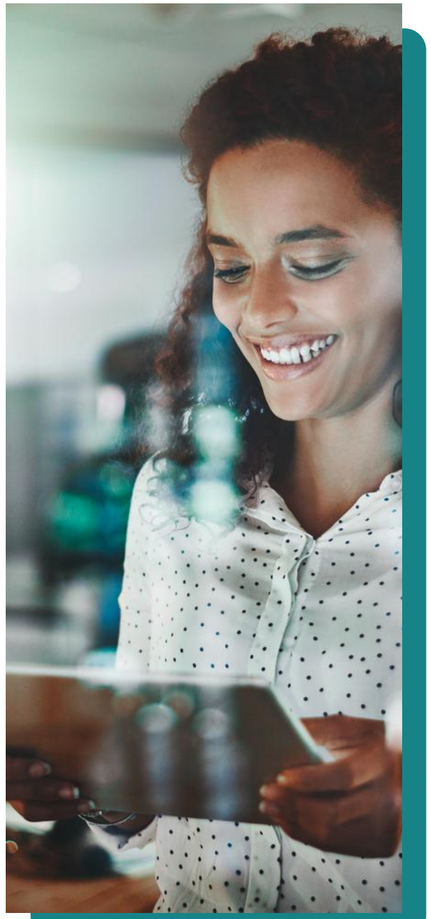
Dicas das principais GPOs que você pode aplicar na sua organização

DINAMIO

As Políticas de Grupo (GPOs) são essenciais para fortalecer a segurança, padronizar configurações e otimizar a gestão do Active Directory. Aqui estão as principais GPOs que você pode aplicar na sua organização:

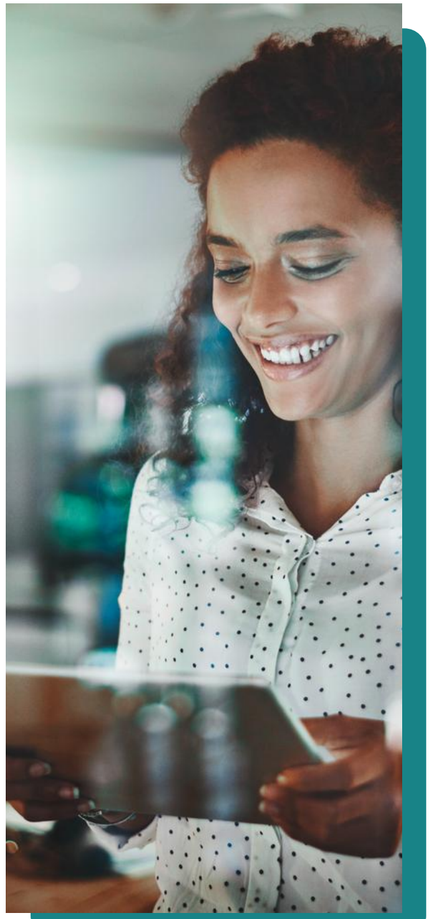


1.1 Segurança de Contas e Senhas

Essas políticas ajudam a evitar acessos não autorizados:

Política de Senhas

- Comprimento mínimo: 12-14 caracteres
- Complexidade: Habilitada (Maiúsculas, minúsculas, números e símbolos)
- Expiração: 90 dias (ou política de senha longa sem expiração)
- Histórico de senhas: 24 senhas anteriores
- Bloqueio de conta: 5 tentativas falhas em 15 min



1.2 Segurança de Contas e Senhas

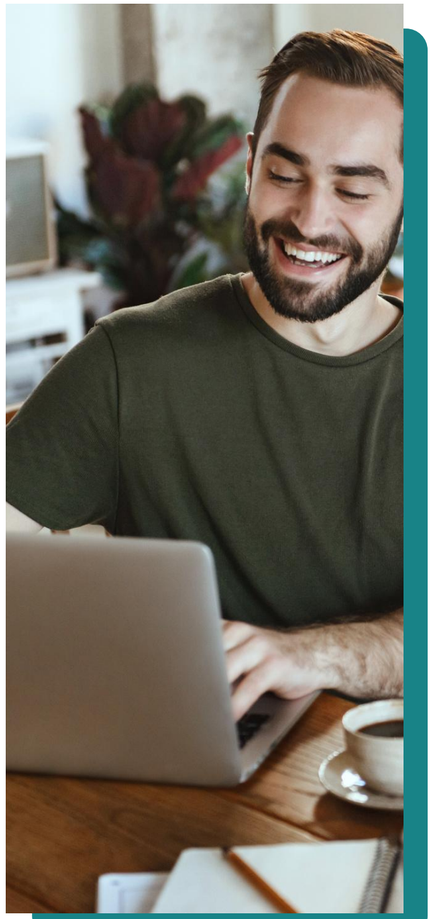
Essas políticas ajudam a evitar acessos não autorizados:

