1. OBJETIVO

O objetivo deste procedimento é garantir que o acesso a sistemas, aplicativos e dados confidenciais seja concedido somente a indivíduos autorizados e para fins específicos, minimizando o risco de acesso não autorizado, uso indevido e violações de segurança.

2. ABRANGÊNCIA

Este procedimento aplica-se a todos os bolsistas, fornecedores e terceiros que tenham acesso a sistemas, aplicativos e dados 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 Direitos de Acesso Privilegiados (DAP): São aqueles que permitem aos usuários realizarem ações que podem comprometer a segurança da informação, como instalar software, modificar configurações de sistema ou acessar dados confidenciais.

4.2 Usuário Privilegiado: Indivíduo que possui DAP.

5. DIRETRIZES

5.1 Responsabilidades

5.1.1 Diretor de Segurança da Informação (DSI): Responsável pela implementação e monitoramento deste procedimento.

5.1.2 Administrador de Segurança da Informação: Responsável pela gestão do DAP, incluindo a concessão, revogação e monitoramento de acessos.

5.1.3 Usuários Privilegiados: Responsáveis por utilizar os DAP de forma segura e ética.

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-04-28 22:50
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-04-28 23:59
Aprovador: André Magno Costa de Araújo, , em 2025-05-20 19:56

5.2 Procedimentos para Concessão, Revogação e Monitoramento de DAP

5.2.1 Concessão de DAP

- A solicitação de DAP deve ser feita através do ServiceDesk (https://atendimento.nees.ufal.br) com o usuário autenticado com e-mail institucional, justificando seu pedido e indicando a duração do DAP, esta solicitação deverá ser aprovada pelo responsável da área de negócio.
- DSI deve avaliar a necessidade do DAP e determinar o nível de acesso adequado.
- O administrador de segurança da informação deve conceder o DAP no sistema de controle de acesso.
- O usuário privilegiado deve receber treinamento sobre o uso seguro dos DAP.

5.2.2 Revogação de DAP

- DAP deve ser revogado quando o usuário não precisar mais dele, quando não fizer mais parte da equipe do NEES, ou quando expirar o prazo de concessão.
- O administrador de segurança da informação deve revogar o DAP no sistema de controle de acesso.

5.2.3 Monitoramento de DAP

- O uso de DAP deve ser monitorado para detectar atividades suspeitas.
- Os registros de acesso devem ser revisados periodicamente pelo administrador de segurança da informação.
- Incidentes de segurança relacionados ao DAP devem ser investigados e remediados.

5.3 Controles

- **Segregação de funções:** Implementar a segregação de funções para garantir que nenhum usuário tenha controle total sobre um sistema ou aplicativo.
- **Princípio do menor privilégio:** Conceder aos usuários apenas os DAPs necessários para realizar suas tarefas, baseado sempre no princípio do *ZeroTrust*.

- **Autenticação forte:** Exigir autenticação forte para todos os usuários privilegiados, como senhas complexas, autenticação multifator (MFA) ou biometria.
- **Monitoramento e registro:** Monitorar o uso de DAP e registrar todas as atividades.
- **Treinamento e conscientização:** Treinar os usuários privilegiados sobre o uso seguro dos DAP e os riscos de segurança da informação.

6. REGISTROS

- Não se aplica.

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	07/05/2024	Criação do documento.	Francisco Meneses
02	14/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e assinaturas, via sistema INTEGRA	Shirley Vital