PLANO DE MANUAIS TÉCNICOS RECOMENDADOS

iT GUYS SOLUTIONS

PLANO DE MANUAIS TÉCNICOS RECOMENDADOS

Este documento lista os manuais essenciais recomendados para compor a base de conhecimento da iT Guys, organizados por tecnologia. A seleção baseia-se em melhores práticas de mercado e necessidades operacionais de MSPs.

1. REDE E SEGURANÇA (PFSENSE / SURICATA / OPENVPN)

• **pfSense:**
• [Nível 1] Diagnóstico de Conectividade e Logs: Verificação de status de interfaces, gateways e análise de logs do system/firewall.
• [Nível 2] Gestão de Regras de Firewall e Aliases: Boas práticas de criação de regras "default deny", uso de aliases.
• [Nível 2] Configuração e Troubleshooting de VPN (OpenVPN/IPsec): Site-to-site e client-to-site.
• [Nível 3] Backup e Restauração de Configurações: AutoConfigBackup e restauração em caso de desastre.
• [Nível 3] Atualização e Hardening: Checklist de segurança e procedimento de update.
• **Suricata (IDS/IPS):**
• [Nível 2] Instalação e Integração com pfSense/OPNsense: Deploy como IDS inline.
• [Nível 2] Gestão de Regras (ET Open/Snort): Atualização e customização de rulesets.
• [Nível 3] Análise de Alertas e Tuning: Supressão de falsos positivos e otimização.
• **OpenVPN (Standalone):**
• [Nível 1] Instalação do Servidor OpenVPN: Deploy em Linux (Ubuntu/Debian).
• [Nível 2] Configuração de Clientes e Certificados: Geração de .ovpn e PKI.
• [Nível 3] Troubleshooting de Conexão: Logs, MTU, e problemas de NAT.
• **VLANs:**
• [Nível 2] Conceitos e Configuração em Switches Gerenciáveis: Tagged vs Untagged.
• [Nível 2] Configuração de VLANs em pfSense/Linux: Interfaces virtuais e roteamento inter-VLAN.
• [Nível 3] Troubleshooting de VLANs: Diagnóstico de tagging incorreto e isolamento.

2. STORAGE E ARMAZENAMENTO (TRUENAS SCALE / SAMBA / ISCSI)

• **[Nível 1] Monitoramento de Saúde de Discos e Alertas:** Interpretação de alertas SMART, verificação de temperatura e status básico do pool ZFS.
• **[Nível 2] Gestão de Users, Groups e ACLs (SMB/NFS):** Criação de compartilhamentos, mapeamento de permissões Windows (ACLs) e exportações NFS.
• **[Nível 2] Configuração de Snapshots e Replicação:** Agendamento de snapshots automáticos e tarefas de replicação para backup offsite.
• **[Nível 3] Manutenção de ZFS (Scrub e Substituição de Disco):** Procedimento crítico de substituição de disco com falha (resilvering) e agendamento de Scrubs.

• **[Nível 3] Configuração de iSCSI Target para Virtualização:** Criação de zvols, portals e targets para uso em VMware/Proxmox.

3. BANCOS DE DADOS (POSTGRESQL / MYSQL / REDIS)

• **[Nível 1] Backup e Restore Básico (dump/restore):** Uso de `mysqldump` e `pg_dump` para backups lógicos e restauração.
• **[Nível 2] Manutenção Preventiva e Limpeza:**
• **Postgres:** Explicação e agendamento do `VACUUM` e `ANALYZE`.
• **MySQL:** Uso do `mysqlcheck` e `OPTIMIZE TABLE`.
• **[Nível 2] Gestão de Usuários e Permissões:** Criação de usuários com privilégios mínimos (GRANT/REVOKE).
• **[Nível 3] Troubleshooting de Performance e Slow Queries:** Ativação e análise de logs de queries lentas (`slow query log`).
• **Redis:**
• [Nível 1] Instalação e Comandos Básicos: `redis-cli`, `SET`, `GET`, `KEYS`.
• [Nível 2] Persistência e Backup: RDB vs AOF, snapshots.
• [Nível 2] Segurança: Autenticação, bind e firewall.
• [Nível 3] Troubleshooting de Memória e Performance: Monitoramento com `INFO`, eviction policies.

