Administração de Sistemas Windows: Caso Prático GV Beauty.

GV Beauty

Júlia Carlini Dornelas

Leiria, maio de 2025

Lista de Tabelas

Índice

Introdução

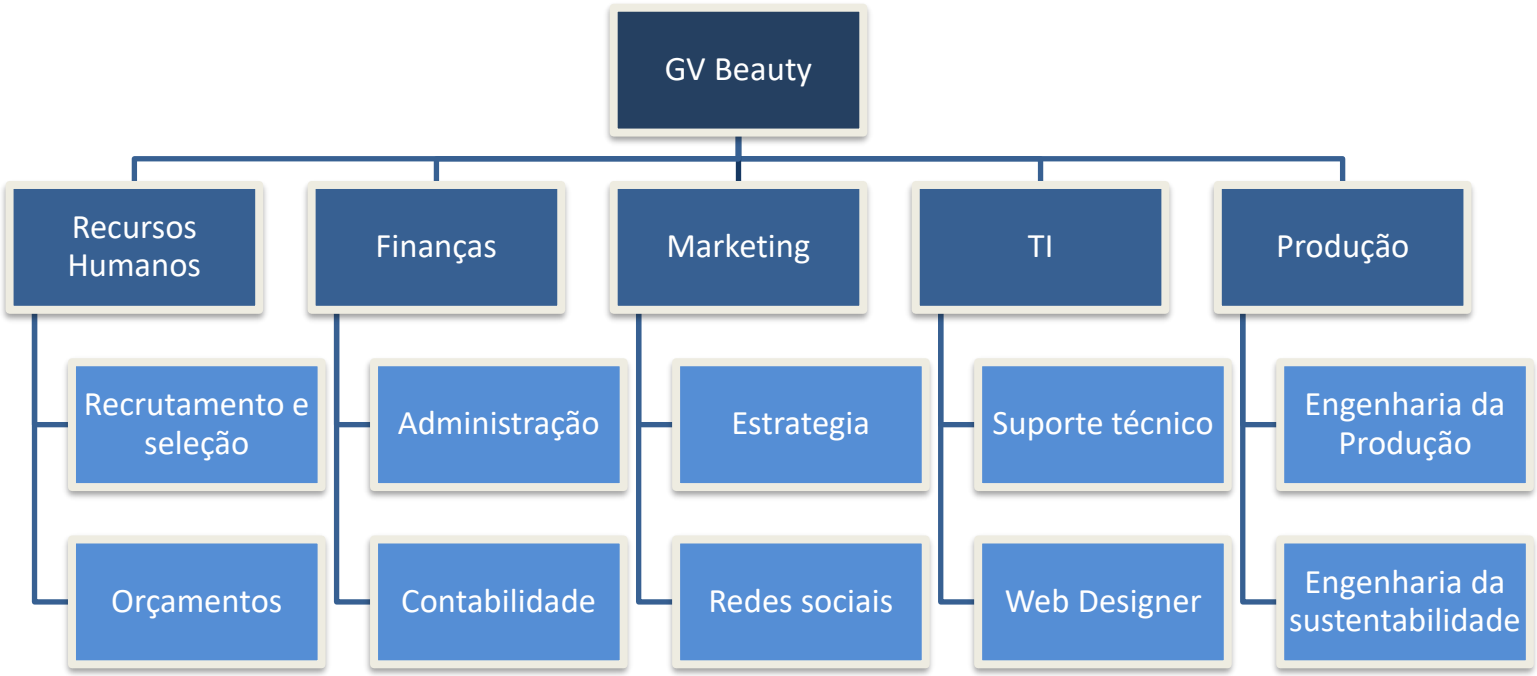
1.1. O objeto do projeto

Este projeto detalha a conceção e implementação de uma infraestrutura de gestão centralizada para a **GV Beauty**. O foco principal é a modernização administrativa através do Active Directory, garantindo que a tecnologia suporte o crescimento sustentável da empresa com segurança e automação.

1.2. Apresentação da empresa

Empresa: GV Beauty – Beleza, Tecnologia e Sustentabilidade

A GV Beauty, uma empresa especializada em produtos capilares comprometida com a saúde dos fios e o respeito ao meio ambiente, enfrenta desafios específicos em termos de gestão de sistemas e eficiência operacional.A empresa opera em uma sede de 200 m², equipada com tecnologia de ponta para produção e distribuição, contando com uma equipe de 26 funcionários. Para manter sua posição no mercado, a empresa precisa equilibrar a gestão eficiente de sistemas, a sustentabilidade e a consistência da marca.



