**DOCUMENTAÇÃO TÉCNICA - AMBIENTE ADSEGURO**

## 1. VISÃO GERAL DA ARQUITETURA

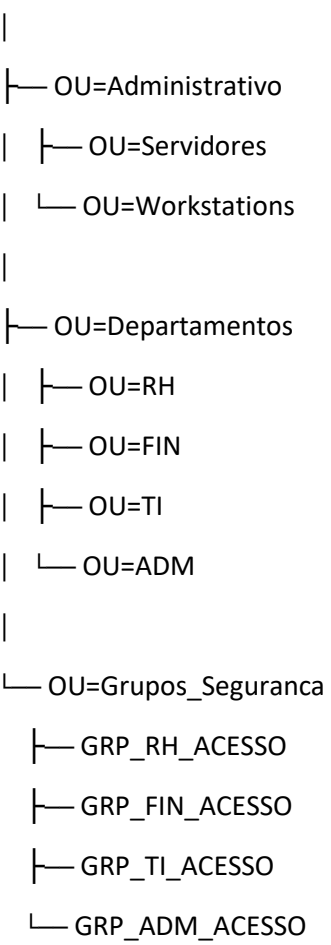
### 1.1. Especificações usadas no protótipo

- **Domínio:** ADSEGURO.local
- **Controlador de Domínio:** WIN-MV9DG2BH64S
- **IP do Servidor:** 192.168.1.10/24
- **Gateway:** 192.168.1.1
- **DNS:** Local (127.0.0.1) + Forwarder (8.8.8.8)

Estas configurações podem ser alteradas manualmente ao editar o script de instalação, logo nas linhas inciais.

### 1.2. Topologia Lógica

ADSEGURO.local



## 2. ESTRUTURA DE COMPARTILHAMENTOS

### 2.1. Shares Departamentais

| Share | Caminho Local | Permissões NTFS | Permissões Share |
|---|---|---|---|
| \\WIN-MV9DG2BH64S\RH | E:\Shares\RH | GRP_RH_ACESSO: Modify<br>GRP_ADM_ACESSO: Full Control | GRP_RH_ACESSO: Change<br>GRP_ADM_ACESSO: Change |
| \\WIN-MV9DG2BH64S\FIN | E:\Shares\FIN | GRP_FIN_ACESSO: Modify<br>GRP_ADM_ACESSO: Full Control | GRP_FIN_ACESSO: Change<br>GRP_ADM_ACESSO: Change |
| \\WIN-MV9DG2BH64S\TI | E:\Shares\TI | GRP_TI_ACESSO: Modify<br>GRP_ADM_ACESSO: Full Control | GRP_TI_ACESSO: Change<br>GRP_ADM_ACESSO: Change |
| \\WIN-MV9DG2BH64S\ADM | E:\Shares\ADM | GRP_ADM_ACESSO: Modify | GRP_ADM_ACESSO: Full |

### 2.2. Modelo de Permissões

Cada departamento possui acesso exclusivo à sua pasta, enquanto administradores (ADM) possuem acesso completo a todas as pastas. Dessa forma, há um isolamento total entre os departamentos. Uma pessoa do financeiro não tem acesso às pastas do RH, por exemplo.

Isso garante que o princípio do privilégio mínimo seja respeitado em um nível operacional nos departamentos, enquanto ainda mantém a existência de contas de administração com privilégios elevados para gerenciamento e troubleshooting.

## 3. POLÍTICAS DE GRUPO (GPO) DETALHADAS

### 3.1. GPO_Padrao_Seguranca (Domínio)

**Políticas de senhas**:

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System

├── PasswordComplexity: 1 (DWORD)

├── MinimumPasswordLength: 12 (DWORD)

├── MaximumPasswordAge: 0 (DWORD)

├── MinimumPasswordAge: 1 (DWORD)

├── LockoutBadCount: 5 (DWORD)

├── ResetLockoutCount: 30 (DWORD)

└── LockoutDuration: 30 (DWORD)

Explicação: Exige o uso de uma senha complexa com um mínimo de 12 caracteres que precisa ser alterada no primeiro logon pelo usuário e não possui data de expiração. Após 5 tentativas falhas dentro de 30 minutos, o acesso fica bloqueado por 30 minutos.