Autenticação Multifator (MFA):

- Configure via Azure AD MFA para acesso remoto e administrativo.

Proteção contra ataques de força bruta:

- Habilite Account Lockout Policy.



2.1 Configurações de Estações de Trabalho e Servidores

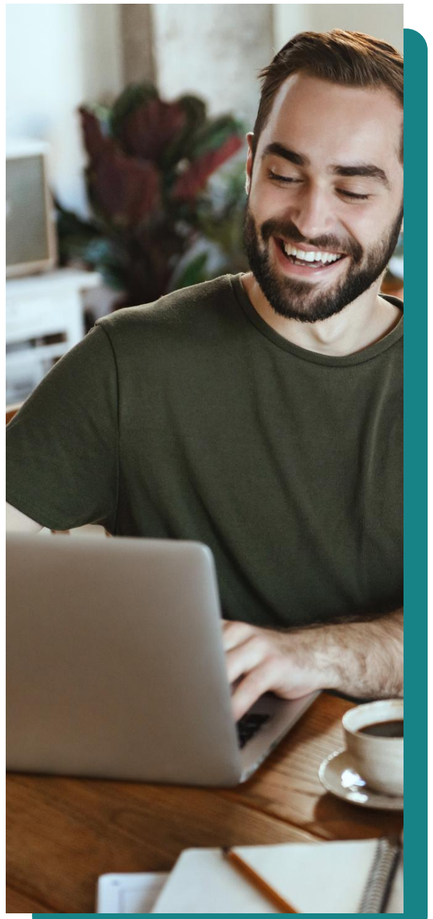
Essas GPOs garantem que todas as máquinas tenham um padrão seguro:

Tela de bloqueio automática

- Bloqueio de tela após 10-15 minutos de inatividade.
- Exigir senha para desbloquear.

Restrições de mídia removível

- Bloquear uso de USBs não autorizados.



2.2 Configurações de Estações de Trabalho e Servidores

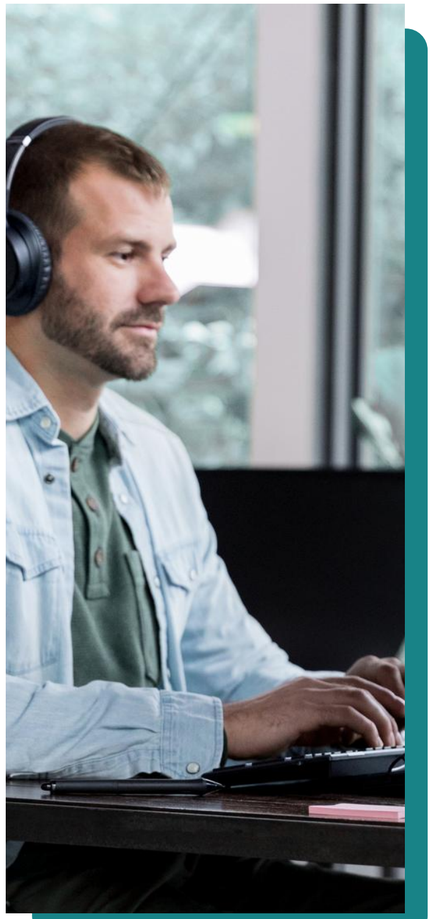
Essas GPOs garantem que todas as máquinas tenham um padrão seguro:

Firewall do Windows ativado:

- Bloquear conexões não autorizadas em todas as redes.

Windows Defender ativado

- Habilitar proteção em tempo real e varreduras automáticas.
- Permitir apenas aplicativos aprovados pela TI.