GV Beauty										
Recursos	Recursos Humanos		Finanças		Marketing		TI		Produção	
	Recrutamento	Orçamento	Adminis tração.	Contabilidade	Estratégia	Redes sociais	Suporte técnico	Web Designer	Eng. Produção	Eng. Sustentabilidade
Users	2	3	3	3	3	2	3	2	3	2
Groups	1	1	1	1	1	1	2	1	1	1
Computers	2	3	3	3	3	2	3	2	3	2

Total	
Utilizadores	26
Grupos	11
Computadores	26

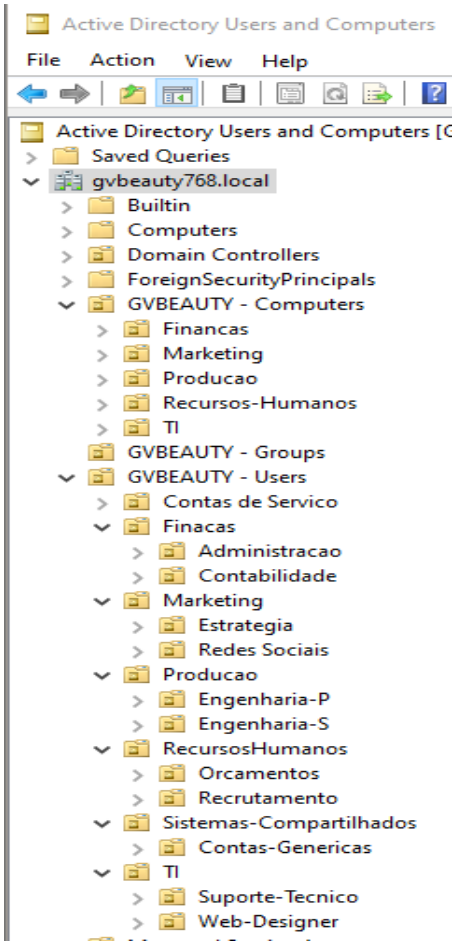
2. Infraestrutura Lógica Active Directory (AD)

A implementação do domínio **gvbeauty768.local** serviu como o alicerce para a administração centralizada.

2.1. Estrutura de Unidades Organizacionais (OUs):

Seguindo as boas práticas da Microsoft, a estrutura foi desenhada para separar objetos por tipo e função, facilitando a aplicação de GPOs:

- **GVBEAUTY - Computers:** rganizados por sub-OUs departamentais.
- **GVBEAUTY - Users:** Contém as contas de funcionários, segmentadas por área e sub-funções (ex: Estratégia vs Redes Sociais no Marketing).
- **GVBEAUTY - Groups:** Centraliza todos os grupos de segurança.



2.2. Automação e Padronização

Para garantir a eficiência, foram utilizados **scripts PowerShell** para a criação de utilizadores e computadores, assegurando uma nomenclatura rigorosa:

- **Utilizadores:** nome.sobrenome (ex: joao.silva).

```
# Importar o módulo do Active Directory
Import-Module ActiveDirectory

# Carregar os dados do CSV com codificação aceitável (Default)
$ADUsers = Import-Csv "C:\Users\Administrator\Documents\funcionarios_gvbeauty.csv" -Deli

# Definir o domínio para o UPN
$UPN = "gvbeauty.local"

# Loop para criação dos usuários
foreach ($User in $ADUsers) {
    try {
        # Definir os parâmetros usando um hashtable
        $UserParams = @{
            SamAccountName        = $User.Username
            UserPrincipalName     = "$($User.Username)@$UPN"
            Name                  = "$($User.FirstName) $($User.Lastname)"
            GivenName             = $User.FirstName
            Surname               = $User.Lastname
            Initial               = $User.Initials
            Enabled               = $True
            DisplayName           = "$($User.FirstName) $($User.Lastname)"
            Path                  = $User.OU    # OU deve estar no formato completo (DN)
            City                  = $User.City
            PostalCode            = $User.ZipCode
            Country               = $User.Country
            Company               = $User.Company
            State                 = $User.State
            StreetAddress         = $User.Street
            OfficePhone           = $User.OfficePhone
            EmailAddress          = $User.Email
            Title                 = $User.JobTitle
            Department            = $User.Department
            AccountPassword       = (ConvertTo-SecureString $User.Password -AsPlainText
            ChangePasswordAtLogon = $True
        }

        # Verificar se o usuário já existe
        if (Get-ADUser -Filter "SamAccountName -eq '$($User.Username)'") {
            Write-Host "A user with username $($User.Username) already exists in Active
        }
        else {
            New-ADUser @UserParams
            Write-Host "The user $($User.Username) is created." -ForegroundColor Green
        }
    }
    catch {
        Write-Host "Failed to create user $($User.Username) - $_" -ForegroundColor Red
    }
}
```

```
    }
    catch {
        Write-Host "Failed to create user $($User.Username) - $_" -ForegroundColor Red
    }
}

The user william.zanetti is created.
The user samuel.henriques is created.
The user paulo.almeida is created.
The user leonardo.ferreira is created.
The user gabriel.lima is created.
The user vitoria.pagnossin is created.
The user gabriela.ramos is created.
The user julia.carlini is created.
The user vanessa.campos is created.
The user leticia.teixeira is created.
The user gabriel.henriques is created.
The user olivia.almeida is created.
The user gabriel.pereira is created.
The user tiago.silva is created.
The user ulisses.dias is created.
The user paulo.gomes is created.
The user gabriel.esteves is created.
The user paulo.esteves is created.
The user igor.igrejas is created.
The user lucas.machado is created.
The user zuleica.vasconcelos is created.
The user ana.xavier is created.
The user nelson.ribeiro is created.
The user fernanda.nogueira is created.
The user nelson.teixeira is created.
The user samuel.campos is created.

PS C:\Users\Administrator> cls
```

