1. OBJETIVO

Esse documento tem como objetivo detalhar como ocorre a segregação de funções no NEES.

2. ABRANGÊNCIA

Este procedimento é aplicável aos bolsistas do NEES.

3. DOCUMENTOS DE REFERÊNCIA

3.1 ISO/IEC 27001 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos.

4. DEFINIÇÕES

4.1 Segregação de Funções: A segregação de funções e áreas de responsabilidade visa separar as funções conflitantes entre diferentes indivíduos, a fim de evitar que executem potenciais funções conflitantes por conta própria. Tem como propósito, reduzir o risco de fraude, erro e desvio de controles de segurança da informação. (ISO 27002:2022)

Os princípios que podem ser aplicados a segregação de funções são:

- Separação Sequencial – Quando uma atividade da organização é dividida em etapas realizadas por diferentes pessoas (Ex: solicitações, autorização e implementação de direitos de acessos).
- Separação Individual – Quando no mínimo duas pessoas devem aprovar uma atividade antes que ela seja feita (Ex: pagamento de fornecedores; aquisições materiais).
- Separação Espacial – Quando diferentes atividades são realizadas em diferentes locais.
- Separação Fatorial – Quando vários fatores contribuem para se completar a atividade (Ex: acesso por autenticação de dois fatores: senha + código de verificação por SMS, senha + aplicativo de autenticação, ou senha + biometria (impressão digital ou reconhecimento facial).

5. DIRETRIZES

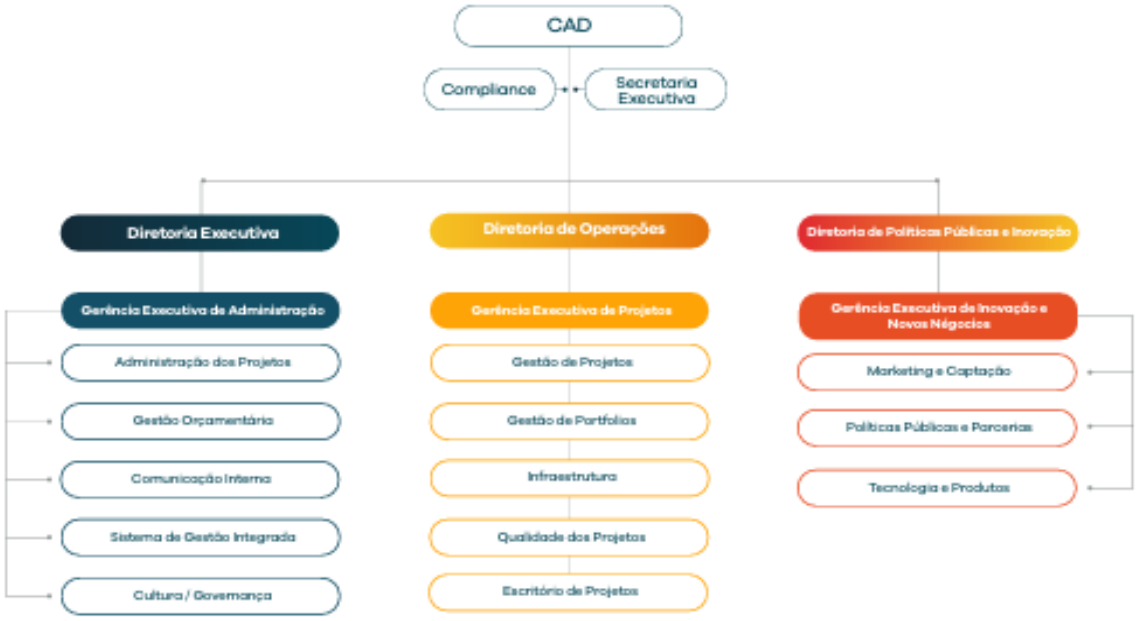
5.1 Estrutura Organizacional do NEES

O NEES está estruturado em 03 níveis hierárquicos, sendo:

Elaborador: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-14 10:30
Revisor: Milka Alves Correia Barbosa, Coordenadora de Cultura/Governança, em 2025-05-14 17:41
Aprovador: Edmilson Gomes Fialho, Diretor Executivo, em 2025-05-14 19:26

1. O Conselho Administrativo (CAD) é composto por seis integrantes. Além dos integrantes estão diretamente ligados: a Secretaria Executiva e a Gerência de Compliance/Jurídico.
2. Diretoria Executiva e Diretoria de Políticas Públicas: compostas por dois diretores, os quais contam com suas respectivas equipes de Gestores.
3. Gerências Executivas: compostas pelos gerentes executivos e respectivas unidades de apoio.
4. Equipe de Projeto – Coordenador, Vice-Coordenador, Gerentes de Projeto e Desenvolvimento (profissionais com competências técnicas específicas, que executam as ações dos projetos).

