1. OBJETIVO

A finalidade deste documento é definir regras claras para o uso do sistema de informações e outros ativos de informações no Núcleo de Excelência em Tecnologias Sociais - NEES.

2. AMPLITUDE

Este documento aplica-se a todos os ativos de informações e sistemas de informações usados no escopo do SGSI.

3. DOCUMENTOS DE REFERÊNCIA

- Norma ABNT NBR ISO 27002 - Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação.

4. DEFINIÇÕES

Sistema de informação - inclui os servidores, a infraestrutura de rede, o suporte ao programa de aplicativos e ao sistema, os dados e outros subsistemas e componentes de computador de propriedade de ou usados pela organização ou que estão sob responsabilidade da organização. O uso de um sistema de informações também inclui o uso de serviços internos ou externos, como o acesso à Internet, o e-mail, etc.

Ativos de informações - no contexto desta política, o termo "ativos de informações" aplica-se a sistemas de informações e a outras informações/outros equipamentos utilizados no ambiente controlado pelo NEES.

Usuários - Estão incluídos no grupo de usuários todas as pessoas que utilizam os sistemas de informações do ambiente da organização.

5. DIRETRIZES

5.1 Uso aceitável dos ativos de informação

5.1.1 Uso aceitável

Os ativos de informação só podem ser usados para as atividades profissionais com a finalidade de realizar tarefas relacionadas à organização.

5.1.2 Responsabilidade pelos ativos

Todos os ativos de informações possuem um proprietário designado no Inventário de ativos. O proprietário do ativo é responsável pela confidencialidade, integridade e disponibilidade das informações no ativo em questão.

5.1.3 Atividades não autorizadas

Os ativos de informações não devem ser utilizados de forma que enfraqueça o desempenho do sistema de informações, represente uma ameaça à segurança, ou consuma a capacidade sem a devida necessidade. Também é proibido:

- Fazer download de arquivos de imagem ou vídeo sem finalidade comercial, enviar correntes por e-mail, jogar;
- Instalar softwares em computador local sem a permissão explícita da Gerência de Infraestrutura;
- Usar aplicativos Java, controle Active X e outros códigos móveis, exceto quando autorizado pelo gestor da sua área, formalizando através de abertura de chamado no endereço https://atendimento.nees.ufal.br
- Usar ferramentas de criptografia em computador local, exceto em casos especificados na Política de classificação da informação;
- Fazer download de códigos de programa a partir de mídias externas;
- Instalar ou usar dispositivos periféricos, como modems, cartões de memórias ou outros dispositivos de armazenamento e leitura de dados (por exemplo, pen drives USB) sem permissão explícita da Gerência de Infraestrutura.

5.2 Retirada de ativos do local

Os equipamentos, as informações ou os softwares, independente de suas formas ou meio de armazenamento, podem ser retirados do local após assinatura dos documentos: Termo de Comando / Fundação Parque; Termo de Responsabilidade / FUNDEPES, e o Termo de Cessão de Uso de Retirada de Equipamentos, fica de posse do NEES, nas pastas dos respectivos projetos.

A solicitação deve ser feita pelo Gerente/Assessor da área via e-mail ou abertura de chamado através do endereço https://atendimento.nees.ufal.br.

Se os ativos em questão estiverem fora da organização, eles precisam ser controlados pela pessoa que concedeu a permissão de retirada.

5.3 Devolução de ativos no encerramento do contrato

Mediante o encerramento de contrato de atividade ou outro tipo de contrato em relação ao uso de equipamentos, softwares ou informações em formato eletrônico ou em papel, o usuário deve devolver os ativos de informações, para que seja registrada no sistema.

5.4 Procedimento para cópias de segurança

As informações em meio eletrônico, armazenadas no ambiente NEES, possuem cópia de segurança com proteção adequada. Para a criação das cópias de segurança devem ser considerados os aspectos legais, históricos, de auditoria e de recuperação do ambiente.
As evidências dos projetos devem ser mantidas nos servidores, onde existe sistema de backup, tornando os dados seguros.
Arquivos pessoais não fazem parte da rotina de backup, apenas arquivos e dados relacionados diretamente ao NEES.

5.5 Proteção por antivírus

O Microsoft Defender deve ser instalado em todos os computadores e notebooks Windows com atualizações automáticas ativadas.
O antivírus deve ser instalado também nos servidores da organização quando aplicável.

