas de "*jamming"*.

7.6 Executar os registros de auditoria (*logs*) gerados pelos Pontos de Acesso observando-se:

a) Proteção contra acessos indevidos;

b) Armazenamento em servidor centralizado e em local de acesso restrito; e

c) Monitoração periódica de sua qualidade (os registros deverão se manter íntegros, disponíveis e confidenciais).

NOTA: Um sistema de prevenção de intrusão sem fio (*Wireless Intrusion Prevention System* – WIPS) deve ser implementado nas redes sem fio.

8. DO ACESSO

8.1 De Usuários:

a) Apenas usuários autorizados poderão fazer uso das redes sem fio; e

b) Os usuários autorizados deverão obedecer às regras dessa Política de Segurança da Informação e Comunicação.

8.2 De Dispositivos:

Dispositivos que acessam as redes sem fio, tais como notebooks, PDAs e outros devem passar por um processo adicional de instalação e configuração segura que vise o aumento de sua proteção, incluindo:

a) A instalação de *firewall* pessoal;

b) A instalação e atualização de antivírus;

c) O desligamento do compartilhamento de disco, impressora; e

d) As orientações da norma de segurança NS 29/CGD/FNDE – Uso de Dispositivos Móveis.

NOTA: Não será permitido o acesso às redes sem fio, caso não se observe as orientações acima.

9. PENALIDADES

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

10. RESPONSABILIZAÇÃO

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

10.2 **Disposições Gerais**

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

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

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

11. VIGÊNCIA E ATUALIZAÇÃO

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

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

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

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

11.3 **Condições obrigatórias de atualização do documento**

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

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

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

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

11.4 **Responsável pela atualização**

11.4.1 Conforme Mapa de Responsabilidades.

ANEXO II

IDENTIFICAÇÃO DA SEGURANÇA DA INFORMAÇÃO E COMUNICAÇÃO NOS CONTRATOS COM TERCEIROS

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

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

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

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

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

ABNT NBR ISO/IEC 20000-1 – Tecnologia da Informação – Gestão de Serviços – Requisitos do sistema de Gestão de Serviços.

ISO/IEC 27036-2 – Information Technology – Security techniques – Information Security for Supplier Relationships

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-002-2005-PRES: Norma de Segurança sobre padrões para contratação de prestadores de serviço, 1ª Atualização*, publicada em 2005.

APROVAÇÃO

Carlos Alberto Decotelli da Silva
Presidente do FNDE

1. OBJETIVO

Estabelecer requisitos de Segurança da Informação e Comunicação a serem atendidos por terceiros na relação contratual com o FNDE.

2. DESCRIÇÃO E ESCOPO

Definir regras para o manuseio seguro das informações acessadas por terceiros dentro da sua relação contratual com o FNDE.

3. PÚBLICO-ALVO

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

4. CONCEITOS E DEFINIÇÕES

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

5. PRINCÍPIOS

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

6. SEGURANÇA DA INFORMAÇÃO NA RELAÇÃO CONTRATUAL COM TERCEIROS

6.1 Na relação contratual com terceiros, o FNDE deverá definir, especificamente, quais serviços e atividades serão autorizados para acesso e manuseio por terceiros. Deverá ser considerado, sempre, o menor perfil de privilégio para acesso às informações da Autarquia.

6.2 Todo acesso por terceiros às informações e ativos do FNDE só será autorizado após preenchimento de Termo de Ciência, de acordo com modelo encartado na Política de Segurança da Informação e Comunicação (POSIC) do FNDE.

6.3 Toda autorização de acesso a terceiros deverá apresentar prazo de início e fim, com exceção de colaboradores que, pela sua relação contratual com o FNDE e enquanto o contrato viger estará autorizado a realizar os acessos necessários para desenvolver suas atividades.

6.4 O FNDE deverá realizar, periodicamente, auditorias e inspeções para verificar o cumprimento das orientações estabelecidas nessa norma de segurança.

6.5 Toda relação contratual deverá trazer obrigações claras a serem atendidas por terceiros contratados.

6.6 Toda transição contratual entre FNDE e empresas contratadas deverá ser feita dentro de prévio planejamento e avaliação de riscos e impactos. Toda informação necessária deverá ser repassada à empresa contratada, a fim de se evitar paradas dos serviços prestados à Autarquia.

NOTA1: O FNDE deverá exigir de toda empresa contratada a assinatura do Termo de Compromisso, segundo modelo encartado na POSIC do FNDE.

NOTA2: Todo Termo de Ciência, bem como Termo de Compromisso deverão orientar ao terceiro acerca de regras de proteção de dados corporativos, direito de propriedade intelectual e direito autoral pertencente ao FNDE.

NOTA3: É de responsabilidade de empresa terceirizada o fornecimento de todas as informações relativas à sua força de trabalho alocada para serviços na Autarquia.

NOTA4: A empresa deverá formalizar pedido de autorização de acesso para cada colaborador ao ambiente tecnológico da Autarquia, o qual deverá ser corroborado pela chefia imediata do colaborador. Também deverá formalizar pedido de desligamento de sua força de trabalho quando necessário. O preposto da empresa é o responsável por manter atualizada toda a informação repassada ao FNDE.

NOTA5: A legislação referente à relação contratual deve ser aplicada subsidiariamente, no que for compatível com essa Norma de Segurança.

NOTA6: Toda informação produzida, veiculada e acessada deverá passar por classificação antes de ser ou não disponibilizada para terceiros. Observar a Lei de Acesso à Informação (Lei nº 12.527/2011) e seu Decreto de regulamentação (Decreto nº 7.724/2012) para se realizar a adequada classificação.

NOTA7: Na aquisição de soluções e equipamentos de Tecnologia da Informação, a área de TI deverá observar, ainda:

a) Requisitos de segurança da informação e comunicação (SIC) aplicáveis com base na POSIC do FNDE; e

b) Verificação do atendimento de boas práticas de segurança da POSIC no momento do recebimento provisório e definitivo das soluções e equipamentos adquiridos.

NOTA8: O FNDE deve monitorar, analisar criticamente e auditar em intervalos regulares a entrega dos serviços executados pelos terceiros contratados.

NOTA9: Toda atualização da POSIC do FNDE bem como de procedimentos, sistemas e processos envolvidos deverão ser repassados a terceiros contratados a fim de se manter alinhado o conhecimento e implementação de mudanças de segurança necessárias à Autarquia.

7. PENALIDADES

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

8. RESPONSABILIZAÇÃO

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

9. DISPOSIÇÕES GERAIS

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

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

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

10. VIGÊNCIA E ATUALIZAÇÃO

10.1 **Este documento entra em vigor em 90 (noventa) dias a partir da data de sua publicação e pode ser atualizada ou revogada 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.

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

10.3 **Condições obrigatórias de atualização do documento**

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

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

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

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

10.4 **Responsável pela atualização**

10.4.1 Conforme Mapa de Responsabilidades.

ANEXO III

GESTÃO DE ATIVOS DE INFORMAÇÃO

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

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

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

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

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

NC 10/IN01/DSIC/GSIPR – Estabelece diretrizes para o processo de Inventário e Mapeamento de Ativos de Informação, para apoiar a Segurança da Informação e Comunicações (SIC), dos órgãos e entidades da Administração Pública Federal, direta e indireta – APF.

ABNT NBR 14565:2013 – Cabeamento estruturado para edifícios comerciais e data centers.

ABNT NBR ISO 7240-1:2017 – Sistemas de detecção e alarme de incêndio Parte 1: Generalidades e definições.

ABNT NBR ISO 7240-23:2016 – Sistemas de detecção e alarme de incêndio Parte 23: Dispositivos de alarme visual.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-003-2002-SEXEC: Norma de Segurança sobre contabilização dos ativos e classificação das informações no FNDE*, publicada em 8 de novembro de 2002.

APROVAÇÃO

Carlos Alberto Decotelli da Silva
Presidente do FNDE

1. OBJETIVO

Mitigar perdas, danos, furtos e comprometimento dos ativos de informação do FNDE dentro do seu ciclo de vida.

2. DESCRIÇÃO E ESCOPO

Estabelecer regras de segurança para devida gestão dos ativos de informação para reduzir os riscos relativos às perdas, aos danos, aos furtos e ao comprometimento dos ativos de informação do FNDE dentro do seu ciclo de vida.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores responsáveis pela posse temporária dos ativos de informação.

4. CONCEITOS E DEFINIÇÕES

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

5. PRINCÍPIOS

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

6. O QUE CONSIDERAR PARA REALIZAR UM INVENTÁRIO DE ATIVOS DE INFORMAÇÃO

6.1 Um bom inventário de ativos de informação deve levar em consideração os ativos necessários para o atendimento de objetivos corporativos, ou seja, deve ser levantado e mapeado ativos que impactam/influenciam nos resultados organizacionais. Assim, mapear ativos representa levantar processos organizacionais, tecnologia da informação e estrutura de apoio aos objetivos estratégicos do FNDE.

6.2 Todo levantamento realizado deve considerar ainda:

a) Ativos críticos ao negócio que não podem sofrer paradas sem danos ao órgão;

b) Ativos não críticos que podem sofrer paradas por meio de cronograma de manutenção preventiva;

c) Periodicidade necessária de revisão para se manter mapeado e atualizado todos os ativos que são importantes ao negócio; e

d) Roteiro preestabelecido e padronizado para se manter constância de informações corretas.

7. ETAPAS EM UM LEVANTAMENTO DE ATIVOS DE INFORMAÇÃO

7.1 Para um correto levantamento de ativos de informação, devem ser observadas as seguintes etapas:

a) Identificação e classificação de ativos da informação; e

b) Identificação de potenciais ameaças e vulnerabilidade e avaliação de riscos.

7.1.1 **Identificação e Classificação de Ativos de Informação**:

7.1.1.1 Na etapa identificação de ativos da informação a organização deverá:

a) Definir um processo claro e simples para identificar todos os ativos necessários ao atendimento da missão da instituição;

b) Relacionar os responsáveis pela coleta em seu âmbito de atuação;

c) Basear-se nos objetivos estratégicos e de negócio do FNDE;

d) Definir o escopo da coleta;

Nesta etapa, deve-se considerar, no mínimo, um conjunto essencial de informações suficiente para:

a) Determinar com clareza e objetividade o conteúdo do ativo de informação;

b) Identificar o responsável – proprietário e custodiante – de cada ativo de informação;

c) Identificar o valor de cada ativo de informação;

Na sub-etapa de identificação do responsável (proprietário do ativo da informação), o proprietário deverá:

a) Descrever o ativo de informação;

b) Solicitar auxílio para o devido mapeamento de risco e continuidade de negócios dos ativos sob sua responsabilidade; e

c) Rotular os ativos dentro de um mapa de riscos e impacto de negócio.

NOTA: Todo levantamento de ativos corporativos deverá ser apoiado pela identificação de riscos desses ativos, bem como pela sua análise de impacto nos negócios do FNDE.

7.1.1.2 Na etapa classificação de ativos da informação a organização deverá:

a) Classificar seus ativos conforme metodologia de classificação adotada pelo FNDE; e

b) Considerar os resultados de análises de riscos e impacto de negócio para rotular seus ativos dentro de critérios de severidade, criticidade, pertinência, relevância e urgência.

NOTA1: Todo ativo da informação custodiado pela área de tecnologia da informação deverá ser protegido conforme rótulo fornecido pelo proprietário do ativo da informação, ou seja, de acordo com a severidade, a criticidade, a pertinência, a relevância e a urgência desse ativo.

NOTA2: A área de tecnologia da informação deverá assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação sob sua custódia.

NOTA3: Todo ativo de informação considerado crítico para o negócio deverá ser mapeado e controlado desde sua criação, seu processamento, seu armazenamento, sua veiculação, sua exclusão e destruição dentro do seu ciclo de vida.

7.1.2 **Identificação de potenciais ameaças e vulnerabilidade e avaliação de riscos**:

7.1.2.1 Na etapa identificação de potenciais ameaças e vulnerabilidades e avaliação de riscos o FNDE deverá desenvolver metodologia específica para se analisar os riscos a que os ativos de informação estão expostos, a fim de se mitigar potenciais ameaças e vulnerabilidades. Também será necessário desenvolver metodologia para se analisar o impacto dos ativos na continuidade dos negócios da organização.

7.1.2.2 Após o desenvolvimento das metodologias em questão, o FNDE deverá separar, tecnicamente, todos os ativos pelos critérios de riscos e continuidade dos negócios, aplicando métricas e padrões de segurança da informação distintos, conforme a severidade, a criticidade, a pertinência, a relevância e a urgência de cada ativo relativo ao negócio corporativo.

8. PROPRIETÁRIO DOS ATIVOS

8.1 O FNDE deverá identificar todos os proprietários responsáveis por ativos da informação.

8.2 Cada proprietário será responsável por manter atualizados os rótulos dos seus ativos custodiados junto à área de tecnologias da informação. Essa orientação tem por finalidade avaliar se, dentro do ciclo de vida da informação, o ativo mantém ou não seu valor de segurança e importância e se deve ser realocado para repositório computacional com períodos de manutenção menos constantes ou com segurança menor.

