GOVERNO DO ESTADO DE MINAS GERAIS

Presidência

Instrução Normativa FUNED/PRES nº. 03/2022/2022

Belo Horizonte, 23 de maio de 2022.

Dispõe sobre diretrizes de Segurança da Informação de Tecnologia da Informação e Comunicação no âmbito da Fundação Ezequiel Dias - FUNED e dá outras providências.

O Presidente da Fundação Ezequiel Dias – FUNED, no uso das atribuições legais que lhe confere o Decreto nº 47.910, de 07 de abril de 2020, em consonância com a Resolução SEPLAG nº 107, de 26 de dezembro de 2018, com o Decreto nº 47974, de 05 de junho de 2020 e com boas práticas preconizadas pelas normas ABNT NBR ISO/IEC, série 27000 e outras normas nacionais e internacionais relativas à Segurança da Informação

RESOLVE:

CAPÍTULO I

DO OBJETIVO

Art. 1º Esta Instrução Normativa tem por objetivo estabelecer diretrizes de Segurança da Informação no âmbito da Fundação Ezequiel Dias, visando orientar quanto ao uso adequado das informações e dos recursos de tecnologia da informação que as suportam de forma a garantir a proteção de dados, informações e conhecimentos gerados e custodiados, a redução de riscos de ocorrência de perdas, alterações e acessos indevidos, preservando os princípios da Segurança da Informação.

Parágrafo único: A segurança da Informação alinha-se as seguintes estratégias organizacionais:

1. Garantir a continuidade do negócio através da adoção, implantação, teste e melhoria contínua de planos de continuidade e recuperação de desastres;
2. Economicidade da proteção dos ativos de informação;
3. Pessoalidade e utilidade do acesso aos ativos de informação;
4. Responsabilização do usuário pelos atos que comprometam a segurança dos ativos de informação;
5. Garantir a educação e conscientização sobre as boas práticas adotadas pela FUNED em segurança da informação para Servidores, terceiros, contratados, parceiros, alunos e, onde pertinente, clientes.
6. Atender integralmente requisitos de segurança da informação aplicáveis ou exigidos por regulamentações, leis e/ou cláusulas contratuais;
7. Tratar integralmente incidentes de segurança da informação, garantindo que os mesmos sejam adequadamente registrados, classificados, investigados, corrigidos, documentados e, quando necessário, comunicando as autoridades pertinentes;
8. Melhorar continuamente a Gestão de Segurança da Informação através da definição e revisão sistemática de objetivos de segurança em todos os níveis da organização.

CAPÍTULO II

DOS TERMOS E DEFINIÇÕES

Art. 2º Para os fins desta Instrução Normativa, entende-se por:

1. ACESSO: ato de ingressar, transitar, conhecer ou consultar a informação, bem como possibilidade de usar os ativos de informação de um órgão ou entidade, observada eventual restrição que se aplique;
2. ACESSO REMOTO: conexão entre dispositivos (microcomputadores, servidores, etc.), por meio da rede de comunicação de dados corporativa. Quando se tratar de redes corporativas distintas o mesmo deverá ser realizado por meio de VPN;
3. ANTIVÍRUS: programa que permite identificar e eliminar vírus em computadores;
4. ATIVOS DE INFORMAÇÃO: meios de armazenamento, transmissão e processamento da informação, equipamentos necessários a isso, sistemas utilizados para tal, locais onde se encontram esses meios, recursos humanos que a eles têm acesso e conhecimento ou dado que tem valor para um indivíduo ou organização;
5. AUDITORIA: processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas e em conformidade à consecução dos objetivos;
6. AUTENTICAÇÃO: é um processo de verificação da identidade que consta em um sistema, ou seja, o sistema verifica as credenciais de quem está tentando acessar, com as que constam na base de dados, caso positivo, o sistema é liberado pois as credenciais foram validadas;
7. COLABORADOR: todo aquele que possui permissão de acesso à rede corporativa e exerça, ainda que transitoriamente e sem remuneração, por eleição, nomeação, designação, contratação ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública na FUNED.

8. CONTAS: código de acesso atribuído a cada usuário. A cada conta é associada uma senha individual e intransferível, destinada a identificar o usuário, permitindo-lhe o acesso aos recursos disponíveis;

9. CORREIO ELETRÔNICO: meio de comunicação baseado no envio e recepção de mensagens, através de uma rede de computadores;

10. DISPOSITIVO MÓVEL: equipamentos com capacidade de armazenamento e processamento de dados, de fácil locomoção, interligados ou não à rede corporativa do órgão ou entidade, tais como notebooks, smartphones, Tablets e Coletores de Dados;

11. *DOWNLOAD*: transferência de um arquivo de um computador para outro por meio da Internet;