**Firewall Windows**:

HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile

└── EnableFirewall: 1 (DWORD)

HKLM\SOFTWARE\Policies\Microsoft\WindowsFirewall\StandardProfile

└── EnableFirewall: 1 (DWORD)

Explicação: Firewall do Windows sempre habilitado para perfis de Domínio e Standard.

**Windows Update:**

HKLM\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU

├── NoAutoUpdate: 0 (DWORD)

└── AUOptions: 4 (DWORD)

Explicação: Windows Update automático configurado para baixar e instalar automaticamente.

**Auditoria:**

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security

└── Retention: 0 (DWORD) # Não sobrescrever eventos

Explicação: Logs de segurança ficam configurados para não sobrescrever eventos.

**3.2. GPO_Padronizacao_Workstations (OU=Workstations)**

**Proteção de tela:**

HKLM\SOFTWARE\Policies\Microsoft\Windows\Control Panel\Desktop

├── ScreenSaveTimeOut: "600" (STRING)

└── ScreenSaverIsSecure: "1" (STRING)

Explicação**:** Bloqueio automático de tela após 10 minutos de inatividade, exigindo senha para desbloquear.

**Personalização restrita:**

HKLM\SOFTWARE\Policies\Microsoft\Windows\Personalization

└── NoChangingLockScreen: 1 (DWORD)

Explicação**:** Impede os usuários de alterar a tela de bloqueio.

**Configurações de energia:**

HKLM\SOFTWARE\Policies\Microsoft\Power\PowerSettings\29f6c1db-86da-48c5-9fdb-f2b67b1f44da

├── ACSettingIndex: 0 (DWORD)

└── DCSettingIndex: 0 (DWORD)

Explicação**:** Desabilita a hibernação e a suspensão nas estações de trabalho.

### 3.3. GPO_Padronizacao_Servidores (OU Servidores)

**Tamanho máximo dos logs:**

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\System

└── MaxSize: 4294967295 (DWORD) # 4GB - Máximo permitido

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security

└── MaxSize: 2147483648 (DWORD) # 2GB - Para auditoria detalhada

HKLM\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application

└── MaxSize: 1073741824 (DWORD) # 1GB - Para aplicações

Explicação**:** Configura o tamanho máximo dos logs de sistema, segurança e aplicação para manter um histórico detalhado.

### 3.4. GPO_RH_Restrictions & GPO_FIN_Restrictions

**Bloqueio de linha de comando:**

HKLM\SOFTWARE\Policies\Microsoft\Windows\System

└── DisableCMD: 2 (DWORD)

Explicação**:** Prompt de comando (CMD) completamente bloqueado, incluindo execução de scripts.

**Bloqueio de Painel de Controle:**

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explorer

└── NoControlPanel: 1 (DWORD)

Explicação**:** Painel de Controle inacessível para usuários dos departamentos RH e FIN.

**Bloqueio de dispositivos USB:**

HKLM\SOFTWARE\Policies\Microsoft\Windows\RemovableStorageDevices

└── Deny_All: 1 (DWORD)

Explicação**:** Dispositivos de armazenamento removível (USB, HD externo) completamente bloqueados.

**3.5. GPO_TI_Scripts**

**Liberação de linha de comando:**

HKLM\SOFTWARE\Policies\Microsoft\Windows\System

└── DisableCMD: 0 (DWORD)

Explicação**:** Uso do prompt de comando (CMD) fica liberado para o departamento de TI.

**Política de execução PowerShell:**

HKLM\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell

└── ExecutionPolicy: "Unrestricted" (STRING)

Explicação**:** PowerShell fica configurado sem restrições de execução para permitir o uso de scripts.

**3.6. GPO_Admins**

**Acesso Remoto:**

HKLM\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services

├── fDenyTSConnections: 0 (DWORD)

└── UserAuthentication: 0 (DWORD)

Explicação**:** Acesso Remoto (RDP) habilitado sem exigir a autenticação de nível de rede (NLA).