Figura 01 – Organograma Institucional (V4)



5.2 Funções Indispensáveis

As funções e áreas de responsabilidade para a segurança da informação, que precisam ser segregadas, estão listadas a seguir:

a. **Diretoria Executiva de Gestão:** responsável por analisar e aprovar as políticas e parâmetros de segurança da informação que atendam aos padrões administrativos do NEES. Estão diretamente ligados a esta diretoria:

- **Gerência Administrativa dos Projetos:** Tem como uma das responsabilidades, a gestão do patrimônio, compreendendo as ações voltadas ao planejamento, controle e monitoramento dos ativos relacionados aos projetos.
- **Gerência de Cultura / Governança:** responsável pelo levantamento das competências, registrar papéis e responsabilidades, acessar informações sobre o perfil dos bolsistas, dentre outras.
- **Gerência de Marketing e Comunicação:** responsável por divulgar as políticas de SI definidas pelo NEES.
- **Gerência de Sistema de Gestão Integrada:** responsável por monitorar a implantação das políticas e procedimentos de segurança da informação, de acordo com as premissas adotadas pelo NEES.
- **Gestão Orçamentária**: responsável pelos processos de controle e acompanhamento dos recursos financeiros dos projetos.

b. Gerência Executiva de Projetos, vinculada às duas Diretorias (Executiva e de Políticas Públicas), é responsável por aprovar políticas e parâmetros de SI mediante interesses operacionais do NEES. Conta com 05 (cinco) gestores em sua equipe, sendo as funções indispensáveis para SI:

- **Gerência de Infraestrutura:** responsável por monitorar e implementar políticas e parâmetros de SI, de acordo com as premissas adotadas pela Diretoria Operacional.
- **Gerência da Qualidade dos Projetos:** Desenvolver políticas e padrões de controle de qualidade para o NEES, em consonância com a segurança da informação.

c. Coordenador de Projeto, Vice-coordenador e o Gerente de Projeto: Coordenam e gerenciam as ações e as evidências dos projetos, trabalhando em estreita colaboração com a equipe de desenvolvimento, atendendo aos requisitos de Segurança da Informação.

5.3 Controles de Melhoria

O NEES além da segregação pré-determinada optou por fazer a implementação de alguns requisitos operacionais e técnicos para auxiliar na segurança da informação da organização, baseados na norma ABNT NBR ISO/IEC 27002:2022, tais como:

- O controle organizacional 5.15: controle de acessos aos serviços de rede da organização e todo o monitoramento de acesso, pré-determinados na PSI 004 - Política de Controle de Acesso.

- O controle tecnológico 8.15 - Log: controle baseado no registro de atividades, exceções, falhas e outros eventos relevantes; sendo produzidos, armazenados, protegidos e analisados. Este controle está definido na PSI 011 - Política de Coleta de Evidências e no procedimento POP.SGSI_007 - Gerenciamento da trilha de auditoria e informações de log do sistema.

Assim como, outras medidas adicionais são adotadas:

- auditorias internas que permitem a organização recriar os reais eventos desde o início até a sua situação atual, existindo sempre em conjunto com a supervisão pela gestão que tem por objetivo avaliação e tratativa apropriada e em tempo hábil de situações excepcionais;
- cuidados para impedir que uma única pessoa possa acessar, modificar ou usar ativos sem a devida autorização ou detecção, como a recomendação de que o início de um evento seja separado de sua autorização.
- para todos os ambientes da organização, sejam eles da governança ou equipe de projetos, é obrigatória a implementação de segregação de funções. Para casos de exceção, seja por limitação técnica ou de negócio, é obrigatório o uso de controles adicionais de segurança da informação, após aprovação do Gerente de Infraestrutura.

6. REGISTROS

Registro relacionado com este procedimento:

6.1 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 REVISÕES

Revisão	Data	Descrição	Responsável
01	19/01/2024	Criação do documento	Shirley Vital
02	27/09/2024	Inclusão do item 3.1 e revisão do item 4.1, sendo incluída a nova estrutura organizacional do NEES.	Shirley Vital, Milka Barbosa
03	06/04/2025	Mudança na estrutura do documento, atualização do itens 1.	Milka Barbosa
04	13/05/2025	Mudança da fig. 01-Organograma	Milka Barbosa

Elaborador: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-14 10:30
Revisor: Milka Alves Correia Barbosa, Coordenadora de Cultura/Governança, em 2025-05-14 17:41
Aprovador: Edmilson Gomes Fialho, Diretor Executivo, em 2025-05-14 19:26