12. DTI: Sigla de Divisão de Tecnologia da Informação;

13. E-MAIL: vide "correio eletrônico";

14. ESTAÇÃO DE TRABALHO: computadores e notebooks do órgão ou entidade interligados ou não à rede corporativa;

15. GESTOR DA UNIDADE: supervisor ou chefe imediato do usuário;

16. INCIDENTE DE SEGURANÇA DA INFORMAÇÃO: um ou mais eventos de segurança da informação, indesejados ou inesperados, que tenham grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação;

17. INTERNET: rede mundial de computadores;

18. INFORMAÇÃO: dados, processados ou não, que podem ser utilizados para produção e para transmissão de conhecimento, contidos em qualquer meio, suporte ou formato;

19. INSTRUÇÃO NORMATIVA DE SEGURANÇA: conjunto de definições, diretrizes, restrições e requisitos que servem para nortear o uso de boas práticas no trato com os ambientes, recursos e ativos computacionais, em aspectos físicos, lógicos e de pessoal, com a finalidade de proporcionar maior segurança às informações;

20. PROCEDIMENTOS: detalham no plano operacional configurações de um determinado produto ou funcionalidade que devem ser feitas para implementar os controles e tecnologias estabelecidas nas normas;

21. RECURSOS DE TECNOLOGIA DA INFORMAÇÃO E COMUNICAÇÃO: sistemas e equipamentos cuja finalidade é coletar, manter, armazenar, processar e disseminar informações eletronicamente;

22. SEGURANÇA DA INFORMAÇÃO: : A segurança da informação (SI) está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. A segurança da informação abrange aspectos físicos, tecnológicos e humanos;

23. SENHA: conjunto de caracteres utilizado para permitir a validação da identidade do usuário, a fim de tornar possível seu acesso a um sistema de informação ou serviço de uso restrito;

24. SISTEMA DE INFORMAÇÃO - conjunto de elementos materiais ou intelectuais, colocados à disposição dos usuários, em forma de serviços ou bens, que possibilitam a agregação dos recursos de tecnologia, informação e comunicações de forma integrada;

25. TIC: sigla de tecnologia da informação e comunicação;

26. USUÁRIO: pessoa física, seja servidor ou equiparado, empregado ou prestador de serviços, devidamente habilitada pela DTI para acessar os recursos de TIC da FUNED. Os usuários se classificam em:

a. Usuários internos: os que possuem vínculo funcional com a FUNED;

b. Usuários externos: os que não possuem vínculo funcional com a FUNED e que, pela natureza de suas atividades, necessitam de cadastro prévio para uso dos recursos tecnológicos;

27. VÍRUS: programa desenvolvido com intenção nociva que, se inserido em um computador, pode causar queda do seu desempenho, destruição de arquivos e disco rígido, ocupar espaço livre de memória, entre outros danos;

28. VPN (*VIRTUAL PRIVATE NETWORK*): forma de comunicação que permite que uma ou mais máquinas acessem uma rede privada, utilizando como infraestrutura as redes públicas, tal como a Internet. Os dados trafegam na rede de forma segura, utilizando encapsulamento, criptografia e autenticação;

CAPÍTULO III

DA ABRANGÊNCIA

Art. 3º As normas desta Instrução Normativa aplicam-se a todos os usuários da FUNDAÇÃO EZEQUIEL DIAS, seja ele nomeado, designado, contratado ou qualquer outra forma de investidura ou vínculo, mandato, cargo, emprego ou função pública. Aplica-se também a fornecedores no desempenho de alguma atividade internamente na FUNED.

CAPÍTULO IV

DOS FUNDAMENTOS DA REGULAMENTAÇÃO

Art. 4º A regulamentação para utilizar os recursos de TIC na FUNED decorre:

1. da necessidade de organização e racionalização de recursos para imprimir mais eficiência e economicidade à manutenção e à evolução do parque de Tecnologia da Informação e Comunicação;

2. da necessidade de se prevenir o acesso não autorizado e de se evitar o comprometimento das informações e dos recursos tecnológicos;

3. Estar em conformidade com a Lei Geral de Proteção de Dados, Lei Nº 13.709 de 14 de agosto de 2018, com o objetivo de garantir a privacidade dos dados pessoais das pessoas e permitir um maior controle sobre eles.