9. USO ACEITÁVEL DOS ATIVOS

9.1 O FNDE deverá conscientizar os servidores, colaboradores e partes externas a respeito dos requisitos de Segurança da Informação associados ao ativo da informação e aos recursos de processamento da informação.

9.2 O FNDE é o proprietário corporativo/institucional dos ativos de informação e seu uso está restrito aos servidores, colaboradores e partes externas autorizadas, conforme os acordos de segurança assinados.

9.3 Os ativos de informação do FNDE utilizados externamente devem seguir o mesmo padrão de segurança dos utilizados internamente, e seu uso deve ser autorizado pelo proprietário do ativo de informação.

10. DEVOLUÇÃO DE ATIVOS

10.1 Após desligamento de servidores, colaboradores e partes externas, o FNDE deverá recolher todos os ativos físicos e informações sob custódia desses agentes.

10.2 Durante o processo de desligamento, o FNDE deverá monitorar possíveis cópias de informações relevantes pelo agente desligado.

11. RESPONSABILIDADES PELO INVENTÁRIO

11.1 Cabe à área de tecnologia da informação o levantamento e mapeamento dos ativos de informação armazenados em meio lógico, bem como sob sua custódia.

11.2 Cabe a cada diretoria do FNDE a responsabilidade pelo levantamento e mapeamento dos ativos de informação gerados por seus proprietários de ativos de informação bem como sob sua custódia.

12. REQUISITOS DE SEGURANÇA PARA PROTEÇÃO DE TIC

12.1 Diretrizes Gerais de Segurança

12.1.1 Para prover a gestão adequada dos ativos de tecnologia da informação e comunicação, a área de tecnologia da informação deverá implementar:

a) Proteção contra ameaças ambientais e acessos não autorizados;

b) Aviso de proibição para consumo de alimentos e bebidas próximo as máquinas;

c) Controle eficiente que mitigue os seguintes riscos: roubo, fogo, explosivos, fumaça, água, poeira, exposição à luz solar, vibração, interferência no fornecimento elétrico e radiação eletromagnética;

d) Controle de temperatura e umidade conforme orientações dos fabricantes dos ativos de tecnologia da informação e comunicação; e

e) Controles contra oscilações, picos e surtos de energia elétrica e outras interrupções que prejudiquem as máquinas.

12.1.2 Quanto ao suprimento de energia elétrica, telecomunicação, água, gás, ventilação e ar-condicionado, a área de tecnologia da informação deverá observar:

a) A conformidade com as especificações do fabricante dos ativos de tecnologia da informação e comunicação e com os requisitos legais pertinentes;

b) A regular inspeção e testes para assegurar o funcionamento adequado dos ativos de tecnologia da informação e comunicação;

c) A implementação de alarmes para detectar o mau funcionamento das máquinas; e

d) A implementação de fontes de alimentação e rotas físicas diferentes para o adequado e ininterrupto suprimento ao ambiente de tecnologia.

NOTA: Ativos de tecnologia da informação e comunicação que necessitem de proteção adicional devido a sua criticidade e importância devem ser isolados e com controle restrito de acesso físico e lógico. O FNDE deve adotar ações de caráter preventivo para a contínua segurança e disponibilidade desses ativos de tecnologia da informação e comunicação.

12.2 **Diretrizes de Segurança em Cabeamentos**

12.2.1 A área responsável pela gestão e disponibilização de energia e telecomunicação ao FNDE deverá prover a adequada proteção contra interceptação, interferência ou danos no cabeamento que transporta dado ou dá suporte aos serviços de informações do FNDE.

12.2.2 As linhas de energia e de telecomunicação que entram nas instalações de processamento da informação devem ser subterrâneas (ou ficar abaixo do piso).

12.2.3 Os cabos de energia e os cabos de comunicação devem ser separados.

12.2.4 Nos sistemas críticos do FNDE:

a) Devem ser instalados conduites blindados e salas ou caixas trancadas em pontos de inspeção e terminais;

b) Deve ser utilizada blindagem eletromagnética para a proteção dos cabos;

c) Devem ser realizadas varreduras técnicas e inspeções físicas para detectar a presença de dispositivos não autorizados conectados aos cabos; e

d) O acesso aos painéis de conexões e às salas de cabos deve ser controlado.

NOTA: A instalação, o controle e a manutenção do cabeamento elétrico e lógico devem estar alinhados com a norma ABNT NBR 14565:2007.

13. DIRETRIZES PARA A MANUTENÇÃO DOS ATIVOS DE TIC

A área de tecnologia da informação responsável pela manutenção de equipamentos de tecnologia deve atender às seguintes orientações:

a) Realizar manutenção regular nos intervalos recomendados pelo fornecedor e de acordo com as suas especificações;

b) A manutenção deverá ser realizada apenas profissional autorizado; e

c) Registrar todas as falhas (suspeitas ou reais) e todas as operações preventivas e corretivas realizadas.

14. DIRETRIZES PARA A REUTILIZAÇÃO OU DESCARTE SEGURO DOS ATIVOS DE TIC

14.1 A área de tecnologia da informação deverá implementar processo de sanitização de todas as mídias de armazenamento de dados antes de descartar, reutilizar ou doar os ativos de tecnologia da informação e comunicação.

14.2 A sanitização pode ser realizada utilizando duas técnicas:

a) Física (destruição): deverá ser aplicada a toda mídia que contenha informação confidencial ou relativa aos direitos autorais e à propriedade intelectual; e

b) Lógica (apagamento interno efetivo das trilhas de registros de dados contidas nas mídias): deverão ser aplicadas às demais mídias não enquadradas no item acima.

NOTA: A área de tecnologia da informação deverá possuir ferramentas que realizem a deleção/remoção efetiva de informações das mídias de armazenamento em questão. Não deverá ser possível a recuperação de dados por meio de uso de ferramentas específicas de tecnologia após a sanitização.

15. DIRETRIZES PARA A RETIRADA DE ATIVOS DE TECNOLOGIA

15.1 A área de tecnologia da informação deverá implementar procedimentos para a retirada segura de ativos de tecnologia das instalações do FNDE.

15.2 Para a retirada de ativos de tecnologia, devem ser observados os seguintes procedimentos:

a) Apresentar, previamente, autorização formal e motivada para retirada e transporte de ativos de tecnologia;

b) A autorização deverá conter dados da empresa, do empregado responsável, data/hora da retirada e o prazo para devolução do ativo de tecnologia;

c) O ativo deve ser previamente sanitizado para evitar vazamento de informações confidenciais; e

d) O ativo deve retornar conforme especificações observadas quando da retirada.

16. PENALIDADES

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

17. RESPONSABILIZAÇÃO

17.1 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.

17.2 **Disposições Gerais**

17.3 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.

18. VIGÊNCIA E ATUALIZAÇÃO

18.1 **Este documento entra em vigor em 90 (noventa) dias a partir da data de sua publicação e pode ser atualizada ou revogada 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.

ANEXO IV

Fundo Nacional de Desenvolvimento da Educação

GERENCIAMENTO DA SEGURANÇA EM REDES

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2018-CGD: Diretrizes de Segurança

NS-007-2002-SEXEC: Norma de Segurança sobre a Infraestrutura Computacional do FNDE

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

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

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

ABNT NBR ISO/IEC 38500:2009 – Governança corporativa de tecnologia da informação.

ISO/IEC 15408-1:2009 – Information technology – Security techniques – Evaluation Criteria for IT security – Part 1: Introduction and general model.

ISO/IEC 15408-2:2008 – Information technology – Security techniques – Evaluation Criteria for IT security – Part 2: Security functional requirements.

ISO/IEC 15408-3:2008 – Information technology – Security techniques – Evaluation Criteria for IT security – Part 3: Security assurance requirements.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-007-2002-SEXEC: Norma de Segurança sobre a Infraestrutura Computacional do FNDE*, publicada em 10 de dezembro de 2002.

APROVAÇÃO

Carlos Alberto Decotelli da Silva
Presidente do FNDE

1. OBJETIVO

Definir uma metodologia para a gestão segura da rede corporativa.

2. DESCRIÇÃO E ESCOPO

Descrever as atividades para a proteção da infraestrutura computacional do FNDE, de forma a minimizar os riscos de segurança da informação nos ativos de rede fornecendo diretrizes para a especificação de focos de segurança.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores que exercem função de administração dos recursos de tecnologia da informação.

4. CONCEITOS E DEFINIÇÕES

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

5. PRINCÍPIOS

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

6. DAS RESPONSABILIDADES

6.1 **Da Área de Tecnologia da Informação**

6.1.1 A área de tecnologia da informação é responsável por observar toda regulamentação afeta à TI abordada na Política de Segurança da Informação (POSIC) do FNDE. Também é responsável, em seu âmbito de atuação, por observar a legislação de segurança afeta a tecnologia em âmbito federal.

6.1.2 A área de TI poderá implementar, em decisão de sua direção, boas práticas de segurança da informação e comunicação difundidas por meio de instituições legalmente constituídas, a exemplo da ABNT e ISO.

6.1.3 Toda criação, alteração, manuseio e execução de atividades em âmbito da TI que não esteja de acordo com essa Política de Segurança da Informação e Comunicação deverá ser cancelada. A direção da área de tecnologia da informação deverá direcionar, com o apoio de suas coordenações gerais, orientação para sua força de trabalho a fim de se cumprir a POSIC.

6.1.4 A área de tecnologia da informação deverá, ainda:

a) Promover ações de divulgação e conscientização dos usuários para a correta utilização dos recursos de TI do FNDE;

b) Promover auditorias e inspeções na busca de ameaças e vulnerabilidades em seu parque computacional de forma regular;

c) Promover checagem regular do atendimento da POSIC em seu âmbito de atuação;

d) Assegurar a disponibilidade e a integridade dos recursos de tecnologia da informação do FNDE;

e) Registrar todos os acessos ou tentativas realizadas por meio de redes de computadores externas para a rede de computadores interna do FNDE, definindo, inclusive, os prazos de armazenamento e guarda desses registros; e

f) Mitigar as vulnerabilidades existentes na rede de computadores do FNDE.

6.2 **Da Área de Recursos Humanos**

A área de recursos humanos é responsável por informar a área de TI acerca de toda movimentação de usuários (admissão, demissão, transferência, afastamento e outros) dentro do perímetro corporativo para fins do controle de acesso lógico e atendimento às regras de segurança da organização.

7. DOS PROCEDIMENTOS

7.1 ÁREAS DE ARMAZENAMENTO LOCAL

a) Não deverá ser realizado serviço de cópia de informações localizadas em estação de trabalho de usuário; e

b) A área de TI deve possuir serviço central de armazenamento de informações corporativas geradas pelo FNDE (discos compartilhados de rede). Esse serviço realizará, periodicamente, cópias (*backups*) de todas as informações consideradas necessárias ao funcionamento da Autarquia.

NOTA1: A área de TI não tem a responsabilidade e obrigação de realizar cópias de informações pessoais armazenadas em computadores disponibilizados para usuários da Autarquia.

NOTA2: Toda disponibilização de informação corporativa em meio lógico em rede computacional deverá ser ofertada, exclusivamente, pela área de TI, cabendo a esta área garantir adequada segurança na criação, manuseio, armazenamento, transporte e descarte de informação organizacional.

7.2 PONTOS DE ACESSO DE REDE

a) Devem ser bloqueados todos os pontos sem equipamentos;

b) Cada ponto de rede deve ser vinculado a equipamento autorizado e identificado; e

c) Toda instalação ou mudança de ponto de rede deve, antes, ser autorizada pela área de TI.

7.3 ACESSO EXTERNO À REDE CORPORATIVA

a) Todo acesso externo à rede corporativa deverá ser previamente autorizado pela direção da área de TI, depois de adequada formalização da área demandante; e

b) Os sistemas acessados externamente deverão ser monitorados regularmente e medidas de segurança adequadas deverão ser implementadas a fim de se evitar quebra de segurança interna.

7.4 **TOPOLOGIA DE REDE**

a) A área de TI é responsável por manter atualizada toda a topologia de rede corporativa ofertada ao órgão; e

b) A topologia produzida deverá sofrer restrição em sua consulta. Apenas os responsáveis da área devem ter conhecimento dessa topologia.

8. SEGURANÇA DOS SERVIÇOS DE REDE

8.1 Os canais de comunicação em rede (Interno-Externo) deverão atender às seguintes regras:

a) Limitação do número de linhas telefônicas dedicadas;

b) Canais com portas específicas de acesso;

c) Negação de acesso às configurações de *softwares* referentes às rotas pré-definidas e controladas para usuários não autorizados;

d) Controle dos endereços de origem e destino na comunicação;

e) Registro das ligações de linhas dedicadas para serviços com modem na rede corporativa do FNDE; e

f) Restrição de acesso a segmentos de rede através de mecanismos de controle de rota e filtros.

8.2 Todo serviço de acesso externo deve ser precedido do estabelecimento de convênio e contrato formal entre o provedor e o FNDE.

