1. OBJETIVO

O objetivo desta política é estabelecer a finalidade, a direção, os princípios e as regras básicas de gestão da segurança da informação do sistema de gestão de segurança da informação (SGSI) do NEES.

2. ABRANGÊNCIA

Os usuários deste documento são os bolsistas do NEES assim como as partes externas relevantes, que possuem acesso aos dados (Informações) que transitam no Núcleo.

Esse documento tem caráter particular e confidencial, não podendo ou devendo ser redistribuído sem prévia autorização e supervisão do(a) responsável pelo controle de documentos do SGSI, sendo a infração passível de punição pelas regras internas, bem como ações legais.

3. DOCUMENTOS DE REFERÊNCIA

- Norma ABNT ISO / IEC 27001 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisito
- MG.SGI_001 - Manual do Sistema de Gestão de Segurança da Informação, ítem 2 - Escopo do SGSI
- POP.SGSI_026 - Gestão de Risco Corporativo
- FP008 - Requisitos Legais, Estatutários, Regulamentares e Contratuais
- FP016 - Declaração de Aplicabilidade
- FP024 - Termo de Confidencialidade, Sigilo e Tratamento de Dados

4. DEFINIÇÕES

Confidencialidade: características das informações que estão disponíveis somente para pessoas autorizadas ou sistemas.

Integridade: características das informações que são alteradas somente por pessoas da forma permitida.

Disponibilidade: características das informações que somente pode ser acessada por pessoas autorizadas quando for necessário.

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-05-12 21:05
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-12 23:07
Aprovador: Edmilson Gomes Fialho, Diretor Executivo, em 2025-05-13 12:17

Informação: é um ativo que, como qualquer outro item importante para os negócios, têm um valor para a organização e consequentemente necessita ser adequadamente protegida.
A informação pode existir de diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou através de meios eletrônicos, mostrada em filmes ou falada em conversas. Seja qual for à forma pela qual a mesma é apresentada, transmitida, armazenada ou compartilhada, é recomendado que a mesma seja protegida adequadamente.
Segurança da informação - preservação da confidencialidade, integridade e disponibilidade da informação. A Segurança da Informação protege a informação de diversas ameaças para garantir a continuidade dos negócios, a integridade e a disponibilidade da mesma.
Sistema de gestão da segurança da informação (SGSI) - a parte do sistema de gestão que cuida do planejamento, implementação, manutenção, revisão e aprimoramento da segurança da informação.
Política de Segurança: é uma série de normas internas padronizadas pela empresa que devem ser seguidas à risca para que todas as possíveis ameaças sejam minimizadas e combatidas eficientemente por todos e pela equipe de segurança.

5. DIRETRIZES

As normas aqui estabelecidas devem ser seguidas por todos os bolsistas, parceiros e prestadores de serviços.
Ao ter acesso a Política de Segurança da Informação o bolsista estará comprometido a respeitar os tópicos aqui abordados e estará ciente de que seus e-mails e navegação na internet/intranet podem estar sendo monitorados. A equipe de segurança encontra-se a disposição para sanar dúvidas e prestar o apoio técnico necessário.

5.1 Política de Segurança da Informação do NEES

O descumprimento desta política ensejará em sanções administrativas, trabalhistas e judiciais.

5.1.1 Política de Controle de Acesso

Antes de serem autorizados a acessar as redes e serviços de rede, os usuários devem ler e concordar com a PSI_004 - Política de Controle de Acesso da organização, que inclui diretrizes para o uso apropriado das redes e serviços de rede.

Todos os usuários devem usar uma identificação exclusiva e uma senha segura para acessar as redes e serviços de rede. A autenticação é realizada por meio de um sistema de autenticação centralizado.

O acesso aos serviços de rede, como correio eletrônico, arquivos e aplicativos, são concedidos de acordo com as necessidades de trabalho dos usuários e com as diretrizes da política de acesso baseado em ***Zero-Trust***.

No primeiro acesso de todos os usuários, o mesmo deve entrar com o nome de seu usuário e senha, sendo obrigado pelo sistema automaticamente a mudar para uma senha nova contendo alguns parâmetros obrigatórios, conforme descritos no item 4.1.1.

A senha terá um tempo de vida útil pré-determinado pela equipe de segurança, devendo o mesmo ser respeitado, caso contrário o usuário ficará sem acesso.

