

Módulo NIA Go

# Os seus dados críticos. Protegidos e imutáveis.

Backups seguros, encriptados, auditáveis e preparados para retenção imutável em cloud — para bases de dados SQL Server e ambientes ERP. Implementado pela Emptor.

## SQL

SQL Server & ERP

## AES

Encriptado antes da cloud

## S3

Cloud imutável · object lock

## Audit

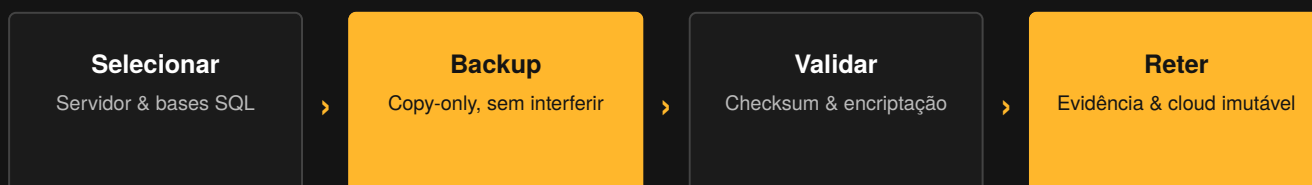
Evidência & checksum

## O PROBLEMA

# Backups locais não são suficientes.

Muitas empresas dependem diariamente do ERP para faturação, contabilidade, stocks, salários, compras e tesouraria. Na prática, a base de dados SQL Server é um dos ativos mais importantes da organização — mas a proteção real desses dados continua frágil. Quando acontece uma falha grave, muitas empresas descobrem tarde demais que o backup não existia, estava corrompido, era antigo ou não podia ser restaurado.

## Como funciona — o processo controlado de proteção



### Onde os backups ficam frágeis

Ficheiros apenas no servidor local, feitos manualmente ou de forma irregular, com dependência excessiva do SQL Server Agent e de tarefas configuradas informalmente.

### Sem evidência, sem confiança

Não existe prova simples de que o backup foi realmente criado e validado, nem visibilidade clara, para a administração, sobre o estado real dos backups.

### Um único ponto de falha

Os ficheiros podem ser apagados por erro, falha de disco, ransomware ou má operação. Não existe retenção imutável fora da infraestrutura local.

### Recuperação nunca testada

O processo de restauro não é testado — e um backup que não pode ser restaurado, na prática, não é um backup.

# Uma camada de governação e segurança.

O NIA Go Backup Vault não é apenas “fazer uma cópia da base de dados”. É um processo controlado de proteção de dados, com validação, evidência, segurança e capacidade futura de retenção imutável.

## Seleção controlada

Selecionar o servidor SQL Server, identificar as bases de dados elegíveis e escolher bases específicas ou proteger todas as bases relevantes.

## Backups copy-only

Execução de backups copy-only, sem interferir com cadeias de backup existentes nem com as rotinas actuais do cliente.

## Artefactos com evidência

Preparação dos artefactos com metadados e checksum, validação do ficheiro gerado e geração de manifestos e pacotes de evidência.

## Encriptação antes da cloud

Encriptação dos artefactos antes de qualquer armazenamento externo, reduzindo o risco de exposição de dados sensíveis.

## Retenção & limpeza

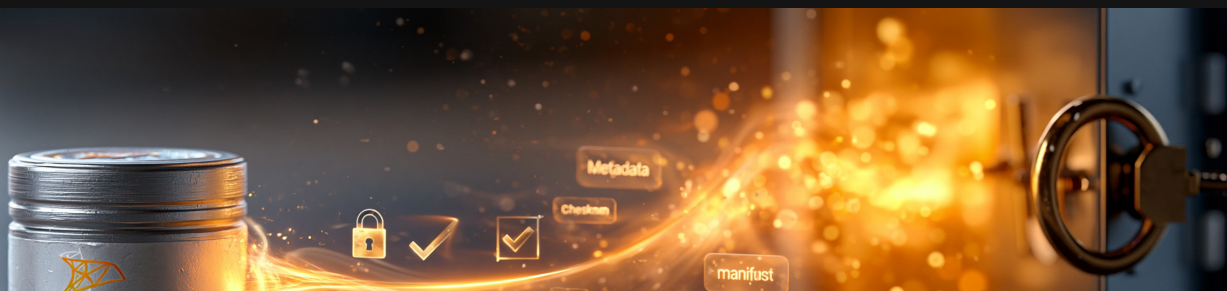
Controlo de retenção e limpeza local, com preparação do upload futuro para fornecedores compatíveis com armazenamento imutável.

## Independente do SQL Agent

Processo orquestrado pelo NIA Go, independente do SQL Server Agent, com o estado de prontidão num painel simples para operadores.

# Continuidade de negócio, com prova e controlo.

O ERP concentra informação operacional e financeira crítica. O Backup Vault acrescenta uma camada de proteção contra falhas locais, erro humano, corrupção de ficheiros e incidentes de segurança.