CAPÍTULO V

DOS PRINCÍPIOS

Art. 5º A segurança da informação na Fundação Ezequiel Dias alinha-se às estratégias organizacionais e aos seguintes princípios:

1. Confidencialidade: garantia de que o acesso à informação seja obtido somente por pessoas devidamente autorizadas;

2. Integridade: garantia de que a informação seja mantida em seu estado original, visando protegê-la contra alterações indevidas, intencionais ou acidentais;

3. Disponibilidade: garantia de que os usuários autorizados obtenham acesso à informação e aos ativos correspondentes sempre que necessário;

4. Autenticidade: garantia da identidade de quem está enviando a informação;

5. Legalidade: Garantia de que ações sejam realizadas em conformidade com os preceitos legais vigentes e que seus produtos tenham validade jurídica;

CAPÍTULO VI

DAS RESPONSABILIDADES

Seção I

Presidência

Art. 6º É responsabilidade da Presidência:

1. Analisar, revisar e aprovar a Instrução Normativa e normas relacionadas à segurança da informação;

2. Dar subsídios para a disponibilidade dos recursos necessários para uma efetiva Gestão de Segurança da Informação;

3. Apoiar para que as atividades de segurança da informação sejam executadas em conformidade com a essa Instrução Normativa;

Seção II

Divisão de Tecnologia da Informação

Art. 7º É responsabilidade da Divisão de Tecnologia da Informação:

1. Promover a divulgação da Instrução Normativa de Segurança da Informação e tomar as ações necessárias para disseminar uma cultura de segurança da informação no ambiente da FUNED.

2. Conduzir a Gestão e Operação da segurança da informação, tendo como base esta Instrução Normativa e demais resoluções do Comitê de Tecnologia da Informação e Comunicação do Governo do Estado de Minas Gerais;

3. Promover o cumprimento das deliberações da PRESIDÊNCIA;

4. Elaborar e propor para PRESIDÊNCIA, normas e procedimentos de segurança da informação, necessários para se fazer cumprir a Instrução Normativa de Segurança da Informação;

5. Identificar e avaliar as principais ameaças à segurança da informação, bem como propor e, quando aprovado, implantar medidas corretivas para reduzir o risco;

6. Tomar as ações cabíveis para se fazer cumprir os termos desta Instrução Normativa;

7. Realizar a gestão dos incidentes de segurança da informação, garantindo tratamento adequado.

8. Receber e analisar solicitações para criação de contas de acesso ou fornecimento de privilégios para usuários internos e externos;

9. Conceder, quando autorizado, o acesso aos usuários internos e externos, conforme indicado pelos gestores da unidade;

10. Revogar, quando solicitado, o acesso dos usuários internos e externos, conforme indicado pelos gestores da unidade;

11. Orientar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação dos usuários internos e externos, fornecendo informações sobre os privilégios atualmente efetivados em ativos/sistemas de informação.

Seção III

Gestor da Unidade

Art. 8º É responsabilidade do Gestor da Unidade:

1. Gerenciar as informações geradas ou sob a responsabilidade da sua área de negócio durante todo o seu ciclo de vida, incluindo a criação, manuseio e descarte.
2. Identificar, classificar e rotular as informações geradas ou sob a responsabilidade da sua área de negócio conforme normas, critérios e procedimentos adotados pela FUNED;
3. Periodicamente revisar as informações geradas ou sob a responsabilidade da sua área de negócio, ajustando a classificação e rotulagem das mesmas conforme necessário;
4. Autorizar e revisar os acessos à informação e sistemas de informação sob sua responsabilidade;
5. Solicitar a concessão ou revogação de acesso à informação ou sistemas de informação de acordo com os procedimentos adotados pela FUNED.
6. Solicitar a Divisão de Tecnologia da informação a concessão de acesso novos usuários que necessitem de novos acessos conforme mudanças em suas atividades laborais;
7. Solicitar a Divisão de Tecnologia da informação concessão de acesso a terceiros/prestadores de serviços contratados justificando a necessidade de acesso a ativos/sistemas de informação;
8. Informar, de maneira imediata, a Divisão de Tecnologia da informação quando ao encerramento do contrato com terceiros/prestadores de serviços contratados que tenham a ativos/sistemas de informação.

Seção IV

Serviço Pessoal

Art. 9º É responsabilidade do Serviço Pessoal:

1. Reportar o desligamento de colaboradores da FUNED a DTI para que contas de acesso possam ser revogadas;
2. Apoiar a gestão de identidades enviando relatórios periódicos sobre colaboradores desligados ou que mudaram de posição na FUNED;
3. Apoiar a revisão periódica da validade de credenciais de acesso a ativos/sistemas de informação fornecendo informações sobre os colaboradores.

Seção V

Usuários

Art. 10 É responsabilidade dos Usuários:

1. Ler, compreender e cumprir integralmente os termos da Instrução Normativa de Segurança da Informação, bem como as demais normas e procedimentos de segurança aplicáveis;
2. Encaminhar quaisquer dúvidas e/ou pedidos de esclarecimento sobre a Instrução Normativa de Segurança da Informação, suas normas e procedimentos a Divisão de Tecnologia da Informação;
3. Comunicar à Divisão de Tecnologia da Informação qualquer evento que viole esta Instrução Normativa ou coloque/possa vir a colocar em risco a segurança das informações ou dos recursos computacionais da FUNED;
4. Assinar o Termo de Responsabilidade de uso de Sistemas de Informação da FUNED, formalizando a ciência e o aceite integral das disposições da Instrução Normativa de Segurança da Informação, bem como as demais normas e procedimentos de segurança, assumindo responsabilidade pelo seu cumprimento;
5. Responder pela inobservância da Instrução Normativa de Segurança da Informação, normas e procedimentos de segurança, conforme definido no item sanções e punições.
6. Acompanhar o andamento de suas ordens de serviços, na central de serviços da TI, desde sua abertura até a finalização.