- **Computadores:** Tipo-Departamento-ID (ex: W-RH-001).
- **Grupos:** Departamento-Função-Nível (ex: RH-Recrutamento-RW).

Delegação de Permissões: Permissões específicas atribuídas a cada área, como o RH gerir contas e senhas da sua unidade, e a TI deter o controlo total sobre servidores e GPOs.

3. POLÍTICAS DE SEGURANÇA E HARDENING (GPOs)

As GPOs foram configuradas para garantir que todos os dispositivos seguem as diretrizes de segurança da empresa sem intervenção manual em cada máquina.

3.1. Segurança do Sistema (Windows 10)

Conforme detalhado na **Tabela 1**, as políticas focam-se no bloqueio de vetores de ataque comuns:

- **Restrição USB:** Bloqueio de armazenamento removível para prevenir fuga de dados e malware.
- **PowerShell Restriction:** Impedimento de execução de scripts por utilizadores não autorizados.

Tabela 1 – GPO Windows 10

Departamento	Políticas de Grupo	Nome da GPO
Finanças	- Configuração de senhas seguras - Restringir a instalação de dispositivos USB - Configurar política de bloqueio de ecrã - Restringir o acesso ao Painel de Controlo -Desativar a execução de scripts do PowerShell	• C_PasswordPolicy • C_USBRestriction • U_ScreenLockPolicy • U_ControlPanelRestriction • U_PowerShellRestriction
Markenting	- Configuração de senhas seguras - Restringir a instalação de dispositivos USB - Configurar política de bloqueio de ecrã	• C_PasswordPolicy • C_USBRestriction • U_ScreenLockPolicy • U_ControlPanelRestriction • U_PowerShellRestriction

	- Restringir o acesso ao Painel de Controlo -Desativar a execução de scripts do PowerShell	
Produção	- Configuração de senhas seguras - Restringir a instalação de dispositivos USB - Configurar política de bloqueio de ecrã - Restringir o acesso ao Painel de Controlo -Desativar a execução de scripts do PowerShell	• C_PasswordPolicy • C_USBRestriction • U_ScreenLockPolicy • U_ControlPanelRestriction • U_PowerShellRestriction
RH	- Configuração de senhas seguras - Configurar política de bloqueio de ecrã - Restringir o acesso ao Painel de Controlo -Desativar a execução de scripts do PowerShell	• C_PasswordPolicy • U_ScreenLockPolicy • U_ControlPanelRestriction • U_PowerShellRestriction
TI	- Restringir a instalação de dispositivos USB - Restringir o acesso ao registo do sistema - Configurar políticas de atualização do Windows - Desativar aplicações não autorizadas	• C_USBRestriction • U_RegistryAccessBlock • C_WindowsUpdatePolicy • UC_BlockUnauthorizedApps

3.2. Controlo de Aplicações (Office e Chrome)

- **MS Office (Tabela 2):** Proteção de macros e integridade de ficheiros financeiros.
- **Google Chrome (Tabela 3):** Gestão centralizada de extensões e limpeza de dados de navegação para privacidade.

