|  |  |  |
| --- | --- | --- |
|  | **INSTRUÇÃO DE SERVIÇOS – GTI/INFRA/003** | **SECRETARIA DE ESTADO DA SAÚDE** |
| CódigoINFRA-003 | Data EmissãoMAI/2025 | Data de VigênciaMAI/2025 | Próxima RevisãoMAI/2025 | Versão nº1.0 |
| **ÁREA EMITENTE: SUB-GERÊNCIA DE INFRAESTRUTURA E SEGURANÇA DA INFORMAÇÃO** |
| **ASSUNTO:** Institui medidas de governança de TI para padronização e parametrização de backup utilizando a ferramenta Bacula para sistemas legados das unidades hospitalares na Secretaria de Estado da Saúde. |

**Introdução**

A Subgerência de Infraestrutura e Segurança da Informação, pertencente à Gerência de Tecnologia da Informação (GTI) desta Secretaria de Estado da Saúde da Paraíba, estabelece diretrizes de padronização e parametrização para os serviços de backup dos sistemas legados das unidades hospitalares utilizando a ferramenta Bacula.

As diretrizes dispostas neste documento são de utilização obrigatória para os setores de TI das unidades hospitalares pertencentes à Secretaria de Estado da Saúde da Paraíba que gerenciam sistemas legados que necessitam de rotinas de backup, visando garantir a integridade, disponibilidade e recuperabilidade dos dados críticos para o funcionamento da rede de saúde do Estado.

No processo de modernização e padronização da infraestrutura tecnológica na rede de saúde do Estado da Paraíba, estão previstas várias ações que visam implementar políticas consistentes de backup e recuperação de dados, centralizando o armazenamento no data center da CODATA e garantindo que todas as unidades hospitalares sigam o mesmo padrão de backup para os sistemas legados. Estas diretrizes de serviços serão direcionadas por procedimentos, fluxos e métodos que servirão de alinhamento para serem adotadas como regra por todas as Gerências, Núcleos, Unidades Hospitalares, Estabelecimentos de saúde, entre outros órgãos que compõem a Gestão Estadual pertencentes à Secretaria de Estado da Saúde da Paraíba.

Pretende-se, com essas diretrizes, estabelecer uma infraestrutura robusta de backup utilizando a ferramenta Bacula, garantindo que todos os dados críticos dos sistemas legados hospitalares estejam devidamente protegidos e possam ser recuperados em caso de falhas, desastres ou outros incidentes que comprometam a disponibilidade dos sistemas.

**Objetivos**

* Estabelecer padrões e parâmetros para a implementação de rotinas de backup utilizando a ferramenta Bacula nas unidades hospitalares;
* Definir a arquitetura e o fluxo de comunicação entre os servidores cliente nas unidades hospitalares e o servidor principal na CODATA;
* Especificar os tipos de backup (Full , Differential e Incremental ) e suas respectivas periodicidades;
* Padronizar processos de verificação, validação e recuperação de dados;
* Garantir a disponibilidade, integridade e recuperabilidade dos dados críticos dos sistemas legados hospitalares.

**Referências Normativas**

* Estratégia de Saúde Digital para o Brasil 2020-2028.
* Ações Estratégicas para Saúde Digital na Paraíba Gestão 2023-2026.
* Política de Segurança da Informação da Secretaria de Estado da Saúde da Paraíba.
* Lei 13.709, de 14 de agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD).
* NBR -- ABNT ISO/IEC 27002 - Segurança da Informação, Segurança Cibernética e Proteção da Privacidade -- Controles de Segurança da Informações.
* NBR -- ABNT ISO/IEC 27031 - Tecnologia da informação — Técnicas de segurança — Diretrizes para a prontidão da tecnologia da informação e comunicação para continuidade de negócios.