NOTA: A área de TI deverá observar, em todo ciclo de gestão para a segurança em redes, os normativos de segurança da informação e comunicação do FNDE (POSIC), em especial as seguintes normas:

a) NS003-Implementação, operacionalização, manutenção e acesso às redes sem fio;

b) NS005-Gestão de ativos de informação;

c) NS006-Sensibilização, conscientização e capacitação em segurança da informação e comunicações;

d) NS008-Proteção contra códigos maliciosos;

e) NS009-Monitoramento de sistemas;

f) NS010-Procedimentos e responsabilidades operacionais;

g) NS011-Administração do correio eletrônico;

h) NS012-Administração da internet;

i) NS013-Classificação e tratamento de incidentes computacionais;

j) NS014-Aquisição desenvolvimento e manutenção de sistemas;

k) NS017-Controle de acesso ao sistema operacional;

l) NS019-Uso de dispositivos móveis dentro do FNDE;

m) NS022-Trabalho remoto;

n) NS023-Segregação de funções;

o) NS025-Instalação e configuração segura de dispositivos de roteamento computacional;

p) NS026-Instalação e configuração segura de dispositivos de SI do FNDE; e

q) NS027-Instalação e configuração segura de sistemas operacionais.

9. 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.

10. RESPONSABILIZAÇÃO

Ao colaborador não é dado o direito de desconhecimento da Política de Segurança da Informação e Comunicações, devendo seguir rigorosamente o proposto nas normas de segurança.

11. DISPOSIÇÕES GERAIS

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

a) Comitê de Governança Digital – CGD, com apoio, se necessário, das áreas técnicas do FNDE; e

b) Presidência do FNDE, em decisão final, caso o CGD não tenha autonomia para tomar as providências cabíveis.

12. VIGÊNCIA E ATUALIZAÇÃO

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

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

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

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

12.3 **Condições obrigatórias de atualização do documento**

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

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

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

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

12.4 **Responsável pela atualização**

12.4.1 Conforme Mapa de Responsabilidades.

ANEXO V

MONITORAMENTO DE SISTEMAS

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

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

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

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

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

ISO/IEC TR 27008 – Information Technology – Security Techniques – Guidelines for Auditors on Information Security Controls.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-009-2002-SEXEC: Norma de Segurança para Monitoração do Uso e Acesso aos Sistemas*, publicada em 10 de dezembro de 2002.

APROVAÇÃO

_____

Carlos Alberto Decotelli da Silva
Presidente do FNDE

1. OBJETIVO

Reduzir o risco de acesso indevido às soluções de tecnologia do FNDE.

2. DESCRIÇÃO E ESCOPO

Estabelecer requisitos a serem seguidos quanto ao monitoramento de soluções de tecnologia e as devidas ações de segurança para identificação e mitigação de riscos.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores responsáveis pelo monitoramento das soluções de tecnologia da informação da rede corporativa.

4. CONCEITOS E DEFINIÇÕES

Termos, expressões e definições utilizados na Política de Segurança da Informação e Comunicações localizam-se no "Dicionário de 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 moralidade, do interesse público e da motivação, visando a proteção e a preservação das informações necessárias às atividades do FNDE.

6. MONITORAMENTO DE SISTEMAS

6.1 Todos os recursos de tecnologia da informação deverão ser monitorados e seus registros (*logs*) armazenados em local apropriado. Prazos de retenção e locais diferenciados deverão ser implementados conforme a informação seja crítica ao negócio ou não.

6.2 Os principais eventos deverão ser monitorados, a exemplo de:

a) Acessos autorizados;

b) Operações executadas por perfis específicos e privilegiadas, como:

   i. Utilização de conta de administração; e

   ii. Cessão e remoção de direitos de acessos aos sistemas.

c) Tentativas de acessos não autorizados, tais como:

   i. Falhas; e

   ii. Violação da política de acesso.

d) Alertas e falhas de sistemas,

e) Registro das exceções do sistema;

f) Alarmes do gerenciamento da rede;

g) Identificação dos usuários (ID);

h) Atividades do sistema;

i) Datas, horário de entrada (log-on) e saída (log-off) no sistema;

j) Identificador do dispositivo e sua localização;

k) Alterações na configuração do sistema;

l) Uso de aplicações e utilitários de sistema;

m) Arquivos acessados e o tipo de acesso;

n) Endereços e protocolos de rede;

o) Ativação e desativação dos sistemas de proteção, como sistemas de antivírus e sistemas de detecção de intrusos; e

p) Registros de transações executadas pelos usuários nas aplicações.

6.3 O monitoramento não deverá impactar, tecnicamente, as atividades usuais do ambiente de produção, ou seja, o monitoramento deverá ser transparente e não sobrecarregar as aplicações monitoradas.

6.4 O monitoramento deve ser realizado, preferencialmente, com a utilização de ferramentas automatizadas que gerem alarmes imediatos de eventos e indiquem ações necessárias para diminuir riscos de quebra de segurança.

NOTA: Essas ferramentas deverão conter, ainda, alarmes que alertem acerca de limites de armazenamento atingidos (evitar estouro de armazenamento ou rotação automática de *logs* sem prévia transferência de informações à repositório próprio).

6.5 O monitoramento deve observar, ainda, as seguintes regras:

a) Possibilitar configuração de alarmes e destinatários a serem contatados em caso de falhas de segurança; e

b) Conter "inteligência automatizada" para recomendar medidas de mitigação de riscos de quebra de segurança.

6.6 **Registros de Eventos (*Log*) para perfis privilegiados**

6.6.1 Perfis privilegiados, como administradores de sistemas, deverão ser monitorados em intervalos estabelecidos e regulares. Ações deverão ser implementadas quando se verificar abuso no uso de privilégios, como acesso desses perfis em soluções/plataformas de tecnologia fora das suas atribuições regulamentares; e

6.6.2 Deverá ser implementado um sistema de detecção de intrusos gerenciados fora do controle desses perfis privilegiados para monitorar a conformidade das atividades executadas por esses.

7. PROTEÇÃO DAS INFORMAÇÕES DOS REGISTROS DE EVENTOS (LOG)

7.1 As informações dos registros de eventos (*log*) e os seus recursos devem ser protegidos contra acesso não autorizado e adulteração. Em especial, atentar para:

a) Modificações não autorizadas;

b) Arquivos de registros (*log*) editados ou excluídos; e

c) Alterações da padronização/alertas de mensagens que são gravadas.

7.2 Uma cópia isolada e segura de registros dos *logs* de informações críticas ao negócio deverá ser produzida e armazenada em ambiente inalterável por perfis privilegiados. Deverá ser garantida a confidencialidade, integridade, disponibilidade e autenticidade dessa cópia para fins de investigação interna quando necessário.

8. SINCRONIZAÇÃO DOS RELÓGIOS DA REDE

8.1 Todos os sistemas/soluções de tecnologia da informação do FNDE deverão ser sincronizados de acordo com o horário oficial do Observatório Nacional.

8.2 A área de tecnologia da informação deverá realizar checagens periódicas em toda a infraestrutura de tecnologia da informação para garantir o correto sincronismo entre as diversas plataformas e soluções tecnológicas ofertadas.

NOTA1: Todo monitoramento realizado deverá fornecer insumos suficientes para subsidiar auditorias internas (trilhas, evidências e achados de auditoria).

NOTA2: Revisões periódicas deverão ser realizadas nas ferramentas de monitoramento, em especial quando houver atualizações no parque de informática (hardware ou software) ou em aplicações utilizadas pelo FNDE. Tal medida é necessária para o correto e constante monitoramento do ambiente de tecnologia da informação.

NOTA3: Todo monitoramento deverá implementar segurança suficiente, em caso de coleta de dados pessoais de usuários, em atendimento aos preceitos de legislação pertinente, em especial a Lei de Acesso à Informação.

NOTA4: É proibida aos perfis privilegiados a deleção de suas próprias informações/atividades nas ferramentas de monitoramento.

NOTA5: Salvo legislação pertinente, o período de retenção de *logs* será de 06 (seis) meses.

9. 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.

10. RESPONSABILIZAÇÃO

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

10.2 **Disposições Gerais**

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

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

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

11. VIGÊNCIA E ATUALIZAÇÃO

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

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

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

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

11.3 **Condições obrigatórias de atualização do documento**

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

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

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

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

11.4 **Responsável pela atualização**

11.4.1 Conforme Mapa de Responsabilidades.

ANEXO VI

CLASSIFICAÇÃO E TRATAMENTO DE INCIDENTES COMPUTACIONAIS

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 05/IN01/DSIC/GSIPR - Disciplina a criação de Equipes de Tratamento e Respostas a Incidentes em Redes Computacionais - ETIR nos órgãos e entidades da Administração Pública Federal.

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

ISO/IEC 27035-1 - Information Technology - Security Techniques - Information Security Incident Management - Principles of incident management

ISO/IEC 27035-2 - Information Technology - Security Techniques - Information Security Incident Management - Guidelines to plan and prepare for incident response

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-013-2002-SEXEC: Norma sobre Resposta a Incidentes de Segurança da Informação*, publicada em 14 de março de 2003.

APROVAÇÃO

Carlos Alberto Decotelli da Silva
Presidente do FNDE

1. OBJETIVO

Estabelecer regras para a gestão dos incidentes de Segurança da Informação e Comunicação.

2. DESCRIÇÃO E ESCOPO

Estabelecer critérios e regras para assegurar um enfoque consistente e efetivo para gerenciar incidentes, incluindo a comunicação sobre fragilidades e eventos de Segurança da Informação e Comunicação.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores responsáveis pela avaliação, decisão, resposta e notificação dos incidentes de Segurança da Informação e Comunicação.

4. CONCEITOS E DEFINIÇÕES

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

5. PRINCÍPIOS

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

6. ORIENTAÇÕES GERENCIAIS

6.1 Os eventos de Segurança da Informação devem ser avaliados, podendo ser classificados como incidentes de Segurança da Informação ou não.

6.2 Os incidentes de Segurança da Informação devem ser reportados de acordo com procedimentos pré-mapeados e documentados.

6.3 Deverá ser criada uma Equipe de Tratamento e Resposta a Incidentes Computacionais (ETIR) subordinada à Diretoria de Tecnologia e Inovação (DIRTI).

6.3.1 A ETIR será responsável pela troca de informações sobre o gerenciamento de incidentes de segurança em redes de computadores do FNDE com a Coordenação Geral de Tratamento de Incidentes de Segurança em Redes de Computadores – CGTIR do Centro de Tratamento de Incidentes de Redes do Governo – CTIR Gov.

6.3.2 A ETIR deverá classificar e tratar todos os incidentes computacionais direcionados para essa equipe.

6.3.3 A ETIR deverá observar, como atribuição, as seguintes orientações:

a) Promover o intercâmbio científico-tecnológico relacionado a incidentes de segurança em redes de computadores com os demais órgãos da Administração Pública Federal;

b) Apoiar o FNDE nas atividades de gerenciamento e tratamento de incidentes de segurança em redes de computadores;

c) Monitorar e analisar tecnicamente os incidentes de segurança em redes de computadores do FNDE, permitindo a criação de métricas e/ou alertas;

d) Implementar mecanismos que permitam a avaliação dos danos ocasionados por incidentes de segurança em redes de computadores do FNDE; e

e) Apoiar, incentivar e contribuir com o FNDE para a correta capacitação relativa ao tratamento de incidentes de segurança em redes de computadores.

6.3.4 A ETIR deve observar e adotar, no mínimo, os seguintes aspectos e procedimentos:

a) Registro de incidentes de segurança em redes de computadores: todos os incidentes notificados ou detectados devem ser registrados, com a finalidade de assegurar registro histórico das atividades da ETIR;

b) Tratamento da informação: o tratamento da informação pela ETIR deve ser realizado de forma a viabilizar e assegurar disponibilidade, integridade, confidencialidade e autenticidade da informação, observada a legislação em vigor, naquilo que diz respeito ao estabelecimento de graus de sigilo;

c) Recursos disponíveis: a ETIR deve possuir recursos materiais, tecnológicos e humanos suficientes para prestar os serviços objeto de sua constituição; e

d) Capacitação dos membros da ETIR: os membros da ETIR devem estar capacitados para operar com eficácia e eficiência os recursos disponibilizados.

6.3.5 Durante o gerenciamento de incidentes de segurança em redes de computadores, havendo indícios de ilícitos criminais a ETIR tem como dever:

a) Observar procedimentos técnicos necessários para preservação de evidências; e

b) Priorizar a continuidade dos serviços da ETIR e da missão institucional do FNDE.

6.4 Todos os servidores, colaboradores e partes externas que usam os sistemas de Informação do FNDE devem estar cientes dos procedimentos para a devida notificação dos diversos tipos de incidentes e fragilidade de Segurança da Informação nos sistemas ou serviços corporativos. Esses procedimentos deverão ser disponibilizados pela ETIR.

6.5 O mecanismo de notificação deve ser fácil e acessível.

6.5.1 A estrutura da ETIR do FNDE **a ser construída** deverá, pelo menos, conter os seguintes componentes:

a) Uma metodologia de gestão de ETIR;

b) Orientações para sua implantação;

c) Sua missão institucional;

d) Sua constituição (componentes);

e) Seu detalhamento de serviços, tarefas e ações;

f) Uma classificação de incidentes computacionais;

g) Um formulário para reporte de incidentes computacionais;

h) Ferramentas para limpeza completa de dados;

i) Um procedimento de comunicação da ETIR do FNDE para o CTIR Gov; e

j) Um procedimento de comunicação da ETIR do FNDE em caso de indícios de ilícitos criminais.