Tabela 2 – GPO MSOffice

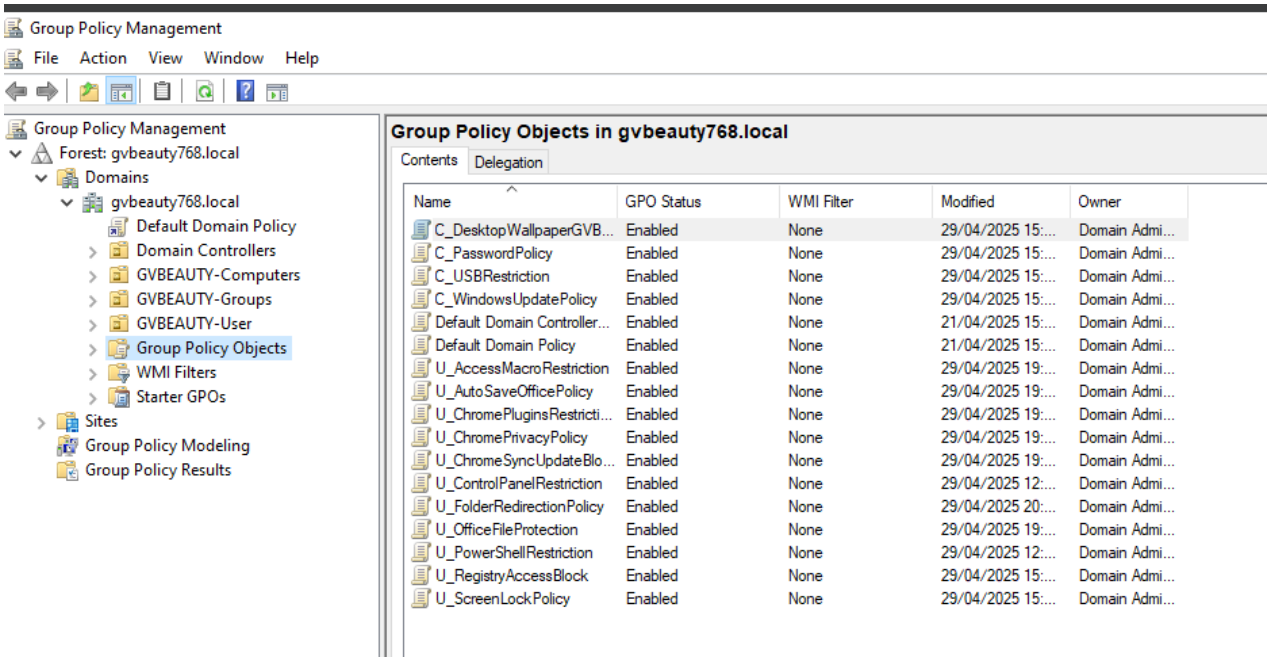
Departamento	Políticas de Grupo	Nome da GPO
Finanças	-Configurar proteção de folhas no Excel -Configurar proteção de ficheiros do Word	• U_OfficeFileProtection
Markenting	-Configurar guardar automático no PowerPoint -Verificação ortográfica no Outlook	• U_AutoSaveOfficePolicy
Produção	-Configurar proteção de folhas no Excel -Restringir macros no Access	• U_OfficeFileProtection • U_AccessMacroRestriction
RH	-Configurar proteção de ficheiros do Word -Verificação ortográfica no Outlook	• U_AutoSaveOfficePolicy
TI	-Restringir macros no Access -Configurar guardar automático e verificação ortográfica	• U_AccessMacroRestriction • U_AutoSaveOfficePolicy