4. WINDOWS SERVER (AD / DNS / GPO / FIREWALL)

• **[Nível 1] Criação e Bloqueio de Usuários (Padrão):** Procedimento padrão de admissão e demissão (onboarding/offboarding).
• **[Nível 2] Manutenção de DNS e DHCP:** Limpeza de registros obsoletos (Scavenging), verificação de Forwarders e Root Hints.
• **[Nível 3] Diagnóstico de Replicação do AD (DCDIAG):** Uso de ferramentas (`dcdiag`, `repadmin`) para garantir saúde do domínio e replicação entre DCs.
• **[Nível 3] Gestão Centralizada via GPO:**
• Mapeamento de Drives e Impressoras.
• Políticas de Senha e Bloqueio de Tela.
• Deploy de Software (.msi).
• **[Nível 3] Disaster Recovery do Active Directory:** Backup do System State e restauração autoritativa vs não-autoritativa.

5. LINUX (UBUNTU / DEBIAN / ALPINE / CENTOS / ALMALINUX)

• **[Nível 1] Comandos Essenciais de Diagnóstico:** Uso de `top`, `htop`, `df`, `free`, `ip addr` para check rápido de saúde.
• **[Nível 2] Gerenciamento de Pacotes e Updates:**
• **Debian/Ubuntu:** `apt update/upgrade`, limpeza com `autoremove`.

• **CentOS/AlmaLinux:** `dnf update`, limpeza com `dnf autoremove`.
• **[Nível 2] Configuração de Firewall (UFW/IPTables/firewalld):** Bloqueio padrão e liberação de portas.
• **[Nível 3] Hardening de Servidor Linux:** SSH seguro (chaves, porta não-padrão), Fail2Ban e usuários sudo.
• **[Nível 3] Análise de Logs (Journalctl/Syslog):** Como buscar erros críticos em `/var/log` e `journalctl`.
• **[Nível 1] Leitura de Logs Linux:** Uso de `cat`, `tail -f`, `less`, `grep` em `/var/log/syslog`, `auth.log`, `messages`.

6. VIRTUALIZAÇÃO (PROXMOX VE)

• **[Nível 1] Gestão Básica de VMs e Containers (LXC):** Ligar, desligar, reiniciar e acessar console (VNC/Spice).
• **[Nível 2] Gestão de Backups e Snapshots (PBS):** Configuração de rotinas de backup para Proxmox Backup Server ou armazenamento local.
• **[Nível 3] Gestão de Cluster e High Availability (HA):** Adicionar nós ao cluster, configurar fencing e grupos de HA.
• **[Nível 3] Troubleshooting de Rede (Linux Bridge/Bonding):** Diagnóstico de conectividade em interfaces virtuais e vlans.

7. CONTAINERS (DOCKER / DOCKER-COMPOSE / PORTAINER)

• **[Nível 1] Deploy e Update de Stacks (Portainer):** Como atualizar um container recriando-o com nova imagem (pull).
• **[Nível 2] Diagnóstico de Containers:** Verificação de logs (`docker logs`), inspeção (`docker inspect`) e monitoramento de recursos (`docker stats`).
• **[Nível 2] Manutenção de Disco (Docker Prune):** Limpeza de imagens, volumes e builders não utilizados para liberar espaço.
• **[Nível 3] Backup de Volumes e Dados Persistentes:** Estratégias para backup dos diretórios mapeados nos volumes.

