1. OBJETIVO

Esta política estabelece os requisitos para garantir a segurança da informação e do software em caso de troca de informação dentro e fora da organização.

2. ABRANGÊNCIA

Este documento aplica-se a todo o escopo do Sistema de gestão da segurança da informação (SGSI). Os usuários deste documento são os bolsistas do NEES.

3. DOCUMENTOS DE REFERÊNCIA

- Norma ABNT NBR ISO 27002 - Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação.
- Norma ABNT NBR ISO/IEC 27001 - Sistemas de gestão de segurança da informação – Requisitos.
- Norma ABNT NBR ISO 31.000 - Sistema de Gestão de Riscos.
- PSI.002 - Política de classificação da informação.

4. DEFINIÇÕES

- **Partes Interessadas:** as partes interessadas correspondem a todos os elementos (pessoas, instituições, grupos, órgãos governamentais, etc.) que de alguma forma afetam ou são afetados pela organização.

5. DIRETRIZES

5.1 Transferência de informações

5.1.1 Canais de comunicação eletrônica

A comunicação é realizada, principalmente, por meio dos canais de comunicação apresentados na tabela 01. A Gestão de Infraestrutura define as possíveis restrições de permissão para uso de canais como: e-mail, HD externo no ambiente NEES. As divulgações em site e redes sociais são realizadas pela equipe de comunicação, atendendo às solicitações das equipes.

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-07-16 17:47
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-07-16 19:08
Aprovador: André Magno Costa de Araújo, Coordenador de Projeto, em 2025-07-25 18:26

Tabela 01 - Canais de comunicação eletrônica

CANAL DE COMUNICAÇÃO	TIPO DE INFORMAÇÃO	PROIBIÇÃO
E-mail	Externa, Interna e Restrita	Informações Confidenciais
Download de Arquivos	Pública	Download de informações internas e restritas só é permitido com autenticação. Informações confidenciais não devem ser baixadas via download de arquivos
OneDrive	Pública, Interna e Restrita	Informações Confidenciais
Telefones	Pública, Interna e Restrita	Informações Confidenciais
HD Externo	Pública e Interna	Informações restritas e confidenciais apenas criptografadas
WhatsApp	Pública e Interna	Informações restritas e confidenciais
Google Meet/Teams	Pública, Interna e Restrita	Informações confidenciais
SFTP	Pública, Interna, Restrita e Confidencial	Informações confidenciais
Site e redes sociais (Facebook, Instagram e LinkedIn)	Pública	Informações confidenciais
fileSender@RNP	Interna, Restrita e Confidencial	Compartilhamento com membros não federados.

5.1.2 Relações com partes externas

As partes interessadas externas do NEES estão identificadas no FP013. As trocas de informações do NEES com as partes interessadas, como: fornecedor, cliente, só devem acontecer após a assinatura de contrato ou documento equivalente que comprove o compromisso das partes com a segurança da informação, dentre os outros itens acordados. O coordenador do projeto que solicitou a aquisição do produto / serviço é responsável por assinar o contrato, por meio da Fundação de apoio, onde devem constar:

- A identificação da parte interessada externa,
- A responsabilidade com a segurança da informação,
- Dentre outras.

6. REGISTROS

Esta norma não gera nenhum registro, não necessitando assim, do quadro de controle de registros.

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	17/05/2024	Criação do documento.	Francisco Meneses
02	13/04/2025	Revisão da estrutura de todo o documento, revisão do item 5.1.1 e inclusão do INTEGRA no controle e assinatura do documento	Francisco Meneses
03	30/06/2025	Revisão do item 5.1, tab. 01 e do item 5.2	Shirley Vital