CAPÍTULO VII

DAS DISPOSIÇÕES REGULAMENTARES

Seção I

Das Disposições Gerais

Art. 11 Toda informação produzida ou armazenada na Fundação Ezequiel Dias é de sua propriedade e não de seu colaborador, exceto os casos onde a Instituição atua como custodiante dessa informação.

Art. 12 Os recursos de Tecnologia da Informação e Comunicação da FUNED são de uso restrito, devendo ser empregados exclusivamente no desenvolvimento das atividades da Fundação.

Art. 13 As solicitações de serviços direcionadas à Divisão de Tecnologia da Informação deverão ser realizadas por meio da Central de Serviços da TI, mediante abertura de ordem de serviço.

Parágrafo Único. Somente equipamentos patrimoniados e softwares homologados pela DTI serão objeto de atendimento, salvo quando houver autorização formal da Autoridade Competente para atendimento diverso desses.

Art. 14 Cabe aos usuários o fiel cumprimento das orientações de segurança emitidas pela DTI, de maneira que haja condições de executar a manutenção preventiva e periódica de todo o parque de equipamentos de Tecnologia da Informação e Comunicação da FUNED.

Art. 15 Cabe à DTI criar e executar o programa de manutenção preventiva de todo o parque de equipamentos de Tecnologia da Informação e Comunicação da FUNED, bem como zelar pelo seu fiel cumprimento de acordo com a periodicidade definida.

Art. 16 Os projetos que tenham em vista a aquisição de bens, serviços e aplicativos relacionados com Tecnologia de Informação e Comunicação deverão ter parecer técnico prévio da DTI, conforme procedimentos adotados pela FUNED;

Seção II

Do Acesso aos Recursos de Tecnologia da Informação e Comunicação

Art. 17 O acesso aos recursos de Tecnologia da Informação e Comunicação será permitido mediante identificação e autenticação dos usuários.

§ 1º Será fornecida identificação eletrônica - pessoal e intransferível - bem como senha a todos os usuários dos recursos de Tecnologia da Informação e Comunicação da FUNED.

§ 2º Os usuários serão responsáveis por todas as ações realizadas com a utilização de sua identificação e senha, devendo zelar pelo sigilo e pela confidencialidade das mesmas.

§ 3º Os usuários somente terão acesso às informações e aos recursos de tecnologia necessários para a realização das respectivas atividades funcionais.

§ 4º As identificações criadas para serviços temporários deverão ter validade definida de acordo com o tempo necessário para a realização das respectivas atividades profissionais e poderão ser prorrogadas em caso de necessidade.

Seção III

Da Segurança das Senhas

Art. 18 A cada usuário deve ser disponibilizada apenas uma identificação de acesso aos recursos de TI. Essa identificação deve ser única, pessoal e intransferível, sendo dever do usuário zelar por sua guarda e sigilo:

Parágrafo Único. A senha de acesso ao recurso de TI qualifica o usuário como responsável por todos os acessos realizados. A definição e a utilização de senhas estão condicionadas às regras definidas pela DTI.

Art. 19 Os usuários deverão adotar medidas de prevenção para garantir o acesso seguro a ativos e serviços de informação, incluindo:

1. Não anotar ou registrar senhas de acesso em qualquer local;
2. Não utilizar sua conta, ou tentar utilizar qualquer outra conta, para violar controles de segurança estabelecidos pela FUNED;
3. Não compartilhar a conta de acesso e senha com outro usuário, colaborador e/ou terceiro;
4. Trocar sua senha de acesso aos recursos de TI periodicamente, seguindo as orientações DTI.
5. Informar imediatamente a DTI caso identifique qualquer falha ou vulnerabilidade que permita a utilização não autorizada de ativos de informação, sistemas e/ou recursos computacionais da FUNED;

Art. 20 Qualquer utilização não autorizada ou tentativa de utilização não autorizada de credenciais e senhas de acesso a ativos/serviços de informação ou recursos computacionais será tratada como um incidente de segurança da informação, cabendo uma análise da infração.

Seção IV

Do Uso dos Recursos de Tecnologia da Informação e Comunicação

Art. 21 Os equipamentos fornecidos aos usuários da FUNED serão configurados de forma padronizada pela DTI

Parágrafo Único. Toda solicitação de alteração da configuração padronizada deverá ser previamente autorizada pela DTI.