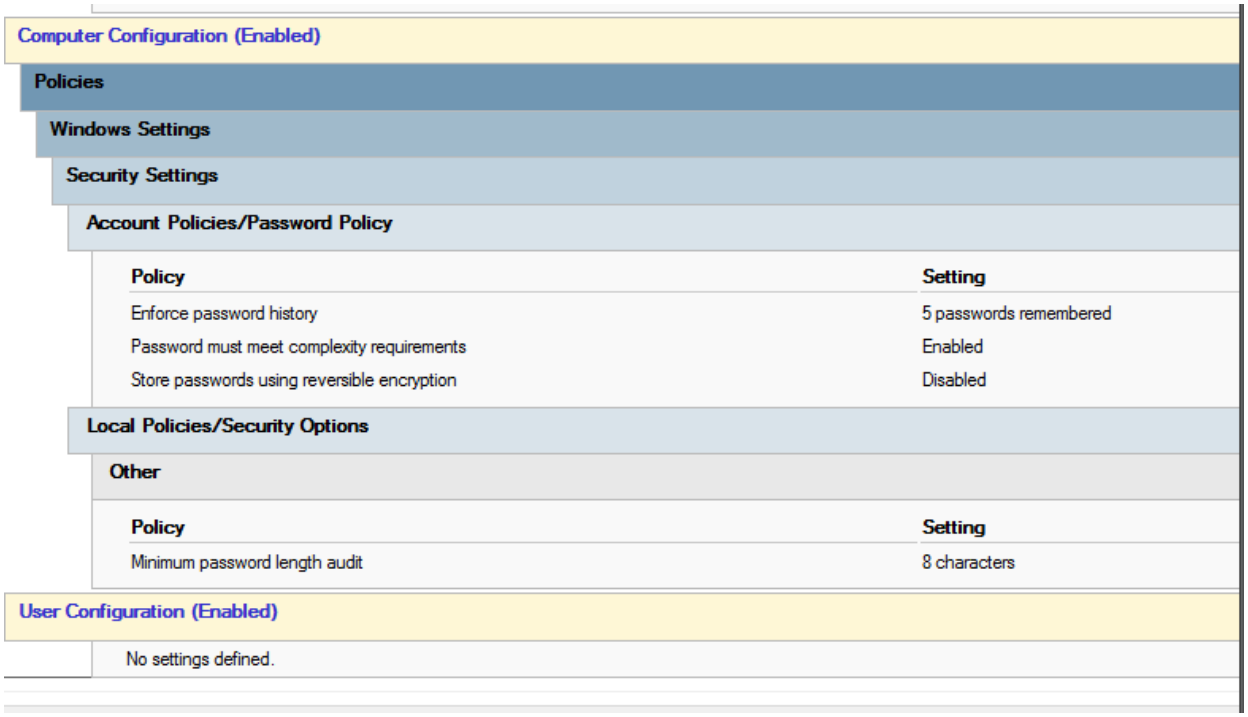
Tabela 3 – GPO Google Chrome

Departamento	Políticas de Grupo	Nome da GPO
Finanças	- Restringir instalação de extensões e plugins - Configurar políticas de cookies e cache	• U_ChromePluginsRestriction • U_ChromePrivacyPolicy
Marketing	- Configurar políticas de cache	• U_ChromePrivacyPolicy
Produção	-Restringir sincronização e atualizações automáticas - Restringir instalação de extensões e plugins	• U_ChromeSyncUpdateBlock • U_ChromePluginsRestriction
RH	-Restringir sincronização e cookies	• U_ChromePrivacyPolicy
TI	- Todas as opções para garantir segurança e controlo centralizado - Bloquear atualizações e plugins indevidos	• U_ChromePrivacyPolicy • U_ChromeSyncUpdateBlock • U_ChromePluginsRestriction

3.3. Redireccionamento de Pastas

Foi implementada a GPO de redirecionamento para garantir que os dados dos utilizadores (Documentos e Desktop) residam no servidor. Isto assegura a realização de backups centrais e a continuidade do trabalho em qualquer estação da rede.


Group Policy Management
File Action View Window Help
Group Policy Management
Forest: gvbeauty768.local
Domains
gvbeauty768.local
Default Domain Policy
Domain Controllers
GVBEAUTY-Computers
GVBEAUTY-Groups
GVBEAUTY-User
Group Policy Objects
WMI Filters
Starter GPOs
Sites
Group Policy Modeling
Group Policy Results
Group Policy Objects in gvbeauty768.local
Contents
Delegation
Name
GPO Status
WMI Filter
Modified
Owner
C_DesktopWallpaperGVB... Enabled None 29/04/2025 15:... Domain Admi...
C_PasswordPolicy Enabled None 29/04/2025 15:... Domain Admi...
C_USBRestriction Enabled None 29/04/2025 15:... Domain Admi...
C_WindowsUpdatePolicy Enabled None 29/04/2025 15:... Domain Admi...
Default Domain Controller... Enabled None 21/04/2025 15:... Domain Admi...
Default Domain Policy Enabled None 21/04/2025 15:... Domain Admi...
U_AccessMacroRestriction Enabled None 29/04/2025 19:... Domain Admi...
U_AutoSaveOfficePolicy Enabled None 29/04/2025 19:... Domain Admi...
U_ChromePluginsRestricti... Enabled None 29/04/2025 19:... Domain Admi...
U_ChromePrivacyPolicy Enabled None 29/04/2025 19:... Domain Admi...
U_ChromeSyncUpdateBlo... Enabled None 29/04/2025 19:... Domain Admi...
U_ControlPanelRestriction Enabled None 29/04/2025 12:... Domain Admi...
U_FolderRedirectionPolicy Enabled None 29/04/2025 20:... Domain Admi...
U_OfficeFileProtection Enabled None 29/04/2025 19:... Domain Admi...
U_PowerShellRestriction Enabled None 29/04/2025 12:... Domain Admi...
U_RegistryAccessBlock Enabled None 29/04/2025 15:... Domain Admi...
U_ScreenLockPolicy Enabled None 29/04/2025 15:... Domain Admi...


