ANALISTA DE PRIVACIDADE

Uma análise e extração de Dados em uma busca por Vagas de Emprego

Flamarion Silva dos Anjos

SET/2025

Definição de Analista de Privacidade

Um analista de privacidade é um profissional responsável por assegurar a **conformidade** de uma organização com as **leis de proteção de dados** e por proteger a **privacidade dos indivíduos** cujos dados a organização coleta, armazena e processa. Suas funções incluem **avaliar** riscos, **elaborar** e **implementar políticas** de privacidade, realizar **auditorias**, **educar funcionários** e **garantir** que o uso de informações pessoais esteja em **conformidade com regulamentos como o GDPR ou a LGPD.**

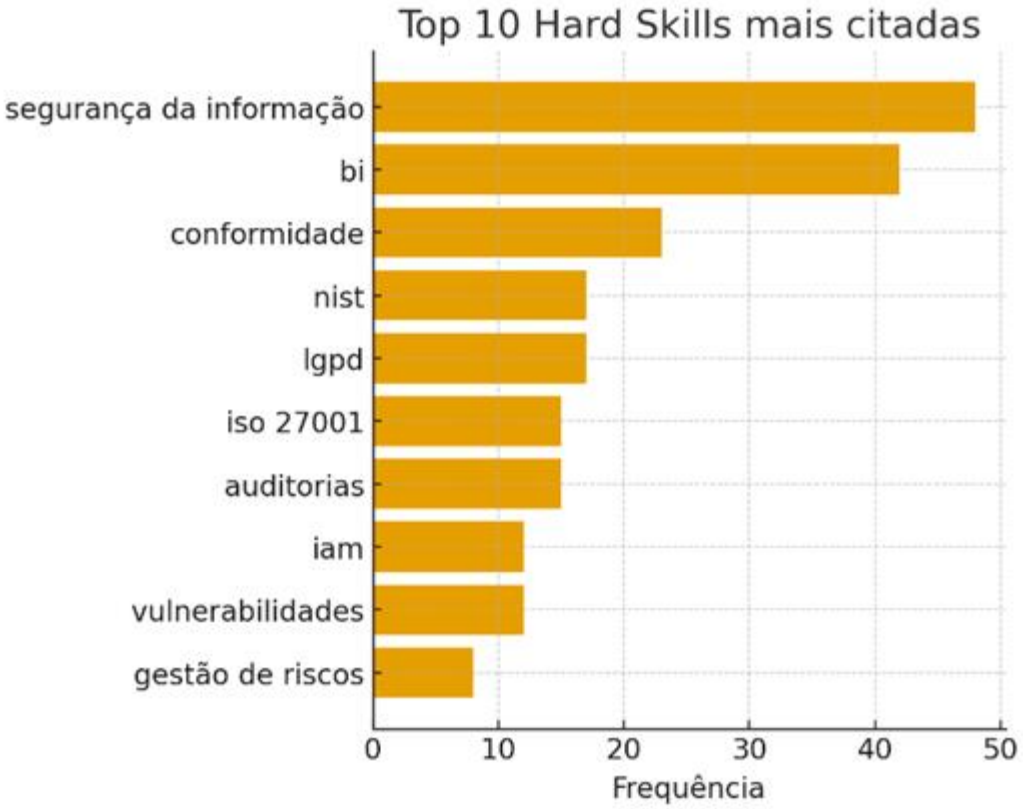
METODOLOGIA

Foi realizada uma busca por 10 (dez) vagas de emprego que se encaixem no perfil de Analista de Privacidade, na cidade de São Paulo -SP, com regimes de trabalho que vão do Presencial, passando pelo hibrido até o Remoto. E analisados requisitos necessários solicitados pelos empregadores para o preenchimento das mesmas. As vagas analisadas foram:

- Analista de Segurança da Informação II (trabalho remoto);
- Analista de Segurança da informação (Blue Team);
- Analista Sênior de Privacidade;
- Analista Pleno de Governança de Segurança da Informação;
- Analista de Segurança da Informação III – Privacidade de Dados;
- Analista de Segurança da Informação (Cibersegurança);
- Analista de Segurança da Informação JR;
- Analista de Segurança da Informação - ISO 27001 e Assessments;
- Analista de Segurança da Informação;
- Analista de Privacidade e Proteção de Dados;