7. NOTIFICAÇÃO DE INCIDENTES COMPUTACIONAIS

7.1 Os incidentes computacionais devem ser relatados à Central de Atendimento ao Usuário (CAU) que repassará as informações à ETIR do FNDE. As seguintes situações são exemplos que podem ocasionar notificação:

a) Suspeita de quebra de segurança;

b) Violação da disponibilidade, confidencialidade e integridade da informação;

c) Não conformidade com políticas ou diretrizes;

d) Mau funcionamento de *software* ou *hardware;* e

e) Violação de acesso aos sistemas corporativos.

NOTA: O mau funcionamento ou outro comportamento estranho do sistema pode ser um indicador de um ataque computacional ou violação na segurança atual e, portanto, deve ser reportado como um incidente computacional.

8. APRENDENDO COM OS INCIDENTES COMPUTACIONAIS DE SEGURANÇA DA INFORMAÇÃO

A ETIR deverá:

a) Coletar e armazenar os conhecimentos obtidos da análise e resolução dos incidentes computacionais de segurança da informação para reduzir a probabilidade ou o impacto de incidentes futuros no FNDE;

b) Avaliar o incidente computacional de segurança da informação e indicar a necessidade de melhoria ou controles adicionais para diminuir sua frequência; e

c) Utilizar o histórico de incidentes atuais em treinamentos e conscientização dos usuários.

9. 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.

10. **RESPONSABILIZAÇÃO**

Ao colaborador não é dado o direito de desconhecimento da Política de Segurança da Informação e Comunicações, devendo seguir rigorosamente o proposto nas normas de segurança.

11. **DISPOSIÇÕES GERAIS**

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

a) Comitê de Governança Digital – CGD, com apoio, se necessário, das áreas técnicas do FNDE; e

b) Presidência do FNDE, em decisão final, caso o CGD não tenha autonomia para tomar as providências cabíveis.

12. **VIGÊNCIA E ATUALIZAÇÃO**

12.1 **Este documento entra em vigor em 90 (noventa) dias a partir da data de sua publicação e pode ser atualizada ou revogada 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.

13. **ANEXO "A"**

Categorias de incidentes de segurança da informação de acordo com ameaças.

ANEXO A

CATEGORIAS DE INCIDENTES DE SEGURANÇA DA INFORMAÇÃO DE ACORDO COM AMEAÇAS

Este anexo fornece exemplos de abordagens para a categorização e classificação de incidentes de segurança da informação. Essas abordagens permitem que o FNDE documente incidentes de segurança da informação de maneira consistente, para que os seguintes benefícios sejam alcançados:

a) Promover o intercâmbio e compartilhamento de informações sobre incidentes de segurança da informação;

b) Facilitar a automatização de relatórios e respostas a incidentes de segurança de informações;

c) Melhorar a eficiência e eficácia da gestão e gestão de incidentes de segurança da informação;

d) Facilitar a coleta e análise de dados sobre incidentes de segurança da informação; e

e) Identificar os níveis de gravidade dos incidentes de segurança da informação usando critérios consistentes.

Os incidentes de segurança da informação podem ser causados por ações deliberadas ou acidentais do ser humano, e podem ser causados por meios técnicos ou físicos. A abordagem a seguir classifica os incidentes de segurança da informação, considerando as ameaças como fatores de categorização (para ameaças, ISO / IEC 27005: 2008).

Categoria	Descrição	Tipos
Desastre natural	A perda de segurança da informação é causada por desastres naturais além do controle humano.	Terremoto, vulcão, inundação, vento violento, raios, tsunami, colapso, etc.
Incidente de agitação social	A perda de segurança da informação é causada pela instabilidade da sociedade.	Ataque terrorista, guerra, etc.
Incidente de danos físicos	A perda de segurança da informação é causada por ações físicas deliberadas ou acidentais.	Incêndio, água, ambiente eletrostático, abominável (como poluição, poeira, corrosão, congelamento), destruição de equipamentos, destruição de mídia, roubo de equipamentos, roubo de mídia, perda de equipamentos, perda de mídia, adulteração de equipamentos, adulteração de mídia, etc.
Incidente de falha de infraestrutura	A perda de segurança da informação é causada pelas falhas dos sistemas e serviços básicos que suportam a execução de sistemas de informação.	Falha na fonte de alimentação, falha de rede, falha de ar condicionado, falha no fornecimento de água, etc.
Incidente de perturbação de radiação	A perda de segurança da informação é causada pela perturbação causada pela radiação.	Radiação eletromagnética, pulso eletromagnético, interferência eletrônica, flutuação de voltagem, radiação térmica, etc.
Incidente de falha técnica	A perda de segurança da informação é causada por falhas nos sistemas de informação ou instalações não técnicas relacionadas, bem como problemas não intencionais causados pelo homem, resultando na indisponibilidade ou destruição dos sistemas de informação.	Falha de hardware, mau funcionamento do software, sobrecarga (saturação da capacidade dos sistemas de informação), quebra de manutenção, etc.
Incidente de ataque técnico	A perda de segurança da informação é causada por informações de ataque em Sistemas através de redes ou outros meios técnicos, explorando as vulnerabilidades dos sistemas de informação em configurações, protocolos ou programas, ou pela força, o que resulta em um status anormal dos sistemas de informação ou dano potencial às operações	Varredura de rede, exploração de vulnerabilidade, exploração de backdoor, tentativas de login, interferência, DoS, etc. A varredura de rede faz uso do software de varredura de rede para obter informações sobre configurações de rede, portas, serviços e vulnerabilidades existentes. A exploração da vulnerabilidade explora e faz uso de defeitos no sistema de informações, como configurações,

Categoria	Descrição	Tipos
	atuais do sistema.	protocolos ou programas. A exploração de backdoor faz uso de backdoors ou programas prejudiciais deixados em processos de design de sistemas de software e hardware. As tentativas de login tentam adivinhar, quebrar ou senhas de força bruta. A interferência obstrui redes de computadores, redes de transmissão de rádio e televisão com ou sem fio, ou sinais de rádio e televisão via satélite, por meios técnicos. O DoS é causado pelo uso avassalador do sistema de informações e recursos de rede como CPU, memória, espaço em disco ou largura de banda da rede, afetando assim a operação normal dos sistemas de informação, por exemplo, SYS-a, PING-Inundação, Email bombing.
Incidente de Violação de Regra	A perda de segurança da informação é causada pela violação de regras deliberada ou acidentalmente.	Uso não autorizado de recursos, violação de direitos autorais, etc. O uso não autorizado de recursos acessa recursos para fins não autorizados, incluindo empreendimentos lucrativos, por exemplo, o uso de e-mail para participar de cartas em cadeia ilegais para fins lucrativos ou esquemas de pirâmide. A violação de direitos autorais é causada pela venda ou instalação de cópias de software comercial não licenciado ou outros materiais protegidos por direitos autorais, por exemplo, warez.
Incidente de Comprometimento de Funções	A perda de segurança da informação é causada por comprometer deliberada ou acidentalmente as funções dos sistemas de informação em termos de segurança.	Abuso de direitos, falsificação de direitos, negação de ações, falta de operações, violação da disponibilidade de pessoal, etc. O abuso de direitos usa direitos além dos termos de

Categoria	Descrição	Tipos
		referência. A falsificação de direitos faz falsos direitos para enganar. Negação de ações é quando alguém nega o que fez. Operações incorretas realizam a operação incorreta ou não intencionalmente. A violação da disponibilidade de pessoal é causada pela falta ou ausência de recursos humanos.
Comprometimento do incidente de informação	A perda de segurança da informação é causada por comprometer deliberadamente ou acidentalmente a segurança das informações, como confidencialidade, integridade, disponibilidade, etc.	Interceptação, espionagem, divulgação, engenharia social, phishing de rede, roubo de dados, perda de dados, adulteração de dados, erro de dados, análise de fluxo de dados, detecção de posição etc. A interceptação captura dados antes que seja possível alcançar os destinatários pretendidos Espionar é secretamente coletar e relatar informações sobre as atividades de outra organização. Escutas é escutar a conversa de uma festa externa sem o seu conhecimento. A divulgação é divulgar informações confidenciais publicamente. A engenharia social é manipular psicologicamente as pessoas (de maneira não técnica) para divulgar informações ou realizar ações, por exemplo, mentiras, truques, subornos ou ameaças.

Categoria	Descrição	Tipos
		O phishing de rede consiste em utilizar tecnologia de rede de computadores fraudulenta para induzir os usuários a divulgar informações importantes, como a obtenção de detalhes de contas bancárias e senhas de usuários por e-mails enganosos. Roubar dados. A adulteração de dados é tocar ou fazer alterações nos dados sem autorização. Erro de dados é cometer erros ao imputar ou processar dados. A detecção de posição é para detectar a posição de informações ou sistemas sensíveis.
Incidente de Conteúdo Nocivo	A perda de segurança da informação é causada pela propagação de conteúdo indesejável através de redes de informação, o que põe em perigo a segurança nacional, a estabilidade social e / ou a segurança pública e os benefícios.	Conteúdo ilegal, conteúdo de pânico, conteúdo malicioso, conteúdo abusivo, etc. Conteúdo ilegal é conteúdo publicado que viola constituições, leis e regulamentos nacionais ou internacionais, por exemplo, pornografia infantil, glorificação da violência, falsificação, fraude. Conteúdo de pânico é a discussão maliciosamente sensacionalista ou comentário sobre questões sensíveis na internet, resultando em eventos como turbulência social ou pânico. Conteúdo malicioso é a disseminação de conteúdo que

Categoria	Descrição	Tipos
		ataca maliciosamente pessoas, por exemplo, fraude, assédio. Conteúdo abusivo é a transmissão de conteúdo que não foi concedido por destinatários, por exemplo, spam.
Outros incidentes	Não classificado em nenhuma das categorias de incidentes acima.	-x-

ANEXO VII

FNDE
Fundo Nacional de Desenvolvimento da Educação

TROCA DE INFORMAÇÃO

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

DS-001-2002-SEXEC: Diretrizes de Segurança.

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

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

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

ISO/IEC – 27010:2015 – Information technology – Security techniques – Information security management for inter-sector and inter-organizational communications

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

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

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

Norma Complementar nº 14/IN01/DSIC/GSIPR - Estabelece princípios, diretrizes e responsabilidades relacionados à segurança da informação para o tratamento da informação em ambiente de computação em nuvem nos órgãos e entidades da Administração Pública Federal.

Norma Complementar nº 15/IN01/DSIC/GSIPR – Estabelece diretrizes de Segurança da Informação e Comunicação para o uso de redes sociais na Administração Pública Federal.

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

LEI Nº 12.527, de 18 de NOVEMBRO de 2011 (LAI) - Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990.

LEI Nº 12.965, de 23 de ABRIL de 2014 (Marco Civil) – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

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.

DECRETO Nº 7.724, de 16 de MAIO de 2012 – Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

DECRETO Nº 8.789, de 29 de JULHO de 2016 – Dispõe sobre o compartilhamento de bases de dados na administração pública federal.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-015-2002-SEXEC: Norma de Segurança da troca de informações e softwares do FNDE entre os agentes internos e externos da Autarquia*, publicada em 14 de março de 2003.

APROVAÇÃO

Carlos Alberto Decotelli da Silva
Presidente do FNDE

1. OBJETIVO

Garantir a proteção na troca de informação entre o FNDE e partes externas.

2. DESCRIÇÃO E ESCOPO

Disciplinar as trocas de informação entre os agentes internos e externos à Autarquia de modo que as permutas transcorram em ambiente seguro, possibilitando a preservação da confidencialidade, integridade, disponibilidade e autenticidade das informações.

3. PÚBLICO-ALVO

Esta norma destina-se a todos servidores e colaboradores que realizam trocas de informação entre o FNDE e partes externas.

4. CONCEITOS E DEFINIÇÕES

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

5. PRINCÍPIOS

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

6. DIRETRIZES PARA TROCA DE INFORMAÇÕES

6.1 Toda informação institucional do FNDE armazenada em qualquer suporte, material, área, comunicação e sistema de informação é patrimônio da Autarquia, e deve ser tratada segundo as diretrizes descritas nesta Norma e nos termos da legislação pertinente em vigência.

6.2 Na troca de informação entre o FNDE e partes externas, o tratamento da informação ao longo de seu ciclo de vida deve ser realizado de modo ético e responsável pelos servidores e colaboradores.

6.3 O tratamento da informação deve ser feito conforme os normativos de Segurança da Informação e Comunicação - SIC, assegurado os requisitos da disponibilidade, da integridade, da confidencialidade e da autenticidade da informação em todo seu ciclo de vida.

6.4 O tratamento da informação institucional do FNDE deve observar o disposto na Lei nº 12.527/2011 e nos Decretos nº 7.724/2012 e 7.845/2012.

6.5 É dever dos servidores e dos colaboradores salvaguardar a informação sigilosa e a pessoal, bem como assegurar a publicidade da informação ostensiva, utilizando-as, exclusivamente, para o exercício das atribuições desenvolvidas no FNDE, sob pena de responsabilidade administrativa, civil e penal.

