1. OBJETIVO

Estabelecer diretrizes, responsabilidades e controles necessários para garantir a segurança da informação dos serviços críticos de Tecnologia da Informação e Comunicação (TIC) utilizados pelo NEES, com ênfase em: serviços em nuvem, hospedagem local, desenvolvimento de software, gestão de identidade, banco de dados, redes, e serviços terceirizados.

2. ABRANGÊNCIA

Este procedimento se aplica a todos os serviços críticos de SI sob responsabilidade do NEES, incluindo:

- Serviços em nuvem (IaaS, PaaS, SaaS);
- Servidores e serviços on-premises;
- Ambientes de desenvolvimento de software;
- Sistemas internos de gestão de dados e identidades;
- Plataformas educacionais e repositórios digitais;
- Contratações de serviços externos;
- Equipes: Infraestrutura, Qualidade, DevOps, Gestão de Projetos e Suporte Técnico.

3. DOCUMENTOS DE REFERÊNCIA

- ISO/IEC 27001 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos
- https://cloudsecurityalliance.org/
- https://www.nist.gov/

4. DEFINIÇÕES

- **Provedor Externo:** fornecedor contratado para realizar serviços, produtos e/ou processos.
- **Qualificação do Provedor Externo:** é o processo de avaliar e selecionar fornecedores que vão fornecer produtos ou serviços que possam impactar na segurança da informação e diretamente na qualidade do produto ou serviço final.

- **Gerenciamento de identidade e acesso (IAM):** com as ferramentas e os serviços do IAM, os administradores gerenciam e controlam de maneira centralizada quem tem acesso a recursos específicos baseados na nuvem e no local. Com o IAM, é possível monitorar ativamente e restringir o modo como os usuários interagem com os serviços. Dessa forma, você aplica as políticas em toda a organização.
- **Prevenção contra perda de dados (DLP):** a DLP pode ajudar a ter visibilidade dos dados armazenados e processados, fornecendo recursos para descobrir, classificar e desidentificar automaticamente os dados regulamentados utilizados por serviços críticos.
- **Informações de segurança e gerenciamento de eventos (SIEM) :** as soluções de SIEM combinam informações de segurança e gerenciamento de eventos de segurança para oferecer monitoramento automatizado, detecção e resposta a incidentes até ameaças nos seus ambientes de nuvem. Ao usar as tecnologias de IA e ML, as ferramentas de SIEM permitem examinar e analisar dados de registros gerados nos aplicativos e dispositivos de rede, além de agir rapidamente caso uma possível ameaça seja detectada.
- **Infraestrutura de chave pública (ICP):** o framework é usado para gerenciar a troca de informações segura e criptografada usando certificados digitais. As soluções de ICP geralmente fornecem serviços de autenticação para aplicativos e verificam se os dados permanecem comprometidos e confidenciais por meio do transporte. Os serviços de ICP baseados na nuvem permitem que as organizações gerenciem e implantem certificados digitais usados para autenticação de usuários, dispositivos e serviços.
- **Serviços críticos:** Serviços cuja indisponibilidade, alteração ou violação impactam as operações, dados sensíveis ou reputação institucional.
- **Ambiente híbrido:** Infraestrutura que combina ambientes locais e baseados em nuvem.
- **Gestão de vulnerabilidades:** Processo contínuo de identificação, avaliação e mitigação de riscos técnicos.

5. DIRETRIZES

5.1 Responsabilidades

- **Alta Administração**: É responsável por garantir os recursos necessários à segurança da informação nos serviços contratados.

- **Gerente de Infraestrutura**: É responsável por validar a aquisição de produtos e serviços críticos necessários para a segurança da informação. O quadro 01 define as responsabilidades, no caso de serviço de computação em nuvem.

Quadro 01 - Distribuição de responsabilidades para serviço em nuvem

Modelo de serviço em nuvem	Responsabilidade do NEES	Responsabilidade da CSP
Infraestrutura como serviço (IaaS)	Proteger dados, aplicativos, controles de rede virtual, sistema operacional e acessos de usuários	O provedor de nuvem protege a computação, o armazenamento e a rede física, incluindo todos os patches e configurações.
Plataforma com serviços (Paas)	Proteger os dados, acesso de usuários e aplicativos.	O provedor de nuvem protege a computação, o armazenamento e a rede física, os controles de rede virtual e o sistema operacional.
Software como serviço (SaaS)	Proteger os dados e o acesso do usuário.	O provedor de nuvem protege a computação, armazenamento, rede física, controles de rede virtual, sistema operacional, aplicativos e middleware.

- **Usuários de serviços críticos**: São responsáveis por seguir os requisitos de segurança da informação definidos neste procedimento.

5.2 Avaliação de Risco

- O NEES e os projetos devem realizar uma avaliação de risco para identificar os riscos de segurança da informação associados ao uso de serviços em nuvem.
- A avaliação de riscos deve abranger todos os serviços críticos. Classificação dos ativos com base em impacto (confidencialidade, integridade e disponibilidade – CIA).