ANALISE DE COMPETÊNCIAS

Hard Skills

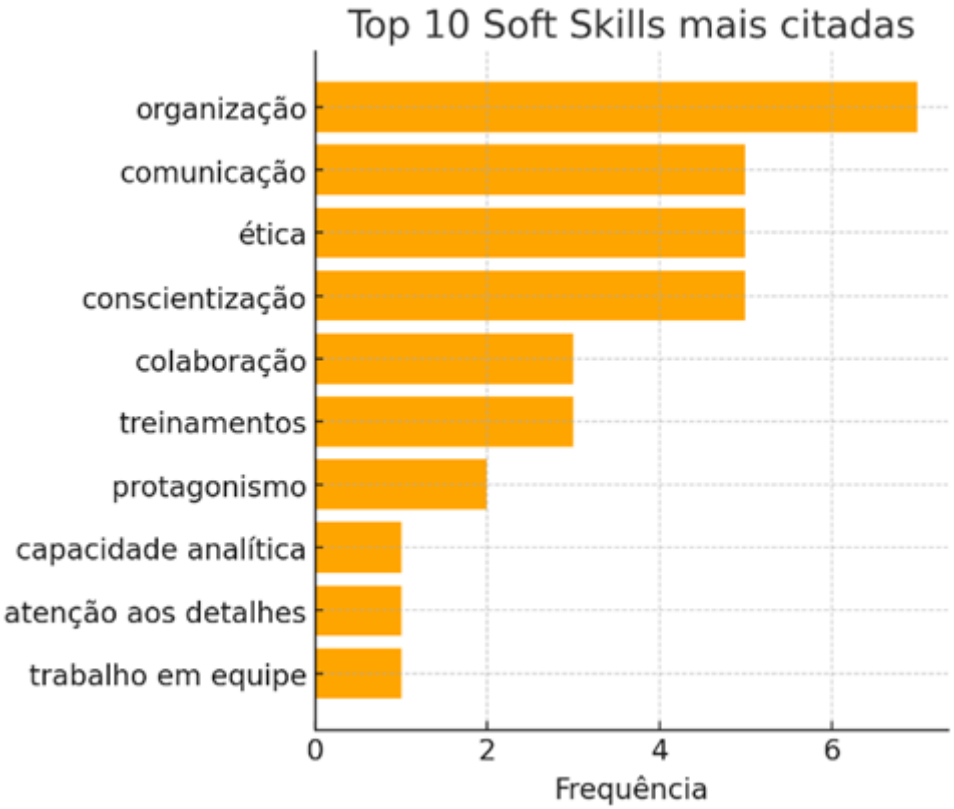


Foram citadas como **Hard Skills obrigatórias**, ou seja, que aparecem ligadas diretamente como *requisito ou pré-requisito*: **Segurança da Informação** (conceitos, práticas, frameworks); **Redes e Protocolos** (TCP/IP, VLANs, VPN, roteamento, firewalls, proxies) **Ferramentas de Segurança** (SIEM, EDR, antivírus, IDS/IPS, DLP, WAF, IAM, PAM); **Cloud Security** (AWS, Azure, GCP, Microsoft 365); **Normas e Frameworks** (ISO 27001 / ISO 27002 , NIST, CIS Controls, COBIT); **Governança e Compliance** (LGPD, GDPR ,PCI, DSS); **Gestão de riscos e vulnerabilidades**; **Auditorias e conformidade** (internas/externas); **Ferramentas de privacidade** (OneTrust ou similares); **Pacote Office avançado** (Excel, PowerPoint, relatórios e dashboards); **Administração de sistemas** (Linux básico, Windows Server/AD).