6.6 As medidas e os procedimentos relacionados ao tratamento da informação a ser realizado com apoio de empresa terceirizada, em qualquer fase do ciclo de vida da informação, devem ser estabelecidas contratualmente para que se assegure o cumprimento das diretrizes previstas nesta Norma, bem como nas legislações vigentes.

6.7 O FNDE deve promover ações para conscientização dos servidores e dos colaboradores, segundo a NS 006-CGD-FNDE – Sensibilização, Conscientização e Capacitação em Segurança da Informação e Comunicação, visando à disseminação das diretrizes de tratamento da informação.

6.8 A Autarquia deve identificar o proprietário e o custodiante da informação.

6.9 O proprietário da informação é responsável pelas seguintes atividades:

a) Descrever a informação;

b) Definir as exigências de SIC da informação;

c) Comunicar as exigências de SIC da informação a todos os custodiantes e usuários;

d) Assegurar o cumprimento das exigências de SIC por meio de monitoramento; e

e) Indicar os riscos que podem afetar a informação.

6.10 O custodiante da informação deve aplicar os níveis de controles de segurança conforme as exigências de SIC, comunicadas pelo proprietário da informação, de forma a assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação.

6.11 **Ciclo de Vida da Informação**

6.11.1 O ciclo de vida da informação a ser gerido no FNDE deve ater-se ao conjunto de ações referentes ao tratamento da informação:

a) Produção e Recepção;

b) Organização;

c) Uso e Disseminação; e

d) Destinação.

6.11.1.1 **Produção e Recepção**

6.11.1.2 Os processos de produção, recepção e custódia da informação devem ser planejados e implementados, considerando:

a) Os interesses do FNDE;

b) O período previsto para a retenção da informação; e

c) Os custos com recursos materiais, financeiros e humanos.

6.11.1.3 A informação produzida e custodiada pelo FNDE deve ser mantida disponível e acessível aos servidores e colaboradores para o desempenho de suas atribuições.

6.11.1.4 O FNDE deve verificar se a informação produzida, recebida ou custodiada se enquadra em quaisquer hipóteses de sigilo, a fim de adotar as medidas cabíveis quanto ao seu tratamento (Anexo A).

6.11.1.5 O FNDE deve garantir que a produção, a recepção e a custódia de informação sejam feitas com a devida proteção da informação pessoal (Anexo A).

6.11.1.6 Nas reuniões em que são produzidas e recebidas informações sigilosas e pessoais, devem ser adotados controles de segurança para acesso ao ambiente, aos documentos, as anotações, as mídias e aos demais recursos utilizados.

6.11.1.7 Quando a produção, recepção e custódia de informação sigilosa e pessoal exigir impressão em tipografias, impressoras, oficinas gráficas ou similares, a operação deve ser acompanhada por pessoa oficialmente designada, responsável pelas medidas de salvaguarda necessárias à garantia do sigilo durante todo o processo.

6.11.1.8 Quando a produção, recepção e custódia de informação sigilosa (em qualquer grau de sigilo) exigir impressão em tipografias, impressoras, oficinas gráficas ou similares, a operação deve ser acompanhada por pessoa credenciada, ou excepcionalmente, que tenha assinado o Termo de Compromisso de Manutenção de Sigilo (TCMS), de acordo com a Lei 12.527/2011- Lei de Acesso à Informação (LAI).

6.11.1.9 O registro da documentação produzida nos termos dos itens 6.11.1.7 e 6.11.1.8 deve descrever o conteúdo do documento incluir número sequencial de identificação, sua origem, ano de produção, assunto, classificação e indicação de sigilo.

6.11.1.10 Para toda informação classificada, em qualquer grau de sigilo, o FNDE deve adotar o código de Indexação de Documento que contém Informação Classificada (CIDC), de acordo com Lei 12.527/2011- Lei de Acesso à Informação (LAI).

6.11.1.11 As informações classificadas devem ser produzidas e custodiadas utilizando criptografia baseada em algoritmo de Estado compatível com o grau de sigilo, conforme padrões mínimos estabelecidos na norma NC 09 DSIC/GSI/PR - Uso de recursos criptográficos em Segurança da Informação e Comunicações.

6.11.2 **Organização**

6.11.2.1 O armazenamento, arquivamento e controle da informação devem considerar:

a) As características físicas do suporte e do ambiente;

b) O volume de informação produzida e sua estimativa de crescimento;

c) O período previsto para a retenção da informação;

d) A proteção contra incidentes de SIC;

e) As eventuais necessidades de classificação e preservação da informação conforme atos normativos correlatos;

f) As perdas por destruição, furto ou sinistro;

g) A frequência de uso; e

h) Os custos inerentes aos processos de armazenamento, arquivamento e controle da informação.

6.11.2.2 É dever do servidor a manutenção dos registros de documento formal utilizado como fundamento para tomada de decisão ou de ato administrativo.

6.11.2.3 O armazenamento de informação classificada em grau de sigilo secreto ou ultrassecreto deve ser realizado em cofre ou estrutura que ofereça segurança equivalente.

6.11.2.4 Informações sigilosas e pessoais devem ser armazenadas e arquivadas em ambiente com acesso restrito e controlado.

6.11.2.5 A informação deve ser armazenada em servidores de arquivos e sistemas corporativos instalados em ambiente seguro.

6.11.2.6 Devem ser estabelecidas ações de Segurança da Informação e Comunicação para a Gestão de Continuidade de Negócio (GCN).

6.11.3 **Uso e Disseminação**

6.11.3.1 A utilização, o acesso, a reprodução, o transporte, a transmissão e a distribuição da informação devem seguir:

6.11.3.1.1 Os princípios da disponibilidade, integridade, confidencialidade e autenticidade, conforme normativos de SIC e legislação pertinente vigente; e

6.11.3.1.2 As orientações específicas que garantam a salvaguarda de informação sigilosa e pessoal, bem como a divulgação de informação ostensiva.

6.11.3.2 A informação a ser disponibilizada por meio da transparência ativa e passiva deve ser objeto de prévia análise, a fim de identificar se há parcela da informação com restrição de acesso.

6.11.3.3 Os recursos de Tecnologia da Informação e Comunicação (TIC) disponibilizados ao público devem ser isolados da rede corporativa.

6.11.3.4 No transporte, transmissão e distribuição de documentos em suporte físico que for realizado por empresa terceirizada, cabe ao FNDE estabelecer contratualmente as medidas e procedimentos de SIC adequados.

6.11.3.5 É vedada a expedição de documento ultrassecreto por meio postal.

6.11.4 **Destinação**

6.11.4.1 Deve ser constituída a Comissão Permanente de Avaliação de Documentos (CPAD).

6.11.4.2 Deve ser constituída a Comissão Permanente de Avaliação de Documentos Sigilosos (CPADS).

6.11.4.3 A disponibilidade, integridade, confidencialidade e autenticidade devem ser observadas na avaliação, destinação, arquivamento ou eliminação da informação, conforme legislação pertinente vigente.

6.11.4.4 A destinação de informação que conste de sítios eletrônicos institucionais e de repositórios internos do FNDE deve seguir as determinações das legislações vigentes.

6.11.4.5 Na eliminação efetiva da informação em meio eletrônico deve ser realizada sanitização dos dados nas mídias de armazenamento, tais como dispositivos móveis, discos rígidos, memórias das impressoras, *scanners* e multifuncionais antes do descarte.

6.11.5 Implementação

6.11.5.1 Adotar mecanismos de gestão dos processos e procedimentos envolvidos no tratamento da informação ao longo do ciclo de vida.

6.11.6 **Planejamento**

6.11.6.1 A Alta Administração do FNDE deve assegurar que a Política de Segurança da Informação e Comunicações (POSIC) estabeleça diretrizes gerais de tratamento da informação ao longo do ciclo de vida.

6.11.6.2 As normas e procedimentos internos de tratamento da informação devem ser elaborados com participação do Gestor de Segurança da Informação e Comunicação do FNDE, aprovados no âmbito respectivo do Comitê de Segurança da Informação e Comunicação, e submetidos à Alta Administração para aprovação e publicação.

6.11.6.3 Devem ser identificadas, em normativos internos, ações necessárias ao aprimoramento do processo de tratamento da informação a serem implementadas na etapa de execução.

6.11.7 **Execução**

6.11.7.1 As normas e procedimentos internos de tratamento da informação devem garantir a sua implementação em todo ciclo de vida da informação, observando:

a) Promoção de capacitação;

b) Mudança de cultura;

c) Estímulo de boas práticas em todas as fases do ciclo de vida da informação; e

d) Adoção de metodologias e tecnologias adequadas e atuais.

6.11.8 **Avaliação**

6.11.8.1 Avaliar, periodicamente, o processo de tratamento da informação, identificando as revisões e as alterações pertinentes.

6.11.8.2 Posteriormente, elaborar os ajustes e as alterações cabíveis ao processo de tratamento da informação instituído.

6.11.9 **Ações de Melhoria**

6.11.9.1 As ações de melhoria devem ser desenvolvidas continuamente.

6.11.10 Responsabilidades

6.11.10.1 Cabe à Alta administração do FNDE, no âmbito de suas atribuições aprovar as diretrizes estratégicas de SIC que norteiam o tratamento da informação.

6.11.10.2 Cabe ao Gestor de SIC, no âmbito de suas atribuições no Comitê de Segurança da Informação e Comunicação, propor, avaliar, realizar periódica análise de melhorias de normas e procedimentos internos de tratamento da informação.

7. CONEXÃO DE REDES DE TERCEIROS À REDE CORPORATIVA

7.1 É proibida a conexão de redes de terceiros com a rede corporativa sem a autorização da Área de TI.

7.2 Antes da conexão da rede de terceiros com a rede corporativa, deve ser realizada análise de riscos a fim de identificar possíveis vulnerabilidades capazes de expor as informações institucionais às pessoas não autorizadas, bem como os impactos provenientes deste acesso.

7.3 Os usuários externos somente poderão ter acesso aos serviços que tenham sido autorizados pela Área de TI.

7.4 Elaborar regras relativas ao uso de redes e serviços por usuários externos, observando:

a) Redes e serviços com acesso permitido;

b) Procedimentos de autorização de acesso às redes e serviços;

c) Gerenciamento dos controles e procedimentos para proteger o acesso a conexões e serviços de redes; e

d) Os meios de comunicação que serão usados para acessar redes e serviços.

7.5 A rede corporativa deve ser segregada em perímetros para facilitar o controle e a monitoração dos acessos de usuários externos.

7.6 As conexões de redes de terceiros devem ser realizadas somente em perímetros específicos autorizados para este fim.

7.7 Todas as conexões de terceiros à rede corporativa devem ser precedidas da assinatura do Termo de Responsabilidade.

8. OPÇÕES DE CONECTIVIDADE

8.1 As conexões de redes de terceiros à rede corporativa devem obedecer aos seguintes padrões, salvo exceções que serão analisadas pela Área de TI:

8.1.1 **Conexão direta**: as conexões diretas devem ser implementadas nos segmentos específicos para conexão de redes de terceiros. Devem ser implementados controles de segurança para garantir que os acessos à rede corporativa, por meio de redes de terceiros, sejam realizados somente nestes segmentos.

8.1.2 **Rede Virtual Privada (VPN)**: as conexões diretas devem terminar no segmento específico destinado para redes de terceiros, segundo a norma NS022-CGD-FNDE - Trabalho Remoto.

8.1.3 **Acesso remoto**: devem ser realizados somente após autenticação e autorização no segmento de redes designado para conexão de redes de terceiros, segundo a norma NS022-CGD-FNDE – Trabalho Remoto.

8.2 **Autenticação de Conexão de Redes de Terceiros**

8.2.1 Todas as conexões de rede de terceiros à rede corporativa devem passar por processo de autorização, autenticação, controle e auditoria pela Área de TI.

8.3 **Proteção de Informação Restrita**

8.3.1 A equipe responsável pela instalação de redes de terceiros à rede corporativa deve garantir que todas as medidas de segurança foram tomadas para proteger a integridade, a confidencialidade e a disponibilidade das informações.

8.3.2 Implementar dispositivos de firewall para filtro, controle e gerenciamento do tráfego de dados entre a rede corporativa e a rede de terceiros a fim de proteger as informações.

9. SERVIÇOS DE REDE

9.1 Serviços de rede que podem ser disponibilizados aos usuários externos:

a) **Troca de arquivos via FTP**: a troca de arquivos deve ser realizada via FTP nos servidores destinados para este fim;

b) **Acesso via SSH**: acessos por meio de SSH a servidores específicos da rede corporativa podem ser disponibilizados a usuários externos, desde que autorizados e de forma controlada por lista de controle de acesso, rotas estáticas ou qualquer outro modo de controle;

c) **Acesso a sistemas web**: os acessos a sistemas web internos somente devem ser fornecidos aos usuários externos quando formalmente justificados, homologados e autorizados;

d) **Acesso ao repositório de códigos fonte de sistemas**: **-** esse tipo de acesso deve ser analisado e, se for o caso, autorizado pelos proprietários dos ativos de informação; e

e) **Acesso a bancos de dados**: esse tipo de acesso deve ser provido com devida autorização dos proprietários dos ativos de informação: bases de dados e sistemas.