5.6 Autorizações para uso do sistema de informações

Os usuários só podem acessar os ativos do sistema de informações para o qual obtiverem autorização explícita do proprietário do ativo.
Os usuários só podem usar o sistema de informações para as finalidades que obtiverem autorização, isto é, direitos de acesso.
Os usuários não devem participar de atividades que possam ser usadas para contornar controles de segurança do sistema de informações.
A liberação de acesso ao uso de sistema de informações é concedida através de chamado no endereço https://atendimento.nees.ufal.br e posterior autorização via e-mail institucional.

5.7 Responsabilidades da conta dos usuários

O usuário não deve, direta ou indiretamente, permitir que outra pessoa use seu direito de acesso, ou seja, seu login e senha não deve ser repassado para outra pessoa.

O proprietário da conta é o usuário, que é responsável pelo uso e por todas as transações realizadas por meio desta conta.

5.8 Responsabilidades de senha

As regras e responsabilidade do uso de senhas estão descritas no documento: PSI001 - Política de segurança da informação.

5.9 Política de mesa limpa e tela limpa

Todas as informações classificadas como "Interno", "Restrito" e "Confidencial", conforme especificado na PSI002 - Política classificação de informação e na PSI007 - Política de mesa limpa e tela limpa, são consideradas confidenciais neste item.
É recomendável que se a pessoa autorizada não estiver no local de trabalho, os documentos em papel e todas as mídias de armazenamento de dados classificadas como confidenciais devem ser removidas da mesa ou de outros locais (impressoras, máquinas de fax, copiadoras, etc.) para evitar o acesso não autorizado.
Esses documentos e essas mídias devem ser armazenados de forma segura de acordo com a política de classificação de informação e na política de mesa limpa e tela limpa.
As informações confidenciais devem ser removidas da tela, caso a pessoa autorizada não esteja no local de trabalho, e o acesso deve ser negado a todos os sistemas aos quais essa pessoa possua autorização de acesso.

5.10 Proteção de instalações e equipamentos compartilhados

Os locais onde se encontram os recursos de informações do NEES devem ter proteção e controle de acesso físico compatíveis com o seu nível de criticidade. A definição e implementação das medidas de prevenção e recuperação, para situações de desastre e contingenciamento, devem ser efetuadas e atualizadas de forma permanente.
Os documentos que contêm informações restritas ou confidenciais devem ser removidos imediatamente de impressoras, máquinas de fax e copiadoras.

5.11 Datacenter

O acesso ao Datacenter é realizado através de leitor biométrico ou senha de acesso, sendo restrito a equipe da Gerência de Infraestrutura e Gerente Administrativo (em caso de emergência).

O acesso de visitantes ou terceiros somente poderá ser realizado com acompanhamento de um colaborador autorizado.

O acesso ao Datacenter, por meio de chave, apenas poderá ocorrer em situações de emergência, quando a segurança física do Datacenter for comprometida, como por: incêndio, inundação ou abalo da estrutura predial.

O Datacenter deverá ser mantido limpo e organizado, qualquer procedimento que gere lixo ou sujeira nesse ambiente somente poderá ser realizado com a colaboração da Gerência de Infraestrutura.

Não é permitida a entrada de nenhum tipo de alimento, bebida, produto fumígeno ou inflamável.

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência, via chamando à Gerência de Infraestrutura e a Diretoria responsável pelo acesso ao Datacenter.

5.12 Uso da Internet

A Internet pode ser acessada somente por meio da rede local da organização com a infraestrutura adequada e proteção do firewall.

O acesso direto à Internet por meio de modem, acesso móvel à Internet, rede sem fio ou outros dispositivos de acesso direto à Internet convém que seja autorizado pelo gestor da área, em caso de falha no link de internet do NEES.

O uso de Internet deve ser apenas através da arquitetura segura definida pela Gerência de Infraestrutura, utilizando-se de recursos firewall (software que serve como parede de proteção contra invasões externas à rede local).

O usuário não deve alterar a configuração do navegador da sua máquina no que diz respeito aos parâmetros de segurança. Havendo necessidade, a Gerência de Infraestrutura deve ser acionada para informar o procedimento a ser seguido.

