



Nexus

BACKUP DE SISTEMAS – CONFIGURAÇÕES E DADOS CRÍTICOS

NEXUS

BACKUP DE SISTEMAS – CONFIGURAÇÕES E DADOS CRÍTICOS

INTRODUÇÃO

O backup de sistemas é um procedimento essencial para garantir a continuidade operacional da Nexus. Diferente dos backups comuns, que envolvem apenas arquivos e documentos, o backup de sistemas abrange **configurações, bancos de dados, aplicações, softwares, registros internos e componentes críticos** necessários para que os setores funcionem corretamente.

Este manual foi criado para orientar os colaboradores responsáveis sobre todos os passos, práticas, cuidados e protocolos necessários para realizar backups de sistemas com segurança e precisão.

O objetivo deste guia é garantir:

- Restauração rápida em caso de falhas
- Proteção contra perda de configurações importantes
- Salvamento das informações mais sensíveis
- Continuidade dos serviços internos
- Integridade dos dados corporativos

1. O QUE É BACKUP DE SISTEMAS?

1.1 Definição

Backup de sistemas consiste em salvar cópias:

- Da estrutura de configurações
- Dos arquivos do software
- Das dependências necessárias
- Dos bancos de dados associados
- Das rotinas automatizadas
- Dos componentes críticos para funcionamento

1.2 Diferença entre backup de arquivos e backup de sistemas

Backup de arquivos → Salva documentos, planilhas, PDFs etc.

Backup de sistemas → Salva tudo que mantém um software ou aplicação funcionando.

1.3 Por que isso é importante para a Nexus?

- ✓ Evita paralisação de setores
- ✓ Minimiza danos em falhas técnicas
- ✓ Protege dados sensíveis do sistema
- ✓ Mantém consistência entre versões
- ✓ Permite restaurar softwares rapidamente

2. COMPONENTES QUE DEVEM SER SALVOS

Diferentes sistemas exigem diferentes tipos de backup. Na Nexus, os componentes críticos incluem:

2.1 Banco de dados

- Estruturas
- Tabelas
- Registros
- Logs
- Consultas salvas

2.2 Configurações internas

- Preferências do sistema
- Ajustes avançados
- Parâmetros de funcionamento
- Regras e permissões

2.3 Arquivos do sistema

- Execução
- Bibliotecas
- Pastas de instalação
- Scripts automáticos

2.4 Dependências

- Plugins
- Extensões
- Componentes adicionais

2.5 Usuários e permissões

- Contas ativas
- Grupos internos
- Permissões específicas

3. TIPOS DE BACKUP DE SISTEMAS UTILIZADOS NA NEXUS

3.1 Backup completo

Copia todos os arquivos e configurações do sistema.

3.2 Backup incremental

Copia somente o que mudou desde o último backup.

3.3 Backup de imagem

Cria uma cópia exata da máquina ou servidor.

3.4 Snapshot

Salva o estado atual da aplicação naquele instante.

3.5 Backup do banco de dados

Focado nas estruturas e dados essenciais.

4. PROCEDIMENTO GERAL PARA BACKUP DE SISTEMAS

Este é o passo a passo padronizado usado internamente.

4.1 Identificar o sistema

Alguns sistemas que exigem backup:

- Ferramentas internas
- Softwares administrativos
- Sistemas financeiros
- Banco de dados corporativo

- Sistema de gestão interno
- Aplicações web internas

4.2 Preparar o ambiente

Antes de iniciar o backup:

- ✓ Feche as aplicações que podem interferir
- ✓ Verifique o estado do banco de dados
- ✓ Verifique a conexão com servidor
- ✓ Realize login com conta administrativa
- ✓ Certifique-se de que há espaço suficiente
- ✓ Não faça alterações enquanto o backup está sendo criado

4.3 Realizar o backup das configurações

Passo a passo:

1. Acesse as configurações internas do sistema
2. Procure a opção “Exportar Configurações”
3. Escolha o diretório de armazenamento interno
4. Salve com nome padronizado:

