Nexus

SEGURANÇA DE ARQUIVOS – PROCEDIMENTOS DE BACKUP

NEXUS

SEGURANÇA DE ARQUIVOS – PROCEDIMENTOS DE BACKUP

INTRODUÇÃO

A segurança dos arquivos é uma das prioridades fundamentais da Nexus. Todos os documentos, planilhas, registros internos, fotos técnicas, backups, relatórios e dados operacionais precisam estar devidamente protegidos contra perdas, acessos indevidos, corrupção de arquivos, ataques cibernéticos ou falhas técnicas.

Este manual apresenta **todos os procedimentos oficiais da Nexus** relacionados à segurança e organização dos arquivos. Aqui você encontrará:

- Como proteger arquivos internos
- Como organizar pastas corretamente
- Como realizar backups seguros
- Como evitar acessos não autorizados
- Como prevenir perda de dados
- Como manter a integridade das informações

É obrigatório que todos os colaboradores sigam este guia ao manipular arquivos da empresa.

1. CONCEITOS DE SEGURANÇA DE ARQUIVOS

Antes dos procedimentos, é importante entender como funciona a proteção de dados na prática.

1.1 O que é segurança de arquivos?

É o conjunto de práticas que garantem que os arquivos:

- Não sejam perdidos
- Não sejam modificados sem autorização
- Não sejam acessados por pessoas externas
- Não sejam corrompidos
- Estejam sempre disponíveis quando necessário

1.2 Por que isso é importante na Nexus?

- Evita vazamento de dados internos
- Mantém a continuidade operacional
- Garante controle sobre documentos sensíveis
- Evita retrabalho causado por arquivos danificados
- Protege a empresa contra falhas técnicas

2. ORGANIZAÇÃO E DIVISÃO DE ARQUIVOS INTERNOS

A organização deve seguir uma estrutura clara, que facilita a navegação e impede erros.

2.1 Estrutura oficial de pastas

Os arquivos devem ser armazenados em:

Nexus – Arquivos Internos

├── Administrativo

├── Financeiro

├── Comercial

├── Recursos Humanos

├── Projetos

├── Sistemas

└── Backups

2.2 Regras fundamentais de organização

✔ Nunca salve arquivos soltos
✔ Sempre coloque dentro do setor correto
✔ Nomeie as pastas com clareza

✔ Evite abreviações incompreensíveis
✔ Não misture arquivos pessoais com arquivos da empresa

2.3 Pastas de trabalho e pastas finais

A Nexus exige que arquivos sejam separados assim:

- **Área de Trabalho / Rascunhos:** arquivos temporários
- **Pasta Oficial:** arquivos finalizados
- **Backup:** cópia do finalizado

Isso evita confusão entre versões.

3. CONTROLE DE ACESSO A ARQUIVOS

A segurança começa ao controlar quem pode ver, editar ou excluir arquivos.

3.1 Tipos de acesso

A Nexus utiliza três níveis:

- **Leitura** → pode visualizar
- **Edição** → pode modificar
- **Administrador** → pode excluir, mover e autorizar acessos

Cada colaborador tem permissões específicas vinculadas ao seu setor.

3.2 Regras internas de acesso

✔ Não compartilhe senhas
✔ Não copie arquivos sensíveis para pendrives pessoais
✔ Não envie arquivos internos pelo WhatsApp ou redes sociais
✔ Utilize sempre as pastas e ferramentas oficiais

3.3 Solicitação de acesso

Caso um colaborador precise acessar um arquivo de outro setor:

1. Solicitar via e-mail ao coordenador do setor responsável
2. Justificar o motivo
3. Aguardar aprovação
4. TI realizará a liberação, caso autorizado

4. PROCEDIMENTOS DE SEGURANÇA ANTES DO BACKUP

4.1 Verifique se o arquivo está correto

Antes de copiar para o backup:

- O arquivo deve estar completo
- Não deve conter erros
- Deve estar com nome atualizado
- Deve estar revisado
- Não deve estar corrompido

4.2 Verifique permissões

Nunca faça backup de um arquivo ao qual você:

❌ Não tem autorização
❌ Não tem certeza da versão
❌ Não sabe se é oficial
❌ Não sabe se está atualizado

4.3 Bloqueio de edição

Arquivos sensíveis devem ser protegidos:

- Com senha
- Com permissões de edição limitadas
- Com histórico de alterações ativado

Sempre consulte o gestor antes de alterar documentos críticos.