**Arquitetura do Sistema de Backup**

**Componentes do Bacula**

O Bacula é uma solução de backup open-source que consiste nos seguintes componentes principais:

1. **Director (Diretor)**: Componente central do Bacula que controla e coordena todos os processos de backup, restauração e verificação. Será instalado no servidor principal da CODATA.
2. **Storage Daemon (Daemon de Armazenamento)**: Responsável por gravar e ler dados nos dispositivos de armazenamento. Será instalado no servidor principal da CODATA.
3. **File Daemon (Daemon de Arquivo)**: Cliente Bacula que será instalado em cada servidor das unidades hospitalares para permitir o backup dos sistemas legados.
4. **Catalog (Catálogo)**: Banco de dados que armazena informações sobre todos os arquivos de backup, permitindo indexação e recuperação rápida. Será hospedado no servidor principal da CODATA.
5. **Bacula Console**: Interface de administração para gerenciar o ambiente Bacula. Será utilizada pelos administradores da GTI na CODATA.

**Topologia do Sistema**

* **Servidor Principal (CODATA)**:
	+ Executa o Director, Storage Daemon e Catalog do Bacula
	+ Gerencia todas as políticas de backup
	+ Armazena todos os dados de backup
	+ Centraliza os registros e relatórios
	+ Possui redundância e alta disponibilidade
* **Servidores Cliente (Unidades Hospitalares)**:
	+ Executam o File Daemon do Bacula
	+ Comunicam-se com o servidor principal através de canal seguro (VPN)
	+ Enviam os dados de backup dos sistemas legados conforme políticas definidas
	+ Mantêm registros locais dos processos de backup

**Dos Acordos de Serviços -- SLA**

Os serviços oriundos da Subgerência de Infraestrutura e Segurança da Informação, relacionados ao sistema de backup Bacula, têm como finalidade garantir a integridade e disponibilidade dos dados críticos dos sistemas legados das unidades hospitalares. Estes serviços atenderão a todas as unidades hospitalares sob gestão estadual.

Portanto, para termos um alinhamento nos serviços, se faz necessário o cumprimento de algumas premissas, para juntos podermos garantir a efetividade e confiabilidade do sistema de backup.

**Descrição dos Serviços:**

1. Implementação da infraestrutura de backup Bacula
2. Configuração e parametrização dos servidores Bacula
3. Monitoramento e manutenção do sistema de backup
4. Recuperação de dados em caso de desastres
5. Geração de relatórios e auditoria do sistema de backup

**Premissas:**

1. **Quanto à implementação da infraestrutura de backup Bacula:**

A) Instalação e configuração do servidor Bacula Director na CODATA;

B) Instalação e configuração do Storage Daemon no servidor da CODATA;

C) Instalação e configuração do File Daemon em cada servidor de unidade hospitalar;

D) Configuração do banco de dados Catalog no servidor da CODATA;

E) Configuração da comunicação segura entre servidores (TLS/SSL);

F) Documentação completa da infraestrutura implementada.

1. **Quanto à configuração e parametrização dos servidores Bacula:**

A) Definição das políticas de backup (Full, Differential e Incremental);

B) Configuração dos pools de armazenamento;

C) Definição dos períodos de retenção para cada tipo de backup;

D) Parametrização dos jobs de backup para cada sistema legado;

E) Configuração das janelas de backup para minimizar impacto nos sistemas em produção;

F) Implementação de mecanismos de compressão e criptografia;

G) Configuração dos processos de verificação e validação dos backups.

1. **Quanto ao monitoramento e manutenção do sistema de backup:**

A) Implementação de ferramentas de monitoramento dos processos de backup;

B) Configuração de alertas para falhas e erros no sistema de backup;

C) Manutenção preventiva periódica do sistema;

D) Atualização regular das versões do software Bacula;

E) Verificação periódica da integridade dos dados armazenados;

F) Geração de relatórios de desempenho e utilização do sistema.

1. **Quanto à recuperação de dados em caso de desastres:**

A) Definição dos procedimentos de recuperação para diferentes cenários;

B) Realização de testes periódicos de restauração de dados;

C) Documentação detalhada dos procedimentos de recuperação;

D) Treinamento da equipe de TI das unidades hospitalares para procedimentos básicos de recuperação;

E) Estabelecimento de tempos máximos para recuperação (RTO - Recovery Time Objective) de acordo com a criticidade dos dados.