O NEES revisará regularmente as permissões de acesso às redes e serviços de rede para garantir que os usuários só tenham acesso às informações e serviços de que precisam para realizar suas funções.

a) Critérios para Criar Senha

Os critérios aceitos para criação de senha forte e mais segura, pelos usuários, estão listados a seguir:

- O tamanho da senha precisa ter entre 8 e 100 caracteres;
- Deve conter uma combinação de letras, números e símbolos (apenas caracteres ASCII padrão);
- Conter pelo menos uma letra maiúscula, uma minúscula, um número e um símbolo;
- Opcionalmente utilizar mecanismos de autenticação de 2 fatores (2FA).

b) Segurança de Senhas

Além da senha ser criada com os critério informados em 4.1.1, faz-se necessário alguns atitudes, como:

- Manter o sigilo e confidencialidade da senha, garantindo a não divulgação para quaisquer outras partes, incluindo autoridades e lideranças.

- Evitar manter a senha anotada seja em papel, arquivos ou dispositivos móveis.
- Alterar sempre que existir qualquer indicação de comprometimento.
- Não utilizar a mesma senha para finalidades profissionais e pessoais.

LEMBRE-SE:

- Sua senha não deve ser passada a ninguém (em nenhuma hipótese), nem mesmo para a equipe de segurança. Caso desconfie que sua senha não está mais segura, sinta- se à vontade para mudá-la, mesmo antes do prazo determinado de validade.
- Tudo que for executado com a sua senha será de sua inteira responsabilidade, por isso tome todas as precauções possíveis para mantê-la secreta.

5.1.2 Política de e-mail

Os servidores de e-mail do NEES encontram-se protegidos contra vírus e códigos maliciosos, sendo requeridas algumas atitudes do usuário final, tais como:

- Não abra anexos com as extensões .bat, .exe, .src, .lnk e .com
- Desconfie de todos os e-mails com assuntos estranhos e/ou em inglês. Normalmente eles vêm com assuntos de receita federal, boleto de pagamento, contas de banco, ou algum tipo de coisa, que tenta enganar as pessoas, se passando por um conteúdo legítimo.
- Não reenvie e-mails do tipo corrente, criança desaparecida, criança doente, pague menos em alguma coisa, não pague alguma coisa, pandemias, fake News, informações políticas etc.
- Caso não seja necessário, não mande e-mails para mais de 08 pessoas de uma única vez (to, cc, bcc), todas as pessoas que receberem, vão utilizar espaço em disco no servidor, aumentando o tráfego de rede e de armazenamento nos servidores.
- Evite anexos muito grandes.
- Bancos, Receita Federal, Serasa, Solicitação de recadastramento etc., não deve ser aberto ou clicado. Não envie nenhum tipo de informação pessoal para e-mails que você não conheça. Em todo caso, sempre duvide e solicite ajuda da equipe de segurança.

“Não utilize o e-mail da empresa para assuntos pessoais. Todos os e-mails de domínio @nees.ufal são armazenados e auditados todos os dias”.

“É expressamente proibido o uso de e-mail profissional, para fins particulares”.

5.1.3 Política de Internet

O acesso à internet, nas dependências do NEES, dar-se-á, exclusivamente, pelos meios autorizados e configurados pela Gerência de Infraestrutura do NEES.

No caso dos usuários utilizarem o ambiente NEES, o acesso à internet será restrito aos seguintes tópicos:

- O uso recreativo da internet não deverá existir sem autorização da diretoria.
- É permitida apenas a navegação de sites, casos específicos que exijam outros protocolos deverão ser solicitados diretamente a equipe de segurança com prévia autorização do Gerente de Infraestrutura.
- Acesso a sites com conteúdo pornográfico, jogos, bate-papo, apostas e assemelhados estará bloqueado e monitorado.
- É proibido o uso de ferramentas P2P (bittorrent, Morpheus, Whatsapp, etc).
- É proibido o uso de IM (Instant Messenger, Skype, WhatsApp) não homologados/autorizados pela equipe de segurança. Exceto com autorização expressa da diretoria.

“Lembrando novamente que o uso da internet está sendo auditado constantemente e o usuário pode vir a prestar contas de seu uso”.

5.1.4 Política de uso de estação de trabalho

I. A entrada de pessoas em áreas de segurança do NEES deve ser controlada para que apenas pessoas autorizadas tenham acesso;

II. Uma vez concedido o acesso às áreas de segurança, as seguintes regras devem ser atendidas:

a) Ter registrado data e hora de entrada e saída de visitantes;

b) Ser proibido o consumo de comidas ou bebidas, ao se manipular algum ativo de informação, bem como ao se ter acesso a alguma área de segurança;

c) Em áreas de segurança, temperatura, umidade, poeira e gases devem ser controlados por dispositivos automatizados e sob manutenção regular para garantir seu perfeito funcionamento;

d) As proteções devem estar alinhadas aos riscos identificados.

