1. OBJETIVO

A finalidade deste documento é definir regras para o controle de acesso físico e lógico às informações e outros ativos associados com base nos requisitos de segurança da informação e dos projetos que o Núcleo de Excelência em Tecnologias Sociais – NEES atua, para obtenção de acesso.

Este documento aplica-se a todo o escopo do Sistema de Gestão da Segurança da Informação - SGSI do NEES (sistemas, equipamentos, instalações e informações do escopo do SGSI).

2. ABRANGÊNCIA

Os usuários destes documentos são os bolsistas do NEES.

3. DOCUMENTOS DE REFERÊNCIA

- ISO/IEC 27001 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos
- PSI 001 - Política de segurança da informação
- Declaração de aplicabilidade
- PSI 002 - Política de Classificação da Informação
- Lei Geral de Proteção de Dados (LGPD)

4. DEFINIÇÕES

4.1 Controle de acesso: O controle de acesso é um elemento central de segurança da informação que formaliza quem tem permissão para acessar determinados aplicativos, dados e recursos e sob quais condições.

O princípio básico é que o acesso a todos os sistemas, redes, os serviços e as informações sejam proibidos a menos que expressamente permitido a usuários e grupos de usuários.

O acesso a todas as áreas físicas não é permitido, exceto às áreas que requerem concessão de privilégios por parte da pessoa autorizada, (item 4.2- Gerenciamento de privilégios).

5. DIRETRIZES

Para concessão de acesso, exclusão, alteração ou suspensão de acesso aos sistemas e a rede, é necessário que os Diretores, Gestores, Coordenadores de Projetos e/ou pessoas

designadas por estes, solicitem via e-mail: gerencia.infraestrutura@nees.ufal.br, ao responsável pelo acesso ao Datacenter.

5.1 Perfis de usuários por sistema

Os Perfis de acesso de usuários da Governança, Equipe de Infra e Equipes dos Projetos do NEES, possuem os seguintes direitos de acesso.

NOME DO SISTEMA	SERVIÇOS	NÍVEL DE ACESSO
Sistema SIPAC	Inventário dos ativos	Não temos acesso para definir perfis.
GITLAB	Controle de acesso ao código-fonte de programas	Equipe de Infra do NTI: Owner Coordenadores de projeto: Maintainer Equipe de Projeto: Developer ou Reporter (definido pelos coordenadores de projeto)
KEYCLOAK	Gerenciamento de chaves	Gerências de Qualidade e Infra: admin geral Líder Técnico de Projeto: admin do seu próprio realm Equipe de Projeto: user do seu próprio realm
VAULT	Gerenciamento de secrets	Equipe de Infra: admin Equipe de Projeto: User (acesso restrito a pasta do projeto)
EKS / LOKI	Registros de eventos	Gerências de Qualidade e Infra: admin geral Líder Técnico de Projeto: admin do seu próprio namespace Equipe de Projeto: user do seu próprio space
Orchestra	Gerenciamento do Datacenter	Equipe da Gerência de Infraestrutura: admin Equipe de Projeto: User
Portainer	Gerenciamento do Cluster Swarm	Equipe da Gerência de Infraestrutura: admin Equipe de Projeto: User (acesso apenas as stacks do projeto por ambiente: dev, hmg ou prod)
TrueNAS	Gerenciamento de armazenamento compartilhado	Equipe da Gerência de Infraestrutura: admin Equipe de Projeto: User (acesso apenas as stacks do projeto por ambiente: dev, hmg ou prod)
Bacula	Gerenciamento de backup	Gerência de Infraestrutura: admin Equipe da Gerência de Infraestrutura: user
pfSense	Firewall	Equipe de segurança: admin

Grafana	Dashboards de monitoramento	Gerências de Infra e Qualidade: admin Demais usuários: user (acesso concedido sob demanda)
Integra	Cadastro de pessoal e monitoramento de projetos	Gerências de Infra e Qualidade: admin Demais usuários: user (acesso concedido sob demanda)

5.2 Gerenciamento de privilégios

Os privilégios relacionados aos perfis de usuários mencionados acima (concedendo ou removendo os direitos de acesso são alocados da seguinte forma):

- Todas as concessões e revogações de privilégios são feitas pela gerência de infraestrutura, por meio de abertura de chamado por parte dos Coordenadores / Vice-Cooordenadores de projeto, ou pessoa designada por estes, através do e-mail atendimento@nees.ufal.br.
- Ao alocar os privilégios, o responsável deve levar em consideração os requisitos dos negócios e de segurança para acesso, conforme definido na avaliação de riscos, bem como a classificação das informações que são acessadas com esses direitos de acesso, de acordo com a PSI002 - Política de classificação da informação.