Computer Configuration (Enabled)
Policies
Windows Settings
Security Settings
Account Policies/Password Policy
Policy
Setting
Enforce password history
5 passwords remembered
Password must meet complexity requirements
Enabled
Store passwords using reversible encryption
Disabled
Local Policies/Security Options
Other
Policy
Setting
Minimum password length audit
8 characters
User Configuration (Enabled)
No settings defined.

4. SEGURANÇA DE REDE (FIREWALL)

A gestão da **Windows Defender Firewall** via GPO (**Tabela 4**) define o perímetro interno:

- **Regras de Entrada:** Permissão estrita para serviços essenciais (DNS, DHCP, RDP de gestão).
- **Regras de Saída:** Bloqueio de portas de risco e permissão apenas para tráfego web seguro (HTTPS).

Foram criadas três GPOs com configurações específicas de firewall:

Tabela 4 – GPO Firewall

Departamento	Políticas de Grupo	**Nome da GPO**
Servidores	Permitir RDP apenas a IPs internos, DNS (porta 53) e DHCP (porta 67).	• C_FirewallServidores
Todas as OUs de PCs	Permitir apenas tráfego HTTP/HTTPS de saída e partilha de ficheiros/impressoras com controlo por grupo.	• C_FirewallPCsGerais
TI	Permitir Remote PowerShell, WinRM, SSH e VPN para gestão remota de sistemas.	• C_FirewallTI

5. SERVIÇOS DE REDE (DHCP E DNS)

A conectividade é gerida de forma dinâmica e segura:

- **DHCP:** Segmentação em âmbitos (Scopes) por departamento (ex: TI em 10.0.2.x, RH em 10.0.5.x).
- **DNS:** Zona primária integrada no AD com atualizações dinâmicas seguras e mecanismos de *scavenging* para manter os registos atualizados.

5.1. Definição de todos os âmbitos DHCP de acordo com a estrutura

A GV Beauty conta com uma única sede, e a sua rede foi organizada por departamentos, com sub-redes atribuídas a cada um. Com base nas boas práticas, foi definido um único servidor DHCP, que também desempenha o papel de servidor DNS e controlador de domínio, garantindo centralização e integração total com o Active Directory. Cada âmbito (scope) foi configurado para um segmento de rede lógica, permitindo isolamento, gestão eficiente e futura escalabilidade.

Tabela 5 – Endereçamento Ip

Departamento	Âmbito	Intervalo de IPs	Máscara	Gateway	DNS Interno
TI	DHCP_TI	10.0.2.100-150	255.255.255.0	10.0.2.1	10.0.2.15
Finanças	DHCP_Financas	10.0.3.100-150	255.255.255.0	10.0.3.1	10.0.2.15
Marketing	DHCP_Marketing	10.0.4.100-150	255.255.255.0	10.0.4.1	10.0.2.15
RH	DHCP_RH	10.0.5.100-150	255.255.255.0	10.0.5.1	10.0.2.15
Produção	DHCP_Producao	10.0.6.100-150	255.255.255.0	10.0.6.1	10.0.2.15
Convidados	DHCP_Convidados	10.0.7.100-150	255.255.255.0	10.0.7.1	10.0.2.15

