1. OBJETIVO

Estabelecer os requisitos internos para gerir os eventos adversos que possam comprometer a segurança da informação.

2. ABRANGÊNCIA

Todos os bolsistas do NEES são responsáveis pela gestão de incidentes de segurança da informação.

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.

4. DEFINIÇÕES

- **Gestão de Incidentes de Segurança da Informação:** procedimentos estabelecidos para identificar, gerenciar, registrar, analisar e comunicar eventos relativos à segurança da informação, a fim de reduzir o impacto negativo causado, restabelecendo as operações em tempo hábil.
- **Evento de segurança da informação**: é um evento simples ou uma série de eventos de segurança da informação indesejados ou inesperados, que têm uma grande probabilidade de comprometer as operações do negócio e ameaçar a segurança da informação.
- **Incidente de segurança da informação**: é uma ocorrência identificada de um estado de sistema, serviço ou rede, indicando uma possível violação da política de segurança da informação ou falha de controles, ou uma situação previamente desconhecida, que possa ser relevante para a segurança da informação.

5. DIRETRIZES

5.1 Planejamento e preparação da gestão de incidentes

Os bolsistas e partes externas que usam os sistemas e serviços de informação do NEES, devem registrar e notificar quaisquer fragilidades de segurança da informação, suspeita ou

observada, nos sistemas ou serviços, devendo ser reportados a Gerência de Infraestrutura ou a Equipe de Resposta a Incidentes através do e-mail ***csirt@nees.ufal.br*** ou através do formulário web https://faleconosco.nees.ufal.br na categoria ***Incidente de Segurança da Informação*** se for um usuário interno do NEES ou cidadão brasileiro (login via gov.br).

5.1.1 Treinamento

Os membros da equipe de resposta a incidentes de segurança da informação devem estar treinados no plano de gestão de incidentes de segurança da informação.

- O treinamento deve cobrir os seguintes tópicos:
  - ✓ O papel e as responsabilidades da equipe de resposta a incidentes de segurança da informação.
  - ✓ O processo de resposta a incidentes de segurança da informação.
  - ✓ As ferramentas e técnicas utilizadas na resposta a incidentes de segurança da informação.

5.1.2 Testes e Simulados

- O NEES deve realizar testes e simulações de incidentes de segurança da informação para verificar a eficácia do plano de gestão de incidentes de segurança da informação.
- Os testes e simulações de incidentes de segurança da informação devem ser realizados periodicamente para garantir que o plano esteja atualizado e que a equipe de resposta a incidentes de segurança da informação esteja preparada para responder a incidentes de segurança da informação.

5.2 Avaliação e decisão sobre eventos da segurança da informação

Os eventos de segurança da informação são avaliados e é decidido se são classificados como incidentes de segurança da informação. Se classificado como incidente é realizada a abertura e registro de não conformidade para indicar o incidente, bem como a ação corretiva no sistema INTEGRA.

5.2.1 Avaliação de Eventos de Segurança da Informação

- O Gerente de Infraestrutura ou a Equipe de Resposta a Incidentes deve avaliar cada evento de segurança da informação para determinar seu impacto potencial na organização.
- A avaliação deve considerar os seguintes fatores:

- ✓ A natureza do evento.
- ✓ A severidade do evento.
- ✓ O escopo do evento.
- ✓ O impacto potencial do evento na organização.

5.2.2 Tomada de Decisão

- Com base na avaliação do evento de segurança da informação, o Gerente de Infraestrutura ou a Equipe de Resposta a Incidentes deve tomar uma decisão sobre as medidas a serem tomadas.
- As medidas a serem tomadas podem incluir:
  - ✓ Contenção do evento.
  - ✓ Investigação do evento.
  - ✓ Recuperação do evento.
  - ✓ Ações disciplinares.

5.2.3 Responsabilidades

- Gerente **de Infraestrutura**: É responsável por liderar a avaliação e a tomada de decisão sobre eventos de segurança da informação.
- Equipe **de Resposta a Incidentes**: É responsável por auxiliar na avaliação e na tomada de decisão sobre eventos de segurança da informação.

5.2.4 Documentação

- Todos os eventos de segurança da informação devem ser documentados na ferramenta SIEM.
- A documentação deve incluir:
  - ✓ A data e hora do evento.
  - ✓ A natureza do evento.
  - ✓ A severidade do evento.
  - ✓ O escopo do evento.
  - ✓ O impacto do evento na organização.
  - ✓ As medidas tomadas para conter, investigar e recuperar o evento.

5.3 Resposta a incidentes da segurança da informação

Os incidentes de segurança da informação são reportados para pessoas relevantes da

organização, ou ainda, partes externas.

Convém que a notificação, quando possível, inclua os seguintes itens:

a) contenção, se as consequências do incidente podem se espalhar, dos sistemas afetados pelo incidente;
b) coleta de evidências o mais rápido possível após a ocorrência;
c) escalonamento, conforme necessário, incluindo atividades de gestão de crises e possivelmente invocação de planos de continuidade de negócios;
d) garantia de que todas as atividades de resposta envolvidas sejam devidamente registradas para análise posterior;
e) comunicação da existência do incidente de segurança da informação ou quaisquer detalhes relevantes deles a todas as partes interessadas internas e externas relevantes seguindo o princípio da necessidade de conhecer;
f) coordenação com partes internas e externas, como autoridades, grupos de interesse externo e fóruns, fornecedores e clientes para melhorar a eficácia da resposta e ajudar a minimizar as consequências para outras organizações;
g) uma vez que o incidente foi tratado com sucesso, formalmente fechá-lo e registrá-lo;
h) análise forense de segurança da informação, conforme necessário;
i) análise pós-incidente para identificar a causa-raiz. Assegurar que seja documentada e comunicada de acordo com os procedimentos definidos;
j) identificação e gestão de vulnerabilidades e fragilidades de segurança da informação, incluindo aquelas relacionadas com os controles que causaram, contribuíram ou falharam em prevenir o incidente.

5.4 Aprendizado com incidentes de segurança da informação

O NEES usa o conhecimento adquirido com incidentes de segurança da informação para fortalecer e melhorar os controles, identificando incidentes recorrentes ou graves e suas causas para atualizar o processo de avaliação de risco de segurança da informação e determinar e implementar controles adicionais necessários para reduzir a probabilidade ou as consequências de futuros incidentes semelhantes.

6. REGISTROS

Os registros relacionados com este procedimento são:

- Sistema INTEGRA – Registro de não conformidade de incidente de segurança da informação.

- SIEM/Wazuh – Registro de identificação dos incidentes de segurança da informação.

7. Distribuição e Controle

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

8. Histórico de Alterações

Revisão	Data	Descrição	Responsável
1.0	19/03/2024	Emissão Inicial	Francisco Meneses
2.0	06/04/2025	Junção dos seguintes documentos: PSI011-Política de Coleta de Evidências; PSI016 - Política de Gestão de Incidentes e POP.SGSI014-Avaliacao e decisão sobre eventos de segurança da informação	Francisco Meneses