10. POLÍTICAS E PROCEDIMENTOS PARA TROCA DE INFORMAÇÃO

10.1 Estabelecer políticas, procedimentos e controles de transferência formal para proteger a transferência de informação, por meio do uso de todos os tipos de recursos de comunicação.

10.2 Estabelecer os seguintes procedimentos e controles para a troca de informação em recursos eletrônicos de comunicação:

a) Procedimentos para proteger a informação transferida contra interceptação, cópia, modificação, desvio e destruição;

b) Procedimentos para detecção e proteção contra código malicioso que pode ser transmitido através do uso de recursos eletrônicos de comunicação, de acordo com a norma NS008-CGD-FNDE – Proteção Contra Códigos Maliciosos;

c) Procedimentos para proteção de informações eletrônicas sensíveis transmitidas na forma de anexos, de acordo com a norma NS011-CGD-FNDE – Administração do Correio Eletrônico;

d) As responsabilidades de servidores, colaboradores, fornecedores e partes externas que possam comprometer o FNDE;

e) Uso de técnicas de criptografia para proteger a confidencialidade, a integridade e a autenticidade das informações;

f) Retenção e descarte de toda correspondência de negócios, incluindo mensagens, de acordo com a Lei 12.527/2011- Lei de Acesso à Informação (LAI);

g) Controles e restrições associados à retransmissão através de recursos de comunicação como a retransmissão automática de mensagens eletrônicas (*e-mails*) para endereços externos, conforme a norma NS011-CGD-FNDE – Administração do Correio Eletrônico;

h) Orientar os usuários para não revelar, em hipótese alguma, informações confidenciais; e

i) Não deixar informações críticas ou sensíveis em secretárias eletrônicas.

10.3 Os usuários não devem revelar informações classificadas como Reservadas, Secretas e Ultrassecretas, conforme o disposto na Lei 12.527/2011- Lei de Acesso à Informação (LAI), de forma digital, escrita e falada para evitar que sejam captadas ou interceptadas por pessoas não autorizadas.

10.4 **Computação em nuvem**

Caso o FNDE venha a adotar computação em nuvem, por decisão estratégica, deverá observar as diretrizes estabelecidas na sua Política de Segurança da Informação e Comunicação.

10.4.1 Ao contratar ou implementar um serviço de computação em nuvem, o usuário deve assegurar que:

a) O ambiente de computação em nuvem, sua infraestrutura e canal de comunicação estejam aderentes às diretrizes e normas de Segurança da Informação e Comunicação, estabelecidas pelo Gabinete de Segurança Institucional da Presidência da República (GSIPR); e

b) O contrato de prestação de serviço contenha cláusulas relevantes que garantam a disponibilidade, a integridade, a confidencialidade e a autenticidade das informações hospedadas na nuvem, em especial aquelas sob custódia e gerenciamento do prestador de serviço.

10.4.2 Avaliar as informações que serão hospedadas na nuvem, considerando:

a) O processo de classificação da informação de acordo com as normas internas, o contrato e a legislação vigente;

b) O valor do ativo de informação;

c) Os controles de acesso físicos e lógicos relativos à Segurança da Informação e Comunicação;

d) O modelo de serviço e de implementação de computação em nuvem a serem adotados; e

e) A localização geográfica onde as informações serão fisicamente armazenadas.

10.5 **Acordos de Confidencialidade e não Divulgação**

10.5.1 Os requisitos para acordos de confidencialidade e de não divulgação que reflitam as necessidades do FNDE para a proteção da informação devem ser identificados, analisados criticamente e documentados.

10.5.2 Os acordos de confidencialidade e de não divulgação devem considerar os requisitos para proteger as informações confidenciais, nos termos da legislação vigente.

10.5.3 Para identificar os requisitos para os acordos de confidencialidade ou de não divulgação, considerar:

a) A definição da informação a ser protegida (confidencial);

b) O prazo do acordo, incluindo situações onde a confidencialidade tenha que ser mantida indefinidamente;

c) Ações requeridas quando do encerramento de um acordo;

d) Responsabilidades e ações dos signatários para evitar a divulgação não autorizada da informação;

e) O proprietário da informação, segredos comerciais, de propriedade intelectual e a relação com a proteção da informação confidencial;

f) O uso permitido da informação confidencial e os direitos do signatário para usar a informação;

g) O direito de auditar e monitorar as atividades que envolvam as informações confidenciais;

h) O processo para notificação e o relato de divulgação não autorizada ou vazamento das informações confidenciais;

i) Termos para a informação ser retornada ou destruída quando do término do acordo;

j) Ações a serem tomadas no caso de violação do acordo.

10.6 **Acordos para Transferência de Informações**

10.6.1 A troca de informações e de arquivos de programas (eletrônica ou manual) deve ser estabelecida mediante acordos, nos quais constem os requisitos de segurança e o nível de classificação das informações envolvidas na permuta.

10.6.2 Os acordos devem ser formais, principalmente quando se tratar de informações classificadas como Reservadas, Secretas e Ultrassecretas.

10.6.3 As condições de segurança descritas nos acordos devem considerar:

a) Responsabilidades pelo controle e comunicação de transmissões, expedições e recepções;

b) Procedimentos para assegurar a rastreabilidade dos eventos e o não repúdio;

c) Padrões técnicos mínimos para embalagem e transmissão;

d) Acordos para procedimentos de custódia;

e) Normas para identificação de portadores;

f) Responsabilidades e obrigações na ocorrência de incidentes de segurança da informação (perda de dados);

g) Acordo de utilização de um sistema de identificação para informações críticas e sensíveis, garantindo que o significado dos rótulos seja imediatamente entendido e a devida proteção da informação, conforme o disposto na Lei 12.527/2011- Lei de Acesso à Informação (LAI);

h) Normas técnicas para a gravação e leitura de informações e *software* de acordo com a norma NS018-CGD-FNDE - Garantia da Integridade e da Disponibilidade das Informações;

i) Controles especiais para proteção de itens sensíveis, como chaves criptográficas;

j) Manutenção de uma cadeia de custódia enquanto a informação estiver em trânsito; e

k) Níveis aceitáveis de controle de acesso à informação.

10.7 **Mídias em Trânsito**

10.7.1 As mídias contendo informações devem ser protegidas contra acesso não autorizado, uso impróprio ou corrupção durante o transporte, considerando as seguintes recomendações:

a) O meio de transporte ou o serviço de mensageiros devem ser confiáveis;

b) Definir uma relação de portadores autorizados em concordância com o gestor;

c) Estabelecer um procedimento para a verificação da identificação dos transportadores;

d) A embalagem deve ser suficiente para proteger o conteúdo contra qualquer dano físico; e

e) Guardar os registros (*logs*), identificando o conteúdo da mídia, a proteção aplicada, bem como o tempo de deslocamento entre o custodiante e o destino final.

11. SISTEMAS DE INFORMAÇÕES DO NEGÓCIO

11.1 Para a disponibilização e manuseio de recursos envolvidos em sistemas de informação:

a) Identificar às vulnerabilidades da informação nos sistemas de informação;

b) Adotar políticas específicas e controles apropriados para gerenciamento de recursos, com compartilhamento de informações;

c) Observar a classificação das informações a fim de evitar que transitem em sistemas de informação que não tenham o nível de proteção adequado;

d) Observar as regras de classificação da informação de modo a assegurar restrição de acesso, conforme categoria ou grupos específicos de usuários.

e) Manter no sistema a geração e retenção de arquivos de cópia da informação; e

f) Definir requisitos e acordos de recuperação e contingência.

12. COMPARTILHAMENTO DE BASES DE DADOS

12.1 O FNDE deverá disponibilizar sua base de dados oficial aos órgãos e às entidades da administração pública federal direta, autárquica e fundacional interessados no acesso aos dados sob a sua gestão, nos termos:

a) Ficam excluídos os dados protegidos por sigilo fiscal sob gestão da Secretaria Federal do Brasil; e

b) Permanecem vigentes os mecanismos de compartilhamento de dados estabelecidos por acordos voluntários entre os órgãos e entidades.

12.2 O acesso a dados de que trata o item 12.1 tem como finalidades:

a) A simplificação da oferta de serviços públicos;

b) A formulação, a implementação, a avaliação e o monitoramento de políticas públicas;

c) A análise de regularidade da concessão ou do pagamento de benefícios, ou da execução de políticas públicas; e

d) A melhoria da qualidade e da fragilidade dos dados constantes das bases dos órgãos e das entidades.

12.3 Os dados cadastrais sob gestão do FNDE tratados no item 12.1 serão compartilhados entre as bases de dados oficiais, preferencialmente de forma automática.

12.3.1 Consideram-se dados (identificadores) cadastrais junto a órgãos públicos:

a) Número do Cadastro de Pessoas Físicas – CPF;

b) Cadastro Nacional de Pessoas Jurídicas – CNPJ;

c) Número de Identificação Social – NIS;

d) Programa Integração Social – PIS;

e) Programa de Formação do Patrimônio do Servidor Público – Pasep;

f) Título de eleitor;

g) Razão social, data de constituição, tipo societário, composição societária, Classificação Nacional de Atividades Econômicas – CNAE e outros dados públicos de pessoa jurídica ou empresa individual;

h) Nome civil e/ou social de pessoas naturais, data de nascimento, filiação, naturalidade, nacionalidade, sexo, estado civil, grupo familiar, endereço; e

i) Vínculos empregatícios.

12.4 É dispensada a celebração de convênio, acordo de cooperação técnica ou ajustes congêneres para a efetivação do compartilhamento das bases de dados caso seja pertinente.

12.5 Com relação ao acesso a dados e informações compartilhados se faz necessário observar as normas e os procedimentos específicos que garantam a segurança, proteção e confidencialidade.

12.6 O acesso a bases de dados será solicitado ao FNDE, com as seguintes informações:

a) Data da solicitação;

b) Identificação do solicitante;

c) Telefone e endereço eletrônico institucional do solicitante;

d) Descrição clara dos dados objeto da solicitação, incluindo periodicidade; e

e) Descrição das finalidades de uso dos dados.

12.6.1 O responsável pela base de dados deverá manifestar-se quanto à solicitação em até 20 (vinte) dias.

NOTA: As informações recebidas não poderão ser transmitidas a outros órgãos ou entidades, exceto quando previsto expressamente na autorização concedida pelo responsável pela base de dados do FNDE.

13. PENALIDADES

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

14. RESPONSABILIZAÇÃO

14.1 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.

14.2 **Disposições Gerais**

14.3 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.

15. VIGÊNCIA E ATUALIZAÇÃO

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

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

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

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

15.3 **Condições obrigatórias de atualização do documento**

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

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

c) 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).

15.4 **Responsável pela atualização**

15.4.1 Conforme Mapa de Responsabilidades.

16. ANEXO

16.1.1 Anexo A – Quadro Exemplificativo de Tipos de Informação.

16.1.2 Anexo B – Termo de Compromisso de Manutenção de Sigilo (TCMS).

ANEXO A

QUADRO EXEMPLIFICATIVO DE TIPOS DE INFORMAÇÃO

TIPO	DESCRIÇÃO
1. OSTENSIVA	Transparência Ativa
	Transparência Passiva
2. SIGILOSA CLASSIFICADA EM GRAU DE SIGILO	2.1 **Reservada** – Prazo máximo de restrição de acesso de 5 anos
	2.2 **Secreta** – Prazo máximo de restrição de acesso de 15 anos
	2.3 **Ultrasecreta** – Prazo de restrição de acesso de 25 anos, prorrogável por uma única vez, e por período não superior a 25 anos, limitado ao máximo de 50 anos o prazo total da classificação.
3. SIGILOSA PROTEGIDA POR LEGISLAÇÃO ESPECÍFICA (As hipóteses legais de restrição de acesso à informação elencadas neste item não são exaustivas)	3.1 **Sigilos Decorrentes de Direitos de Personalidade**
	3.1.1 Sigilo Fiscal
	3.1.2 Sigilo Bancário
	3.1.3 Sigilo Comercial
	3.1.4 Sigilo Empresarial
	3.1.5 Sigilo Contábil
	3.2 **Sigilos de Processos e Procedimentos**
	3.2.1 Acesso a Documento Preparatório
	3.2.2 Sigilo do Procedimento Administrativo Disciplinar em Curso
	3.2.3 Sigilo do Inquérito Policial
	3.2.4 Segredo de Justiça no Processo Civil
	3.2.5 Segredo de Justiça no Processo Penal
	3.3 **Informação de Natureza Patrimonial**
	3.3.1 Segredo Industrial
	3.3.2 Direito Autoral e Propriedade Intelectual de Programa de Computador
	3.3.3 Propriedade Industrial
4. PESSOAL	**4.1 Pessoal** – Prazo máximo de restrição de acesso 100 anos, independente de classificação de sigilo e quando se referir à intimidade, vida privada, hora e imagem das pessoas.