8. APLICATIVOS E VOIP (GITEA / ZABBIX / ASTERISK / NAVEGADORES)

• **Gitea:**
• [Nível 2] Backup e Restore Completo (Database + Repositórios).
• [Nível 3] Procedimento de Upgrade de Versão (Docker).
• **Zabbix:**
• [Nível 1] Adição de Hosts e Templates.
• [Nível 2] Criação de Triggers e Ações de Alerta.
• [Nível 3] Otimização de Database e Housekeeping.
• **VoIP (Asterisk/Issabel):**
• [Nível 1] Diagnóstico de Ramais Offline (Sip Show Peers).

• [Nível 2] Troubleshooting de Áudio Unidirecional (NAT/RTP).
• [Nível 2] Análise de Logs de Chamadas (CDR/Verbosity).
• **MagnusBilling:**
• [Nível 1] Gestão de Usuários e Créditos: Criação de contas e recarga.
• [Nível 2] Configuração de Troncos SIP: Integração com operadoras VoIP.
• [Nível 2] Relatórios de Chamadas e CDR: Análise de consumo e faturamento.
• [Nível 3] Troubleshooting e Manutenção: Logs, asterisk CLI, atualizações.
• **Navegadores (Chrome/Firefox):**
• [Nível 2] Gestão via GPO (ADMX): Definir homepage, extensões obrigatórias e bloqueios.

9. FERRAMENTAS (SSH / PUTTY / WINSCP / SCP)

• **[Nível 0] Acesso Remoto Seguro:** Guia de como usar chaves SSH (PPK/PEM) no Putty e Terminal.
• **[Nível 1] Tunelamento SSH (Port Forwarding):** Como acessar serviços internos de forma segura via túnel.
• **[Nível 1] SCP via Terminal:** Transferência de arquivos via linha de comando (`scp origem destino`).
• **WinSCP:**
• [Nível 0] Transferência de Arquivos via SFTP/SCP: Conexão segura e upload/download de arquivos.
• [Nível 1] Sincronização de Diretórios: Automatizar cópia de pastas entre servidor e máquina local.

10. SERVIDORES WEB (NGINX / APACHE)

• **Nginx:**
• [Nível 1] Configuração Básica de Virtual Hosts: Criação de sites e redirecionamentos.
• [Nível 2] Configuração de Proxy Reverso: Encaminhamento de requisições para serviços internos.
• [Nível 2] Configuração de SSL/TLS (Let's Encrypt): Certificados gratuitos via Certbot.
• [Nível 3] Otimização de Performance e Cache: Gzip, buffer tuning e cache de conteúdo estático.
• **Apache:**
• [Nível 1] Configuração Básica de Virtual Hosts: Criação de sites com .htaccess.
• [Nível 2] Módulos Essenciais (mod_rewrite, mod_ssl): Configuração de redirecionamentos e HTTPS.
• [Nível 3] Troubleshooting de Erros 500/502: Análise de logs e debug de configuração.

11. TRANSFERÊNCIA DE ARQUIVOS (FTP)

• **[Nível 1] Configuração de Servidor FTP/SFTP:** Instalação e configuração básica (vsftpd, ProFTPD).
• **[Nível 2] Segurança e Chroot Jail:** Isolamento de usuários e permissões de diretório.
• **[Nível 2] FTP Passivo vs Ativo:** Configuração de portas e NAT para ambientes complexos.

12. GERENCIAMENTO DE ENDPOINTS (MANAGEENGINE ENDPOINT CENTRAL)

• **[Nível 1] Instalação de Agentes em Endpoints:** Deploy manual e automático de agentes.
• **[Nível 2] Deploy de Patches e Atualizações:** Configuração de políticas de patching

(Windows/Mac/Linux).

• **[Nível 2] Inventário de Hardware e Software:** Relatórios de ativos e conformidade.

• **[Nível 3] Gestão Remota e Scripts:** Execução de scripts remotos e troubleshooting via console.

