1. OBJETIVO

Esta política tem como objetivo:

- Definir as regras aplicáveis com base na estrutura do NEES.
- Assegurar que todos os envolvidos e partes interessadas conheçam o Plano de Continuidade de Negócio (PCN);
- Promover um entendimento mais evidente e amplo das operações organizacionais, o que possibilita melhoria contínua;
- Identificar processos críticos e os impactos de sua paralisação para todo o Núcleo, e,
- Minimizar possíveis impactos negativos ao patrimônio e às partes interessadas.

2. AMPLITUDE

Este documento é aplicável às áreas que possam apresentar ameaças com grau de vulnerabilidade significantes.

3. DOCUMENTOS DE REFERÊNCIA

- Norma ABNT NBR ISO 27002 - Segurança da informação, segurança cibernética e proteção à privacidade — Controles de segurança da informação.

4. DEFINIÇÃO

- 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, reestabelecendo as operações em tempo hábil.

5. DIRETRIZES

5.1 Responsáveis pela Continuidade do Negócio

Tabela 01 – Contatos dos responsáveis

CARGO (PCN)	NOME	CONTATO	CARGO
Diretor de Crise	André Magno Costa de Araújo	(82) 99938-2012 andre.araujo@nees.ufal.br	Vice-Diretor do NEES
Gerente de Crise	Francisco Bruno de Souza Meneses	(82) 98801-3139 gerencia.infraestrutura@nees.ufal.br	Gerente de Infraestrutura

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-05-09 17:22
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-05-09 18:33
Aprovador: Edmilson Gomes Fialho, Diretor Executivo, em 2025-05-09 18:35

5.2 Responsável pelo Plano

O Plano de Continuidade de Negócios (PCN) assegurará ao NEES a continuidade de seus negócios em caso de paralisação, decorrente de sinistro, de um ou mais processos considerados críticos.

O sinistro torna-se realidade quando ameaças internas ou externas exploram as vulnerabilidades dos processos.

Os processos críticos ao negócio do NEES foram mapeados por meio de levantamento de informações com os Gestores das principais áreas de negócio.

Para tanto, o PCN é definido como (PCN = PAC + PCO + PRD), a saber:

- PAC = Programa de Administração da Crise – É acionado após decretada a Crise, e é voltado para todo o processo. Tem seu término quando se volta à normalidade;
- PCO = Plano de Continuidade Operacional – São acionados os primeiros procedimentos do PAC, e é voltado aos processos de negócio;
- PRD = Plano de Recuperação de Desastre – É acionado junto com o PCO, e é focado na recuperação/restauração de componentes que suportam o PCN.

O desenvolvimento do Plano de Continuidade de Negócios é baseado na avaliação dos processos críticos estabelecidos pela administração compreendendo às suas principais etapas:

- Análise de riscos de TI;
- Análise de Impacto nos Negócios (BIA);
- Estratégia de recuperação.

Desta forma será necessário simular situações de emergência, definir responsabilidades e escopo de atuação para os bolsistas que têm acesso às instalações do NEES, principalmente a sala cofre, na execução do PCN.

5.3 Site Principal e de Redundância

O NEES conta com duas unidades: a principal e a de redundância.

A unidade principal (site principal) situa-se na Sala Cofre da Universidade Federal de Alagoas onde os principais processos e operações da empresa são realizados.

A unidade de redundância (site redundância) contém exatamente todos os mesmos recursos tecnológicos da Unidade Principal. Portanto, em situações de contingência, para reduzir esse impacto, o site de redundância contém um espelho em tempo real do servidor do site principal do NEES.

5.3.1 Site de Redundância

Tabela 02 – Localização do site

LOCALIZAÇÃO	Amazon AWS Services
CONTATO	N/A

5.4 Plano de Monitoração e Declaração de Desastre

5.4.1 Critério para Definição de Desastre

Será considerado desastre quando o tempo total de recuperação dos processos for superior ao tempo máximo apontado no subitem 5.4.4 – Processos e Sistemas Críticos.

5.4.2 Monitoração de Comunicação de Eventos

Qualquer bolsista do NEES ao constatar alguma anormalidade que paralise quaisquer processos apontados no item 5.4.4 – Processos e Sistemas Críticos, tabela 04 deste Plano, deverá comunicar o fato ao seu superior imediato, este por sua vez comunicará o fato a um dos Líderes de Contingência, conforme apresentado na tab. 03.