Art. 22 É vedado aos usuários, salvo nos casos autorizados pela DTI:

1. qualquer procedimento de manutenção física ou lógico, instalação, desinstalação, configuração ou modificação, sem o conhecimento prévio e o acompanhamento de um técnico DTI, ou de quem essa determinar;
2. abertura ou o manuseio de computadores ou outros equipamentos de informática para qualquer tipo de reparo que não seja realizado por um técnico da DTI ou por terceiros devidamente contratados para o serviço;
3. modificar as configurações de rede e de acesso à internet, incluindo as configurações de endereçamento IP, DNS, WINS, GATEWAY e PROXY.

Art. 23 Não será permitido conectar, na rede corporativa da FUNED, equipamento não autorizado previamente pela DTI.

Art. 24 O usuário deve armazenar os arquivos com informações institucionais nos servidores de arquivos disponibilizados na rede local da Unidade e evitar o armazenamento de dados institucionais nas estações de trabalho.

Art. 25 Cabe aos usuários dos equipamentos de informática:

1. Informar à DTI sobre danos à integridade física ou lógica do equipamento por ele utilizado;
2. Bloquear o computador, quando se ausentar do local em que esse esteja instalado;
3. Desligar os equipamentos ao final de cada período de trabalho, salvo expressa disposição em contrário da DTI.
4. Zelar pelos recursos utilizados, conectando equipamentos em rede elétrica de tensão e intensidade de corrente compatíveis com as suas especificações técnicas, posicionando-os fisicamente de forma a impossibilitar o risco de espionagem e não consumindo bebidas e alimentos próximo aos computadores e a seus periféricos;
5. Utilizar, armazenar, transportar e proteger adequadamente todos os equipamentos de Tecnologia da Informação e Comunicação de que faz uso;
6. Solicitar manutenção corretiva à DTI quando identificar problemas no uso do recurso de tecnologia;
7. Manter-se capacitado na operação básica dos equipamentos de Tecnologia da Informação e Comunicação.

Parágrafo Único. Nos casos em que o monitoramento dos equipamentos indique a existência de contaminação em recurso computacional, o acesso à rede corporativa poderá ser bloqueado pela DTI, a fim de se evitar o comprometimento da segurança, e o usuário será comunicado acerca da medida.

Art. 26 A DTI poderá remover, por meio de rotinas automatizadas, arquivos suspeitos ou contaminados sem necessidade da anuência do usuário, que será comunicado acerca do fato e orientado para evitar novas ocorrências.

Seção V

Do Uso da Rede Corporativa

Art. 27 É vedada a conexão de recursos de comunicação, estações de trabalho, notebooks, impressoras e quaisquer outros recursos não pertencentes a FUNED na rede interna, salvo quando devidamente autorizado pela DTI.

Art. 28 A autorização e o nível permitido de acesso ativos/serviços de informação da FUNED é feita com base em perfis que definem o nível de privilégio dos usuários.

Art. 29 O acesso à ativos/serviços de informação é fornecido a critério da FUNED, que define permissões baseadas nas necessidades laborais dos usuários;

Art. 30 Autorizações de acesso a perfis são fornecidas e/ou revogadas com base na solicitação dos gestores da unidade. Solicitações deverão ser encaminhadas via central de serviços da DTI.

Art. 31 Os usuários devem ainda observar as seguintes diretrizes:

1. Os Servidores de arquivos possuem tamanho limitado, conforme a capacidade e disponibilidade de área de armazenamento, ficando a cargo da DTI definir esses limites;
2. É expressamente proibido o armazenamento de informações de caráter pessoal, que infrinjam direitos autorais ou que não sejam de interesse da FUNED;
3. Os servidores de arquivos são monitorados e auditados pela DTI, quanto à tipo de arquivo, tipo de conteúdo, tamanho do arquivo. E caso encontrados arquivos que violem o estabelecido nos parâmetros da segurança da informação, o responsável pelo diretório será comunicado acerca do fato e orientado para evitar novas ocorrências;
4. Durante o monitoramento a FUNED se resguarda o direito de, sem qualquer notificação ou aviso ao usuário, ler, copiar, e divulgar arquivos, através de ato administrativo, judicial ou de acordo com o interesse da Administração Pública.

Art. 32 Todo recurso de tecnologia que não pertença ao patrimônio da FUNED e que, por determinação superior, de portaria, de convênio, de contrato ou outro tipo de ajuste necessite utilizar a rede corporativa deverá estar em conformidade com a presente Instrução Normativa de Segurança da Informação.

Parágrafo Único. A verificação prévia da conformidade com as normas será realizada pela DTI.

Art. 33 Os recursos de Tecnologia da Informação e Comunicação que utilizam a rede corporativa da FUNED deverão possuir sistema operacional e antivírus instalados e atualizados.

Art. 34 Os técnicos da DTI deverão possuir acesso físico e/ou lógico, para fim de checagem de conformidade e auditoria, a todos os recursos conectados à rede corporativa da FUNED.