13. ADMINISTRAÇÃO DE SERVIDORES (WEBMIN)

• **[Nível 1] Instalação e Acesso Seguro:** Instalação inicial e configuração de HTTPS.

• **[Nível 2] Gestão de Serviços via Interface Web:** Gerenciamento de Apache, MySQL, Postfix, etc.

• **[Nível 2] Agendamento de Tarefas (Cron):** Criação e monitoramento de jobs agendados.

• **[Nível 3] Backup e Restauração de Configurações:** Exportação e importação de configurações do sistema.

14. EDITORES DE TEXTO (NANO / VIM / VI)

• **[Nível 0] Nano - Editor Básico:** Abrir, editar e salvar arquivos. Atalhos essenciais (Ctrl+O, Ctrl+X).

• **[Nível 1] Vim/Vi - Comandos Essenciais:** Modos (Normal, Insert, Command), navegação básica, salvar e sair (`:wq`, `:q!`).

• **[Nível 2] Vim - Produtividade:** Busca e substituição, macros, configuração de `.vimrc`.

15. COMANDOS DE TERMINAL

• **Linux:**

• [Nível 0] Navegação e Arquivos: `ls`, `cd`, `pwd`, `cp`, `mv`, `rm`, `mkdir`, `cat`, `less`.

• [Nível 1] Permissões e Ownership: `chmod`, `chown`, `chgrp`.

• [Nível 1] Processos e Recursos: `ps`, `top`, `htop`, `kill`, `df`, `du`, `free`.

• [Nível 2] Rede e Diagnóstico: `ping`, `traceroute`, `netstat`, `ss`, `curl`, `wget`, `dig`, `nslookup`.

• [Nível 2] Compressão e Arquivos: `tar`, `gzip`, `zip`, `unzip`.

• **Windows (CMD/PowerShell):**

• [Nível 0] Navegação e Arquivos: `dir`, `cd`, `copy`, `move`, `del`, `mkdir`, `type`.

• [Nível 1] Rede e Diagnóstico: `ping`, `tracert`, `ipconfig`, `netstat`, `nslookup`.

• [Nível 2] PowerShell Essencial: `Get-Command`, `Get-Help`, `Get-Process`, `Get-Service`, pipelines.

16. AGENDAMENTO DE TAREFAS (CRON / TASK SCHEDULER)

• **Cron (Linux):**

• [Nível 1] Sintaxe do Crontab: Entendendo os 5 campos (min, hora, dia, mês, semana).

• [Nível 1] Gerenciamento de Jobs: `crontab -e`, `crontab -l`, logs em `/var/log/cron`.

• [Nível 2] Variáveis e Scripts: Definindo PATH, MAILTO, executando scripts complexos.

• **Task Scheduler (Windows):**

• [Nível 1] Criação de Tarefas Básicas: Agendamento via GUI (Agendador de Tarefas).

• [Nível 2] Tarefas Avançadas (schtasks): Criação via linha de comando e triggers complexos.

• **Leitura de Logs Windows (Event Viewer):**

• [Nível 1] Navegação no Visualizador de Eventos: Application, Security, System logs.
• [Nível 2] Filtragem e Busca de Eventos: IDs de evento críticos, exportação de logs.
• [Nível 2] Análise de Falhas de Login e Segurança: Eventos 4625, 4624, 4648.

17. DIAGNÓSTICO DE REDE (FERRAMENTAS)

• **[Nível 1] Ping e Conectividade:** Uso de `ping` para testar alcance de hosts.
• **[Nível 1] Traceroute/Tracert:** Diagnóstico de caminho de pacotes (`traceroute` Linux, `tracert` Windows).
• **[Nível 2] Dig e Nslookup:** Consultas DNS avançadas, verificação de registros A, MX, TXT, PTR.
• **[Nível 2] Netstat/SS:** Verificação de portas abertas e conexões ativas.
• **[Nível 2] Curl/Wget:** Testes de HTTP, headers, download de arquivos.