**Auditoria de linha de comando:**

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\Audit

└── ProcessCreationIncludeCmdLine_Enabled: 1 (DWORD)

Explicação**:** Auditoria habilitada para capturar linha de comando completa durante a criação de processos.

**Política de execução PowerShell:**

HKLM\SOFTWARE\Microsoft\PowerShell\1\ShellIds\Microsoft.PowerShell

└── ExecutionPolicy: "Unrestricted" (STRING)

Explicação**:** PowerShell fica sem restrições para permitir rodar scripts administrativos completos.

## 4. SCRIPTS AUTOMATIZADOS

### 4.1. Script de Logon (MapDrives.vbs)

Localização**:** \\WIN-MV9DG2BH64S\NETLOGON\MapDrives.vbs

Funcionalidade**:** Mapeamento automático da unidade S para as pastas share correspondentes aos seus respectivos departamentos:

- RH → \WIN-MV9DG2BH64S\RH
- FIN → \WIN-MV9DG2BH64S\FIN
- TI → \WIN-MV9DG2BH64S\TI
- ADM → \WIN-MV9DG2BH64S\ADM

## 5. USUÁRIOS E GRUPOS

### 5.1. Estrutura de Usuários

Usuários de exemplo adicionados pelo script:

| Usuário | Departamento | Grupo | OU |
|---|---|---|---|
| ana.silva | RH | GRP_RH_ACESSO | OU=RH |
| carlos.santos | FIN | GRP_FIN_ACESSO | OU=FIN |
| roberto.alves | TI | GRP_TI_ACESSO | OU=TI |

### 5.2. Grupos de Segurança

- **GRP_RH_ACESSO:** Acesso ao share do departamento de RH.
- **GRP_FIN_ACESSO:** Acesso ao share do departamento de FIN.
- **GRP_TI_ACESSO:** Acesso ao share do departamento de TI.
- **GRP_ADM_ACESSO:** Acesso completo a todos os shares dos departamentos.

## 6. PROCEDIMENTOS OPERACIONAIS

Abaixo constam exemplos de comandos no PowerShell para realizar procedimentos comuns no Active Directory através de scripts.

### 6.1. Adicionar Novo Usuário

Exemplo utilizado: Adicionar um novo usuário ao departamento de RH

```
New-ADUser -Name "novo.usuario" -SamAccountName "novo.usuario" -UserPrincipalName "novo.usuario@ADSEGURO.local" -Path "OU=RH,OU=Departamentos,DC=ADSEGURO,DC=local"

Add-ADGroupMember -Identity "GRP_RH_ACESSO" -Members "novo.usuario"
```

### 6.2. Verificar Aplicação de GPO

Verificar as GPOs aplicadas a uma OU específica

```
Get-GPInheritance -Target "OU=RH,OU=Departamentos,DC=ADSEGURO,DC=local"
```

Verificar as configurações de uma GPO específica

```
Get-GPRegistryValue -Name "GPO_RH_Restrictions" -All
```

### 6.3. Monitoramento de Logs

Verificar os logs de aplicação de GPO

```
Get-WinEvent -LogName "Microsoft-Windows-GroupPolicy/Operational" | Where-Object {$_.TimeCreated -gt (Get-Date).AddHours(-1)}
```

## 7. CONFIGURAÇÕES PENDENTES APÓS A INSTALAÇÃO POR SCRIPT

As seguintes GPOs precisam ser configuradas manualmente através do Console de Gerenciamento de Política de Grupo (GPMC):

- GPO_RH_Redirect
- GPO_FIN_Redirect
- GPO_TI_Redirect

Para estar de acordo com o diagrama apresentado no começo deste documento, recomenda-se que as pastas Documentos e Área de Trabalho sejam redirecionadas para \WIN-MV9DG2BH64S\Redirect%USERNAME%.

Nesta configuração, as pastas mencionadas ficariam organizadas no servidor separadas por usuário (Nota ao professor: Eu não consegui descobrir corretamente como fazer isso).