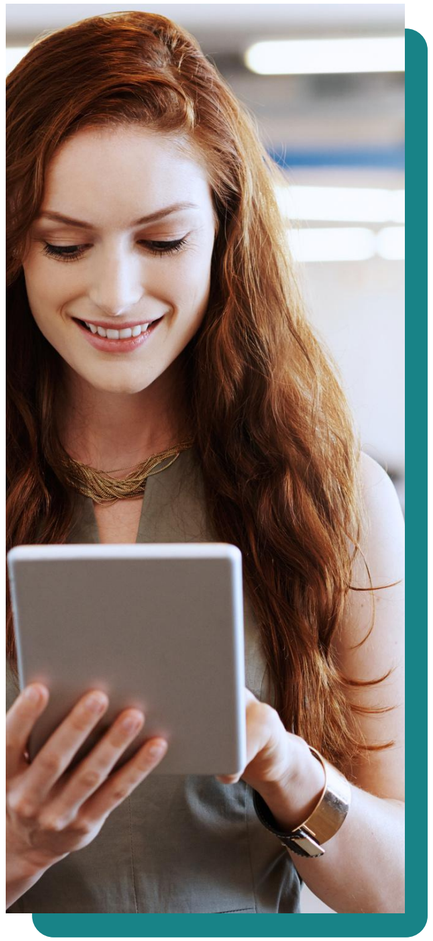
3. Gerenciamento de Acesso e Permissões

Evite que usuários tenham permissões desnecessárias:

Usuários locais sem privilégios administrativos
- Remova usuários do grupo Administradores Locais.

Redução do uso da conta Administrador
- Use Grupos de Segurança e Delegação de Permissões.

Permissões de compartilhamento e pastas
- Controle rigorosamente o acesso a compartilhamentos de rede.
- Bloqueie o uso do PowerShell, Prompt de Comando e Regedit para usuários comuns.



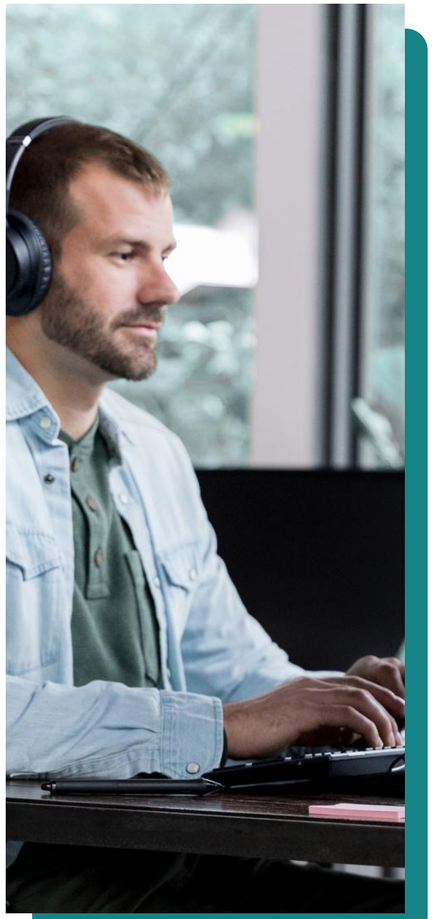
4. Controle de Rede e Internet

Mantenha a comunicação dentro dos padrões da empresa:

Configuração de Proxy e Bloqueio de Sites
- Redirecionar tráfego por proxy corporativo.
- Bloquear sites indesejados como redes sociais e torrents.

Bloquear compartilhamento de Wi-Fi e conexões ad-hoc
- Impedir criação de redes pessoais dentro da empresa.

Restringir conexões RDP
- Permitir RDP somente para administradores autorizados.



5. Monitoramento e auditoria

Mantenha a comunicação dentro dos padrões da empresa:

✅ **Auditoria de logon**

Registre tentativas de login bem-sucedidas e falhas.

✅ **Auditoria de alterações no Active Directory**

Monitorar mudanças em usuários, grupos e permissões.

✅ **Auditoria de acesso a arquivos**

Log de acessos e modificações em arquivos críticos.

DINAMIO

Potencializando empresas e suas pessoas

dinamio.com.br

@dinamiotecnologia

+55 (47) 3032-8100

+55 (11) 3185-6975

comercial@dinamio.com.br