

1. OBJETIVO

Este procedimento tem como objetivo definir as diretrizes e procedimentos para o gerenciamento de identidade utilizado pelo NEES.

2. ABRANGÊNCIA

Este procedimento se aplica a todos os usuários, fornecedores e terceiros que tenham acesso às redes e serviços de rede do NEES.

3. DOCUMENTOS DE REFERÊNCIA

- Norma ABNT NBR ISO/IEC 27001 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos

4. DEFINIÇÕES

4.1 Autenticação: processo de validação da identidade do usuário, geralmente feito pela combinação de identificação de usuário e senha.

4.2 Concessão de Acesso: procedimento por meio do qual uma pessoa ou máquina passa a poder ler o conteúdo de uma base de dados bem como permissões em sistema de gerenciamento de banco de dados.

4.3 Confidencialidade: propriedade que garante que a informação seja acessada somente por pessoas ou processos que tenham autorização para tal.

4.4 Conta de Acesso: identificação única de usuário, com senha associada, para acesso aos recursos de TIC do NEES.

4.5 Controles: medidas de proteção física ou lógica, conforme cada grau de confidencialidade, que garantam acesso exclusivamente a pessoas e máquinas autorizadas.

4.6 Senhas de Usuários: senhas utilizadas para acesso aos recursos de TIC, tais como estações de trabalho e sistemas do NEES.

4.7 Identidade Digital: representa uma entidade, a qual pode ser uma pessoa, uma coisa da IoT, um serviço, entre outros.

5. DIRETRIZES

5.1 Gestão de identidade utilizada

- a) Para identidades atribuídas às pessoas tais como e-mail, ou login de acesso a qualquer sistema, uma identidade específica somente poderá estar vinculada apenas a uma única pessoa vedado o compartilhamento de identidades;
- b) Identidades atribuídas a várias pessoas (por exemplo, grupos de e-mails ou grupos dentro de um determinado sistema) só são permitidas quando forem necessárias por razões de negócios ou operacionais e estão sujeitas à aprovação e documentação dedicadas e desde que seja possível identificar a autoria do grupo;
- c) Identidades deverão ser desativadas ou removidas em tempo hábil se não forem mais necessárias (por exemplo, se suas entidades associadas forem excluídas ou não mais utilizadas, ou se a pessoa ligada a uma identidade deixou a organização ou mudou o de papel), cabe às lideranças ou pessoas designadas por estas, solicitar a Gerência de Infraestrutura por meio de chamado através do e-mail atendimento@nees.ufal.br para que possa proceder com os bloqueios necessários;
- d) Todos os eventos significativos sobre o uso e gestão de identidades de usuários e as informações de autenticação são mantidas em local seguro e de acesso registro.

6. REGISTROS

Os registros relacionados com este procedimento são:

- Sistema INTEGRA.

7. DISTRIBUIÇÃO E CONTROLE

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

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	05/02/2024	Criação do documento.	Francisco Meneses
02	12/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e assinaturas, via sistema INTEGRA	Shirley Vital