Tabela 03 – Contatos das Lideranças e Equipe de Crise

CARGO (PCN)	NOME	CONTATO
Diretor de Crise	André Magno Costa de Araújo	(82) 99938-2012 andre.araujo@nees.ufal.br
Gerente de Crise	Francisco Bruno de Souza Meneses	(82) 98801-3139 gerencia.infraestrutura@nees.ufal.br
Equipe de Crise	Everton Cleiton	(82) 99607-6333 everton.oliveira@nees.ufal.br
	Evertton Silva	(82) 99634-4327 evertton.silva@nees.ufal.br
	Pedro Raposo	(82) 99615-5747 pedro.raposo@nees.ufal.br
	Glauber Ferreira	(82) 98204-8829 gerencia.qualidade@nees.ufal.br

Este é o meio de comunicação a ser utilizado pelos bolsistas do NEES como ponto central de contato para solicitar ajuda ou relatar alguma situação que demande o acionamento do PCN.

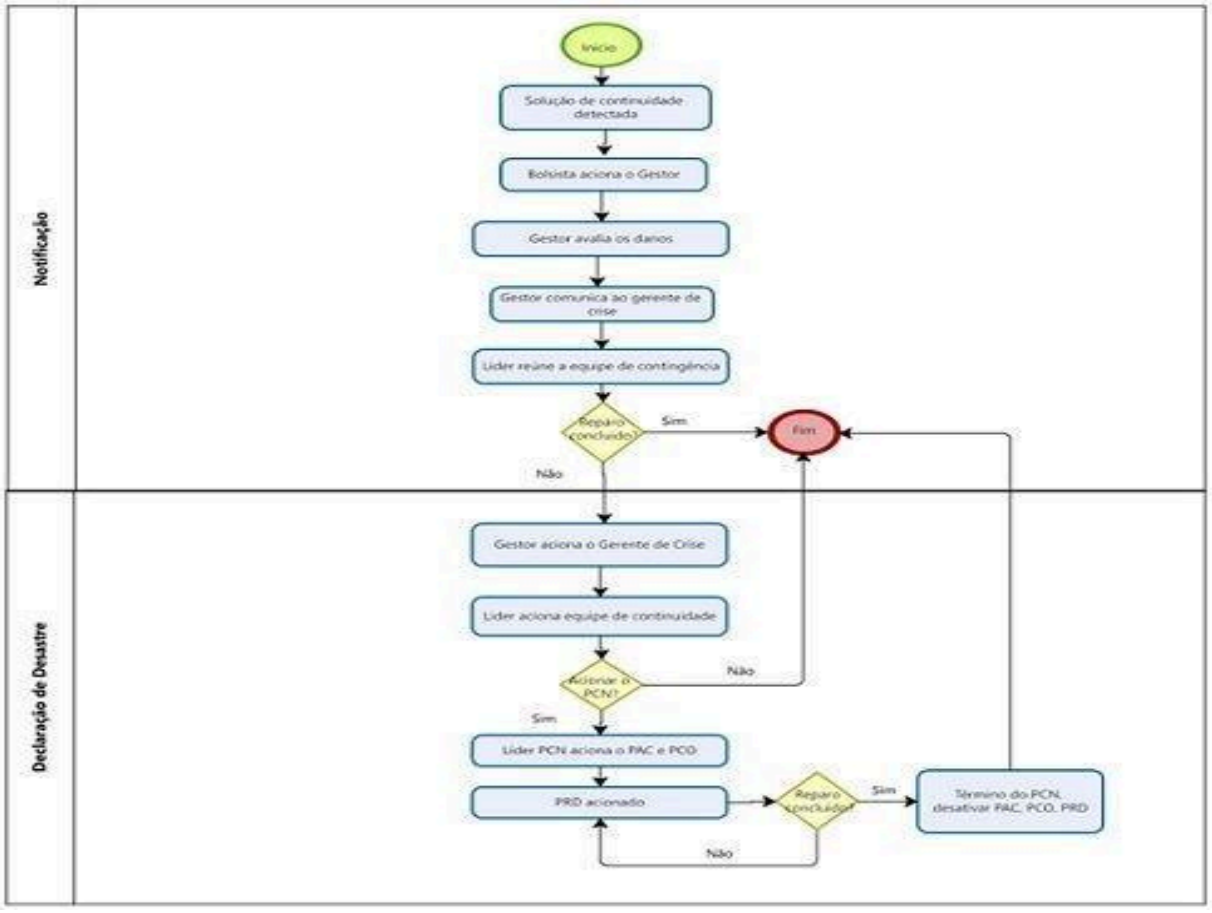
5.4.3 Declaração de Desastre/Contingência

Ao ocorrer qualquer evento que paralise algum processo essencial ao negócio, o gerente de crise avaliará a ocorrência e comunicará ao Diretor responsável pelo PCN.

Com base nas informações recebidas e avaliação do grau de impacto versus horário crítico, compete ao Diretor declarar ou não a contingência.