Como **Hard Skills desejáveis**, ou seja, consideradas como *diferenciais para vaga:* **Programação/Scripts para automação** (Python, PowerShell, Bash, Node.js, Shell Script); **Inglês avançado/técnico**; **Certificações** (CompTIA Security+, Network+, CISSP, OSCP, CEH, DPO, EXIN, ISACA, CIPP/E, CIPM); **Segurança de aplicações web** (OWASP, hardening, análise de vulnerabilidades); **Ferramentas de BI / análise de dados** (SQL, Power BI); **RPA e automação de processos**; **Privacidade aplicada à IA** (gestão de riscos e

conformidade em inteligência artificial – diferencial em uma vaga sênior); **Experiência em setores regulados** (financeiro, saúde, aeronáutico etc.)

Soft Skills



Organização e gestão de tempo dominam as Soft Skills, mas não são as únicas presentes, também aparecem: **Comunicação clara e objetiva** (escrita e verbal, para relatórios, reuniões e apresentações); **Capacidade analítica e atenção aos detalhes**; **Trabalho em equipe e colaboração multidisciplinar**; **Proatividade e protagonismo**; **Ética, sigilo e confidencialidade**; **Perfil investigativo / resolução de problemas**; **Capacidade de aprender continuamente**; **Habilidade de conduzir treinamentos e conscientização.**

ANÁLISE SALARIAL:

Com base nas vagas e em pesquisas no Glassdoor e outros sites para " Analista de Privacidade " em São Paulo, a faixa salarial identificada é a seguinte:

CARGO	*NIVEL*	*MÉDIA SALARIAL*	*SALÁRIO MININO (ESTIMADO)*	*SALÁRIO MAXIMO (ESTIMADO)*	*FONTE*
Analista de Segurança da Informação (G	GERAL	R$ 9.067,52	R$ 7.762,00	R$ 18.082,33	www.salario.com.br
Analista de Segurança da Informação	JUNIOR	R$ 4.048	R$ 3.133	R$ 5.646	www.glassdoor.com.br
Analista de Segurança da Informação	PLENO	R$ 6.983	R$ 5.000	R$ 9.000	www.glassdoor.com.br
Analista de Segurança da Informação	SÊNIOR	R$ 11.625	R$ 8.833	R$ 14.729	www.glassdoor.com.br
Analista de Privacidade e Proteção de Dados	GERAL	R$ 8.164,85	R$ 6.000	R$ 10.000	www.salario.com.br
Analista de Segurança da Informação - ISO 27001 e assessments	GERAL	R$ 9.000	R$ 7.500	R$ 10.500	www.glassdoor.com.br
Analista de Segurança da Informação Cibersegurança	GERAL	R$ 8.400	R$ 6.100	R$ 10.250	www.roberthalf.com
Analista de Governança de Segurança da Informação	GERAL	R$ 7.500	R$ 6.000	R$ 9.000	www.glassdoor.com.br
Analista de Privacidade e Proteção de Dados	JUNIOR	R$ 5.000	R$ 4.000	R$ 6.000	www.glassdoor.com.br

ANÁLISE DE TENDENCIAS

Foi percebido durante as análises realizadas que as empresas ainda priorizam fundamentos clássicos como ISO27001, NIST, auditorias, LGPD/GDPR. Mas há sinais de mudanças no horizonte com adoção do **OneTrust** (ferramenta de gestão de privacidade e conformidade); **Automação com scripts** (Python, PowerShell, Bash, Node.js); **RPA (Robotic Process Automation)** utilizado na automação de processos de segurança e auditorias;

Cabe destacar que embora ainda pouco exigida, mas claramente presente em um campo em expansão a **Privacidade e conformidade em Inteligência Artificia**l.

Nota se ainda que quem dominar **Cloud Security +Automação + Privacidade/IA** terá vantagem competitiva na disputa por essas vagas.

