DISASTER RECOVERY E CONTINUIDADE DE NEGÓCIOS (AD)

Responsável: João Pedro Toledo Gonçalves

Data: 26/01/2026

MANUAL TÉCNICO - DISASTER RECOVERY E CONTINUIDADE DE NEGÓCIOS (AD)

Código: ITGENG 0033/26 | **Classificação:** CONFIDENCIAL
Responsável: João Pedro Toledo Gonçalves | **Data:** 26/01/2026

1. HISTÓRICO DE REVISÃO

Data	Versão	Descrição	Autor
26/01/2026	**1.0**	**Criação Inicial**	**João Pedro Toledo Gonçalves**

2. OBJETIVO

Definir procedimentos para recuperação de objetos deletados, restauração de controladores de domínio (DC) falhos e continuidade do serviço de diretório.

---

3. RECUPERAÇÃO DE OBJETOS DELETADOS (AD RECYCLE BIN)

Cenário: Alguém deletou uma OU inteira "sem querer".

> **NOTA**
> **PRÉ-REQUISITO:** A lixeira deve ter sido ativada PREVIAMENTE no `AD Administrative Center`.

1. [x] Abra o **Active Directory Administrative Center**.
2. [x] Clique no Domínio > **Deleted Objects**.
3. [x] Localize o usuário/OU.
4. [x] Botão direito > **Restore** (Volta para o lugar original) ou **Restore To** (Lugar novo).

Se a lixeira não estiver ativa, você precisará de um Authoritative Restore (muito mais doloroso).

---

4. BACKUP DO SYSTEM STATE (NATIVO - WSB)

O Windows Server Backup (WSB) é a forma "canônica" de salvar o AD.

1. [x] Instale a feature: `Windows Server Backup`.
2. [x] Configure um backup agendado ou único.
3. [x] **O que selecionar?** A opção crítica é **System State**. Ela contém o banco NTDS.dit, registro e SYSVOL.

4. [x] Destino: Disco secundário ou Share de Rede.

---

5. FERRAMENTAS EXTERNAS (VEEAM / AZURE BACKUP)

Em ambientes corporativos, usamos Veeam.

Veeam Backup & Replication:

1. [x] Certifique-se que o "Application-Aware Processing" está ativado no Job.
   • Isso garante que o Veeam fale com o VSS do AD para um backup consistente.
2. [x] **Restore:** Use o "Veeam Explorer for Microsoft Active Directory".
   • Permite restaurar objetos granulares (como um usuário e seus grupos) sem voltar o servidor inteiro.

---

6. RESTORE DE DOMÍNIO (DSRM)

Cenário: O banco corrompeu ou você precisa voltar um backup do System State.

1. [x] Reinicie o DC.
2. [x] Pressione **F8** ou escolha **Directory Services Repair Mode (DSRM)** no boot.
3. [x] Logue com a senha de DSRM (Definida na promoção do DC).
4. [x] Use o WSB para restaurar o System State.

Authoritative vs Non-Authoritative

• **Non-Authoritative (Padrão):** Você restaura o backup, mas se houver outro DC vivo, ele sobrescreve seu backup com os dados "mais novos" dele.
• **Authoritative (ntdsutil):** Você diz "Esse backup é a verdade absoluta".
• Comando `ntdsutil`: `authoritative restore` > `restore subtree "OU=Financeiro,DC=empresa..."`.
• Isso incrementa o USN (número de versão) em +100.000, forçando todos os outros DCs a aceitarem esses dados antigos como novos.

7. VALIDAÇÃO FINAL

[ ] A lixeira do AD está ativa?
[ ] O backup do System State roda diariamente?
[ ] Você sabe a senha de DSRM atual? (Se não, resete com ntdsutil).