Config_System_Nome_DD-MM-AAAA

1. Verifique a integridade após exportar

4.4 Realizar backup do banco de dados

1. Abra a ferramenta de gerenciamento
2. Escolha o banco correto
3. Clique em **Exportar / Backup**
4. Escolha o formato recomendado (SQL, BAK, JSON)
5. Salve com nome padronizado:

Backup_DB_SistemaX_05-11-2025.sql

1. Armazene na pasta correta do setor de TI
2. Teste o arquivo exportado (verificando abertura)

4.5 Realizar backup dos arquivos do sistema

1. Abra o diretório onde o sistema está instalado
2. Copie todas as pastas internas
3. Inclua:
 - bin
 - data
 - config

- extensions
- plugins
- resources
- logs importantes

4. Cole em uma pasta exclusiva para esse sistema:

Sistema_Nome_Backup_05-11-2025

4.6 Backup de automatizações

Caso o sistema possua scripts:

- Tarefas agendadas
- Executáveis
- Macros internas
- Scripts .bat/.sh

Copie tudo para:

Automacoes_Sistema_Nome_DD-MM-AAAA

4.7 Conferências obrigatórias após o backup

- ✓ Arquivo exportado abre corretamente
- ✓ Versão está identificada
- ✓ Tamanho dos arquivos é compatível
- ✓ Logs essenciais foram incluídos
- ✓ Scripts estão completos
- ✓ Configurações estão legíveis
- ✓ Tudo está padronizado

5. ONDE ARMAZENAR OS BACKUPS DE SISTEMAS

Os backups devem ser mantidos simultaneamente em três locais:

5.1 Servidor interno

Pasta oficial:

Nexus – Arquivos Internos → Backups_Sistemas

5.2 Nuvem corporativa

Para redundância adicional.

5.3 HD externo corporativo

Para emergências e restauração offline.

6. SEGURANÇA NO BACKUP DE SISTEMAS

6.1 Proteção dos arquivos

- Criptografia
- Pastas restritas
- Permissões específicas
- Bloqueio de edição

6.2 Controle de acesso

Somente:

- ✓ TI
- ✓ Coordenação autorizada

podem acessar os backups completos de sistemas.

6.3 Não compartilhe arquivos

Nunca envie backups via:

- ✗ WhatsApp
- ✗ E-mail pessoal
- ✗ Dispositivos pessoais
- ✗ Links externos

7. RESTAURAÇÃO DE SISTEMAS

A restauração é usada quando:

- O sistema apresenta falhas
- Arquivos foram corrompidos
- Erros afetam o funcionamento
- Atualizações deram errado

7.1 Procedimento básico

1. Acesse a pasta do backup
2. Localize a versão que deseja restaurar
3. Importe o banco de dados
4. Restaure arquivos do sistema
5. Reaplique as configurações
6. Reinicie o serviço ou servidor

7.2 Conferência pós-restauração

- ✓ Sistema abre sem erros
- ✓ Permissões funcionam
- ✓ Dados aparecem corretamente
- ✓ Funções estão normalizadas

8. BOAS PRÁTICAS GERAIS

- Sempre salve com datas
- Nunca sobrescreva backups antigos
- Teste periodicamente
- Evite nomes genéricos
- Documente versões
- Salve em múltiplos locais

9. ERROS COMUNS QUE DEVEM SER EVITADOS

- ✗ Esquecer de exportar configurações
- ✗ Copiar arquivos incompletos
- ✗ Não testar o arquivo depois
- ✗ Salvar backup no local errado
- ✗ Monopolizar pastas de outros setores
- ✗ Não documentar alterações
- ✗ Misturar arquivos de sistemas diferentes

CONCLUSÃO

O backup de sistemas é uma das atividades mais críticas da empresa, pois garante que toda a operação da Nexus continue funcionando mesmo diante de falhas graves. Ao seguir este manual, você estará protegendo:

- ✓ Configurações essenciais
- ✓ Arquivos críticos
- ✓ Bancos de dados sensíveis
- ✓ Automações internas
- ✓ Serviços operacionais
- ✓ Continuidade da empresa

Este documento deve ser revisado e aplicado rigorosamente sempre que um backup de sistema for realizado.