1. OBJETIVO

A finalidade desta política é garantir a implementação adequada e consistente da criptografia, em todos os sistemas e processos do NEES, visando proteger os dados sensíveis contra acessos não autorizados, garantir a confidencialidade das informações transmitidas e armazenadas, bem como assegurar a integridade e autenticidade dos dados, contribuindo para a preservação da segurança da informação e o cumprimento das regulamentações de privacidade e conformidade. Ao seguir esta política, o NEES fortalece sua postura de segurança cibernética e reduz os riscos de violações de dados.

2. AMPLITUDE

A abrangência inclui as áreas do NEES que lidam com o processamento, armazenamento ou transmissão de dados sensíveis. Isso inclui, mas não se limita a, sistemas de informação, servidores, redes de comunicação, dispositivos móveis e aplicativos. Além disso, esta política se estende a todos os bolsistas e terceiros que tenham acesso aos recursos de TI do ambiente 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

Criptografia: processo de codificação e decodificação de dados para proteção da confidencialidade, integridade e autenticidade.

Dados sensíveis: informações que, se divulgadas ou alteradas de forma não autorizada, podem causar danos à empresa ou a seus clientes. Alguns exemplos são dados pessoais, propriedade intelectual, *secret keys* e *tokens* de aplicações, entre outras.

Algoritmos criptográficos: conjuntos de regras e procedimentos utilizados para criptografar e descriptografar dados. Inclui algoritmos de chave simétrica e algoritmos de chave pública ou assimétricos.

Elaborador: Evertton de Lima Silva, Analista de Redes, em 2025-05-12 14:36
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-12 17:23
Aprovador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-05-12 21:04

Algoritmos de chave simétrica: são algoritmos que utilizam a mesma chave tanto para criptografar, quanto para descriptografar. Isso significa que o remetente e o destinatário devem possuir e compartilhar a mesma chave secreta. Exemplos comuns são AES (*Advanced Encryption Standard*), DES (*Data Encryption Standard*) e 3DES (*Triple Data Encryption Standard*).

Algoritmos de chave pública: também conhecidos como criptografia de chave assimétrica, empregam um par de chaves matematicamente relacionadas: uma chave pública e uma chave privada. A chave pública é usada para criptografar os dados e pode ser distribuída livremente. Enquanto, a chave privada é usada para descriptografar os dados e deve ser mantida em segredo pelo seu detentor. Exemplos comuns são RSA (*Rivest-Shamir-Adleman*) e ECC (*Elliptic Curve Cryptography*). Amplamente utilizada no contexto de troca segura de chaves, assinaturas digitais e autenticação.

Chave de criptografia: valor secreto utilizado para criptografar e/ou descriptografar dados. Pode ser uma chave simétrica ou um par de chaves pública/privada.

Protocolos de comunicação seguros: conjunto de regras e procedimentos para garantir a segurança da comunicação de dados pela rede, incluindo HTTPS, SSL/TLS, SFTP, SMTPS, SSH, entre outros.

Políticas de rotação de chaves: práticas para alterar regularmente as chaves de criptografia, reduzindo os riscos associados à exposição prolongada das mesmas.

Segurança da informação: conjunto de práticas e medidas para proteger a confidencialidade, integridade e disponibilidade dos dados, bem como os sistemas e recursos de TI relacionados.

Conscientização em segurança: treinamento e educação fornecidos aos pesquisadores para aumentar sua compreensão e conscientização sobre os riscos de segurança cibernética e as melhores práticas para mitigá-los.

Auditoria de segurança: processo de avaliação e verificação dos controles de segurança implementados para garantir sua eficácia e conformidade com os requisitos de segurança da informação.

5. DIRETRIZES

5.1 Identificação de dados sensíveis

Realizadas análises abrangentes para identificar todos os tipos de dados sensíveis que requeiram proteção por meio da criptografia. Seguem os critérios para proteção:

5.1.1 Em banco de dados: deverá ter a criptografia de dados em repouso ativadas;

5.1.2 Em aplicação: deverá usar mecanismos de *Vault*, o NEES por padrão adota o *Hashicorp.*

Vault com separação de ambientes, *secrets* devem ser rotacionadas com frequência.

5.2 Seleção de algoritmos criptográficos

O NEES utiliza algoritmos criptográficos robustos e atualizados, levando em consideração os requisitos de segurança e as melhores práticas do setor.

5.2.1 Criptografia de dados em trânsito

- Para aplicações Web, é utilizado o protocolo HTTPS (Hypertext Transfer Protocol Secure).
- Para proteger segredos e *tokens* de aplicações, como credenciais de API ou chaves de acesso, é utilizado o mecanismo de segredos Vault.
- Nos serviços de e-mail, são utilizadas as versões seguras dos protocolos IMAP (Internet Message Access Protocol), POP3 (Post Office Protocol) e SMTP (Simple Mail Transfer Protocol).
- Nas demais aplicações, é utilizado o TLS (Transport Layer Security) para garantir um transporte seguro de dados.

5.3 Implementação consistente

A garantia de que a criptografia tenha sido implementada de forma consistente, abrange todos os sistemas e processos que lidam com dados sensíveis, desde o armazenamento até a transmissão dos dados.

5.4 Gestão eficiente de chaves

Estabelecidos procedimentos para o gerenciamento seguro das chaves de criptografia, incluindo sua geração, armazenamento, distribuição, rotação e revogação, conforme necessário.

5.4.1 Chaves privadas devem ser protegidas por senha;

5.4.2 Chaves públicas SSH, PGP ou GPG podem ser compartilhadas livremente, ou disponibilizadas no perfil do usuário, em ferramentas tais como Gitlab, Odoo etc.

5.5 Proteção da transmissão de dados

São utilizados protocolos de comunicação seguros para proteger a transmissão de dados pela rede, garantindo que as informações permaneçam protegidas durante o tráfego. Aplicações web mandatoriamente devem ser expostas por *https*.

Elaborador: Evertton de Lima Silva, Analista de Redes, em 2025-05-12 14:36
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-12 17:23
Aprovador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-05-12 21:04

5.6 Atualização regular

Os sistemas, aplicações e bibliotecas são mantidos atualizados com as últimas correções de segurança e patches de software para mitigar possíveis vulnerabilidades relacionadas à criptografia.

5.7 Conscientização e treinamento

São realizados treinamentos regulares sobre a importância da criptografia e as práticas recomendadas de segurança da informação para todos os pesquisadores, garantindo que estejam cientes de suas responsabilidades.

5.8 Monitoramento contínuo

As medidas de monitoramento contínuo foram implementadas para detectar e responder a possíveis incidentes de segurança relacionados à criptografia, garantindo a eficácia dos controles implementados.

5.9 Auditorias periódicas

As auditorias de segurança são realizadas periodicamente para avaliar a conformidade com este procedimento, identificar áreas de melhoria e garantir a eficácia das medidas de proteção implementadas.

6. REGISTROS

- Não se aplica.

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	03/05/2024	Criação do documento.	Evertton Silva
02	12/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e assinaturas, via sistema INTEGRA	Shirley Vital

Elaborador: Evertton de Lima Silva, Analista de Redes, em 2025-05-12 14:36
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-12 17:23
Aprovador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-05-12 21:04