ANEXO B

TCMS
MODELO DE TERMO DE COMPROMISSO DE MANUTENÇÃO E SIGILO

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

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

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

Reconheço que, em razão das minhas atividades junto ao FNDE, estabeleço contato com informações sigilosas que não podem ser divulgadas a terceiros não autorizados, conforme orientação da POSIC estabelecida.

Reconheço também que, ao término da minha relação de trabalho, devo entregar todo e qualquer material de propriedade da autarquia como, por exemplo, equipamentos portáteis, arquivos envolvendo informações pertencentes à instituição, documentos e processos de qualquer natureza que tenham sido usados, criados ou estado sob meu controle, entre outros.

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

Afirmo que adotarei as obrigações citadas neste documento, mesmo após o término da minha relação de trabalho com a organização.

[Local], ___ de _____ de _____.

_____
Nome e unidade organizacional: [Agente Público]
Matrícula

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

Testemunhas:

_____

_____

ANEXO VIII

GARANTIA DA INTEGRIDADE E DA DISPONIBILIDADE DA INFORMAÇÃO

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

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

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

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

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

ABNT NBR 11515:2007 – Guia de práticas para segurança física relativa ao armazenamento de dados.

ABNT NBR 15247:2004 – Unidades de armazenagem segura – Salas-cofre e cofres para hardware – Classificação e métodos de ensaio de resistência ao fogo.

ISO/IEC 27040 – Information technology – Security techniques – Storage security

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

Norma Complementar nº 09/IN01/DSIC/GSIPR, (Revisão 02) – Estabelece orientações específicas para o uso de recursos criptográficos em Segurança da Informação e Comunicações, nos órgãos ou entidades da Administração Pública Federal (APF), direta e indireta.

LEI Nº 12.527, de 18 de NOVEMBRO de 2011 (LAI) - Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990.

DECRETO Nº 7.724, DE 16 DE MAIO DE 2012 – Regulamenta a Lei no 12.527, de 18 de novembro de 2011, que dispõe sobre o acesso a informações previsto no inciso XXXIII do caput do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição.

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.

LEI Nº 8.159, DE 08 DE JANEIRO DE 1991 – Dispõe sobre a política nacional de arquivos públicos e privados e dá outras providências.

DECRETO Nº 4.073, DE 3 DE JANEIRO DE 2002 – Regulamenta a Lei nº 8.159, de 8 de janeiro de 1991, que dispõe sobre a política nacional de arquivos públicos e privados.

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

SP 800-88 Rev. 1Guidelines for Media Sanitization

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-018-2002-SEXEC: Norma de Segurança para a garantia da integridade e disponibilidade dos ativos*, publicada em 14 de março de 2003.

APROVAÇÃO

Carlos Alberto Decotelli da Silva
Presidente do FNDE

1. OBJETIVO

Assegurar a integridade e a disponibilidade das informações.

2. DESCRIÇÃO E ESCOPO

Estabelecer procedimentos para execução, armazenamento e transporte de cópias de segurança das informações mantidas em meio eletrônico.

3. PÚBLICO-ALVO

Esta norma destina-se a todos os servidores e colaboradores responsáveis pelo armazenamento, transporte e cópia de segurança das informações.

4. CONCEITOS E DEFINIÇÕES

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

5. PRINCÍPIOS

Esta Política de Segurança da Informação e Comunicação está fundamentada nos princípios da disponibilidade, da integridade, da confidencialidade e da autenticidade, visando à proteção e preservação das informações necessárias às atividades do FNDE.

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

6.1 Toda informação gerada no FNDE deve ser protegida para que não seja alterada, acessada ou eliminada indevidamente.

6.2 Toda informação considerada desnecessária para as atividades da Autarquia deve ser devidamente descartada, de modo a impedir sua parcial ou total restauração não autorizada.

6.3 Toda informação, custodiada pela área de tecnologia, considerada crítica para a execução das atividades do FNDE deve possuir cópia de segurança (*backup*) e ser armazenada em local protegido, compatível com o grau de segurança necessário.

6.4 Todo acesso a *logs* de banco de dados ou sistemas deve ser controlado e configurado apenas para consulta de equipes autorizadas.

7. NECESSIDADE DE SANITIZAÇÃO ADEQUADA DE MÍDIA DE ARMAZENAMENTO E DESCARTE DE INFORMAÇÃO

7.1 Toda mídia que contém informações consideradas sensíveis ao trabalho da Autarquia ou relativa a dados pessoais deve ser devidamente sanitizada.

7.2 A sanitização deverá ser realizada de modo a impossibilitar qualquer recuperação parcial ou total de informações armazenadas em meio magnético.

8. CÓPIA DE ARQUIVOS (*BACKUP*) E SEGURANÇA

8.1 As cópias que contenham arquivos ou dados confidenciais do órgão deverão ser criptografadas e protegidas por senha.

8.2 O acesso à informação e ao dado mantido em cópia (*backup*) deverá ser controlado e auditado de forma regular pela área de tecnologia da informação.

8.3 A solução deverá ser implementada para garantir rastreabilidade, auditoria e inspeção do acesso, manuseio, cópia, transferência e descarte das informações custodiadas pela área de TI.

8.4 CÓPIAS (*BACKUPS*) – ORIENTAÇÕES:

8.4.1 As cópias realizadas pela área de TI deverão observar as seguintes orientações:

8.4.1.1 Deverá estabelecer:

a) Horário para a execução do serviço;

b) Periodicidade de execução;

c) Quantidade de cópias necessárias para manter disponível a informação;

d) Tempo de retenção das cópias armazenadas;

e) Organização das cópias por:

i. Data;

ii. Tipo de cópia (completa, diferencial e incremental).

8.4.1.2 Toda alteração, inclusão e exclusão de informação dos serviços de *Backup* deverá ser, oficialmente, comunicada pela área demandante para área de TI, a fim de se executar o serviço de cópia apenas de informação pertinente e necessária à execução dos serviços da Autarquia. Não deverá ser feita cópia de informação não necessária às atividades do FNDE.

NOTA1: A área de Tecnologia da Informação deverá realizar levantamento completo das informações custodiadas em suas bases de *Backup* a fim de eliminar o serviço de cópia de dados e informações consideradas inúteis e não válidas às atividades da Autarquia.

NOTA2: Os procedimentos documentados para execução e gerenciamento de cópias devem ser elaborados e, periodicamente, revistos e atualizados, a fim de atender as orientações da POSIC do FNDE e as necessidades da Autarquia.

NOTA3: Para aplicações e informações consideradas críticas (de acordo com análise de riscos pertinente), a área de TI deverá gerar tantas cópias quanto necessário para reter, com segurança, as informações e as aplicações importantes.

8.5 **ARMAZENAMENTO E MÍDIAS DE RETENÇÃO DE DADOS**

8.5.1 Todas as cópias de informações e de sistemas críticos do FNDE deverão ser armazenadas em ambiente seguro. As cópias deverão ser replicadas para sítios externos de armazenamento considerados protegidos e disponíveis para acionamento dentro da janela de restauração avaliada e autorizada pelo FNDE.

NOTA1: As cópias mantidas no ambiente externo deverão ser armazenadas em regime de custódia, em organização comprovadamente dotada de condições de atendimento aos requisitos de proteção e armazenamento compatíveis com a solução de segurança de mercado denominada *Off Site Data Protection.*

NOTA2: Tanto o local no FNDE onde se armazena as informações copiadas quanto o local externo utilizado para armazenamento deverão apresentar proteção adequada para os seguintes problemas:

a) Incêndio (dentro e fora do local), e suas consequências: gases e partículas, calor, desmoronamento, alagamento e corrosão;

b) Explosão, considerada em relação ao ambiente externo;

c) Intempéries (raio, vendaval, granizo);

d) Água (vazamento, transbordamento) e outros líquidos;

e) Impacto de veículos ou aeronaves;

f) Falta de energia, curtos-circuitos, variações de tensão e outros eventos que podem resultar em danos elétricos;

g) Atos ilícitos (roubo, assalto, desvio, sabotagem);

h) Descarga eletrostática;

i) Emissões eletromagnéticas (luz, raios-X, raios-gama);

j) Campos magnéticos;

k) Umidade, fungos;

l) Roedores, insetos;

m) Poeira;

n) Vibração;

o) Agentes químicos;

p) Disparo de armas de fogo.

q) Infraestrutura/elétrica:

   i. Proteção contra descargas elétricas;

   ii. Energia (disponibilidade e qualidade).

r) Climatização:

i. Controle da temperatura;

ii. Controle da umidade do ar nos locais de armazenamento;

iii. Renovação do ar;

iv. Riscos inerentes ao sistema de armazenamento.

s) Móveis, utensílios, equipamentos:

i. Inflamáveis;

ii. Riscos de ignição.

t) Medidas, sistemas de controle de acesso e barreiras de segurança;

u) Sistemas de detecção e combate a incêndio, alagamento e outros sinistros.

8.5.2 As mídias de armazenamento a serem utilizadas pelo FNDE deverão observar e atender as tabelas I e II (discos, fitas magnéticas, memórias Flash, RAM, etc.).

Tabela I – Condições Ambientais para Discos, Rígidos e Fitas

Situação	**Temperatura**	**Umidade relativa**	**Partículas no ar Max. nº por m³ (M = milhão)**
Condições ideais - Mín. /Max. - Variação (±)	+ 17 ºC / + 23 ºC Max. 2 ºC por hora	45 % / 55 % Max. 5% por 24 h	< 5 µm: o mínimo > 5 µm: isento
Limites normais - Transporte (Mín. /Máx.) - Operação (Mín/Máx.) - Variação (±)	+ 5 ºC / + 32 ºC [a] + 16 ºC / + 32 ºC máx. 10 ºC por hora	20 % / 60 % 20 % / 60 % máx. 5 % por 24 h	> 0,5 µm: 30 000 > 5 µm: 01
Limites de emergência	+ 75 ºC	85 %	[b]

[a] Fita virgem pode ser exposta a + 48 ºC.
[b] Fita – Contaminação por partículas pode ser resolvida por processo de saneamento, desde que haja corrosão (fuligem, ácido).

Tabela II – Condições Ambientais para Discos flexíveis, Óticos, memórias Flash e RAM

Situação	**Temperatura**	**Umidade relativa**	**Partículas no ar Max. nº por m³ (M = milhão)**
Condições ideais - Mín. /Max. - Variação (±)	+ 17 ºC / + 23 ºC Máx. 2 ºC por hora	45 % / 55 % Máx. 5% por 24 h	< 0,5 µm: 30 000 > 5 µm: 01

Limites normais - Arquivo (Mín. /Máx.) - Transporte (Mín/Máx.) - Operação (Mín. /Máx.) - Variação (±)	 + 4 ºC / + 15,5 ºC - 40 ºC / + 51,5 ºC + 10 ºC / + 51,5 ºC Máx. 20 ºC	 8 % / 65 % 8 % / 65 % 30 % / 65 % Sem restrição	 > 0,3 µm: 540 M > 0,5 µm:85 M > 1,0 µm: 8M > 5 µm: 25 000
Limites de emergência	+ 75 ºC	85 %	[b]

[a] Fita virgem pode ser exposta a + 48 ºC.
[b] Fita – Contaminação por partículas pode ser resolvida por processo de saneamento, desde que haja corrosão (fuligem, ácido).

9. RESTAURAÇÃO DE MÍDIAS DE ARMAZENAMENTO

9.1 Os procedimentos para efetiva restauração de mídias de armazenamento deverão ser revistos periodicamente, de acordo com as necessidades da POSIC e do FNDE.

9.2 A restauração dos dados deverá ser efetuada rapidamente e de forma eficiente para que os serviços não permaneçam inativos por longo período de tempo.

9.3 O processo de restauração deverá observar:

a) Criticidade da informação;

b) Prioridade;

c) Tipo de restauração (simples ou completa); e

d) Horário para restauração.

NOTA1: Toda restauração de dado e informação deverá obedecer à solicitação oficial encaminhada pela área demandante e deverá conter todas as orientações necessárias para a devida restauração.

NOTA2: Toda mídia replicada para ambiente externo deverá obedecer aos procedimentos previamente orientados pelo FNDE a fim de garantir segurança adequada bem como velocidade de restauração apropriada por esse canal utilizado.

NOTA3: Toda restauração deverá ser gerenciada pela área pertinente de TI, conforme a solicitação seja de dado e informação corporativos ou de arquivos de sistemas operacionais ou de banco de dados.

10. TESTE DE INTEGRIDADE DAS MÍDIAS DE ARMAZENAMENTO

10.1 Toda mídia de armazenamento de serviços de *backup* deverá passar por testes para assegurar a integridade do conteúdo dessas mídias. Estes testes deverão ser realizados antes da entrada dessas mídias em operação. Caso a mídia apresente defeito, esta deverá ser desconsiderada para uso corporativo.

10.2 Testes de integridade deverão ser realizados, periodicamente, nos meios de armazenamento dos ambientes locais e externos.

10.3 Os testes realizados deverão gerar *logs* para futura checagem técnica, auditoria e inspeção.

11. RETENÇÃO DE INFORMAÇÃO

Toda informação armazenada deverá obedecer ao prazo de retenção observado em legislação pertinente.

