1. OBJETIVO

A finalidade desta política é garantir que a identificação e o entendimento das necessidades de proteção das informações sejam realizados adequadamente e comunicados, de acordo com a sua importância para o NEES.

2. AMPLITUDE

Este documento aplica-se a todo o escopo do sistema de gestão da segurança da informação (SGSI).

Os usuários destes documentos 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.

4. DEFINIÇÕES

Classificação da Informação: ação de definir o nível de relevância da informação, a fim de assegurar que a informação receba a proteção adequada, conforme seu valor, requisitos legais, sensibilidade e criticidade para a organização.

Informação Interna: são informações destinadas ao uso interno, não podem ser compartilhadas fora da organização sem autorização. Representam baixo nível de confidencialidade.

Informação Pública: são informações que podem ser disponibilizadas e acessíveis a qualquer pessoa, sem restrição.

Informação Confidencial: são informações que requerem níveis mais altos de segurança, por conter informações sensíveis.

Rotulação da Informação: registro, das informações, do nível de classificação e do grupo de acesso atribuído a estas informações.

5. DIRETRIZES

5.1 Classificação da informação

5.1.1 Níveis de confidencialidade

As informações devem ser classificadas de acordo com os níveis de confidencialidade, apresentados na tabela abaixo:

NÍVEL DE CONFIDENCIALIDADE	RÓTULOS	CRITÉRIOS DE CLASSIFICAÇÃO	RESTRIÇÃO DE ACESSO
Público (Site, NEES Comunica, NEES 360)	Sem rótulo	Tornar a informação pública não pode prejudicar a organização de qualquer forma	As informações estão disponíveis para o público
Uso Interno (Políticas, Procedimentos e formulários do SGSI)	INTERNO	O acesso não autorizado às informações pode causar danos pequenos e/ou inconveniências à organização	As informações são disponibilizadas aos bolsistas e a alguns terceiros com controle de acesso.
Restrito (Dados pessoais dos clientes e bolsistas, evidências dos projetos)	CONFIDENCIAL	O acesso não autorizado às informações pode causar danos catastróficos (irreparáveis) aos negócios e/ou à reputação da organização	As informações são disponibilizadas somente para pessoas autorizadas

5.1.2 Proteção da informação confidencial

Para proteção da informação confidencial, o NEES têm estabelecido:

- O Termo de Confidencialidade Sigilo e Tratamento de Dados;
- Implantadas as políticas de segurança de dados;
- Verificar regularmente os sistemas de segurança da informação;
- Implantado o plano de contingência para lidar com incidentes de segurança da informação;
- Conscientizar os usuários sobre a importância da confidencialidade e os riscos de segurança da informação;
- Monitora constantemente o comportamento dos usuários.

5.1.3 Pessoas autorizadas

A informação classificada como "Restrita" / "Confidencial" só deve ser compartilhada com pessoas autorizadas, em que o proprietário da informação especifique o(s) nome(s) ou e-mail da(s) pessoa(s) que têm direito de acesso a este tipo de informação.

A mesma regra aplica-se ao nível de confidencialidade "Interno", o proprietário da informação deve compartilhar com pessoas internas e externas ao NEES, em caso específico de necessidade de acesso a esse tipo de documento.

5.1.4 Reclassificação

Os proprietários de ativos devem analisar o nível de confidencialidade de seus ativos de informações a cada ano e avaliar se o nível de confidencialidade pode ser alterado. Se possível, o nível de confidencialidade deve ser reduzido.

5.2 Gestão de informações classificadas

Todas as pessoas que acessam informações classificadas devem seguir as regras listadas na tabela a seguir. O Comitê do SGSI deve iniciar uma ação disciplinar sempre que as regras forem violadas ou se as informações forem transmitidas a pessoas não autorizadas. Todos os incidentes relacionados à gestão de informações classificadas devem ser informados de acordo com a PSI011 - Política de Gestão de Incidentes.