18. CERTIFICADOS SSL/TLS (CERTBOT / LET'S ENCRYPT)

• **[Nível 1] Instalação do Certbot:** Instalação em Debian/Ubuntu, CentOS/RHEL.
• **[Nível 2] Emissão de Certificados:** Modo standalone, webroot e DNS challenge.
• **[Nível 2] Renovação Automática:** Configuração de cron para `certbot renew`.
• **[Nível 3] Troubleshooting de Expiração:** Diagnóstico de falhas de renovação e rate limits.

19. BACKUP EMPRESARIAL (VEEAM)

• **[Nível 1] Instalação e Configuração Inicial:** Deploy do Veeam Backup & Replication.
• **[Nível 2] Backup de VMs (VMware/Hyper-V):** Criação de jobs de backup e políticas de retenção.
• **[Nível 2] Backup de Endpoints (Veeam Agent):** Proteção de workstations e servidores físicos.
• **[Nível 3] Restauração Granular:** Recuperação de arquivos, itens de Exchange/AD, VMs completas.
• **[Nível 3] Replicação e Disaster Recovery:** Configuração de réplicas e failover plans.

20. COLABORAÇÃO E NUVEM (NEXTCLOUD / OFFICE SERVER)

• **Nextcloud:**
• [Nível 1] Gestão de Usuários e Cotas: Criação de contas e limites de armazenamento.
• [Nível 2] Integração com AD/LDAP: Autenticação centralizada.
• [Nível 2] Tuning de Performance (PHP-FPM/Redis): Otimização para muitos usuários.
• [Nível 3] Hardening e Segurança: 2FA, criptografia server-side, scan de antivírus.
• **Microsoft Office Online Server (2018/2019):**
• [Nível 2] Instalação e Integração com SharePoint/Exchange: Farm configuration.
• [Nível 3] Troubleshooting de Renderização: Análise de logs ULS e eventos do WOPI.

21. ECOSSISTEMA MICROSOFT (EXCHANGE / OFFICE / WINDOWS DESKTOP)

• **Exchange Server 2019:**

• [Nível 1] Gestão de Mailboxes e Grupos: Criação, aliases, permissões (Send As).
• [Nível 2] Configuração de DAG (Database Availability Group): Alta disponibilidade de banco.
• [Nível 3] Fluxo de Correio e Conectores: Troubleshooting de filas, relay e proteção antispam.
• **Microsoft Office (Instalação Local 2024 LTS):**
• [Nível 1] Deploy via ODT (Office Deployment Tool): Criação de XML de configuração.
• [Nível 2] Ativação KMS/MAK: Gestão de licenciamento por volume.
• **Windows Desktop (10 e 11):**
• [Nível 0] Otimização e Limpeza: Desabilitar bloatware, ajustar performance.
• [Nível 1] Troubleshooting de Windows Update: Reset de serviços e catroot2.
• [Nível 2] Sysprep e Captura de Imagem: Criação de imagens padrão para deploy.

22. VIRTUALIZAÇÃO E SEGURANÇA DE E-MAIL (VCENTER / PMG)

• **VMware vCenter:**
• [Nível 2] Gestão de Hosts ESXi e Clusters: Adição de hosts, configuração de HA/DRS.
• [Nível 2] vSwitch e Port Groups: Configuração de redes virtuais e VLANs.
• [Nível 3] Lifecycle Manager (Update Planner): Atualização de hosts e do próprio vCenter.
• **Proxmox Mail Gateway (PMG):**
• [Nível 1] Rastreamento de Logs (Tracking Center): Investigação de e-mails bloqueados.
• [Nível 2] Gestão de Whitelist/Blacklist e Regras: Ajuste de filtros antispam.
• [Nível 3] Configuração de Cluster e Alta Disponibilidade: Sincronização de regras e quarentena.

