GUIA ↗

CG//One

COMO AVALIAR

UM MSSP E ESCOLHER O FORNECEDOR IDEAL

O que avaliar — e o que evitar — ao contratar um provedor de serviços de segurança gerenciada.

ÍNDICE

INTRODUÇÃO

Assim como ocorre em outras áreas de TI, quando falamos de cibersegurança as organizações precisam escolher: **manter toda a operação internamente** (eventualmente complementada por ferramentas pontuais) ou **ter um parceiro especializado que gerencie parte ou toda a segurança**, como um MSSP (Managed Security Service Provider).

Com o aumento do volume e sofisticação dos ataques, a adoção de MSSPs cresce ano após ano. A complexidade técnica, a velocidade das ameaças e a necessidade de monitoramento contínuo tornam cada vez mais difícil para equipes internas assumirem tudo sozinhas.

Ao mesmo tempo, evitar incidentes que resultem em indisponibilidade, vazamento de dados ou multas regulatórias se tornou uma prioridade equivalente à própria continuidade operacional.

Este guia foi criado para ajudar você a:

- **Entender** quando um MSSP faz sentido;
- **Avaliar** os benefícios reais;
- **Saber** o que analisar em potenciais fornecedores;
- E **estruturar** uma migração segura caso decida avançar.

01

POR QUE USAR UM **MANAGED SECURITY SERVICE PROVIDER?**

Analistas de mercado concordam: um MSSP eficaz combina **tecnologia, especialistas qualificados e processos sólidos** para manter o ambiente seguro de forma contínua, sem atrapalhar a operação.

Cibersegurança não é um fim em si — ela sustenta processos de negócio. Isso exige prevenção, monitoramento constante, detecção inteligente, atualização contínua e **resposta rápida** quando necessário.

A maior parte das empresas procura um MSSP pelos mesmos motivos:

- **Falta de profissionais qualificados internamente;**
- **Complexidade crescente das tecnologias de segurança;**
- **Ameaças evoluindo rapidamente — exigindo proteção 24×7;**
- **Restrições de orçamento ou headcount;**
- **Preferência estratégica por terceirização especializada.**

No centro de tudo está o principal fator:

a organização não consegue mais acompanhar, sozinha, o ritmo das ameaças e vulnerabilidades.

Depois que uma solução é implementada, ela precisa ser **ajustada e atualizada imediatamente**. Hackers operam de forma automatizada e contínua — a defesa também precisa operar assim.

O que um MSSP oferece na prática

- Monitoramento e resposta 24×7;
- Especialistas certificados sempre disponíveis;
- Padronização de processos e boas práticas;
- Atualização contínua das defesas;
- Redução de riscos operacionais;
- Conformidade com normas e regulações;
- Previsibilidade de custo;
- Liberação da equipe interna para atividades estratégicas;
- Integração de soluções de múltiplos fabricantes;
- Eliminação da necessidade de um SOC próprio.

02

DESCOBRINDO O **SEU NÍVEL ATUAL DE MATURIDADE**

Antes de contratar um MSSP, é essencial saber **onde você está e para onde quer ir**.

Perguntas iniciais:

1. Por que precisamos de um MSSP?

Clarifique o objetivo:

- É redução de riscos?
- Aumento de cobertura? Economia?
- Conformidade?

2. Como estamos hoje?

Você diria que sua operação de segurança está:

- **No limite,** rezando para nada grave acontecer?
- **Cuidando do básico,** mas sobrecarregada e sem fôlego?
- **Operacional,** mas com gaps evidentes a melhorar?
- **Bem estruturada,** com tudo sob controle?

3. O que será terceirizado? Tudo ou partes?

Identifique:

- Gestão de dispositivos de segurança
- Monitoramento e deteção de ameaças
- Resposta e contenção
- Backup e continuidade
- Gestão de riscos e vulnerabilidades
- Testes especializados (ex.: pentest)

4. Qual é a postura da empresa sobre outsourcing?

Pergunte-se:

- Trabalhamos bem com terceiros?
- Estamos confortáveis em delegar algo crítico como segurança?
- A liderança compreende riscos e benefícios?

5. Como será o modelo de atuação do MSSP?

- Totalmente remoto
- Remoto + visitas presenciais
- Suporte sob demanda
- Ou **full managed**, com operação ponta a ponta

03

COMO SELECIONAR E AVALIAR **UM MSSP**

A escolha do provedor certo exige analisar além do marketing e dos discursos padronizados. Aqui estão os pontos-chave.

Preço

Você recebe aquilo pelo que paga. Não escolha o mais barato, escolha **o que entrega valor e consistência**.

Aderência ao seu negócio

O MSSP precisa entender seus:

- Objetivos estratégicos;
- Setor;
- Regulatórios;
- Prioridades reais.

Procure sinais de alinhamento, não só conhecimento técnico.

Adaptação ao ambiente existente

O ideal não é “rip and replace”. Bons MSSPs:

- Aproveitam o que você já tem;
- Estendem até o fim de vida útil;
- Só substituem quando necessário.