12. DISPONIBILIDADE DA INFORMAÇÃO

12.1 Toda informação corporativa custodiada pela área de TI do FNDE deverá estar, continuamente, disponível para acesso autorizado. Sistemas de armazenamento lógico compatíveis deverão garantir essa disponibilidade contínua.

12.2 Deverá ser realizada avaliação de risco e de continuidade de negócio, periodicamente, pela área de TI a fim de garantir que a informação disponibilizada não sofra interrupção.

13. PENALIDADES

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

14. RESPONSABILIZAÇÃO

Não é dado ao servidor ou colaborador o direito de alegar desconhecimento da Política de Segurança da informação e comunicação, devendo seguir rigorosamente o proposto nesta norma 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:

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

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

16. VIGÊNCIA E ATUALIZAÇÃO

16.1 **Este documento entra em vigor em 90 (noventa) dias a partir da data de sua publicação e pode ser atualizada ou revogada 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**

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

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

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

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

16.4 **Responsável pela atualização**

16.4.1 Conforme Mapa de Responsabilidades.

ANEXO IX

FNDE
Fundo Nacional de Desenvolvimento da Educação

ÁREAS SEGURAS

ORIGEM

Fundo Nacional de Desenvolvimento da Educação.

REFERÊNCIA NORMATIVA

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

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

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

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

ABNT NBR 11515:2008 – Guia de práticas para segurança física relativas ao armazenamento de dados.

ABNT NBR 11584:1991 – Critérios de segurança física, relativos a microcomputadores e terminais, em estações de trabalho.

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.

CAMPO DE APLICAÇÃO

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

SUMÁRIO

INFORMAÇÕES ADICIONAIS

Esse documento substitui a *NS-006-2002-SEXEC: Norma sobre Áreas de Segurança e Prevenção de Acessos Não Autorizados*, publicada em 10 de dezembro de 2002.

APROVAÇÃO

Carlos Alberto Decotelli da Silva
Presidente do FNDE

1. OBJETIVO

Realizar o controle do acesso físico às instalações do FNDE.

2. DESCRIÇÃO E ESCOPO

Estabelecer regras de controle de acesso e os perímetros de segurança física visando a proteção das informações, críticas ou sensíveis, armazenadas ou acessíveis nas instalações do FNDE.

3. PÚBLICO-ALVO

Esta norma destina-se aos servidores e colaboradores responsáveis pelo controle de acesso físico às instalações do FNDE.

4. CONCEITOS E DEFINIÇÕES

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

5. PRINCÍPIOS

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

6. SEGURANÇA FÍSICA

6.1 **Regras gerais**

6.1.1 A área responsável pela segurança organizacional/corporativa do FNDE deverá estabelecer perímetros de segurança a fim de garantir proteção e separação entre ambientes internos e externos. Tais perímetros serão classificados em Público, Corporativos e Protegidos.

6.1.2 Cada perímetro em questão deverá ser mapeado e rotulado segundo a sua classificação. O mapa detalhado dessa classificação de segurança deverá ser distribuído para a Autarquia, com o intuito de cientificar sobre diferentes procedimentos de segurança para acesso a cada uma das áreas mapeadas.

6.1.3 Todo acesso ao FNDE deverá ser direcionado para área de recepção, sendo necessária a apresentação de identificação oficial. Apenas será aceito documento de identificação oficial, exceto se apresentada cópia devidamente autenticada por cartório legalmente criado para esse serviço.

6.1.4 Toda autorização de acesso deverá compreender:

a) As informações de data e hora de entrada e saída de visitantes;

b) Permitir trilha de auditoria eletrônica;

c) O nome completo do visitante;

d) O local a ser visitado;

e) A identificação do servidor/cargo a ser visitado;

f) A confirmação da autorização de entrada por um servidor ou colaborador;

g) O claro entendimento das regras de controle de acesso pelo visitante; e

h) Liberação apenas com acompanhamento de um representante da área autorizadora.

6.1.5 Para que o visitante possa sair do FNDE, a recepção deverá observar:

a) Assinatura do colaborador responsável no documento de controle de visitantes, autorizando sua saída; e

b) Recolhimento do crachá de visitante.

6.2 **Perímetro Público**

O perímetro público é aquele considerado livre para acesso e trânsito de pessoas físicas interessadas em solicitar algum serviço ao FNDE.

NOTA1: No perímetro público não há necessidade de prévia identificação oficial.

NOTA2: Embora o perímetro seja público, a área de segurança organizacional/corporativa deverá garantir segurança adequada a esse perímetro, inclusive com monitoramento por circuito fechado de gravação de imagem (CFTV) e equipe de vigilância 24x7.

6.3 **Perímetro Corporativo**

6.3.1 O perímetro corporativo é aquele considerado restrito ao acesso público em geral, exceto quando da identificação oficial e devida autorização. Este perímetro corresponde às salas e demais instalações internas do órgão.

6.3.2 Neste perímetro, a área de segurança organizacional/corporativa deverá:

a) Garantir proteção adequada e pertinente a esse nível de segurança, inclusive com monitoramento por circuito fechado de gravação de imagem (CFTV) e equipe de vigilância 24x7; e

b) Manter adequado monitoramento das portas contra incêndio que dão acesso ao exterior e interior do órgão por meio de alarmes de intrusão. Estas portas deverão ser bem sinalizadas e permanecer desobstruídas para evacuação de emergência. Deverão possuir ainda, dispositivos de fechamento automático.

6.3.3 Durante todo trânsito em perímetro corporativo, será exigido o uso de crachá oficial, fornecido pelo FNDE ou pelas empresas prestadoras de serviços.

6.3.4 O crachá pessoal deverá:

a) Estar localizado em local visível e de fácil identificação;

b) Ser colocado na parte frontal do portador, acima da linha da cintura e na parte superior do tronco, devendo estar sempre visível o lado que contem informações que identificam o portador.

6.3.5 A área de segurança organizacional/corporativa deverá manter relação atualizada de crachás perdidos e furtados.

6.3.6 O acesso às instalações fora do horário de expediente somente será liberado após prévia comunicação escrita da chefia imediata do servidor ou do colaborador à área pertinente da Diretoria de Administração – DIRAD. Salvo exceções devidamente justificadas, o acesso deve ser restrito à respectiva unidade de lotação.

6.3.7 É responsabilidade da equipe de recepção inventariar os crachás, sob seu controle, a cada troca de turno e apontar possíveis irregularidades à área de segurança organizacional/corporativa.

6.3.8 Deverá ser avisado imediatamente à área pertinente da Diretoria de Administração – DIRAD toda perda, extravio ou furto de crachá a qual tomará as devidas providências.

NOTA: Avisos deverão ser fixados em locais estratégicos para conscientização acerca do uso constante do crachá.

6.3.9 O perfil de visitante só terá acesso aos recursos de processamento da informação configurados para uso específico desse perfil.

6.3.10 Áreas localizadas no térreo e no subsolo devem obedecer às seguintes orientações adicionais:

a) Portas e janelas que dão acesso ao exterior do órgão devem ser mantidas fechadas e protegidas de forma apropriada contra acessos não autorizados, com mecanismos de controle adequados, travas, alarmes e grades;

b) Sistemas de detecção de intrusão devem ser instalados por profissionais especializados e testados regularmente, de modo a monitorar todas as portas e janelas externas acessíveis; e

c) Áreas nas quais não trabalhem pessoas permanentemente, como depósitos e almoxarifados, devem possuir sistema de detecção de intrusão permanentemente ativado.

6.3.11 Todo trabalho realizado em área corporativa deverá ser, constantemente, supervisionado pela gerência ou chefia regularmente nomeada.

6.3.12 Perímetros corporativos não ocupados devem permanecer trancados e periodicamente inspecionados pela área de segurança corporativa/organizacional.

NOTA1: A área de segurança organizacional/corporativa deverá garantir segurança adequada e pertinente a esse perímetro, inclusive com monitoramento por circuito fechado de gravação de imagem (CFTV) e equipe de vigilância 24x7.

NOTA2: Deverá ser implementado um controle autorizativo para acesso físico a cada andar/ conjunto de salas onde são executadas as atividades do FNDE. Não deverá ser permitida a entrada de colaborador ou servidor em sala ou andar sem prévia autorização do responsável.

NOTA3: A autorização de acesso deve ser revista e atualizada em intervalos regulares e cancelada quando necessário.

NOTA4: As instalações devem ser protegidas adequadamente a fim de evitar que informações confidenciais ou atividades sensíveis sejam prejudicadas ou reveladas a quem não tenha autorização.

NOTA5: As listas de funcionários e guias telefônicos internos que identificam a localização das instalações que processam informações sensíveis não devem estar acessíveis às pessoas não autorizadas.

NOTA6: O acesso no perímetro corporativo somente será autorizado após verificação se o crachá de identificação apresentado não se encontra na relação de crachás perdidos e furtados, e a data de validade. Os crachás que se encontrem em situação irregular devem ser recolhidos.

6.4 **Perímetro protegido**

6.4.1 O perímetro protegido é aquele perímetro corporativo com acesso mais restrito. Incluem-se nesta classificação as áreas que contem informações, dispositivos ou serviços imprescindíveis ao atendimento/suporte das atividades-fim do FNDE, incluindo:

a) Locais com equipamentos de conectividade (servidores de rede e recursos de computação de rede: roteadores, switches, hubs e modens);

b) Locais com infraestrutura de conectividade e energia (cabeamento de telefonia, cabeamento lógico e elétrico);

c) Locais com cópias de segurança das informações custodiadas ou de propriedade do FNDE;

d) Ambientes onde se encontram instalados os geradores de energia elétrica ou Nobreaks;

e) Locais onde se encontram instalados os tanques de combustível dos geradores de energia elétrica; e

f) Salas e armários com informações sensíveis associadas aos interesses relevantes do FNDE.

6.4.2 Os perímetros protegidos devem:

a) Estar, quando possível, localizados em áreas onde o fluxo de pessoas seja baixo, a fim de facilitar a identificação de acesso não autorizado;

b) Conter controle de acesso físico mais restritivo que o perímetro corporativo, com mecanismo de registro e prevenção de acessos não autorizados; e

c) Possuir sistema de alarme de presença permanentemente ativado.

6.4.3 A infraestrutura do perímetro protegido deve:

a) Respeitar as normas específicas para esses ambientes, observando, entre outras, climatização adequada, rede elétrica e lógica, tubulação de gás e água da edificação;

b) Estar livre de tubulações relativas à drenagem pluvial, tubulações de esgoto sanitário e tubulações pressurizadas de gases, exceto aquelas cuja finalidade seja combater incêndios.

6.4.4 Todo trabalho realizado em área protegida deverá ser supervisionado pela gerência ou chefia regularmente nomeada.

6.4.5 Perímetros protegidos não ocupados devem permanecer trancados e periodicamente inspecionados pela área de segurança corporativa/organizacional.

NOTA1: Todo perímetro protegido deverá ter alertar sobre a restrição de entrada. Apenas pessoa autorizada deverá acessar esse perímetro.

NOTA2: A autorização de acesso deve ser revista e atualizada em intervalos regulares e cancelada quando necessário.

NOTA3: As instalações devem ser protegidas adequadamente a fim de evitar que informações confidenciais ou atividades sensíveis sejam prejudicadas ou reveladas a quem não tenha autorização.

NOTA4: As listas de funcionários e guias telefônicos internos que identificam a localização das instalações que processam informações sensíveis não devem ser acessíveis a pessoas não autorizadas.

7. ÁREAS DE ENTREGA E DE CARREGAMENTO

7.1 As áreas de entrega, carregamento e outros pontos em que pessoas não autorizadas possam ter acesso às instalações devem ser controlados e isolados das instalações de processamento da informação, atendendo as seguintes diretrizes:

a) O acesso à área de entrega e carregamento, a partir do exterior do prédio, deve ficar restrito ao pessoal identificado e autorizado;

b) As áreas de entrega e carregamento devem ser projetadas de maneira que possibilite o carregamento e o descarregamento de suprimentos sem que os entregadores tenham acesso a outras partes do edifício;

c) Os materiais entregues devem ser inspecionados e examinados para averiguar e evidenciar qualquer alteração indevida, bem como detectar a presença de explosivos, materiais químicos ou outros materiais perigosos antes de serem transportados da área de entrega e carregamento para o local de utilização;

d) Os materiais entregues devem ser registrados; e

e) As remessas que dão entrada no FNDE devem ser segregadas fisicamente das remessas que saem do órgão.

7.2 No caso específico de entrada, saída e movimentação de recursos de tecnologia da informação, as autorizações devem ter dadas pela Área de Tecnologia da Informação.

7.3 Os veículos que entram e saem do FNDE podem estar sujeitos à vistoria, caso se identifique motivação legal que justifique essa vistoria.

NOTA: Deverá ser definidos pontos de entrega e carregamento de material com acesso exclusivo ao pessoal credenciado.

8. PENALIDADES

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

9. RESPONSABILIZAÇÃO

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

9.2 **Disposições Gerais**

9.3 Os casos omissos e não amparados pelas orientações emanadas por esta 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.

10. VIGÊNCIA E ATUALIZAÇÃO

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

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

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

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

10.3 **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).

10.4 **Responsável pela atualização**

10.4.1 Conforme Mapa de Responsabilidades.