Art. 35 É vedado o uso da rede para:

1. Utilizar os serviços de rede como instrumento de ameaça, calúnia, injúria ou difamação, bem como realizar quaisquer outras atividades proibidas pelas legislações, por atos normativos vigentes no País ou por acordos internacionais;
2. Realizar ataques aos sistemas de informação da FUNED ou de terceiros;
3. Realizar atividades comerciais, políticas, ilegais ou imorais;
4. Acessar jogos, redes sociais e *sites* de relacionamento, salvo ferramentas de apoio institucional homologadas pela DTI;
5. Acessar serviços não autorizados de compartilhamento de arquivos ou similares;
6. Conectar recursos de Tecnologia da Informação e Comunicação sem a devida autorização da DTI.

Art. 36 Devem ser estabelecidos procedimentos de controle e concessão de acesso a visitantes que, durante sua permanência, na instituição necessitem conectar seus dispositivos móveis à rede da FUNED;

Art. 37 A concessão de acesso ao visitante deve estar vinculada à conscientização do usuário sobre as normas internas de uso da rede;

Seção VI

Do Uso do Correio Eletrônico

Art. 38 A FUNED fornece o serviço de e-mail para seus usuários autorizados exclusivamente para o desempenho de suas atividades profissionais;

Art. 39 É atribuição exclusiva da DTI definir os softwares homologados para o uso do correio eletrônico institucional

Art. 40 Não é permitido o uso de qualquer serviço de e-mail, que não seja o oficialmente fornecido pela FUNED;

Art. 41 Os usuários externos poderão, a critério do gestor da unidade e no interesse da FUNED, ter acesso ao serviço de correio eletrônico desde que o façam em concordância com as regras estabelecidas nesta Instrução Normativa.

Art. 42 O usuário terá direito a uma única conta de e-mail que o identificará univocamente em toda FUNED

Art. 43 A caixa postal compartilhada ou lista de discussão deve ter um responsável e um substituto formalizados.

Art. 44 As caixas postais do correio eletrônico institucional possuem tamanho limitado, conforme a capacidade e disponibilidade de área de armazenamento, ficando a cargo da DTI definir esses limites

Art. 45 Os arquivos a serem anexados às mensagens no correio eletrônico institucional não poderão ultrapassar o limite de tamanho estabelecido pela DTI

Art. 46 É vedada a utilização do correio eletrônico institucional para:

1. Caráter pessoal ou para fins que não sejam de interesse da FUNED;
2. Utilizar de termos ou palavras de baixo calão na redação de mensagens;
3. Transmitir mensagens de conteúdo potencialmente perigoso, arquivos executáveis ou códigos maliciosos que possam danificar ou comprometer a rede institucional;
4. Inscrever o endereço de e-mail da FUNED em listas de distribuição e grupos de discussão que não estejam relacionadas com atividades laborais ou do interesse da organização;
5. Fazer uso de qualquer técnica de falsificação ou simulação de falsa identidade e manipulação de cabeçalhos de e-mail. Qualquer tentativa, mesmo não consumada, será tratada como um incidente de segurança da informação e estará sujeita a sanções e/ou demais penalidades;
6. Tentar a interceptação ou alteração do conteúdo da mensagem de outros usuários ou terceiros, a menos que devidamente autorizado;
7. Utilizar o serviço de e-mail para o envio de mensagens indesejadas (spam) ou qualquer tipo de técnica que possa levar a sobrecarga do serviço de e-mail;
8. Usar o serviço de e-mail para disseminar ou transmitir mensagens de caráter injurioso, calunioso ou que possam ferir a legislação em vigor;

Art. 47 De forma a preservar o funcionamento do serviço de correio eletrônico institucional, o Usuário da rede de dados deve:

1. Eliminar, periodicamente, as mensagens desnecessárias de sua caixa postal, inclusive as existentes nas pastas personalizadas, na lixeira, rascunho e enviados, de forma a não exceder o limite de tamanho da caixa postal;
2. Evitar clicar em links de acesso a páginas de Internet existentes em mensagens de correio eletrônico recebidas de origem desconhecida, pois esses podem iniciar a instalação de softwares maliciosos ou direcionar o usuário da rede de dados para um site falso, possibilitando a captura de informações;
3. Evitar abrir ou executar arquivos anexados às mensagens recebidas pelo correio eletrônico, sem antes verificá-los quanto à sua procedência. No caso de suspeita de irregularidade na mensagem, o usuário deve solicitar ajuda a área de TI correlata;

Art. 48 O correio eletrônico particular não deve ser utilizado para o envio ou recebimento de informações da FUNED.

Art. 49 O correio eletrônico institucional pode ser monitorado e restringido pela DTI, quanto à origem, destino, quantidade, tipo de conteúdo, tipo de anexo e volume das informações, desde que esses controles sejam feitos por parâmetros gerais (não personalizados).