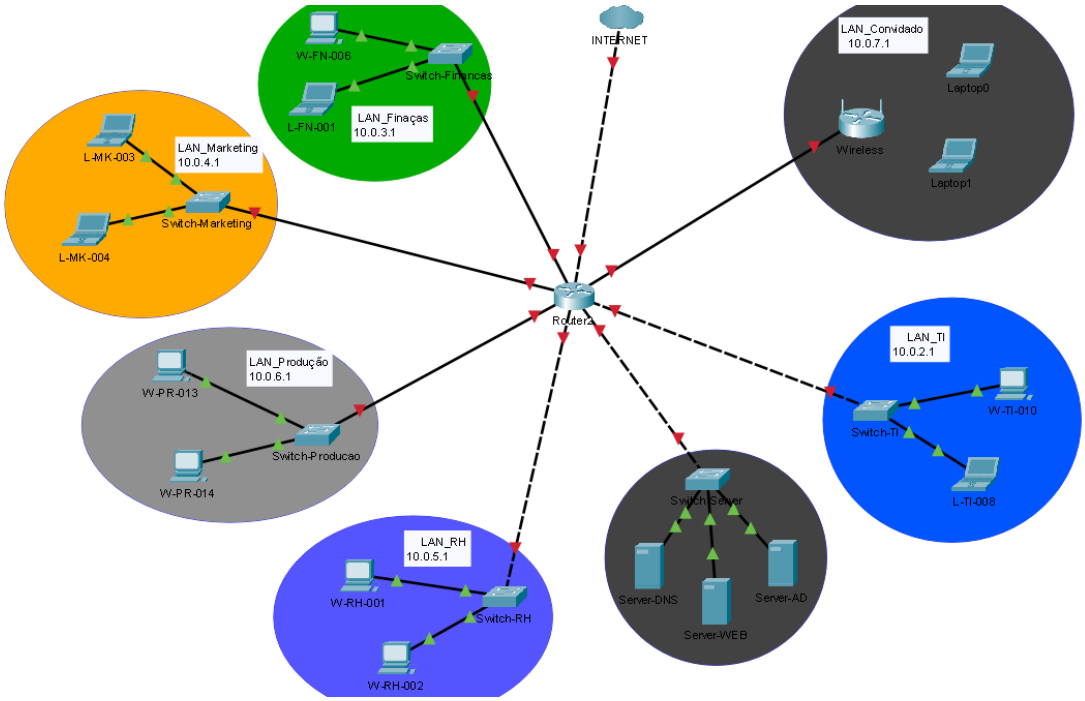


Figura 65 – Cenário da rede

Cada âmbito foi nomeado com base no departamento a que pertence, respeitando a boa prática de identificação clara e direta. Foi definido apenas **um servidor DNS interno**, tal como recomendado nas boas praticas, mas com possibilidade de expansão futura para redundância.

