Aluno: Alexandre Magno Mattos do Espírito Santo
RGM: 4504 1393
Disciplina: Designer Profissional
Curso: CST Análise e Desenvolvimento de Sistemas
Semestre / Ano: 2º semestre de 2025
Título do Trabalho: Análise de Vagas de TI – Segurança da Informação

Relatório — Análise de vagas: Segurança da Informação

Pesquisa: 5–10 vagas reais em plataformas como Glassdoor, Programathor, Indeed e Vagas — resumo e fontes no final

1) Amostra de vagas pesquisadas (títulos + fonte)

1. Analista de Segurança da Informação — vaga genérica (remote / híbrido). Fonte: Glassdoor (resultados agregados). Glassdoor
2. Analista de Segurança da Informação (Back-End / políticas e monitoramento) — Programathor. ProgramaThor
3. Offensive Security Analyst / Pentester (Pleno) — Glassdoor (ex.: Agibank / empresas de fintechs). Glassdoor
4. Analista de Cibersegurança / SOC (Monitoramento, SIEM) — Glassdoor / Indeed. GlassdoorIndeed
5. Analista/AppSec (Foco em segurança de aplicações) — Contabilizei / Glassdoor (vagas AppSec). Glassdoor
6. Vagas técnicas em Security (firewalls, CFTV, acesso físico) — Vagas.com.br / Indeed (ex.: programador/security, segurança patrimonial ligada a sistemas). VagasIndeed

Observação rápida: as vagas aparecem em formatos remoto/híbrido e por todo o Brasil (SP, Campinas, regiões remotas), e os requisitos variam entre Júnior → Pleno → Sênior conforme a função. Fontes agrupadas acima. Glassdoor ProgramaThor

---

2) Hard skills — obrigatórias vs desejáveis (síntese das vagas)

Obrigatórias (com maior frequência nas vagas):

- **Conceitos de redes e TCP/IP (VLAN, NAT, roteamento).** Glassdoor
- **Sistemas operacionais (Linux e Windows) — administração básica.** Glassdoor
- **Conhecimento em SIEM / monitoramento (ex.: Splunk, Elastic, ferramentas SOC).** GlassdoorIndeed
- **Firewall / IDS/IPS / VPN / Gestão de logs.** Glassdoor

Desejáveis (frequentes, mas nem sempre obrigatórias):

- **Scripting e automação (Python, Bash).** ProgramaThor
- **Cloud (AWS / Azure) e segurança em nuvem — CSPM, hardening de workloads.** Check Point SoftwareFortinet
- **Pentest / AppSec / OWASP / metodologias (MITRE ATT&CK).** Glassdoor+1
- **Frameworks e normas (ISO 27001, NIST, políticas de GRC).** Glassdoor

Resumo: Júnior normalmente exige redes, SO e disposição para aprender ferramentas (SIEM) — Pleno/Sênior exige cloud, pentest, arquitetura segura e certificações/experiência. GlassdoorGlassdoor

---

3) Soft skills — as mais pedidas

- **Comunicação clara (documentação / reports / interação com áreas não técnicas).** Glassdooriioiotith yhu¬y™
- **Trabalho em equipe / colaboração com desenvolvimento e infraestrutura (DevOps/DevSecOps).** Glassdoor
- **Capacidade analítica e resolução de problemas (investigação de incidentes).** Glassdoor
- **Organização e atenção a processos (conformidade / auditoria).** Glassdoor

---

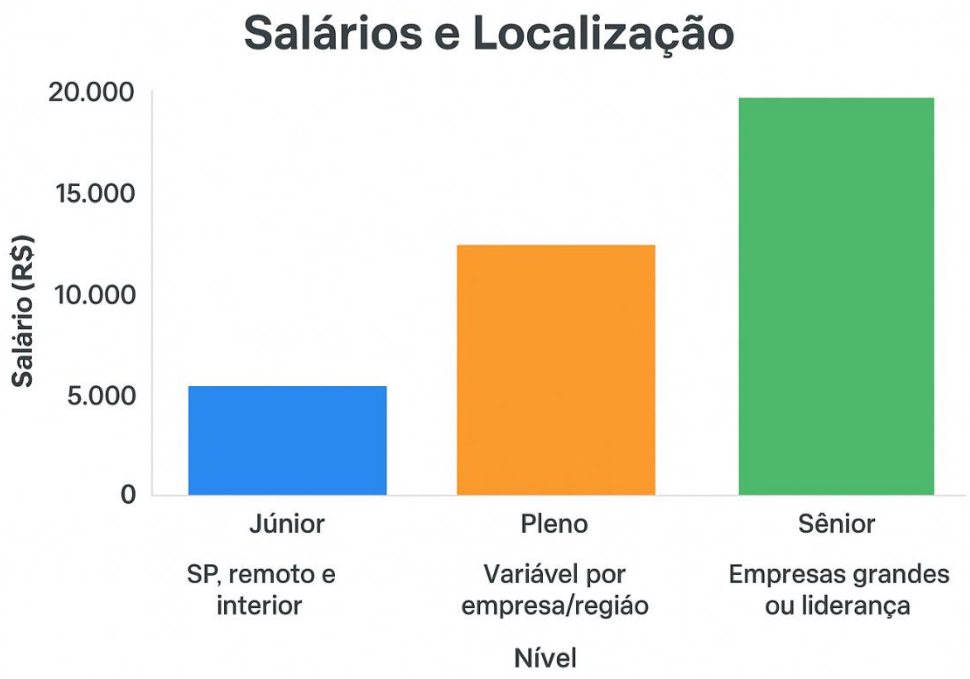
4) Salário e localização (faixas encontradas)