Art. 50 A conta de e-mail da FUNED é pessoal e intransferível e o seu titular é o único responsável pelas ações e pelos danos causados à instituição por meio de seu uso.

Art. 51 O monitoramento do serviço de e-mail da FUNED tem como objetivos proteger a organização, atestar o respeito às regras contidas nessa norma, bem como produzir evidencias relativas à eventual violação das mesmas e/ou à legislação em vigor;

Art. 52 Durante o monitoramento a FUNED se resguarda o direito de, sem qualquer notificação ou aviso, de monitorar, interceptar, registrar, ler, bloquear, redirecionar, retransmitir, copiar e divulgar, através de ato administrativo ou judicial todas as mensagens enviadas ou recebidas pelos usuários através de seu serviço de e-mail;

Art. 53 A DTI poderá bloquear quaisquer mensagens, sem a anuência do usuário, que possam caracterizar vulnerabilidade à segurança da rede corporativa da FUNED.

Seção VII

Acesso à internet

Art. 54 A FUNED fornecerá acesso à Internet aos seus usuários autorizados, conforme as necessidades inerentes ao desempenho de suas atividades profissionais;

Art. 55 O acesso à internet poderá ser fornecido tanto através da rede corporativa da FUNED, quanto através da disponibilização de serviços de internet móvel:

1. O uso dos dispositivos móveis portáteis pelos usuários da rede da FUNED deverá ser realizado no interesse da instituição e de acordo com esta Instrução Normativa;

2. Todo dispositivo móvel usado para acessar a rede corporativa da FUNED estará submetido aos padrões estabelecidos desta Instrução Normativa.

Art. 56 É atribuição exclusiva da DTI definir os softwares para uso da Internet na FUNED.

Art. 57 O acesso à Internet é monitorado e poderá ser restringido pela DTI quanto a endereço de sites, quantidade de acessos, horário, tempo de permanência, tipo de conteúdo e volume de informações trafegadas, desde que estes controles sejam feitos por parâmetros gerais.

Art. 58 A área de recursos humanos ou chefias hierarquicamente superiores podem solicitar formalmente um relatório com as informações de acesso à Internet de um de seus usuários da rede, para si ou para outros, nas seguintes situações:

1. Suspeita de infração à Instrução Normativa de Segurança da Informação e Comunicações;

2. Necessidade de visualizar os sites acessados e o tempo gasto nos mesmos por seus usuários de rede.

Art. 59 Todo serviço disponibilizado na Internet, antes de ser implantado na rede corporativa, deve ser avaliado pela DTI através de avaliação e relatório técnico, considerando os aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

Art. 60 Durante o monitoramento do acesso a internet, a FUNED se resguarda o direito de, sem qualquer notificação ou aviso, interceptar, registrar, ler, copiar e divulgar por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais, toda informação trafegada, seja originada de sua rede interna e destinada a redes externas ou o contrário;

Art. 61 É vedada a utilização da Internet para:

1. Acessar sites com códigos maliciosos e ameaças virtuais;

2. Acessar sites com materiais pornográficos, atentatórios à moral e aos bons costumes ou ofensivos;

3. Acessar sites ou arquivos que contenham conteúdo criminoso ou ilegal, ou que façam sua apologia, incluindo os de pirataria ou que divulguem número de série para registro de softwares;

4. Acessar sites ou arquivos com conteúdo de incitação à violência, que não respeitem os direitos autorais ou com objetivos comerciais particulares;

5. Realizar download de arquivos que não estejam relacionados às necessidades de trabalho da FUNED;

6. Realizar atividades relacionadas a jogos eletrônicos pela Internet;

7. Acessar sites para transferência de arquivos, exceto nos casos em que tais ações sejam condizentes com atividades de trabalho da FUNED;

8. Utilizar serviços de compartilhamento de arquivos online, salvo aqueles homologados pela DTI;

9. Realizar atividades relacionadas a prática de propaganda política nacional ou internacional;

10. O desrespeito a imagem ou aos direitos de propriedade intelectual e industrial da FUNED;

11. Tentativa de expor a infraestrutura computacional da FUNED a ameaças virtuais;

12. Acessar sites ou serviços que busquem contornar controles de acesso à internet.

Art. 62 O usuário deve sempre se certificar da procedência do site, verificando, quando cabível, o certificado digital do mesmo, principalmente para realizar transações eletrônicas via internet, digitando o endereço do site diretamente no navegador.

Art. 63 É vedado aos usuários disponibilizar informações de propriedade da FUNED em sites da Internet sem observar sua classificação e o público a que se destina.