5. REALIZANDO BACKUP COM SEGURANÇA

Um backup só é realmente seguro quando segue as regras da Nexus.

5.1 Escolhendo o local correto

Os backups devem SEMPRE ser feitos dentro da pasta:

Nexus – Arquivos Internos → Backups

Nunca utilize:

❌ Área de Trabalho
❌ Pendrive pessoal
❌ Celular
❌ E-mail pessoal
❌ Google Drive pessoal

5.2 Criando pastas específicas para backup

A Nexus exige padronização nos nomes:

Backup_Diario_05-11-2025

Backup_Semanal_Semana_44

Backup_Mensal_Outubro

Backup_ProjetoX_2025

Isso impede confusões entre versões antigas e novas.

5.3 Copiando os arquivos da forma correta

O processo oficial:

1. Abra o explorador de arquivos
2. Vá até a pasta onde está o arquivo original
3. Clique com o botão direito → **Copiar**
4. Vá até a pasta de backup
5. Clique com o botão direito → **Colar**

IMPORTANTE

Nunca use **CTRL + X** (recortar)
Isso remove o arquivo original, deixando o backup inútil.

5.4 Conferindo a integridade da cópia

Após copiar:

✔ Abra o arquivo
✔ Veja se tudo está completo
✔ Compare com a versão original
✔ Confira o tamanho do arquivo
✔ Verifique a data de modificação

Se tudo estiver correto, o backup está seguro.

6. BOAS PRÁTICAS DE SEGURANÇA DE ARQUIVOS

6.1 Pastas limpas e organizadas

Evite:

- Arquivos duplicados
- Arquivos com nomes confusos
- Pastas vazias
- Registros misturados

6.2 Nomeação correta

Sempre inclua:

- Nome do arquivo
- Setor
- Data atual

Exemplo:

Relatorio_Comercial_05-11-2025.xlsx

6.3 Utilize versões

Salve versões quando necessário:

v1, v2, v3…

Assim você evita perder algo importante.

7. PREVENÇÃO CONTRA PERDA DE ARQUIVOS

7.1 Utilize sempre a nuvem/servidor interno

Nunca salve arquivos somente no computador local.

7.2 Evite desligar o computador durante cópias

Isso pode corromper arquivos.

7.3 Não trabalhe com arquivos dentro do pendrive

Sempre copie para o computador antes de editar.

7.4 Não exclua arquivos antigos sem autorização

Somente gestores podem limpar backups.

8. ALERTAS IMPORTANTES SOBRE SEGURANÇA

❗ Não compartilhe arquivos por aplicativos pessoais
❗ Não copie arquivos internos para mídias externas sem autorização
❗ Não envie documentos da Nexus para e-mails particulares
❗ Nunca deixe arquivos sensíveis abertos em locais públicos
❗ Não deixe pastas fora da estrutura oficial

Qualquer violação pode causar:

- Perda de dados
- Riscos jurídicos
- Falhas operacionais
- Exposição indevida de informações internas

CONCLUSÃO

A segurança de arquivos é responsabilidade de todos os colaboradores. Este documento oferece um passo a passo completo e detalhado para garantir que todos os backups internos da Nexus sejam feitos de maneira correta, organizada e extremamente segura.

Seguindo este guia, você garante:

✔ Proteção dos dados
✔ Organização
✔ Integridade dos arquivos
✔ Continuidade operacional
✔ Conformidade com as normas internas da empresa