HELP NETO

CONTABILIDADE

HELP NETO CONTABILIDADE

CRC PJ RJ-010075/O-4

POLÍTICA DE BACKUP

DO SITE INSTITUCIONAL

Versão 1.2 | Maio de 2026 (versão pública)

São Pedro da Aldeia/RJ

CNPJ: 45.853.794/0001-74 | CRC PJ RJ-010075/O-4

Responsável Técnico: Alcino José da Silva Neto — Contador — CRC-RJ 126897/O

1. OBJETIVO E ABRANGÊNCIA

1.1. Esta Política estabelece princípios e diretrizes institucionais para a proteção, recuperabilidade e disponibilidade do website institucional da Help Neto Contabilidade (hncontabilidade.com), em conformidade com o art. 46 da Lei Geral de Proteção de Dados (Lei nº 13.709/2018) e com as melhores práticas de segurança da informação.

1.2. Os procedimentos operacionais detalhados — incluindo localização física e lógica dos backups, ferramentas específicas, intervalos exatos de execução, provedores e configurações — constam de runbook operacional interno restrito, mantido sob controle de acesso da Direção Técnica da CONTRATADA, e NÃO integram esta política pública (Cláusula 12).

2. PRINCÍPIOS

2.1. Confidencialidade, Integridade e Disponibilidade (CID) — pilares norteadores.

2.2. Menor privilégio — acesso aos backups restrito ao mínimo necessário.

2.3. Defesa em profundidade — múltiplas camadas e múltiplas cópias em locais distintos.

2.4. Separação de domínios — credenciais e dados de acesso são mantidos separadamente dos backups, em cofre dedicado e cifrado.

2.5. Testabilidade — backups têm valor apenas quando comprovadamente restauráveis.

2.6. Auditabilidade — toda operação de backup ou restauração gera registro auditável.

3. ESCOPO PROTEGIDO

3.1. Arquivos da aplicação web (código-fonte, temas, configurações públicas e mídia).

3.2. Banco de dados relacional do sistema de gerenciamento de conteúdo.

3.3. Arquivos de configuração crítica (sem incluir credenciais — ver Cláusula 5).

4. ESTRATÉGIA DE BACKUP — REGRA 3-2-1

4.1. Três cópias dos dados — uma cópia produtiva e duas cópias de backup.

4.2. Duas mídias distintas — armazenamento local e armazenamento em nuvem auditada.

4.3. Uma cópia geograficamente separada — em região distinta da operação primária (off-site).

4.4. Tipos de backup — completo (full) e incremental, ambos versionados e datados.

4.5. Backup pré-alteração obrigatório — exigido antes de mudanças estruturais (atualização de software, alteração de banco de dados, modificação de configuração crítica).

CRC PJ RJ-010075/O-4 | CNPJ 45.853.794/0001-74
hncontabilidade.com | helpneto@hncontabilidade.com
Estr. da Cruz, 6 — São Pedro da Aldeia/RJ — CEP 28940-000

4.6. Frequência — definida em runbook interno conforme criticidade do dado, observada periodicidade mínima compatível com o RPO declarado.

5. SEGURANÇA DAS CREDENCIAIS

5.1. Credenciais de acesso a sistemas (incluindo, mas não limitado a, hospedagem, banco de dados, painel administrativo e interfaces de programação) NUNCA são armazenadas junto com os backups, nem em provedores de sincronização de uso geral.

5.2. Credenciais são mantidas em cofre dedicado, com criptografia em repouso, controle de acesso individualizado e registro de cada acesso (audit log).

5.3. Rotação periódica de credenciais críticas observa cronograma definido em política de gestão de credenciais e ocorre imediatamente em caso de incidente.

6. RETENÇÃO E DESCARTE

6.1. Os períodos de retenção de backups incrementais e completos observam a criticidade do dado, a legislação aplicável e o RPO declarado, sendo precisamente definidos em runbook interno.

6.2. Descarte ao fim do período de retenção observa o art. 16 da LGPD (eliminação ou anonimização), com sobreposição segura ou rotação automatizada, garantindo a impossibilidade de recuperação por terceiros.

7. RECUPERAÇÃO (DISASTER RECOVERY)

7.1. RTO (Recovery Time Objective) — janela máxima de indisponibilidade aceitável, compatível com a criticidade do serviço, documentada e revisada periodicamente em runbook interno.

7.2. RPO (Recovery Point Objective) — perda máxima admissível de dados em caso de falha, alinhada à frequência efetiva dos backups e documentada em runbook interno.

7.3. Cadeia de aprovação — restauração em ambiente produtivo exige autorização documentada da Direção Técnica e registro completo da operação.

8. TESTES PERIÓDICOS

8.1. Teste de restauração é executado periodicamente em ambiente de homologação isolado, jamais sobre o ambiente produtivo.

8.2. Resultados — êxito, falha ou anomalia — são registrados em log auditável, com retenção mínima alinhada à exigência regulatória.

8.3. Falha em teste de restauração dispara revisão imediata desta política e dos procedimentos operacionais associados, com prazo máximo de tratamento definido em runbook interno.

CRC PJ RJ-010075/O-4 | CNPJ 45.853.794/0001-74
hncontabilidade.com | helpneto@hncontabilidade.com
Estr. da Cruz, 6 — São Pedro da Aldeia/RJ — CEP 28940-000

9. RESPONSABILIDADES

9.1. Direção Técnica — aprovação de restauração em produção, gestão do cronograma de testes, custódia do runbook interno e revisão semestral desta política.

9.2. Operação automatizada — execução dos backups conforme cronograma definido em runbook interno e geração de logs de auditoria.

9.3. Auditoria interna — verificação anual da aderência aos procedimentos definidos nesta política e no runbook interno.

10. CONFORMIDADE NORMATIVA

10.1. Esta Política observa o art. 46 da Lei Geral de Proteção de Dados (Lei nº 13.709/2018), a NBR ISO/IEC 27002 (controles A.5.10 — Proteção da Informação, e A.8.13 — Backup das Informações) e o Marco Civil da Internet (Lei nº 12.965/2014).

10.2. Em incidente de segurança que afete a integridade ou disponibilidade dos backups, o protocolo de Resposta a Incidentes da CONTRATADA é acionado, observados os prazos de comunicação à ANPD (art. 48, LGPD) quando aplicável.

11. REVISÃO E VERSIONAMENTO

11.1. Esta política é revisada semestralmente ou imediatamente após mudança significativa de infraestrutura, regulamentação ou incidente relevante.

11.2. Próxima revisão programada: novembro de 2026.

11.3. Versões anteriores ficam arquivadas conforme protocolo interno de versionamento, com registro de motivação de cada alteração.

12. CONFIDENCIALIDADE OPERACIONAL

12.1. As especificações técnicas detalhadas — localizações físicas e lógicas, ferramentas, configurações, intervalos exatos, provedores específicos, identificadores de sistemas e nomes de scripts ou utilitários — constituem informação confidencial e NÃO integram esta política pública.

12.2. O runbook operacional interno é mantido em ambiente de acesso controlado da Direção Técnica e seu compartilhamento, ainda que parcial, exige Acordo de Confidencialidade (NDA) específico, justificativa documentada e autorização expressa.

12.3. A divulgação não autorizada de qualquer trecho do runbook operacional sujeita o responsável às sanções previstas em lei, em contrato de trabalho e em código de conduta institucional.