1. **Quanto à geração de relatórios e auditoria:**

A) Configuração de relatórios periódicos de status dos backups;

B) Implementação de mecanismos de auditoria para todas as operações do sistema;

C) Geração de estatísticas de utilização de armazenamento;

D) Elaboração de dashboards para visualização do status geral do sistema;

E) Relatórios de conformidade com as políticas de backup estabelecidas.

**Tipos de Backup e Periodicidade**

**Backup Completo (Full)**

O backup completo copia todos os dados dos sistemas legados, independentemente se foram alterados desde o último backup.

**Periodicidade:**

* Semanal, preferencialmente aos domingos à noite ou conforme janela definida para cada unidade hospitalar
* Retenção: 4 semanas (1 mês)

**Backup Differential**

O backup differential copia todos os dados que foram alterados desde o último backup completo.

**Periodicidade:**

* Diário, de segunda a sábado, no período noturno
* Retenção: até o próximo backup completo

**Backup Incremental**

O backup incremental cópia apenas os dados que foram alterados desde o último backup incremental ou completo.

**Periodicidade:**

* Para sistemas críticos: Duas vezes ao dia (meio-dia e meia-noite)
* Para sistemas não-críticos: Uma vez ao dia (noite)
* Retenção: 7 dias

**Cobertura e horário de atendimento:**

O acesso aos serviços será de acordo com o acordo estabelecido pela administração da SES-PB:

* Para operações regulares: Dias úteis, das 08:00 às 11:45 e 13:30 às 16:30hs
* Para emergências: Suporte 24x7 através de esquema de plantão

**Fluxo de atendimento e atribuições:**

Nesta seção, o modelo padrão de atendimento aos chamados será detalhado, em seus vários níveis, de ponta a ponta.

**Papéis e responsabilidades:**

Na operação do sistema de backup, fornecedor (GTI/SES-PB) e cliente (unidades hospitalares) são corresponsáveis pela efetividade das operações, ainda que ambos tenham papéis distintos:

**Responsabilidades da GTI/SES-PB:**

* Gerenciamento e administração central do sistema Bacula
* Manutenção do servidor principal na CODATA
* Monitoramento do funcionamento de todo o sistema
* Verificação da integridade dos backups armazenados
* Execução de procedimentos de recuperação quando necessário
* Atualização da infraestrutura de backup

**Responsabilidades das Unidades Hospitalares:**

* Comunicar à GTI quaisquer mudanças nos sistemas que possam afetar os backups
* Garantir o funcionamento adequado do servidor cliente (File Daemon)
* Reportar imediatamente quaisquer falhas ou erros identificados
* Participar dos testes periódicos de recuperação
* Seguir os procedimentos definidos para solicitações de recuperação

**Mapa de severidade: Urgência e Impacto**

Nem todo chamado tem o mesmo grau de urgência e o mesmo impacto sobre as operações, o que gera uma necessidade de priorização.

**Níveis de Severidade:**

1. **Crítico (Severidade 1)**
	* Falha completa do sistema de backup
	* Impossibilidade de recuperação de dados críticos
	* Comprometimento de segurança do sistema
2. **Alto (Severidade 2)**
	* Falha em backup de sistema crítico
	* Atraso significativo na execução de backups
	* Espaço de armazenamento crítico (<10% disponível)
3. **Médio (Severidade 3)**
	* Falha em backup de sistema não-crítico
	* Problemas de desempenho no sistema de backup
	* Avisos de capacidade de armazenamento (<20% disponível)
4. **Baixo (Severidade 4)**
	* Dúvidas sobre o sistema
	* Solicitação de relatórios
	* Ajustes de configuração não urgentes

**Tempo de atendimento por nível de severidade:**

A partir do momento que o chamado chega ao sistema e vai para a fila de atendimento, o tempo máximo para resolução é estabelecido conforme abaixo:

* **Severidade 1 (Crítico)**: Início do atendimento em até 30 minutos, resolução em até 4 horas
* **Severidade 2 (Alto)**: Início do atendimento em até 2 horas, resolução em até 8 horas
* **Severidade 3 (Médio)**: Início do atendimento em até 4 horas, resolução em até 24 horas
* **Severidade 4 (Baixo)**: Início do atendimento em até 8 horas, resolução em até 48 horas

**Métricas e relatórios de performance de serviço:**

O sistema Bacula gera os seguintes relatórios para controle e monitoramento:

* Taxa de sucesso de backups (diário/semanal/mensal)
* Tempo médio de execução dos backups
* Volume de dados armazenados por unidade hospitalar
* Taxa de crescimento do armazenamento
* Tempo médio de recuperação
* Relatório de verificação de integridade
* Estatísticas de compressão e de duplicação

**Base de conhecimento:**

A base de conhecimento reúne informações sobre erros conhecidos e suas soluções, para que fiquem acessíveis a toda a equipe de atendimento.