23. GERENCIAMENTO DE REDE E BI (UNIFI / POWERBI)

• **Unifi Controller:**
• [Nível 1] Adoção de Dispositivos (AP/Switch): Provisionamento básico.
• [Nível 2] Portal Cativo e Voucher: Configuração de rede Guest.
• [Nível 2] Tuning de Rádio (Canais e Potência): Otimização manual de RF.
• **PowerBI Report Server:**
• [Nível 2] Deploy de Relatórios (.pbix): Publicação e gestão de pastas.
• [Nível 2] Configuração de Data Sources e Refresh: Agendamento de atualizações de dados.
• [Nível 3] Backup e Restore de Chaves de Criptografia: Disaster recovery do servidor.

24. DESENVOLVIMENTO REMOTO (VSCODE SERVER)

• **[Nível 1] Instalação e Acesso (Web/Tunnel):** Configuração do serviço code-server ou túnel oficial.
• **[Nível 2] Gestão de Extensões e Ambientes:** Sincronização de perfis e containers dev.

25. SERVICE DESK E ATENDIMENTO (ZAMMAD)

• **[Nível 1] Guia do Agente (SOP):** Fluxo de atendimento, categorização, SLAs e templates de resposta.
• **[Nível 2] Configuração de Canais:** Integração com E-mail (IMAP/SMTP/Microsoft 365), Telegram e

Chat.

• **[Nível 2] Automação (Triggers e Schedulers):** Criação de regras de negócio, escalonamento automático e fechamento de tickets.

• **[Nível 3] Manutenção do Zammad:** Backup/Restore (Postgres/Elasticsearch), reindexação e troubleshooting de trilhos (Rails).

26. HARDWARE E INFRAESTRUTURA (SERVIDORES / UPS)

• **Gerenciamento 'Out-of-Band' (iDRAC / iLO / IPMI):**

• [Nível 1] Acesso Remoto ao Console (KVM): Acesso de emergência ao servidor travado.

• [Nível 2] Atualização de Firmware e BIOS: Manutenção preventiva de hardware.

• [Nível 2] Diagnóstico de Hardware: Leitura de logs de chassis e identificação de falhas de disco/memória.

• **Energia e UPS (APC / Eaton / SMS):**

• [Nível 1] Troca de Baterias e Testes (Self-test): Procedimentos físicos básicos.

• [Nível 2] Configuração de Shutdown Seguro (PowerChute/NUT): Integração USB/Network para desligar servidores em falha de energia.

27. AUTOMAÇÃO E SCRIPTING (POWERSHELL / BASH)

• **PowerShell (Windows):**

• [Nível 2] Biblioteca de Scripts de Manutenção: Scripts para limpeza de disco, reinício de serviços travados.

• [Nível 2] Automação de Onboarding (AD): Script para criação de usuários, grupos e pastas home.

• [Nível 3] Criação de Módulos Personalizados: Empacotando funções da iT Guys.

• **Bash / Shell (Linux):**

• [Nível 2] Scripts de Backup Customizados: Rotinas de tar/rsync para locais específicos.

• [Nível 3] Automação de Instalação (Setup Scripts): Bootstrapping de novos servidores (instalar Docker, Zabbix Agent, Users de uma vez).

28. PROCESSOS E PROCEDIMENTOS OPERACIONAIS (SOPS)

• **Gestão de Incidentes (Crise):**

• [Nível 3] Protocolo de Incidente Cibernético (Ransomware): Isolamento, preservação de evidências e comunicação.

• **Rotinas Operacionais (NOC):**

• [Nível 1] Checklist Diário de Saúde (Morning Checks): Verificação de backups críticos (Veeam), links e alertas do Zabbix.

• [Nível 2] Procedimento de Janela de Manutenção: Como planejar, executar e validar mudanças (Change Management simplificado).

• **Gestão de Pessoas (Interno):**

• [Nível 1] Onboarding Técnico: Checklist de preparação de estação e acessos para novos técnicos da equipe.