Credenciais e provas sociais

Avalie:

- Cases;
- Depoimentos;
- Clientes antigos e atuais;
- Certificações técnicas e de fabricante;
- Prêmios e reconhecimentos.

SLAs

Essenciais para:

- Definir níveis mínimos de serviço;
- Garantir transparência;
- Alinhar expectativas.

Transparência

Exija:

- Linguagem clara;
- Processos documentados;
- Visão de como dados serão tratados;
- Acesso contínuo a métricas e relatórios.

Entendimento do que está incluso

Tudo deve estar no contrato. Se não estiver documentado, **não conte que será entregue**.

Sistemas, ferramentas e processos

Avalie:

- Quais plataformas são usadas?
- Existe governança de incidentes?
- Há rotinas de atualização contínua?
- Como e onde os dados são armazenados?

Resposta a incidentes

Avalie:

- Como agem em caso de brecha?
- Eles já passaram por incidentes reais?
- Quanto tempo levaram para conter e restaurar?

Parcerias de tecnologia

A qualidade das parcerias com fabricantes é reflexo direto da qualidade do serviço entregue.

Escalabilidade e flexibilidade

As necessidades podem aumentar ou diminuir, e o serviço deve acompanhar.

Valor adicional

Um MSSP sólido entrega **mais que dados**:

- Insights;
- Recomendações;
- Relatórios executivos;
- Consultoria de melhoria contínua.

Estabilidade financeira

Avalie se o provedor tem solidez para sustentação de longo prazo.

04

MIGRANDO PARA **SEU NOVO MSSP, O QUE ESPERAR?**

A migração deve ser gradual, não brusca.

Por quê?

Porque envolve:

- Alto risco operacional;
- Complexidade técnica;
- Convivência entre processos internos e do MSSP;
- Adaptação de práticas.

Durante o início:

- Operações podem rodar em modo dual;
- Processos serão ajustados;
- Políticas serão revisadas;
- Métricas serão redefinidas.

Um bom MSSP **não impõe** um modelo rígido. Ele adapta o serviço ao seu ambiente, não o contrário.

E mantenha sempre um **plano de contingência** para retomar o controle caso necessário.

ESCOLHER UM MSSP É UMA DAS DECISÕES **MAIS CRÍTICAS EM CIBERSEGURANÇA.**

Se você chegar a uma shortlist final, avalie seus candidatos principalmente por:

- Expertise e capacidades;
- Flexibilidade;
- Preço justo com a entrega proposta;
- Histórico e reputação;
- Aderência ao seu negócio.

Você sentirá, durante o processo, quando encontrou o parceiro certo.

CG // One

CONHEÇA O **MSS DA CG ONE**

Combinamos **expertise certificada, operação 24/7 e acesso a todo o leque de soluções e serviços**, permitindo que nossos clientes:

- **Tenham previsibilidade de custos**, sem surpresas e ajustado ao tamanho da empresa.
- **Tenham acesso imediato a especialistas e tecnologias de ponta**, sempre atualizadas.
- **Foquem no core do negócio**, enquanto a operação de segurança fica nas mãos de quem vive isso todos os dias.
- **Reduzam riscos financeiros e reputacionais**, contando com uma estrutura preparada para respostas rápidas.
- **Contem com proteção ponta a ponta**, garantindo continuidade de negócio e resiliência a ataques.

Tudo isso estruturado em serviços que se complementam para entregar **segurança contínua, inteligente e proativa**:

- **Security Monitoring & Threat Detection —** monitoramento contínuo e correlação de eventos.
- **Managed Detection & Response (MDR) —** investigação, contenção e erradicação de incidentes com automação e playbooks customizados.
- **Technical Security Services (TSS) —** administração completa de dispositivos e soluções de segurança.
- **Network Operations Center (NOC) —** monitoramento da performance e disponibilidade da infraestrutura.
- **HaaS – Hardware as a Service —** fornecimento e gestão de equipamentos sob modelo OPEX.
- **Cyber Threat Intelligence & Take Down —** inteligência de ameaças com ação ativa contra campanhas e domínios maliciosos.
- **Vulnerability Management —** identificação, priorização e remediação de vulnerabilidades.
- **Cyber Risk Management —** gestão de riscos corporativos com visão de negócio e governança contínua.

ENTRE E CONTATO E **SOLICITE UMA PROPOSTA**

CG // One

SOBRE A **CG ONE**

Somos a CG One, a evolução da marca Compugraf. Com mais de 40 anos de expertise no mercado de tecnologia, somos especialistas em cibersegurança para proteger integralmente o ecossistema digital das empresas.

Desenvolvemos e gerenciamos soluções estratégicas em Infrastructure Security, Identity & User Security, AppSec & DevOps e Managed Security Services (MSS).

Nosso portfólio é orientado pelas práticas e padrões do NIST® Cybersecurity Framework. Contamos com um time altamente qualificado e certificado que já proporcionou operações seguras para mais de 500 empresas de diversos portes e setores em todo o Brasil.