Lembramos que sua estação é sua ferramenta de trabalho, mas também é um importante componente de segurança. Por isso observe as seguintes orientações:

- Não deve ser instalado nenhum tipo de software / hardware sem autorização da equipe técnica ou de segurança.
- Não armazene MP3, filmes, fotos e softwares com direitos autorais ou qualquer outro tipo de softwares.
- Todas as evidências e dados relativos aos projetos devem ser mantidos nos servidores do NEES, sejam códigos fontes, arquivos, apresentações, planilhas, etc, onde existe um sistema de backup diário e confiável. Caso não saiba como fazer isso, entre em contato com a equipe técnica.
- Em caso de cancelamento e/ou encerramento de bolsa, se houver arquivos ou e-mails particulares, os mesmos serão excluídos após auditoria junto com a conta do usuário sendo impossível ser recuperado.

Tudo o que for realizado com sua senha, será de sua responsabilidade.

Considerando que os bolsistas do NEES trabalham em formato home office, utilizando ambientes e computadores pessoais não controlados por códigos internos ou ferramentas de monitoração, a Política de Estações de Trabalho é válida apenas para o caso em que o usuário utilize as dependências do NEES.

No entanto é extremamente recomendável aos bolsistas que, mesmo trabalhando em home office, mantenham seus sistemas de operações e softwares de trabalho sempre atualizados, bem como fazer uso de antivírus.

5.1.5 Interação Social

- Não fale sobre a política de segurança da empresa com terceiros ou em locais públicos.
- Não diga sua senha para ninguém. Nossa equipe técnica jamais irá pedir sua senha.
- Não digite suas senhas ou usuários em outras máquinas de colaboradores, especialmente fora da empresa.
- Somente aceite ajuda técnica de membros de nossa equipe técnica previamente apresentado e identificado.
- Relate a equipe de segurança pedidos externos ou internos que venham a discordar dos tópicos anteriores.

5.1.6 Vírus e códigos maliciosos

Os vírus são os maiores geradores de problemas de segurança, alguns procedimentos simples podem ser adotados para evitar grandes transtornos:

- Mantenha seu computador com antivírus atualizado.
- Não traga HD externo, pen-drives ou CDs de fora da empresa. Caso isso seja extremamente necessário, encaminhe o mesmo para a equipe técnica, onde passará por uma descontaminação.
- Informe atitudes suspeitas em seu sistema a equipe técnica, para que possíveis vírus possam ser identificados no menor espaço de tempo possível.
- Suspeite de softwares que "você clica e não acontece nada".

5.2 Membros da Equipe de Segurança

Esta Política de Segurança da Informação envolve os seguintes papéis e responsabilidades:

a) Administradores de recursos de Tecnologia da Informação e Comunicações: equipe técnica responsável por um sistema de processamento de informações, serviço ou infraestrutura de TIC.

b) Custodiante da informação (qualquer pessoa que detém a posse das informações e dados): responsável por garantir a segurança das informações e dados sob sua posse e comunicar sobre situações que comprometam essa garantia;

c) Gestor da informação (colegiado, autoridade ou dirigente): responsável por classificar as informações e dados sob sua gestão e definir procedimentos e critérios de acesso;

d) Proprietário do ativo de informação: refere-se à parte interessada do órgão ou entidade da APF, indivíduo legalmente instituído por sua posição e/ou cargo, o qual é responsável primário pela viabilidade e sobrevivência dos ativos de informação;

e) Usuário: pessoa física, seja bolsista ou prestador de serviços, habilitada pela administração para acessar os ativos de informação no NEES, formalizada por meio da assinatura de termo de confidencialidade.

Os membros da equipe de segurança da informação, do NEES estão definidos no formulário FP015 - Membros da Equipe de Segurança da Informação, onde constam: os nomes, cargos que ocupam, e-mail e telefone. O formulário deve ser divulgado juntamente com a Política de Segurança da Informação.

6 REGISTROS

Registro relacionado com este procedimento:

- Sistema INTEGRA.

7 DISTRIBUIÇÃO E CONTROLE

Este documento está disponível e controlado através do sistema INTEGRA, módulo conhecimento / ISO 27001/ Procedimentos. Deve ser atualizado anualmente.

8 HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	20/11/2023	Criação do documento.	Francisco Meneses
02	03/06/2024	Mudança do aprovador, revisão no ítem 4, excluído o item 11	Francisco Meneses
03	06/04/2025	Revisão da estrutura de todo o documento para atender ao POP.SGSI_000. Retirado os campos para assinaturas, uma vez que será assinado no Integra.	Shirley Vital

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-05-12 21:05
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-12 23:07
Aprovador: Edmilson Gomes Fialho, Diretor Executivo, em 2025-05-13 12:17