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), isto é, a toda a tecnologia de informação e comunicação que fazem parte do escopo.
Os usuários deste documento são os colaboradores 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 NBRISO/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 sua organização.

5. DIRETRIZES

5.1 Transferência de informações

5.1.1 Canais de comunicação eletrônica

As informações da organização devem ser trocadas por meio dos seguintes canais de comunicação eletrônica: e-mail, download de arquivos da Internet, transferência de dados via fileSender@RNP (https://filesender.rnp.br/), telefones, mídias portáteis, fóruns e redes sociais (Facebook, Instagram e LinkedIn).

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-04-28 22:47
Revisor: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-04-28 23:01
Aprovador: André Magno Costa de Araújo, Coordenador de Projeto, em 2025-05-20 19:55

A Gestão de Comunicação determina o canal de comunicação que pode ser usado para cada tipo de informação, e, com o apoio da equipe de Infraestrutura, definem as possíveis restrições de permissão para uso dos canais de comunicação, isto é, define quais atividades são proibidas.

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 poder ser baixadas via download de arquivos
OneDrive	Pública, Interna e Restrita	Informações Confidenciais
Telefones	Pública, Interna e Restrita	Informações Confidenciais
Fax	Pública, Interna e Restrita	Informações Confidenciais
CD/DVD	Pública, Interna e Restrita	Informações Confidenciais
Pendrives e HD Externo	Pública e Interna	Informações Restritas e Confidenciais apenas criptografadas
WhatsApp	Pública e Interna	Informações Restritas e Confidenciais
Skype/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

Partes externas incluem os fornecedores de serviços, as fundações responsáveis pelo controle administrativo e financeiro dos projetos, as empresas de manutenção de hardware e software, empresas que gerenciam transações ou processamentos de dados, clientes etc.

Antes de trocar informações e/ou softwares com qualquer parte externa, um contrato deve ser assinado, isso é responsabilidade do Gestor de cada contrato. O contrato deve estar em papel ou formato eletrônico (por exemplo, um contrato sobre termos e condições gerais) e deve conter cláusulas que estejam de acordo com a avaliação de riscos, incluindo, no mínimo:

- O método de identificação do terceiro
- As autorizações para acesso às informações
- A resposta a incidentes
- Os rótulos e a gestão de informações confidenciais

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

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-04-28 22:47
Revisor: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-04-28 23:01
Aprovador: André Magno Costa de Araújo, Coordenador de Projeto, em 2025-05-20 19:55