Seção VIII

Aquisição, Desenvolvimento e Manutenção de Sistemas de Informação

Art. 64 Todo projeto de sistema de informação antes da sua concepção, deve ser submetido à DTI para avaliação/homologação dos aspectos de segurança da informação, consumo de recursos tecnológicos e comprometimento de outros serviços.

Art. 65 Toda aquisição de sistema deve possuir o documento de Especificação do Requerimento do Usuário – Softwares, homologado há menos de 12 meses.

Art. 66 Requisitos de segurança de sistemas de informação:

1. Devem ser considerados requisitos de segurança na definição dos novos sistemas;

2. Devem ser considerados requisitos de segurança na aquisição de novos sistemas;

3. Devem ser considerados requisitos de segurança em todas as fases de criação dos sistemas, ou seja, definição, projeto, desenvolvimento, implantação e manutenção.

Art. 67 O acesso aos códigos fontes dos sistemas deve ser controlado e autorizado pela DTI.

Art. 68 Deverão ser documentados os procedimentos para a instalação, atualização e utilização de softwares.

Art. 69 Todos os usuários que utilizarão um sistema devem ser treinados e capacitados para exercer suas atividades.

Art. 70 Deverão ser investigadas e tratadas de forma contínua as vulnerabilidades técnicas dos sistemas de informação em uso.

Seção IX

Acesso Remoto à Rede Corporativa por meio de *Virtual Private Networks* (*VPN)*

Art. 71 O serviço de VPN será disponibilizado para usuários mediante a autorização do Gestor da Unidade.

Art. 72 A DTI deve informar aos usuários os requisitos mínimos de segurança estabelecidos para realização de acesso remoto.

Art. 73 Os recursos de Tecnologia da Informação – TI utilizados no ambiente de trabalho remoto, tal como residências, devem conter mecanismos de proteção contra vírus, software malicioso e controle de acesso.

Art. 74 Quando os recursos de informática forem de propriedade de terceiros, a área de TI correlata deve solicitar a estes que os referidos recursos atendam aos requisitos mínimos de segurança estipulados.

Art. 75 O usuário é responsável por toda e qualquer operação (acesso, processamento, comunicação, etc.) realizada através de um acesso remoto.

Seção X

Monitoramento de ativos/serviços da informação e recursos computacionais

Art. 76 Qualquer ativo/serviço de informação ou recurso computacional da FUNED, bem como qualquer outro recurso computacional com acesso aos mesmos, poderá ser monitorado a qualquer momento.

Art. 77 Todos os ativos/serviços de informação, recursos computacionais da FUNED, bem como toda informação trafegada ou armazenada nos mesmos, incluindo conta de e-mail corporativa e a navegação em sites e serviços da Internet, estão sujeitos à monitoração, não constituindo qualquer violação à intimidade, vida privada, honra ou imagem da pessoa monitorada, visando resguardar a segurança dos ativos de informações, bem como segurança jurídica da FUNED.

Art. 78 Todas as informações dos ativos/serviços de informação ou recursos computacionais da FUNED podem ser interceptadas, gravadas, lidas, copiadas e divulgadas por, ou para, pessoas autorizadas para finalidades oficiais, incluindo investigações criminais. Estas informações incluem dados sensíveis criptografados para cumprir as exigências de confidencialidade e de privacidade.

Seção XI

Sanções e Punições

Art. 79 O usuário que não cumprir as normas estabelecidas nessa Instrução Normativa estará sujeito às penalidades previstas em Lei.

Seção XII

Das disposições finais

Art. 80 Todas as ações que comprometerem a segurança das informações institucionais por meio de recursos de Tecnologia da Informação e Comunicação deverão ser informadas imediatamente à DTI na forma de comunicação oficial.

Art. 81 Os casos omissos serão avaliados pela DTI para posterior deliberação.

Art. 82 As diretrizes estabelecidas nesta Instrução Normativa e nas demais normas e procedimentos de segurança, não se esgotam em razão da contínua evolução tecnológica e constante surgimento de novas ameaças. Desta forma, não se constitui rol enumerativo, sendo obrigação do usuário da informação da FUNED adotar, sempre que possível, outras medidas de segurança além das aqui previstas, com o objetivo de garantir proteção as informações da FUNED.

Art. 83 Esta Instrução Normativa entra em vigor na data de sua publicação.

Belo Horizonte, 23 de maio de 2022.

EDUARDO CAMPOS PROSDOCIMI

Presidente da Fundação Ezequiel Dias

Documento assinado eletronicamente por **Eduardo Campos Prosdocimi**, **Presidente**, em 23/05/2022, às 16:27, conforme horário oficial de Brasília, com fundamento no art. 6º, § 1º, do Decreto nº 47.222, de 26 de julho de 2017.

A autenticidade deste documento pode ser conferida no site http://sei.mg.gov.br/sei/controlador_externo.php?acao=documento_conferir&id_orgao_acesso_externo=0, informando o código verificador **46971695** e o código CRC **3F288FDA**.