Guia de Configuração e Implementação do Sistema de Segurança – Windows 11 Pro

1. Controle de Execução de Software (AppLocker e Políticas de Restrição de Software)

Para garantir que apenas programas autorizados sejam executados na rede corporativa, siga os passos abaixo:
1. Pressione as teclas Windows + R, digite “gpedit.msc” e pressione Enter.
2. Acesse: Configuração do Computador → Configurações do Windows → Configurações de Segurança → Políticas de Controle de Aplicativos → AppLocker.
3. Clique com o botão direito em “Regras de Executáveis” e selecione “Criar Nova Regra”.
4. Defina o tipo de regra (por Editor, Caminho ou Hash do arquivo).
5. Escolha “Permitir” e selecione os programas autorizados.
6. Clique em “Aplicar” e reinicie o computador para que as regras entrem em vigor.

2. Restrição de Acesso a Dispositivos Removíveis

Para restringir o uso de dispositivos USB, siga os passos:
1. Pressione Windows + R, digite “gpedit.msc” e pressione Enter.
2. Vá para: Configuração do Computador → Modelos Administrativos → Sistema → Acesso de Armazenamento Removível.
3. Selecione “Todas as classes de armazenamento removível: negar acesso de leitura” e “negar acesso de gravação”.
4. Ative as opções desejadas e clique em “Aplicar”.

3. Controle de Acesso a Arquivos e Pastas (NTFS ACLs)

Para configurar permissões de acesso:
1. Clique com o botão direito sobre a pasta → Propriedades → Segurança → Editar.
2. Selecione o usuário ou grupo e configure as permissões (Leitura, Escrita, Modificação, Exclusão).
3. Utilize o princípio do menor privilégio: conceda apenas o necessário para o desempenho da função.
4. Clique em “Aplicar” e “OK”.

4. Políticas Baseadas em Horários (Agendador de Tarefas)

Para aplicar políticas em horários específicos:
1. Abra o Agendador de Tarefas (Task Scheduler).
2. Clique em “Criar Tarefa” → aba “Disparadores” → “Novo”.
3. Defina o horário de início e recorrência.
4. Na aba “Ações”, configure o script ou comando a ser executado (por exemplo, ativar/desativar regras de firewall).
5. Clique em “OK” e salve.

5. Notificações Automáticas de Violações (Microsoft Defender)

1. Abra o menu Iniciar → Segurança do Windows → Proteção contra vírus e ameaças.
2. Acesse “Gerenciar configurações” e habilite “Proteção em tempo real”.
3. Em “Notificações”, selecione “Enviar notificações sobre ameaças detectadas”.
4. Para monitoramento centralizado, configure o Windows Security Center no painel do administrador.

6. Registro e Auditoria de Atividades (Event Viewer)

1. Pressione Windows + R e digite “eventvwr.msc”.
2. Em “Logs do Windows”, selecione “Segurança”.
3. Clique em “Filtrar Log Atual” para exibir tentativas de acesso negadas ou alterações de política.
4. Use “Salvar Log Como...” para exportar e integrar com sistemas SIEM.

7. Controle Centralizado via Active Directory (GPMC)

Para ambientes corporativos integrados a domínio:
1. No servidor, abra o “Gerenciador de Política de Grupo” (gpmc.msc).
2. Crie uma nova GPO e edite: Configuração do Computador → Políticas → Configurações do Windows → Segurança → AppLocker.
3. Configure as regras conforme políticas internas.
4. Vincule a GPO à Unidade Organizacional (OU) desejada.
5. Aguarde a replicação ou force a atualização com o comando “gpupdate /force”.

Documento técnico elaborado para demonstrar configuração e implementação de políticas de segurança no ambiente Windows 11 Pro.