5.3 Qualificação de Fornecedor

A qualificação do fornecedor de serviço crítico deve ser realizada antes da contratação do serviço.

Para realizar a qualificação do fornecedor deve ser utilizado o formulário FP026 - Qualificação do Fornecedor de Serviço Crítico.

Após a realização da qualificação, deve ser realizada uma avaliação dos resultados e fazer a escolha com base nos resultados obtidos. Justificar, caso um fornecedor que apresentou uma nota mais baixa foi o escolhido, caso o responsável pela autorização do serviço verifique que o risco pode ser controlado.

Ao solicitar a contratação do fornecedor de serviço crítico para a Fundação, o NEES deve informar os critérios para qualificação inicial, além dos requisitos técnicos específicos, quando for o caso, que poderão variar, de acordo com o tipo de produto ou serviço.

5.3.1 Qualificação de Fornecedor de Serviços em Nuvem

O NEES deve qualificar e solicitar à Fundação a contratação de provedores de serviços em nuvem que ofereçam medidas de segurança adequadas aos riscos identificados na avaliação de riscos.

O NEES deve considerar os seguintes critérios ao selecionar um provedor de serviços em nuvem:

- A reputação do provedor em termos de segurança da informação.
- As medidas de segurança física e lógica implementadas pelo provedor.
- Os processos de auditoria e certificação do provedor.

5.4 Contratos de Serviços

O NEES deve analisar criticamente os contratos dos provedores de serviços críticos, contratados pela Fundação, verificando os requisitos de segurança da informação, dentre outros requisitos técnicos solicitados.

Exigir cláusulas contratuais de segurança e confidencialidade em qualquer serviço terceirizado ou parceria.

5.4.1 Contratos de serviços em nuvem

Os contratos de serviço em nuvem devem incluir os seguintes termos:

- Os tipos de informação que podem ser armazenados ou processados na nuvem.
- As medidas de segurança que o provedor deve implementar.

- Os direitos e responsabilidades da organização e do provedor em caso de incidente de segurança.

5.5 Monitoramento dos Serviços

Centralizar os logs em ferramenta SIEM, abrangendo ambientes físicos e virtuais.

5.5.1 Controle do serviço em nuvem

O NEES tem implementado um sistema de gerenciamento de acessos para controlar quem pode acessar os serviços em nuvem e a informação armazenada ou processada na nuvem.
O sistema de gerenciamento de acessos é baseado nos princípios de menor privilégio e necessidade de conhecimento (***ZeroTrust***).

5.5.2 Gestão de Acessos

Aplicar o princípio do menor privilégio em todos os ambientes. Implementar segregação de funções e autenticação multifator (MFA).

5.5.3 Segurança por Design

Projetos de desenvolvimento devem prever requisitos de segurança desde a concepção (DevSecOps).

5.5.4 Criptografia

O NEES criptografa a informação confidencial que é armazenada ou processada na nuvem, utilizando algoritmos de criptografia fortes e chaves de criptografia gerenciadas de forma segura. Padronizar algoritmos criptográficos conforme o NIST. Garantir backup automatizado e verificado, inclusive fora da nuvem.

5.5.5 Monitoramento e Auditoria

O NEES monitora e audita os serviços em nuvem para garantir que os requisitos de segurança da informação estejam sendo cumpridos. As auditorias devem ser realizadas em periodicidade regular, para verificar se as medidas de segurança estão sendo implementadas de forma eficaz.

5.6 Gestão de Incidentes de Segurança

Seguir a PSI016 - Plano de Continuidade do Negócio, para resposta a incidentes de segurança da informação, possibilitando a identificação e contenção do incidente, a investigação da causa do incidente, definição de medidas para remediar e prevenir a recorrência do incidente, fazer uso de ferramenta SIEM.
O Plano de Resposta a Incidentes deve considerar os tipos de ativos e serviços críticos.

5.7 Treinamento

Programas de conscientização para todas as equipes, com simulações de ataques e phishing.
O NEES deve realizar treinamento aos usuários de serviços em nuvem sobre os requisitos de segurança da informação.
O treinamento deve cobrir os seguintes tópicos:

- As políticas de segurança da informação da organização.
- Os riscos de segurança da informação associados ao uso de serviços em nuvem.
- As medidas de segurança que os usuários podem tomar para proteger a informação.
- Para onde os logs das aplicações devem ser direcionados.
- Como rastrear e auditar os logs.

6. REGISTROS

Os registros relacionados com este procedimento são:

- Ofícios de solicitação de serviços à Fundação;
- FP026 - Qualificação de Fornecedor - Segurança da Informação.

7. DISTRIBUIÇÃO E CONTROLE

Este documento está disponível e controlado através do sistema INTEGRA, módulo conhecimento/ ISO27001/Procedimentos. Deve ser atualizado anualmente ou após alterações em sistemas críticos.

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	19/03/2024	Criação do documento.	Francisco Meneses
02	22/04/2025	Revisão da estrutura de todo o documento, inclusão de outros serviços críticos e do controle via sistema INTEGRA	Francisco Meneses, Kleber José