PLANO DE AÇÃO

Tomando como ponto de partida o que foi analisado até agora foi selecionado 3 (três) competências consideradas estratégicas na busca da vaga. Duas Hard Skills e uma Soft Skill e a partir delas traçado um plano de ação de seis meses para desenvolver as competências escolhidas:

Mês 1 – Fundamentos e diagnóstico

- LGPD + ISO 27001:
  - Ler a Lei 13.709/2018 (LGPD) com foco nos direitos dos titulares e obrigações das empresas.
  - Curso introdutório em ISO 27001 Foundation (Udemy, Coursera ou EXIN).
  - Produzir um resumo pessoal (mindmap ou checklist) de requisitos.
- Cloud Security:
  - Criar conta gratuita na AWS e Azure.
  - Estudar fundamentos de identidade e acesso (IAM, RBAC, MFA).
- Automação:
  - Revisar lógica básica de programação em Python ou PowerShell.
- Comunicação:
  - Iniciar leitura do livro *"Comunicação não violenta" (Marshall Rosenberg)* ou similar.
  - Gravar áudio curto (2-3 min) explicando um conceito técnico de forma simples.

Mês 2 – Consolidação técnica inicial

- LGPD + ISO 27001:
  - Estudar controles de segurança da ISO 27001 (domínios: riscos, acessos, continuidade).
  - Simular a criação de uma Política de Segurança da Informação para uma empresa fictícia.
- Cloud Security:
  - Curso oficial AWS Cloud Practitioner Essentials (grátis na AWS Training).
  - Configurar usuários e permissões na AWS com boas práticas de segurança.
- Automação:
  - Desenvolver scripts simples: automatizar backups de arquivos e relatórios de logs.
- Comunicação:
  - Escrever um artigo curto no LinkedIn explicando um tema de segurança (ex: “O que é a ISO 27001 e por que importa para empresas brasileiras”).

Mês 3 – Aplicação prática

- LGPD + ISO 27001:
  - Estudo dirigido em gestão de riscos e vulnerabilidades (ISO 27005 / NIST).
  - Realizar um mini-DPIA (Data Protection Impact Assessment) com base em um caso fictício.
- Cloud Security:
  - Estudo de Azure Security Fundamentals.
  - Criar laboratório em nuvem com 2 VMs e aplicar boas práticas de firewall e IAM.
- Automação:
  - Criar script para simular alerta de incidentes (ex: verificar logs e enviar e-mail automático).
- Comunicação:
  - Treinar apresentação de 10 minutos explicando um caso de vazamento de dados (ex: Facebook/Cambridge Analytica).

Mês 4 – Profundidade e certificações

- LGPD + ISO 27001:
  - Curso intermediário em ISO 27001 Lead Implementer (ou equivalente online).
  - Criar checklist de auditoria fictícia.
- Cloud Security:
  - Curso de AWS Security Essentials ou AZ-900 (Microsoft Azure Fundamentals).

    - Praticar segurança em buckets S3 (AWS) e Blob Storage (Azure).
- Automação:
    - Script para automação de testes de segurança (ex: varredura de portas com Python).
- Comunicação:
    - Participar de uma comunidade de segurança no Discord/LinkedIn e interagir explicando conceitos.

Mês 5 – Integração prática

- LGPD + ISO 27001:
    - Simular uma auditoria interna usando ISO 27001.
    - Produzir relatório executivo de conformidade simplificado.
- Cloud Security:
    - Configurar alertas de segurança no AWS CloudWatch ou Azure Monitor.
- Automação:
    - Criar script de remediação automática (ex: detectar processo suspeito e bloquear).
- Comunicação:
    - Gravar um vídeo de 5-7 min explicando “Como a LGPD afeta pequenas empresas” e compartilhar com colegas.

Mês 6 – Validação e Portfólio

- LGPD + ISO 27001:
    - Fazer um simulado oficial da certificação ISO 27001 Foundation.
    - Criar documento de Plano de Continuidade de Negócios (PCN) simplificado.
- Cloud Security:
    - Realizar desafio prático de segurança em nuvem (CTF ou laboratório online).
    - Iniciar preparação para certificação AWS Security Specialty (foco médio prazo).
- Automação:
    - Publicar no GitHub scripts de automação de segurança desenvolvidos nos meses anteriores.
- Comunicação:
    - Conduzir uma mini-palestra (15 min) online simulando treinamento de conscientização em segurança da informação.