Os ativos de informações podem ser retirados das instalações somente após autorização de acordo com a PSI003 - Política de Uso Aceitável dos Ativos.

O método de eliminação e destruição de mídia seguro é descrito no POP.SGSI_003 - Descarte e Transferência de Mídias.

MÍDIA	USO INTERNO	RESTRITO	CONFIDENCIAL
Documentos eletrônicos	• Somente pessoas autorizadas podem ter acesso. • Quando os documentos forem enviados por serviços como FTP, mensagens instantâneas, etc., devem ser protegidos por senha. • O acesso ao sistema de informações em que o documento está armazenado deve ser protegido por senha forte. • A tela em que o documento é exibido deve ser bloqueada automaticamente.	• Somente pessoas autorizadas podem acessar a área do sistema de informações em que o documento está armazenado. • quando os documentos forem enviados por serviços como FTP, mensagens instantâneas, etc., eles devem ser criptografados. • Somente o proprietário do documento pode apagá-lo.	• o documento deve ser armazenado em um formato criptografado. • o documento só pode ser armazenado em servidores controlados pela organização. • o documento não deve ser enviado por serviços não seguros como FTP, mensagens instantâneas e outros. Sempre utilizar meios de transmissão com criptografia. Ex: SFTP, SSH.
Sistemas de informações	• somente as pessoas autorizadas podem ter acesso. • os acessos aos sistemas de informações	• Os usuários devem desconectar-se do sistema de informações se saírem temporária ou permanentemente do local	• O acesso ao sistema de informações deve ser controlado por meio de um processo de autenticação seguras de

	devem ser protegidos por senha forte ● a tela deve ser bloqueada automaticamente depois de 5 minutos de inatividade. ● o sistema de informações só pode estar localizado em salas com acesso físico controlado.	de trabalho ● Os dados só devem ser excluídos por meio de um algoritmo que garanta a eliminação segura.	acordo a política de gestão de senhas. ● O sistema de informações só pode ser instalado em servidores controlados pela organização ● o sistema de informações só pode estar localizado em sala com acesso físico controlado e controle de identidade das pessoas que acessam o local
E-mails	● somente pessoas autorizadas podem ter acesso ● o remetente deve verificar atentamente o destinatário ● todas as regras em "Sistemas de informações" são aplicáveis	● o e-mail deve ser criptografado se for enviado para fora da organização	● Todos os e-mails devem ser criptografados.
Mídia de armazena-mento eletrônico	● somente pessoas autorizadas podem ter acesso ● as mídias ou os arquivos devem ser protegidos por senha ● se enviado para fora a organização, a mídia deve ser enviada como carta registrada ● a mídia só pode ser armazenada em salas com acesso físico controlado	● As mídias e os arquivos devem ser criptografados ● se a mídia for enviada para fora da organização, um serviço de confirmação de recebimento deve ser contratado ● somente o proprietário da mídia pode apagá-la ou destruí-la	● a mídia deve ser armazenada em um cofre ● a mídia só pode ser transferida dentro e fora da organização por uma pessoa confiável em um envelope fechado e lacrado
Informações transmitidas oralmente	● Somente pessoas autorizadas podem ter acesso às informações quando forem transmitidas	● A conversa não deve ser gravada. ● Deve ser realizada em salas reservadas.	● Nenhum registro de transcrição deve ser mantido

5.3 Exceções

O uso de alguns sistemas proprietários não permite a rotulação da informação, mas deverão sofrer o tratamento adequado.

6. REGISTROS

Documentos do SGSI - informações de classificação no cabeçalho do documento.

Sistema INTEGRA - informações de pessoal.

Evidências de projetos.

7. DISTRIBUIÇÃO E CONTROLE

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

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	03/01/2024	Criação do documento.	Francisco Meneses
02	03/01/2025	Revisado o item 5.2.2 nível de confidencialidade	Shirley Vital
03	09/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e assinaturas via sistema INTEGRA.	Shirley Vital