É proibido:

- A visualização, transferência, cópia ou qualquer outro tipo de acesso a sites de conteúdo pornográfico ou relacionados a sexo, bem como a distribuição, interna ou externa, de qualquer tipo de conteúdo proveniente destes sites; que defendam atividades ilegais; que menosprezem, depreciem e incitem o preconceito a determinadas classes, como sexo, raça, orientação sexual, religião, nacionalidade.

- A transferência ou cópia de arquivos de vídeo, som, ou quaisquer outros tipos de arquivos que não sejam relacionados aos interesses de negócios do NEES. Este tipo de ação afeta diretamente os recursos de rede.

Participação em:

- Salas de chat ou grupos de discussão de assuntos não relacionados aos negócios do NEES ou qualquer discussão pública sobre os negócios do NEES, através do uso de salas de chat, grupos de discussão, ou qualquer outro tipo de fórum público, a menos que autorizado pela Diretoria Executiva.

A Gerência de Infraestrutura pode bloquear o acesso a algumas páginas da Internet para usuários, grupos de usuários ou todos os bolsistas da organização. Se o acesso a algumas páginas da web for bloqueado, o usuário deve enviar uma solicitação formalizando o registro através de chamado no endereço https://atendimento.nees.ufal.br para obter autorização de acesso a essas páginas. O usuário não deve tentar contornar essa restrição de forma autônoma.

O usuário deve considerar todas as informações recebidas através de sites não sendo confiáveis.

O usuário é responsável por todas as consequências possíveis que surjam do uso não autorizado ou inadequado dos serviços ou do conteúdo da Internet.

O ambiente de internet deve ser usado pelos usuários para o desempenho das atividades profissionais do NEES. Sites que não contenham informações que agreguem conhecimento profissional e para o negócio não devem ser acessados.

Os acessos realizados nesse ambiente são monitorados pelo NEES com o objetivo de garantir o cumprimento dessa política.

O acesso à Internet só será permitido aos sites liberados e autorizados pelo NEES, e poderá ser monitorado pela Gerência de Infraestrutura.

O NEES se reserva o direito de bloquear, sem aviso prévio, o acesso a sites cujo conteúdo não seja do seu interesse.

5.13 E-mail e outros métodos de troca de mensagens

Os métodos de troca de mensagens estão descritos na política de transferência de informação. A Gerência de Infraestrutura determina o canal de comunicação que pode ser utilizado e as possíveis restrições de autorização de uso.

Os usuários só podem enviar mensagens que contenham informações verdadeiras. Não pode originar ou encaminhar mensagens ou imagens que:

- Contenham declarações difamatórias ou linguagem ofensivas de qualquer natureza;
- Menosprezem, depreciem ou incitem ao preconceito a determinadas classes, como sexo, raça, orientação sexual, idade, religião, nacionalidade ou deficiência física;
- Possua informação pornográfica, obscena ou imprópria para um ambiente profissional;
- Possam trazer prejuízo a outras pessoas;
- Sejam hostis ou inúteis;
- Que defendam ou possibilitem a realização de atividades ilegais;
- Sejam ou sugiram a formação ou divulgação de correntes de mensagens;
- Possam prejudicar a imagem da entidade ou seus serviços;
- Possam prejudicar a imagem de outras organizações ou sejam incoerentes com as políticas e códigos da entidade.
- Que somando os cabeçalhos, conteúdo e anexos sejam superiores a 20mb.

Os usuários não devem enviar e-mails não desejados com correntes, propagandas, links e afins para pessoas com as quais não tenham relações comerciais ou que não solicitaram a informação em questão.

Caso o usuário receba e-mail de spam, deve reportar o incidente de acordo com o especificado no Procedimento de Gestão de Incidentes.

Se enviar uma mensagem com um rótulo de confidencialidade, o usuário deve protegê-la conforme especificado na Política de classificação da informação.

Todos os e-mails devem conter avisos de isenção, exceto mensagens enviadas por meio dos sistemas de comunicação determinados pela Gerência de Infraestrutura.

Os bolsistas somente devem ter conta de e-mail quando for estritamente necessário, notadamente para a execução de suas atividades, devendo a criação da conta ser autorizada pelo Coordenador do projeto. A criação da conta de e-mail dar-se-á através de abertura de chamado pelo Coordenador do Projeto ou pessoa designada por este.

5.14 Direitos autorais

Os usuários não devem copiar o software de propriedade do NEES sem autorização, exceto em casos permitidos pela lei ou pelo proprietário do software.