Em caso da ausência do Diretor responsável pelo PCN, o Gerente de crise assumirá interinamente. A fig. 01 apresenta o fluxograma de acionamento do PCN que resultará ou não na declaração da contingência.

Figura 01 - Fluxo de Acionamento do PCN



5.4.4 Processos e Sistemas Críticos

Processo crítico pode ser definido como um processo de trabalho que uma vez paralisado por tempo superior ao definido pela unidade gestora do negócio irá afetar sensivelmente as operações e serviços da organização gerando maior impacto nos clientes internos e externos, sendo definido pela fórmula (MTD = RTO + WRT).

Definição:

- MTD (Maximum Tolerable Downtime) = Trata-se do tempo máximo que um negócio pode tolerar a ausência ou indisponibilidade de uma função de negócio em particular. Diferentes funções de negócio terão diferentes MTD's.
- RTO (Recovery Time Objective) = Tempo disponível para recuperar sistemas e recursos de uma ruptura.
- WRT (Work Recovery Time) = Tempo que leva para copiar e rodar uma vez os sistemas (hardware, software e configuração) a serem restaurados para as funções de negócios críticas.

Tabela 04 - Processos com MTD de 4 horas

Área	Processo	Sistemas
Gerência de Infraestrutura	Criar novo cluster	N/A
Gerência de Infraestrutura	Restaurar Backup	Todos
Gerência de Infraestrutura	Testar acessos	Todos

5.5 Abrangências - Ameaças Relacionadas

No entendimento dos gestores das áreas avaliadas, as ameaças com grau de vulnerabilidade significantes estão divididas em:

a. **Humanas:** Greves, Distúrbio Civil, Falha de Prestador de Serviços/Parceiro, Acesso Indevido às Instalações e Erro Humano não intencional.
b. **Tecnologicas:** Falha em Aplicativo, Falha em Hardware, Falha em sistemas Operacionais, Vírus de Computador, Falha em Rede Interna (LAN), Falha na Entrada de Dados, Falha em Rede Externa (WAN), Falha de Telecom – Dados e Falha em Sistema de Acesso.
c. **Infraestrutura:** Falha em Telecom - Voz, Falha em Sistema de Refrigeração, Interrupção de Energia Elétrica, Falha em Instalações Elétricas.
d. **Naturais:** Alagamento Interno do Ambiente, Queda de Raios, Vendaval e Incêndio.
e. **Físicas:** Problema Estrutural ou de Instalações e Rompimento de Tubulação Interna (água, esgoto e gás).

Cabe ressaltar que paradas não programadas podem resultar em perdas tangíveis e intangíveis aos negócios do NEES, acarretando em perda de confiança das partes interessadas nos processos de negócio. Desta forma, os potenciais impactos apontados pelos gestores numa eventual interrupção no negócio são:

- Interrupção de prestação de serviços a clientes;
- Multas e sanções;
- Perda da capacidade de gestão e controle;
- Comprometimento da imagem da organização;
- Exposição negativa na mídia e perda de vantagem competitiva.

5.6 Ameaças às Instalações

Os bolsistas da Equipe de Crise deverão estar aptos a identificar as ameaças que possam levar a paralisação dos negócios e comunicar imediatamente ao líder do Plano de Continuidade de Negócios.

5.6.1 Ameaças para acesso

Foram destacadas as seguintes ameaças que possam impossibilitar o acesso ao prédio:

- Princípio de incêndio;
- Ameaça de bomba;
- Bloqueios;
- Manifestações.

5.6.2 Ações e Procedimentos

I. Ações de 05 a 10 minutos

Responsável: Líder do PCN

Procedimentos: A área administrativa entrará em contato com os coordenadores de projeto, para esclarecimentos, e, caso necessário, também fazer contato com os órgãos públicos, conforme seguem:

Órgãos Públicos:

- Bombeiros: 193 (Incêndio e Ameaça de Bomba);
- Defesa Civil: 199 (Ameaça de Bomba, Greves, Bloqueios e Inundações);
- Polícia Civil: 147 (Ameaça de Bomba, Roubo e Furto de Informações e ativos).

II. Ações em até 20 minutos após a conclusão da etapa anterior

- Entrar em contato com o responsável pelo backup, para avisá-lo sobre o incidente, bem como avisar os componentes que atuarão em regime Home Office.
- Disponibilizar alertas na intranet do NEES indicando o status de contingência, telefones dos bolsistas para atendimento.

5.6.3 Falha na Infraestrutura e Tecnologia

Para que não haja interrupções nas atividades no ambiente de TI do site principal da sede, a Unidade de Redundância será o site de contingência da sede.
A comunicação entre as unidades de negócio é feita por links redundantes. A seguir destacamos a infraestrutura de TI de cada unidade de negócio.