## Proteção contra perda de dados

Uma camada adicional de proteção contra falhas locais, erro humano, corrupção de ficheiros e incidentes de segurança sobre os dados críticos do ERP.

## Independência do SQL Agent

A orquestração é feita pelo NIA Go — maior controlo sobre permissões, evidência, auditoria, execução, validação e futuras integrações cloud.

## Encriptação antes da cloud

Os artefactos são preparados para serem encriptados antes de qualquer upload futuro, reduzindo o risco de exposição de dados sensíveis.

## Evidência auditável

Cada operação pode gerar metadados, checksum, manifesto e pacote de evidência — respostas claras a perguntas de auditoria e conformidade.

## Preparado para imutabilidade

Arquitectura desenhada para AWS S3, Backblaze B2, Google Cloud Storage, Azure Blob e serviços S3-compatible, com object lock, legal hold e políticas de retenção.

## Menos risco operacional

Gates de segurança, validações por fase, bloqueios por ambiente e autorização explícita, com separação entre teste, não-produção e produção.

# Não basta confiar. É preciso ter prova.

Cada operação gera metadados, checksum, manifesto e pacote de evidência. Isto permite responder, a qualquer momento, às perguntas que realmente importam sobre os backups.

## › Que base de dados foi protegida, e quando foi validada?

Cada artefacto regista a base de dados de origem, a data/hora de criação e de validação, e o resultado da verificação — pronto para auditoria.

## › Qual o tamanho do ficheiro e o checksum?

O manifesto guarda o tamanho do ficheiro e o checksum criptográfico, garantindo integridade e permitindo detectar qualquer alteração posterior.

## › Quem autorizou? Houve upload, restore ou scheduler?

O pacote de evidência regista a autorização explícita e o histórico de operações — upload, restauro e agendamento — de forma rastreável.

## › O ficheiro foi limpo corretamente no fim?

A retenção e a limpeza local são controladas e registadas, fechando o ciclo de vida do artefacto com evidência do que foi removido e quando.

## Independência e governação

O processo é independente do SQL Server Agent e opera com gates de segurança, validações por fase, bloqueios por ambiente e autorização explícita — com separação clara entre modo de teste, não-produção e produção. O operador vê o estado de prontidão e identifica bloqueios antes de qualquer ativação.

## PARA QUEM É INDICADO

# Pensado para quem depende do SQL Server.

Especialmente indicado para empresas que usam ERP sobre SQL Server — Primavera, Cegid, NIA ou outros sistemas críticos — e que precisam de uma camada adicional de proteção, controlo e evidência.

### **Empresas ERP sobre SQL Server**

Clientes com Primavera, Cegid, NIA ou outros sistemas críticos em SQL Server, com múltiplas bases de dados locais.

### **Sem equipa dedicada de DBA**

Organizações sem equipa interna de DBA e com risco elevado de falhas eléctricas, falhas de disco ou operação manual.

### **Necessidade de evidência**

Empresas que precisam de evidência de backup para auditoria e de visibilidade clara sobre o estado da protecção.

### **Estratégia cloud e anti-ransomware**

Clientes que querem preparar backup em cloud sem perder controlo local e reforçar a protecção contra ransomware.

## Integração com o ecossistema NIA Go

### **Módulo opcional e licenciado — totalmente separado**

Não interfere com controlo de acessos, assiduidade, integrações Primavera nem sincronizações existentes. Não altera fluxos operacionais atuais, não ativa backups automaticamente e não executa ações sem configuração e autorização. Uma solução premium para clientes que valorizam continuidade de negócio e protecção de dados.

# Uma abordagem faseada e escalável.

O módulo pode ser comercializado como serviço adicional, em três níveis, do backup local validado até à retenção imutável em cloud com conformidade.

## Backup Vault Essencial

FUNDAÇÃO

- Backup local validado
- Checksum
- Manifesto
- Pacote de evidência
- Painel de prontidão

## Backup Vault Secure

MAIS ESCOLHIDO

- Encriptação local
- Retenção local
- Evidência reforçada
- Readiness dashboard
- Suporte operacional

## Backup Vault Cloud Immutable

PREMIUM

- Integração cloud
- Retenção imutável
- Object lock ou equivalente
- Relatórios de conformidade
- Alertas e monitorização

### Argumentos para a administração

O ERP é crítico e a perda de dados pode parar a empresa. Backups locais não são suficientes; ransomware e erro humano são riscos reais. É necessário ter evidência, e não apenas confiança — e a empresa deve saber, a qualquer momento, se está protegida.

# O backup actual é suficiente para garantir o negócio?

Comece com uma avaliação técnica do ambiente SQL Server: identificar bases críticas, avaliar o estado dos backups, validar permissões e staging, definir retenção e preparar encriptação, evidência e estratégia cloud. Na maioria dos casos, a resposta à pergunta acima é: não.

[Pedir Avaliação Técnica](#)