Fontes agregadas (Glassdoor / Salario.com.br / Indeed / Robert Half / portais de vagas). As faixas variam muito por local/empresa:

- **Analista de Segurança da Informação — Júnior:** média ~R$ 3.000 — R$ 5.500 / mês (valores reportados por Glassdoor / Indeed). GlassdoorIndeed
- **Analista — Pleno:** média ~R$ 5.500 — R$ 11.000 / mês (Glassdoor / Salario sites mostram médias por nível). GlassdoorPortal Salario
- **Sênior / Especialista / PenTester:** pode variar de ~R$ 11.000 até R$ 20.000+ em cargos de liderança ou empresas grandes (relatos e agências de recrutamento). Robert HalfPortal Salario

Tabela resumida (exemplo):

Nível	Faixa típica (BR)
Júnior	R$ 3.000 — R$ 5.500 / mês. GlassdoorIndeed
Pleno	R$ 5.500 — R$ 11.000 / mês. GlassdoorTrainning
Sênior	R$ 11.000 — R$ 20.000+ / mês (depende empresa). Robert HalfPortal Salario



Nota: em cidades como São Paulo os salários tendem a ser mais altos; vagas remotas também aparecem com faixas diversas. Use esses valores como referência — as plataformas mostram variação por empresa/região. IndeedGlassdoor

---

5) Tendências atuais do mercado (tecnologias em alta) — pontos chave

1. **Cloud security e proteção de workloads/IA na nuvem** — Cloud Security e proteção de cargas de IA estão entre as prioridades em 2025 (CSPM, postura de segurança, hardening). Check Point SoftwareTenable®

2. **AI/ML aplicada a detecção de ameaças e automação (Defender/EDR/SIEM com IA).** Check Point SoftwareSentinelOne

3. **DevSecOps / shift-left e segurança em pipelines CI/CD (AppSec).** CheckmarxGlassdoor

4. **Zero Trust e gestão de identidade/controle de acessos (IAM).** SentinelOneThales Group

Em resumo: nuvem + automação (AI) + integração de segurança no ciclo de desenvolvimento (DevSecOps/AppSec) são as tendências mais fortes que continuam dominando as descrições de vagas e investimentos do mercado. Orca SecurityGoogle Cloud

---

6) Plano de Ação — 6 meses (escolha de 3 habilidades para desenvolver)

2 técnicas + 1 comportamental — objetivo: conseguir entrar em vaga Júnior/estágio e ganhar experiência prática.

Habilidades escolhidas

- **Técnica 1 — Fundamentos de Redes + Linux (base sólida)**
  Por que: requisitado em praticamente todas as vagas Júnior; permite operar ferramentas e interpretar logs.
  O que estudar (6 meses): 8 semanas de redes (TCP/IP, VLAN, NAT, modelos OSI), 8 semanas Linux (comandos, permissões, logs), laboratórios práticos (máquinas virtuais).
  Recursos sugeridos: cursos gratuitos e mãos na massa (ex.: Linux Essentials / cursos no YouTube / docs).

- **Técnica 2 — SIEM / SOC basics + introdução a Cloud (AWS/Azure) e scripting leve (Python básico)**
  Por que: SIEM/SOC aparece em muitas vagas; cloud é tendência e aumenta empregabilidade. Python ajuda automação de tarefas.
  O que estudar (6 meses em paralelo): 6–8 semanas SIEM (conceito, busca em logs, alertas), 6–8 semanas AWS/Azure fundamentals (IAM, EC2, S3), 4–6 semanas de Python scripting orientado a automação de segurança (parsing logs, requests).
  Recursos sugeridos: TryHackMe (rotas SOC), cursos introdutórios da AWS/Azure, labs gratuitos.

- **Comportamental — Comunicação técnica e relato de incidentes**
  Por que: habilidade diferencial — produzir reports, explicar problemas para não técnicos, trabalhar em equipe.
  Como praticar: fazer exercícios de writing (resumos de exercícios de pentest/incident), simular apresentações curtas (5–10 min) explicando um incidente ou um relatório técnico.

Cronograma prático (resumido para 6 meses)

- Meses 1–2: Redes + Linux (prática 5 dias/semana — 1h a 2h/dia)
- Meses 3–4: SIEM/SOC + Python básico (labs no TryHackMe / Splunk free / ELK)
- Meses 5–6: Cloud fundamentals (AWS/Azure) + projetos pequenos (simular monitoramento e relatório; criar um mini-portfolio)
- Ao longo de todo o período: 1 prática por semana de comunicação (escrever relatório curto; gravar áudio explicando) e montar perfil/README no GitHub com projetos.

---

7) Fontes principais utilizadas (exemplos — consulte cada seção para referência específica)

- Agregador de vagas e descrições (Glassdoor — páginas de vagas e salários). Glassdoor+1
- Programathor — vaga exemplo e descrição operacional. ProgramaThor
- Relatórios e tendências (Check Point Cloud Security Trends 2025; Tenable — riscos da IA na nuvem; Orca / Thales / Datadog estudos 2025). Check Point SoftwareTenable®Orca Security
- Sites de mercado e salários (Salario.com.br, Indeed, Robert Half). Portal SalarioIndeedRobert Half