O processo de cópia/transferência da licença deve ser aprovado pela Diretoria de Operações e executado pela Gerência de Infraestrutura.

Os usuários não devem copiar o software ou outros materiais originais de outras fontes e são responsáveis por todas as consequências que possam surgir de acordo com a lei de propriedade intelectual.

5.15 Computação móvel

Os equipamentos de computação móvel incluem todos os tipos de computadores portáteis, celulares, smartphones, cartões de memória e outros equipamentos móveis usados para armazenar, processar e transferir dado.

5.15.1 Regras básicas

Deve-se tomar cuidados especiais quando o equipamento de computação móvel estiver em carros ou em outros tipos de transporte, espaços públicos, quartos de hotel, locais de reuniões, centros de conferência e outras áreas não protegidas fora das instalações da organização.

O usuário que levar equipamento de computação móvel, pertencente ao NEES, para fora das instalações da organização deve seguir essas regras:

- Os equipamentos de computação móvel que contiverem informações importantes, confidenciais ou críticas não devem ser deixados sem supervisão e, se possível, devem ser trancados fisicamente. Também é possível usar travas especiais para garantir a segurança do equipamento;
- Ao usar equipamentos de computação móvel em locais públicos, o usuário deve tomar cuidado para que os dados não sejam lidos pelas pessoas não autorizadas.
- A proteção contra códigos maliciosos é feita de acordo com o item 5.5.
- A pessoa que usa equipamentos de computação móvel fora das instalações é responsável por, periodicamente, criar cópias de segurança dos dados.
- A conexão com redes de comunicação e a troca de dados deve refletir a confidencialidade dos dados e ser realizada através do acesso via VPN.
- A proteção de dados confidenciais deve ser implementada de acordo com a Política de classificação da informação caso os equipamentos de computação móvel sejam deixados sem supervisão, as regras para uso de equipamentos sem supervisão devem ser aplicadas de acordo com a Política de mesa limpa e tela limpa (Item 5.9).

Para todos os usuários que utilizam dispositivos móveis do tipo celular corporativo será obrigatório assinar um Termo de Responsabilidade pela Guarda e Uso de Equipamento, informando todas as características e acessórios.

5.16 Trabalho remoto

Trabalho remoto significa que equipamentos de informação e comunicação são usados para permitir que os usuários trabalhem fora da organização.

O trabalho remoto não inclui o uso de celulares fora das instalações da organização. Demais orientações encontram-se na PSI008 - Política de Byod.

5.17 Incidentes

Os bolsistas, fornecedores ou terceiros que tenham acesso aos dados e/ou sistemas do NEES devem informar quaisquer fragilidades ou eventos que indiquem um possível incidente, conforme a Política de gestão de incidentes.

6. REGISTROS

Os registros relacionados com este procedimento são:

Nome do Registro	Local de Armazenamento	Responsável pelo Armazenamento	Controles Para Proteção dos Registros	Tempo de Retenção
Termo de Comando	FUNDAÇÃO PARQUE	FUNDAÇÃO PARQUE	Após criado o mesmo não deve ser modificado	5 anos
Termo de Responsabilidade	FUNDEPES	FUNDEPES	Após criado o mesmo não deve ser modificado	(*) 35 anos
Termo de Cessão de Uso de Retirada de Equipamentos	Google drive / Pastas individuais p/ projeto	Apoio Administrativo	Após criado o mesmo não deve ser modificado	35 anos

(*) O termo de responsabilidade fica em guarda no prazo de 35 anos, 5 anos no arquivo intermediário e 30 no tempo de precaução, descritos na tabela de temporalidade documental da FUNDEPES, a qual foi baseada no que norteia o CONARQ-CONSELHO NACIONAL DE ARQUIVOS.

7. DISTRIBUIÇÃO E CONTROLE

Este documento está disponível e controlado através do sistema INTEGRA, módulo conhecimento/ ISO 27001/Políticas. Deve ser atualizado anualmente.

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	18/02/2024	Criação do documento.	Francisco Meneses
02	07/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e assinaturas, via sistema INTEGRA	Shirley Vital

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-04-24 14:45
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-04-24 16:47
Aprovador: Edmilson Gomes Fialho, Diretor Executivo, em 2025-04-24 17:40