5.3 Análise periódica dos direitos de acesso

Os proprietários do sistema e das instalações para os quais são necessários direitos de acessos especiais, devem analisar se os direitos de acesso concedidos estão de acordo com os requisitos dos negócios e de segurança, de acordo com os seguintes intervalos:

- Todos os acessos serão revisados periodicamente a cada ano, ou quando houver demanda por parte de algum projeto específico.

Os relatórios das análises são arquivados no sistema INTEGRA.

5.4 Acesso Físico Datacenter e Arquivo Físico

O acesso ao Datacenter é restrito à Gerência de Infraestrutura e a equipe autorizada, sendo devidamente acompanhados pelo Gestor.

É responsabilidade da Gerência de Infraestrutura monitorar e controlar os serviços residentes no Datacenter.

Somente a Gerência de Infraestrutura está autorizada a liberar o acesso físico às instalações do Datacenter.

No caso do arquivo físico do NEES, apenas os bolsistas da Governança e Apoio Administrativo dos projetos são autorizados a ter acesso ao local, outros bolsistas podem ter acesso com sua devida permissão e acompanhamento.

5.5 Acesso Físico às Instalações Administrativas

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 bolsista autorizado.

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

Caso haja necessidade do acesso não emergencial, a área requisitante deve solicitar autorização com antecedência, via email: gerencia.infraestrutura@nees.ufal.br responsável pelo acesso ao Datacenter.

5.6 Registro e cancelamento de usuário

5.6.1 Concessão

A concessão de acesso ao bolsista deverá ocorrer somente mediante autorização prévia de pessoal devidamente autorizado. A direção e/ou os Gestores devem autorizar os acessos do pessoal administrativo e os coordenadores e/ou vice-coordenadores deverão autorizar os acessos da equipe do projeto. A autorização deve ser feita via abertura de chamado, através do e-mail atendimento@nees.ufal.br.

O procedimento de concessão de registro do usuário deverá ser revisado a cada 6 meses.

5.6.2 Alteração

No caso de mudança de função dentro da empresa, o bolsista deverá ter seus acessos e senhas reajustados de acordo com a sua nova função.

O procedimento de alteração de acesso deverá ser revisado a cada 12 meses.

5.6.3 Revogação

O bolsista que for desligado do NEES deverá ter seus direitos de acesso à sistemas, aplicativos e plataformas revogados imediatamente após o encerramento de sua bolsa.

5.7 Implementação técnica

A implementação técnica da alocação ou remoção dos direitos de acesso é de responsabilidade da gerência de infraestrutura e sua equipe, que será atendida sob demanda mediante abertura de chamado através do e-mail **atendimento@nees.ufal.br.**

A gerência de infraestrutura e sua equipe poderá ou não conceder ou remover direitos de acesso livremente, mas somente com base nos perfis dos usuários definidos nesta Política e nas solicitações das pessoas autorizadas a alocar privilégios.

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
Graylog / Loki	Banco de dados	Gerência de Infraestrutura	Após criado o mesmo não pode ser modificado	5 anos
Termo de Confidencialidade, Sigilo e Tratamento de Dados	Sistema INTEGRA	Gerência de Infraestrutura	Após assinado o mesmo não deve ser modificado	Permanente
Planilha Matriz de acesso às pastas da rede	Google drive / Pasta/Gestão Geral dos projetos	Apoios Administrativos dos projetos	Após criado o mesmo não deve ser modificado	Permanente

7. DISTRIBUIÇÃO E CONTROLE

Este documento está disponível e controlado através do sistema INTEGRA, módulo conhecimento/ ISO27001/Políticas. Deve ser atualizado anualmente.

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	22/12/2023	Criação do documento.	Francisco Meneses
02	03/12/2024	Revisão do item 1, correção de usuário. Item 2, atualização da referência do item da norma ISO 27002. Item 4, mudança do e-mail p/ solicitação de acesso. Subitens 4.1 e 4.3 e item 5, inclusão do INTEGRA. Item 6, mudança no período de revisão.	Francisco Meneses
03	08/04/2025	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 2025-04-28 22:46
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-04-29 00:04
Aprovador: André Magno Costa de Araújo, Coordenador de Projeto, em 2025-05-20 19:56