1. OBJETIVO

Esta política estabelece as diretrizes para garantir que os requisitos de segurança da informação, relativos a recuperação de informações, em caso de perda dos arquivos originais, ou em caso de acidentes operacionais com os equipamentos do NEES, sejam alcançados.

2. AMPLITUDE

Esta política aplica-se a todos os ativos de informação que suportem o armazenamento de dados do NEES. Engloba os seguintes itens do processo de cópia de segurança:

- Tipos de backup
- Rotinas de backup gerais
- Backups especiais
- Tempo de retenção dos backups
- SLA de Restauração

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 - Segurança da informação, segurança cibernética e proteção à privacidade - Sistemas de gestão da segurança da informação - Requisitos

4. DEFINIÇÕES

- **Backup**: é o ato de copiar arquivos, pastas ou discos inteiros (físicos ou virtuais) de dispositivos eletrônicos para sistemas de armazenamento secundários, buscando a preservação do ambiente em caso de qualquer problema. O termo significa fazer cópia dos softwares, arquivos e outros dados em diferentes dispositivos de armazenamento para a recuperação do sistema em caso de falhas.

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-07-16 17:46
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-07-28 11:44
Aprovador: André Magno Costa de Araújo, Coordenador de Projeto, em 2025-07-28 11:55

5. DIRETRIZES

O serviço de backup atende as diversas áreas de negócio do NEES. Para uma melhor operacionalização, as rotinas de backup foram classificadas da seguinte forma:

- Logs
- Banco de dados Oracle
- Banco de dados PostgreSQL
- Banco de dados MySQL
- SLA de Restore

Cada tópico acima citado tem suas características próprias de backup, que serão expostas neste documento. Caso o responsável pelo servidor / sistema necessite de uma política diferenciada, deve entrar em contato com a gerência de Infraestrutura.

5.1 Rotina para realização do backup

5.1.1 Os backups diário possuem retenção de 30 dias e mensalmente é feito um backup full que é mantido por 60 dias.

5.1.2 Backup de Banco de Dados Oracle

i. Bancos de Dados de Produção

Para os bancos de produção, os backups full ocorrem diariamente durante a madrugada.

Os backups de archive ocorrem 03 (três) vezes de forma escalonada durante o dia.

Os backups de Export tem frequência diária, ocorrem durante a noite e são feitos para um diretório no servidor. Após o export concluir, o Bacula arquiva o conteúdo.

O backup de Dump é a cópia para fita de alguns arquivos de configuração no servidor e será executado uma vez por semana, aos domingos. A tab. 01 apresenta a frequência, período e retenção dos backups de produção:

Tabela 01 - Frequência, período e retenção dos backups de produção

Tipo	Frequência	Período	Retenção
Full	Segunda a domingo	Noite	30 dias
Archive	3 vezes / dia	Dia	30 dias
Export	Segunda a domingo	Noite	30 dias

ii. Bancos de Dados de Homologação

Para os bancos de homologação, **não** teremos backup, uma vez que os bancos de homologação são cópias do ambiente de produção.

iii. Bancos de Dados de Desenvolvimento

Para os bancos de desenvolvimento, os backups full ocorrem aos sábados de noite, segundo um escalonamento entre diversos bancos. Os backups de Archive não se aplicam no desenvolvimento. Os backups de Export tem frequência diária, ocorrem durante a noite e são feitos para um diretório no servidor. Após o export concluir, o Bacula arquiva o conteúdo. Abaixo, segue a tabela com a frequência, período e retenção dos backups de desenvolvimento:

Tipo	Frequência	Período	Retenção
Full	Sábado	Noite	30 dias
Archive	Não se aplica		
Export	Segunda a domingo	Noite	30 dias

5.1.3 Backup de Banco de Dados PostgreSQL

iv. Bancos de Produção

Tipo	Frequência	Período	Retenção
Full	Segunda a domingo	Noite	30 dias
Log transação	3 vezes / dia	Dia	30 dias
Dump	Segunda a domingo	Noite	30 dias

v. Bancos de dados de Homologação

Para os bancos de homologação, **NÃO** teremos backup, uma vez que os bancos de homologação são cópias do ambiente de produção.

vi. Bancos de Desenvolvimento

Para os bancos de desenvolvimento, os backups full ocorrem aos sábados pela noite, segundo um escalonamento entre os diversos bancos. Os backups de logs de transação ocorrem três vezes por dia, também de forma escalonada durante o horário comercial. Após

o dump concluir, o Bacula arquiva o conteúdo. Abaixo, segue a tabela com a frequência, período e retenção dos backups de desenvolvimento:

Tipo	Frequência	Período	Retenção
Full	Sábado	Noite	30 dias
Log transação	Não se aplica		
Dump	Segunda a domingo	Noite	30 dias

5.1.4 Backup de Banco de Dados MySQL

Seguirá o mesmo esquema do banco de dados PostgreSQL para todos os ambientes (Produção, Homologação e Desenvolvimento).

5.1.5 SLA de Restore

O atendimento de solicitações de restauração de arquivos, base de dados e demais componentes segue o fluxo abaixo:

Service Desk ➡ Equipe de DevOps ➡ Service Desk.

O tempo de recuperação é proporcional ao volume de dados necessários para o restore. A cada 20GB de dados, o tempo de recuperação é de aproximadamente uma hora. Esta estimativa é do tempo de atendimento da Equipe de DevOps, não contemplando o tempo do Service Desk.

5.2 Tipo de backup utilizado

Basicamente existem dois tipos de backup: Backup Full (Completo) e incremental. O backup Full tem por definição copiar todos os arquivos indicados, enquanto o Incremental copia somente o que foi alterado desde o último backup Full.

5.3 Dados que precisam ser armazenados

Dados que devem fazer parte do processo de backup:

- Bancos de dados
- Arquivos de configuração
- Arquivo de upload de usuários
- Arquivos de integração
- Logs de acesso

Para fazer parte do backup essas informações devem obrigatoriamente estar em um volume compartilhado que será fornecido pela Gerência de Infraestrutura. Volumes locais, ou em outros locais não especificados pela Gerência de Infraestrutura NÃO farão parte das rotinas de backup.

5.4 Locais de armazenamento de dados

Para o datacenter *Onpremisse* será utilizado um servidor NAS ou S3 compatible, para o ambiente em *nuvem AWS* será utilizado um bucket S3 com acesso restrito.

5.5 Responsabilidade pelo backup

O processo de realização do backup é de responsabilidade da Gerência de Infraestrutura juntamente com sua equipe. As equipes dos projetos são corresponsáveis uma vez que devem seguir as diretrizes desta política, para permitir que os mesmos façam parte da rotina de backup do NEES.

6. REGISTROS

Os registros relacionados com este procedimento são:

- Sistema INTEGRA.
- Relatório de backup produzido pela ferramenta de backup.

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	03/05/2024	Criação do documento.	Francisco Menezes
02	07/04/2025	Revisão da estrutura de todo o documento e inclusão do controle de documentos e assinaturas, via sistema INTEGRA	Shirley Vital
03	10/07/2025	Melhorias no conteúdo do item 5	Francisco Menezes

Elaborador: Francisco Bruno de Souza Meneses, Gerente de Infraestrutura, em 2025-07-16 17:46
Revisor: Shirley Jane Felix Vital, Coordenação do Sistema de Gestão de SI, em 2025-07-28 11:44
Aprovador: André Magno Costa de Araújo, Coordenador de Projeto, em 2025-07-28 11:55