- Servidores
- Telecom
- Energia Elétrica

Na falta de energia elétrica, são ativados automaticamente os nobreaks localizados no site principal com autonomia de 15 minutos e o gerador que deve entrar em operação em até 3 minutos a contar da falha na energia elétrica, o gerador possui autonomia para até 72 horas.

As áreas abastecidas pelos nobreaks são:

- Distribuição
- Tecnologia da Informação
- Administrativo/Financeiro

5.7 Acionamento da Contingência Externa

Manter contato com o gestor da empresa contratada para prestação de serviços de redundância / backup e contingência e avisar do início do processo de contingência.
Como o site de contingência fica em nuvem, as equipes irão atuar de maneira remota, sob a coordenação do gerente de crises.

5.8 Procedimento de retorno à normalidade - Site Principal

Cabe ao Líder da Contingência encerrar o PCN e comunicar ao Diretor e aos Gestores envolvidos no processo.

Quando o acesso ao prédio estiver liberado e em condições de normalidade, comunicar aos bolsistas do NEES por meio de seus gestores para que retornem aos seus postos de trabalho no dia seguinte.
Solicitar à área de TI que retire o comunicado publicado no site do NEES sobre a situação de contingência.

5.9 Administração do Plano

A continuidade de negócios de uma organização, assim como a recuperação de desastres é o resultado da execução e da manutenção de um processo contínuo que envolve planejamento, formalização, monitoração e melhorias.
O processo de continuidade de negócios é da Gerência de Infraestrutura, que determina o ciclo e as etapas que deverão ser executadas para que tanto os cenários de risco e impacto sobre os negócios como as estruturas e estratégias que embasam o PCN possam ser atualizadas refletindo o ambiente de negócios do NEES.
Para que a área de TI possa verificar o grau de atualização do PCN e decidir quanto ao momento em que o processo de continuidade de negócios será atualizado, os processos de planejamento de negócios e tecnológico, gerenciamento de mudanças, gerenciamento de riscos, tratamento de problemas e de incidentes devem prever a participação desta área nas decisões relevantes destes processos.

5.10 Divulgação e Treinamento

Um dos fatores primordiais para o funcionamento deste plano são:

- o conhecimento e a familiaridade das pessoas e demais envolvidos na execução das atividades de continuidade de negócios, e,
- recuperação de desastres com as estratégias e recursos definidos no planejamento.

A divulgação do PCN é realizada anualmente para os bolsistas, possibilitando o conhecimento e familiaridade necessários.
Estas sessões serão organizadas pela área de TI em conjunto com a área Administrativa/Financeira com o objetivo de manter os colaboradores atualizados sobre os conceitos de continuidade adotados, os objetivos pretendidos com o planejamento e sobre o funcionamento da estratégia de recuperação de desastres e continuidade de negócios.

Para que este conhecimento seja preservado, os novos bolsistas e os bolsistas que passarem a realizar funções de negócios críticos, principalmente aqueles que pertencem à equipe de contingência, deverão ser instruídos das suas respectivas responsabilidades no plano.

O programa de treinamento deverá contemplar os riscos, ameaças, controles, responsabilidades, premissas e as estratégias do PCN, incluindo as alterações recentes.

5.11 Realização de Testes

Os testes têm por objetivo assegurar a eficiência e a efetividade do PCN e deverão ser planejados e executados com periodicidade mínima anual ou sempre que se adicionar algum equipamento e ou tecnologia nova a partir da data da sua implantação.

A responsabilidade pelo planejamento e organização dos testes, assim como pela definição dos cenários a serem contemplados é da área de Tecnologia da Informação.

Os cenários deverão ser definidos e registrados em um documento formal que deverá ser aprovado pela alta administração, deve ser mantido por um período mínimo de 5 (cinco) anos.

Os testes não deverão provocar quaisquer tipos de indisponibilidade ou parada nos ambientes de negócios do NEES e deverão ser conduzidos pela equipe de contingência em total conformidade com o definido. As simulações deverão ser realizadas sobre cenários e ameaças contemplados no plano, devendo cobrir os riscos e ameaças com maior probabilidade de ocorrência.

6. REGISTROS

Os registros relacionados com este procedimento são:

- Registro de Disaster Recovery - DR.

7. DISTRIBUIÇÃO E CONTROLE

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

8. HISTÓRICO DE ALTERAÇÕES

Revisão	Data	Descrição	Responsável
01	29/07/2024	Criação do documento.	Francisco Meneses
02	08/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e assinaturas no sistema INTEGRA e revisão do item 6.	Shirley Vital