Nexus

BACKUP LOCAL – HD E DISPOSITIVOS EXTERNOS

NEXUS

BACKUP LOCAL – HD E DISPOSITIVOS EXTERNOS

INTRODUÇÃO

O backup local é uma prática complementar aos backups internos e em nuvem realizados pela Nexus. Ele consiste em armazenar cópias adicionais dos arquivos corporativos em dispositivos físicos, como HDs externos, pen drives corporativos autorizados e unidades de armazenamento portátil homologadas pelo setor de TI.

O objetivo deste manual é orientar os colaboradores a utilizar corretamente esses dispositivos, garantindo que os arquivos sejam copiados de forma organizada, segura e padronizada.
O backup local **não substitui** os demais backups, mas funciona como mais uma camada de proteção contra:

- Falhas de conexão
- Erros de sincronização
- Problemas temporários nos servidores
- Arquivos corrompidos
- Situações emergenciais

Seguir este documento é obrigatório para todos que realizam cópias locais.

1. O QUE É BACKUP LOCAL?

1.1 Definição

Backup local é o processo de copiar arquivos para um dispositivo físico externo, como:

- HD externo corporativo
- Pen drive corporativo homologado
- Unidade SSD portátil
- Dispositivos USB aprovados pelo TI

1.2 Objetivo do backup local

- Criar uma cópia adicional
- Garantir recuperação rápida
- Proteger em caso de falha de rede
- Facilitar transporte de dados entre locais internos da empresa

1.3 Importância dentro da Nexus

O backup local é usado principalmente:

- Em auditorias presenciais
- Em migrações internas
- Em compartilhamento entre máquinas
- Em manutenção de sistemas
- Em emergências operacionais

2. DISPOSITIVOS PERMITIDOS

A Nexus autoriza apenas dispositivos certificados.

2.1 Permitidos

✔ HDs externos corporativos identificados
✔ Pen drives fornecidos pela Nexus
✔ SSDs portáteis catalogados pelo TI
✔ Dispositivos com criptografia nativa

2.2 Proibidos

❌ Dispositivos pessoais
❌ Pen drives sem identificação
❌ HDs externos particulares
❌ Dispositivos com vírus relatado
❌ Cartões de memória não registrados

2.3 Por que isso é importante?

Utilizar dispositivos pessoais aumenta riscos de:

- Vírus
- Perda de arquivos

- Acesso indevido
- Vazamento de dados
- Contaminação da rede

3. PREPARAÇÃO DO DISPOSITIVO

Antes de iniciar o backup, é necessário garantir que o dispositivo esteja devidamente preparado.

3.1 Verificar se o dispositivo está limpo

- Abra o HD ou pen drive
- Veja se ele está organizado
- Certifique-se de que não há vírus
- Procure arquivos suspeitos
- Caso haja pastas desconhecidas, solicite limpeza ao TI

3.2 Criar estrutura oficial de pastas

Dentro do dispositivo, crie pastas como:

Backup_Local_Nexus

├── Administrativo

├── Financeiro

├── Comercial

├── Projetos

└── Operacional

3.3 Evitar colocar arquivos soltos

Sempre organize por:

✓ Setor
✓ Data
✓ Nome do projeto ou documento

Exemplo:

Backup_05-11-2025

4. PROCEDIMENTO DE BACKUP LOCAL

Agora, o passo a passo completo:

4.1 Acessar arquivos originais

1. Abra o explorador de arquivos
2. Localize o documento/planilha/relatório original
3. Verifique se está atualizado
4. Confirme o nome padronizado

4.2 Conectar o dispositivo externo

- Conecte o HD externo ou pen drive
- Aguarde o sistema reconhecer
- Certifique-se de que o dispositivo abriu corretamente

OBS:

Se aparecer mensagem de erro, comunique o TI imediatamente.

4.3 Copiar arquivos

1. Selecione o arquivo original
2. Clique com o botão direito → **Copiar**
3. Abra o dispositivo externo
4. Vá até a pasta do setor
5. Cole o arquivo dentro da pasta correspondente

IMPORTANTE:

NÃO USE **CTRL + X** (recortar).
Isso move o arquivo e causa perda do original.

4.4 Criar pastas por datas

Para cada backup, criar uma pasta específica:

Backup_05-11-2025

Backup_Semanal_Semana_44

Backup_ProjetoX

Dentro dela, coloque:

- Planilhas
- Documentos
- PDFs
- Arquivos auxiliares

4.5 Verificar integridade

Depois de colar:

✔ Abra o arquivo
✔ Veja se está completo
✔ Compare com o original
✔ Confirme tamanho e formato
✔ Cheque se não está corrompido

5. BOAS PRÁTICAS DE ORGANIZAÇÃO

5.1 Nomeação correta

Sempre use:

NomeDoArquivo_DD-MM-AAAA

5.2 Não misture arquivos

Evite colocar arquivos de setores diferentes dentro da mesma pasta.

5.3 Manter estrutura limpa

Não deixe:

- Arquivos repetidos
- Pastas sem nome
- Documentos inúteis
- Arquivos temporários

5.4 Criar descrição quando necessário

Exemplo:

Relatorio_Mensal_Financeiro_Explicacao.txt

6. SEGURANÇA NO USO DO DISPOSITIVO

6.1 Retirada com segurança

Antes de remover:

1. Clique no ícone de remoção segura
2. Aguarde confirmação
3. Retire o dispositivo

6.2 Nunca desconectar durante cópias

Isso pode:

- Corromper arquivos
- Danificar o HD

- Perder completamente a cópia

6.3 Não emprestar dispositivos

Apenas usuários autorizados devem utilizá-los.

6.4 Não transportar sem proteção

Use capas protetoras para evitar danos físicos.

7. RISCOS E COMO EVITÁ-LOS

7.1 Vírus

→ Atualize o antivírus
→ Não conecte dispositivos suspeitos
→ Não execute arquivos desconhecidos

7.2 Perda de dispositivo

→ Evite transportar sem necessidade
→ Não leve para casa sem autorização
→ Mantenha sempre guardado em local seguro

7.3 Arquivo corrompido

→ Sempre verifique antes de remover
→ Não desligue o PC durante a cópia

7.4 Erro humano

→ Sempre revise antes de copiar
→ Evite pressa
→ Siga as regras do setor

8. QUANDO UTILIZAR BACKUP LOCAL

Backup local é recomendado em:

- Auditorias internas
- Reuniões offline
- Mapeamento de projetos
- Migração de computadores
- Falhas temporárias de servidores
- Situações emergenciais

9. O QUE NÃO FAZER

❌ Não usar pen drive pessoal
❌ Não armazenar arquivos fora das pastas oficiais
❌ Não copiar arquivos sem revisão
❌ Não excluir conteúdos antigos sem permissão
❌ Não mover arquivos em vez de copiar
❌ Não trabalhar dentro do HD/pen drive diretamente

CONCLUSÃO

O backup local em HDs e dispositivos externos é uma parte essencial do sistema de segurança da Nexus, oferecendo uma camada extra de proteção. Com este manual, você tem todas as orientações necessárias para garantir que seus backups sejam feitos de forma correta, completa e segura.

Ao seguir este documento, você assegura:

✔ Confiabilidade dos arquivos
✔ Segurança operacional
✔ Organização eficiente
✔ Redundância de dados
✔ Rastreabilidade