Todos os incidentes de severidade 1 e 2 solucionados terão sua metodologia de solução documentada na base de conhecimento, assim como problemas recorrentes de qualquer severidade.

**Plano de comunicação:**

A comunicação entre a GTI/SES-PB e as unidades hospitalares se dará através dos seguintes canais:

* Sistema de chamados (ticket) para solicitações e incidentes através do site <https://redmine.aghuse.ses.pb.gov.br>
* E-mail para comunicações formais e relatórios
* Telefone para emergências (severidade 1)
* Reuniões mensais de acompanhamento com os responsáveis de TI das unidades
* Relatórios automáticos enviados semanalmente

**Exceções no atendimento ao SLA:**

Em alguns casos, a GTI/SES-PB se reservará o direito de não cumprir os itens acordados no SLA. Tais situações também precisam estar descritas no documento.

Elas podem ser ocorrências como:

* Período de implementação inicial do sistema (primeiros 30 dias)
* Problemas comprovadamente causados por ação ou omissão da unidade hospitalar
* Modificações no ambiente não comunicadas à GTI/SES-PB
* Emergência, caso fortuito ou de força maior
* Problemas de conectividade ou indisponibilidade da rede entre a unidade e a CODATA
* Manutenções programadas e previamente comunicadas
* Solicitações que dependam da atuação prévia de terceiros

**Anexo: Diagrama de Fluxo do Sistema de Backup Bacula**



**Resumo do fluxo de backup:**

**Backup Completo (Full)**

1. O Bacula Director no servidor principal da CODATA agenda o job de backup completo
2. O File Daemon no servidor da unidade hospitalar é acionado
3. Todos os dados configurados para backup são copiados para o Storage Daemon na CODATA
4. Os dados são armazenados no pool de armazenamento de backups completos
5. A verificação de integridade é executada
6. O relatório de conclusão é gerado e armazenado no Catalog
7. Notificação é enviada aos administradores

**Backup Differential**

1. O Bacula Director no servidor principal da CODATA agenda o job de backup diferencial
2. O File Daemon no servidor da unidade hospitalar é acionado
3. Os dados alterados desde o último backup completo são identificados e copiados
4. Os dados são transferidos para o Storage Daemon na CODATA
5. Os dados são armazenados no pool de armazenamento de backups diferenciais
6. A verificação de integridade é executada
7. O relatório de conclusão é gerado e armazenado no Catalog
8. Notificação é enviada aos administradores

**Backup Incremental**

1. O Bacula Director no servidor principal da CODATA agenda o job de backup incremental
2. O File Daemon no servidor da unidade hospitalar é acionado
3. Os dados alterados desde o último backup (completo ou incremental) são identificados
4. Os dados são transferidos para o Storage Daemon na CODATA
5. Os dados são armazenados no pool de armazenamento de backups incrementais
6. A verificação de integridade é executada
7. O relatório de conclusão é gerado e armazenado no Catalog
8. Notificação é enviada aos administradores

**Processo de Restauração**

1. Solicitação de restauração é registrada via sistema de chamados
2. GTI avalia a solicitação e determina a fonte adequada para restauração
3. Job de restauração é configurado no Bacula Director
4. Dados são recuperados do Storage Daemon e transferidos para o destino
5. Verificação da integridade dos dados restaurados
6. Confirmação da restauração com o solicitante
7. Documentação do processo no sistema de chamados
8. Relatório de restauração é gerado e armazenado

João Pessoa, 02 maio de 2025.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Jhony Wesllys Bezerra Costa

Secretário de Estado Da Saúde

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Kleyber Dantas Torres de Araújo

Gerente de Tecnologia da Informação SES-PB