SUPORTE TÉCNICO TI & ENDPOINTS

# Checklist de Auditoria e Provisionamento

Endurecimento de Segurança com BitLocker e Windows Defender

| NOME DO TÉCNICO / ANALISTA: | HOSTNAME / NOME DO PC: | DATA DO PROCEDIMENTO: |
| --- | --- | --- |
| _____ | _____ | _____ |

## FASE 1: PREPARAÇÃO DE HARDWARE E BIOS / UEFI

| STATUS | ITEM DE VERIFICAÇÃO | AÇÃO / COMANDO RECOMENDADO |
| --- | --- | --- |
| ☐ | **Modo UEFI Ativo**<br>Verificar se o sistema operacional está rodando em modo UEFI puro (sem Legacy/CSM). | `msinfo32` → Modo da BIOS: UEFI |
| ☐ | **Secure Boot Ativado**<br>Garantir que a Inicialização Segura está habilitada para impedir bootkits e rootkits. | `msinfo32` → Estado da Inicialização Segura: Ativado |
| ☐ | **Módulo TPM 2.0 Operacional**<br>Validar se o chip de segurança TPM está visível, ativado e pronto para uso pelo Windows. | `tpm.msc` ou PowerShell: `Get-Tpm` |
| ☐ | **Atualização de Firmware (BIOS)**<br>Confirmar se a BIOS/UEFI está na versão mais recente para evitar falhas no TPM. | Site do fabricante / Suporte Vendor |

## FASE 2: CONFIGURAÇÃO E BACKUP DO BITLOCKER

| STATUS | ITEM DE VERIFICAÇÃO | AÇÃO / COMANDO RECOMENDADO |
| --- | --- | --- |
| ☐ | **Criptografia da Unidade C: (Sistema)**<br>Garantir que o volume principal do SO está 100% criptografado (XTS-AES 128/256 bits). | `manage-bde -status C:` |
| ☐ | **Backup de Chave de Recuperação (48 dígitos)**<br>Exportar e confirmar salvamento da chave no Active Directory, Azure AD/ Entra ID ou Cofre seguro. | `manage-bde -protectors -get C:` |
| ☐ | **Criptografia de Volumes Secundários**<br>Ativar BitLocker e Auto-Unlock em discos de dados adicionais (D:, E:), se houver. | Painel de Controle → Gerenciar BitLocker |

## FASE 3: ENDURECIMENTO DO WINDOWS DEFENDER

| STATUS | ITEM DE VERIFICAÇÃO | AÇÃO / COMANDO RECOMENDADO |
| --- | --- | --- |
| ☐ | **Proteção em Tempo Real & Nuvem Ativas**<br>Verificar se a análise contínua de arquivos e serviços na nuvem estão operacionais. | `Get-MpComputerStatus` |
| | **Proteção Contra Adulteração (Tamper Protection)** | |

| STATUS | ITEM DE VERIFICAÇÃO | AÇÃO / COMANDO RECOMENDADO |
|---|---|---|
| ☐ | Habilitar proteção para impedir que pragas virtuais ou usuários desativem o Defender. | Segurança do Windows → Proteção contra vírus e ameaças |
| ☐ | **Acesso Controlado a Pastas (Anti-Ransomware)**<br>Bloquear alterações não autorizadas em documentos e pastas do perfil do usuário. | Segurança do Windows → Proteção contra Ransomware |
| ☐ | **Atualização de Vacinas / Assinaturas**<br>Forçar atualização da base de conhecimento de inteligência de segurança do antivírus. | `Update-MpSignature` |

### 📌 Dicas de Ouro para o Analista de Suporte (Nível Pleno)

**Troca de Hardware/BIOS:** Sempre clique em *"Suspender Proteção"* do BitLocker no Painel de Controle antes de atualizar a BIOS ou trocar a placa-mãe. Isso evita a solicitação acidental da chave de recuperação de 48 dígitos no boot. **Ambientes Corporativos:** Automatize a ativação do BitLocker e exportação de chaves via GPO ou Intune (Configuration Profiles) para evitar erros manuais.

Assinatura do Técnico / Analista de TI

Visto do Responsável / Validação de Segurança