Manual Operacional de TI & Cyber Segurança

AMÓS Sentinel Health (SRE 24/7) • AMÓS Sentinel Shield (WAF SOC)

ESTRITAMENTE CONFIDENCIAL • TI

QUADRO OFICIAL DE ACESSOS & CHAVES MESTRAS DE TI

SISTEMA / MÓDULO	ENDEREÇO WEB (URL)	USUÁRIO OFICIAL	CHAVE MESTRA
AMÓS Sentinel Health Vigia SRE & Auto-Cura 24/7	`https://sentinel.gomib.com.br` Alias: https://ti.gomib.com.br	`ti@gomib.com.br`	`Sentinel#GOMIB2026!OpsKey$99`
AMÓS Sentinel Shield Cyber Defesa & WAF SOC	`https://shield.gomib.com.br` Porta Interna: 3900	`shield@gomib.com.br`	`Shield#GOMIB2026!WafVault$88`

1. ISOLAMENTO TECNOLÓGICO & DIRETRIZES DE ACESSO

Por diretriz estatutária de segurança da informação, ambos os módulos operam de forma **100% isolada** da aplicação maçônica do AMÓS. Não existem menus, botões ou rotas visíveis no painel do obreiro, das lojas ou do Grão-Mestrado que façam referência ao Sentinel ou ao Shield.

> **Regra de Acesso:** Uso privativo do Administrador de Sistemas e dos Oficiais de Tecnologia da Potência. As credenciais nunca devem ser transmitidas por canais desprotegidos. O Sentinel monitora os logs e armazena trilhas forenses de auditoria.

2. AMÓS SENTINEL HEALTH (SRE & AUTO-CURA 24/7)

O **Sentinel Health** é o robô mantenedor contínuo da infraestrutura. Ele atua como um serviço nativo do sistema operacional Linux (`amos-sentinel.service`), executando fora dos containers Docker para garantir que, caso o Docker ou a aplicação entrem em colapso, o Sentinel permaneça vivo para recuperá-los.

2.1. Sondas Ativas a Cada 30 Segundos

- **Sonda de Latência da API:** Realiza requisição HTTP interna e externa, medindo o tempo de resposta milissegundo a milissegundo e garantindo que o backend atenda requisições com `HTTP 200/401`.
- **Sonda de Container Docker:** Inspeciona o estado de `gomib_amos_core`, detectando paralisações instantaneamente.
- **Sonda do SQLite & Buffer WAL:** Avalia o tamanho de `amos.db-wal` para impedir que transações fiquem represadas em memória.
- **Sonda de Recursos do Host:** Monitora o uso de memória RAM, CPU e espaço livre em disco da VPS.
- **Sonda de Certificados SSL:** Monitora a expiração dos certificados Let's Encrypt e dispara renovação preventiva.

2.2. Playbooks de Auto-Cura (Self-Healing Automático Homologado)

• Queda da API ou Container
Reinicia `gomib_amos_core` automaticamente em 5.4 segundos, retesta com HTTP 200 e registra em banco como `RESOLVED_AUTO`.

• Inchaço de Buffer WAL
Se o WAL ultrapassar 35 MB, força `wal_checkpoint(TRUNCATE)` forçado, consolidando os dados em `amos.db`.

• Pressão de Disco (> 88%)
Executa expurgo automático de caches de compilação Docker e logs residuais temporários, liberando gigabytes de espaço.

• Auto-SSL no Apontamento DNS
Detecta a propagação do domínio para o IP 187.77.60.16 e emite o certificado SSL HTTPS via Certbot de forma autônoma.

2.3. Painel de Intervenções Preventivas (Override de TI)

O operador de TI dispõe de quatro botões de ação imediata na interface web do Sentinel Health:

- **Forçar Checkpoint WAL:** Descarrega e trunca imediatamente o buffer de transações no SQLite.
- **Checagem de Integridade:** Roda `PRAGMA integrity_check` para certificar que não há blocos corrompidos no banco.
- **Reiniciar Container Suave:** Reinicia o processo Node.js sem derrubar o servidor web Nginx.
- **Limpeza de Disco / Cache:** Remove resíduos e libera gigabytes de espaço no disco da VPS.

3. AMÓS SENTINEL SHIELD (WAF & CYBER SOC)

O **Sentinel Shield** é o Centro de Operações de Segurança Cibernética (SOC), operando na porta interna `3900` sob o serviço nativo `amos-shield.service`. Ele atua como muralha de defesa ativa em tempo real contra ataques e invasões na Internet.

3.1. As 7 Camadas de Blindagem do WAF (Grau A+ Militar)

- **Anti-SQL Injection (SQLi):** Intercepta caracteres de escape e comandos SQL perigosos (ex: `UNION SELECT`, `' OR 1=1--`).
- **Anti-Cross Site Scripting (XSS):** Neutraliza tags `<script>` e tentativas de sequestro de sessão no navegador.
- **Anti-Path Traversal:** Bloqueia tentativas de leitura de diretórios restritos do sistema operacional (ex: `../../etc/passwd`).
- **Anti-Remote Code Execution (RCE):** Impede injeção de comandos de terminal (`|`, `;`, `&&`).
- **Bloqueio de Scanners Maliciosos:** Barreia ferramentas conhecidas de invasores (`sqlmap`, `nikto`, `acunetix`, `burpsuite`).
- **Honeypot de Sondas Sensíveis:** Detecta robôs vasculhando por `.env`, `.git` ou `wp-config.php` e bane o IP na hora.
- **Auto-Ban de IPs Reincidentes:** Atacantes com duas ou mais violações graves são banidos automaticamente por 48 a 72 horas.

3.2. Análise Forense & Gestão de Blacklist de IPs

Na interface web do Shield, o analista visualiza cada intrusão com a amostra exata do código malicioso que o atacante tentou enviar. Caso um obreiro legítimo seja bloqueado por falso-positivo, basta acessar a tabela de **Blacklist de IPs** e clicar em **Desbanir**. O desbloqueio tem efeito imediato na rede.

4. COMANDOS DE LINHA DE COMANDO (SSH TERMINAL)

OBJETIVO / AÇÃO OPERACIONAL	COMANDO NO TERMINAL LINUX
Ver status do Sentinel Health	`systemctl status amos-sentinel.service`
Ver status do Sentinel Shield	`systemctl status amos-shield.service`
Acompanhar logs ao vivo do Sentinel	`journalctl -u amos-sentinel.service -f`
Acompanhar logs ao vivo do Shield	`journalctl -u amos-shield.service -f`
Reiniciar ambos os serviços de supervisão	`systemctl restart amos-sentinel amos-shield`
Checar integridade do SQLite diretamente	`docker exec gomib_amos_core node -e "console.log(require('./db/database').getDB().pragma('integrity_check'));"`