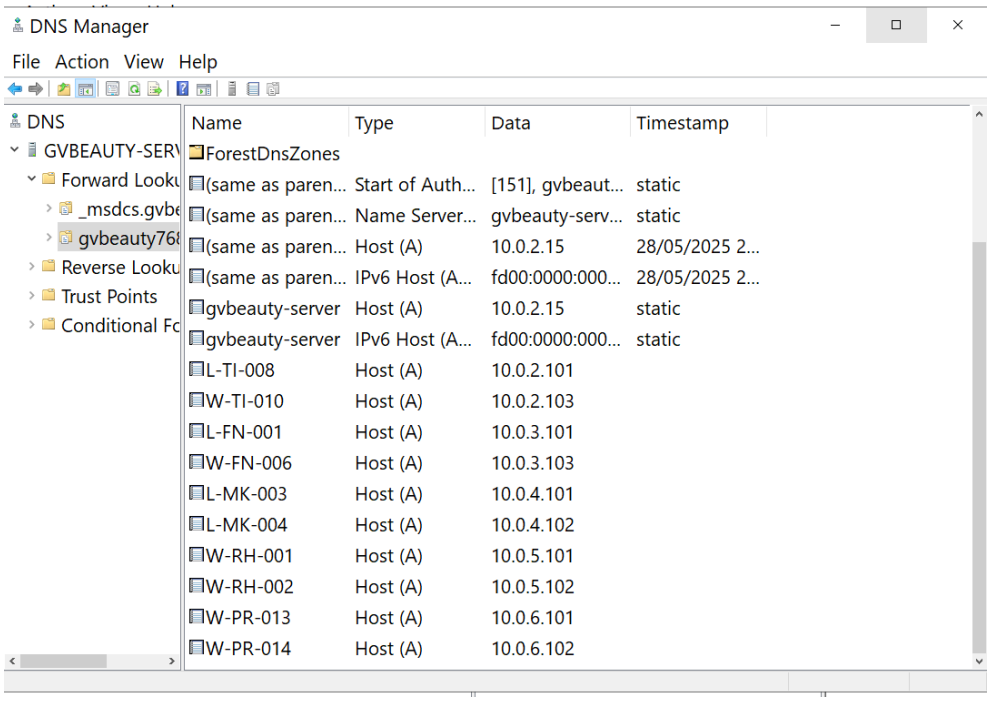


Figura 66 – Configuração server DNS

5.1. Usar o comando nslookup para testar o servidor

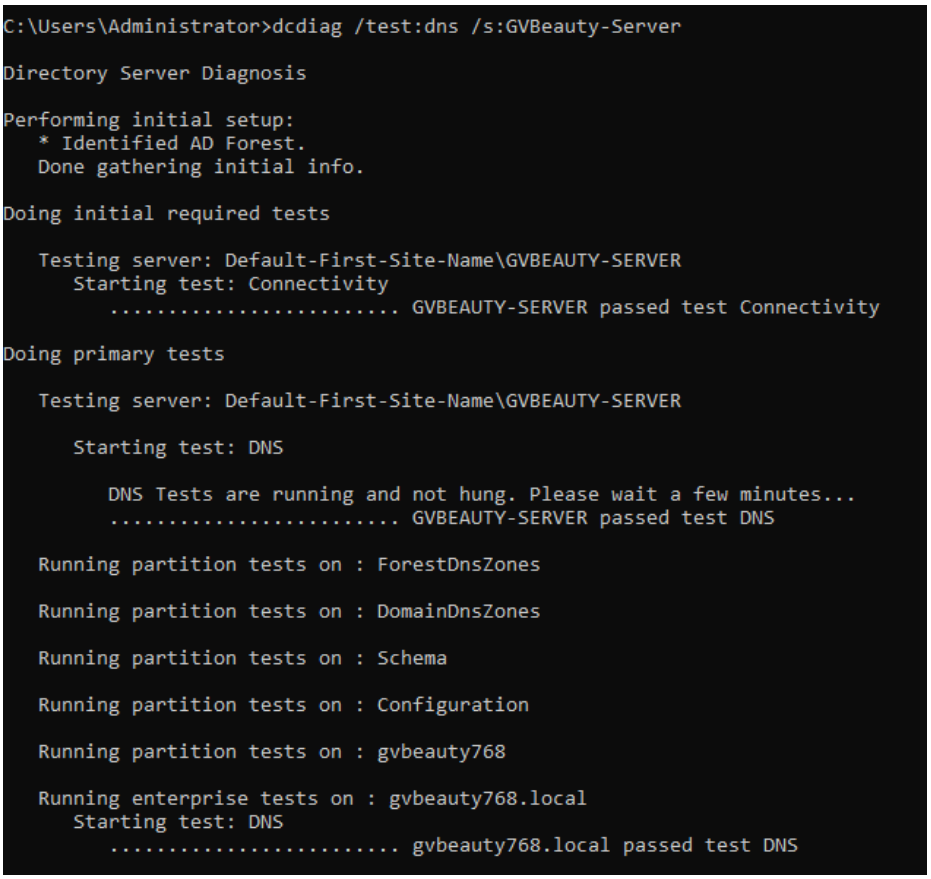


Figura 81 – Comando nslookup

6. CONCLUSÕES TÉCNICAS E RESULTADOS

A implementação do projeto **GV Beauty** demonstrou a eficácia da administração centralizada de sistemas Windows para garantir a integridade e a escalabilidade de uma infraestrutura empresarial. Através das etapas de planeamento e execução, foram alcançados os seguintes resultados:

- **Gestão de Identidades e Acessos:** A estruturação do **Active Directory (AD DS)** com Unidades Organizativas (OUs) específicas por departamento permitiu um controlo granular sobre utilizadores e equipamentos, aplicando o princípio do menor privilégio.
- **Hardening e Segurança via GPO:** A implementação estratégica de **Políticas de Grupo (GPOs)** permitiu padronizar o ambiente de trabalho e mitigar riscos de segurança, através da restrição de dispositivos removíveis (USB), bloqueio de instalações não autorizadas e configuração centralizada do **Windows Defender Firewall**.
- **Automação de Serviços de Rede:** A configuração dos serviços **DHCP e DNS** assegurou uma gestão dinâmica de IPs e uma resolução de nomes fiável. A segmentação das redes por departamento e a implementação de mecanismos de *scavenging* no DNS garantem uma infraestrutura limpa, organizada e preparada para o crescimento.

Considerações Finais: Este projeto reforçou a importância da **padronização** e do **controlo centralizado** como pilares da cibersegurança defensiva. A solução final entregue à GV Beauty não só otimiza a eficiência operacional, como estabelece uma postura de segurança resiliente contra acessos indevidos e falhas de configuração manual.