POS TECH

FIAP + alura

//CIBERSEGURANÇA

//SOFT SKILLS

COMO SE DESTACAR
NO DINÂMICO
E DESAFIADOR

MERCADO CYBER SEC

//NETWORKING

//GESTÃO DE TEMPO

03 04 05 06 07 08 09 10 11 12 13 14

INTRO →

SOFT SKILLS E RESOLUÇÃO DE PROBLEMAS →

COLABORAÇÃO, NETWORKING E FORMAÇÃO TÉCNICA →

APRENDIZADO EM PLATAFORMAS ONLINE →

CONSTRUÇÃO DE EXPERIÊNCIA PRÁTICA →

ESPECIALIZAÇÕES TÉCNICAS →

MENTORIAS, PLANEJAMENTO E GESTÃO DE TEMPO →

CONTEXTO HISTÓRICO →

BENEFÍCIOS DOS CTFS →

PLATAFORMAS PARA JOGAR CTF E TREINAR HABILIDADES →

CTF NO CENÁRIO ATUAL DA CIBERSEGURANÇA →

CONCLUSÃO →

FIAP + alura

EM UMA ÁREA TÃO TÉCNICA,

HÁ ESPAÇO PARA SOFT SKILLS?

As soft skills, habilidades puramente comportamentais que facilitam a interação e a colaboração entre as pessoas, são aderentes a qualquer ambiente corporativo, até mesmo no mercado de Cyber Security.

Embora as habilidades diárias sejam essencialmente técnicas, como base para o trabalho em segurança da informação, as competências interpessoais complementam e até potencializam essas habilidades.

As empresas buscam profissionais que não apenas compreendam profundamente aspectos técnicos, mas também saibam lidar com pessoas, trabalhar em equipe e resolver problemas de forma criativa, empática e eficiente.

Esse mix comportamental tem sido muito procurado por recrutadores de Growth e RH. Então, é melhor você se informar com este documento.

Boa leitura e sucesso na sua trajetória.

FIAP + alura

AS SOFT SKILLS SÃO INDISPENSÁVEIS

PARA PROFISSIONAIS DE SEGURANÇA CIBERNÉTICA

A comunicação empática ajuda a traduzir problemas técnicos em soluções compreensíveis para equipes não técnicas e stakeholders.

A liderança é essencial para coordenar equipes em incidentes críticos, enquanto a empatia e o trabalho em equipe facilitam a colaboração com profissionais de diferentes áreas.

Participar de grupos como Toastmasters e realizar treinamentos de gestão de conflitos pode fortalecer essas competências.

RESOLUÇÃO DE PROBLEMAS

E PENSAMENTO CRÍTICO

A segurança cibernética é repleta de desafios que exigem criatividade e pensamento crítico.

Praticar a resolução de problemas em situações reais ou simuladas, como resolver vulnerabilidades ou criar scripts automatizados, ajuda a desenvolver essas habilidades.

Ferramentas como Hack The Box ou laboratórios caseiros são ótimos para exercitar essa capacidade.

A CAPACIDADE DE TRABALHAR EM EQUIPE É VITAL,

ESPECIALMENTE DURANTE A RESPOSTA A INCIDENTES.

Participar de comunidades de segurança, como os DEF CON Groups, como é o caso do DC5551 de Porto Alegre, eventos locais da OWASP, ou fóruns no Reddit (/r/netsec) ajuda a construir conexões valiosas, trocar experiências e aprender com outros profissionais do setor.

FORMAÇÃO TÉCNICA E CERTIFICAÇÕES

Uma base técnica sólida é o alicerce para qualquer carreira em segurança cibernética.

As certificações são amplamente reconhecidas e oferecem credibilidade profissional. Exemplos:

- CompTIA Security+
- Certified Ethical Hacker (CEH)
- Offensive Security Penetration Tester (OSCP)

E cursos em plataformas ajudam a reforçar o conhecimento teórico, por exemplo:

- Cybrary
- Udemy
- Alura

FIAP + alura

APRENDIZADO EM PLATAFORMAS ONLINE

Existem excelentes plataformas que oferecem ambientes de aprendizado prático e interativo.

Para reforçar habilidades técnicas, você pode usar:

- TryHackMe
- Hack The Box
- RangeForce

Para simulações de cenários reais de ataque e defesa e ideias para aprendizado contínuo, pode utilizar:

- AttackIQ Academy
- Immersive Labs

PARTICIPAÇÃO EM CTFS

Participar desses eventos ajuda a desenvolver habilidades técnicas e a trabalhar sob pressão.

As competições Capture The Flag (CTF) são uma forma divertida e desafiadora de aplicar conhecimentos em segurança cibernética.

- Plataformas como CTFtime listam eventos globais.
- E desafios como PicoCTF são ideais para iniciantes.

LABORATÓRIOS VIRTUAIS SÃO ACESSÍVEIS

PARA OBTER A EXPERIÊNCIA PRÁTICA

Esses ambientes permitem explorar vulnerabilidades, realizar testes de penetração e experimentar diferentes técnicas de táticas de defesa.

Monte laboratórios virtuais usando ferramentas como:

- VirtualBox
- Kali Linux
- Metasploit

LEITURA E ATUALIZAÇÃO CONSTANTE

Acompanhar tendências e se atualizar sobre ameaças emergentes é essencial.

Dicas para se aprofundar em áreas específicas:

Blog:

- Krebs on Security

Whitepapers:

- Palo Alto Networks

Relatórios:

- Verizon Data Breach Investigations Report (DBIR)

Livros técnicos:

- The Web Application Hacker's Handbook
- OPSEC: Inteligência Cibernética na Prática

ESPECIALIZAÇÕES TÉCNICAS

Ao dominar o básico, busque especializações como um fator de diferencial competitivo.

Pesquise em áreas específicas, como:

- Forense digital
- Análise de Malware
- Resposta a Incidentes

Cursos avançados em plataformas como: SANS Institute ajudam a consolidar conhecimentos em segmentos específicos.

CONTRIBUIÇÃO PARA A COMUNIDADE

Ao compartilhar, você multiplica para dividir seus conhecimentos.

Contribuir para projetos de código aberto relacionados à segurança cibernética ou criar ferramentas próprias no GitHub demonstra uma iniciativa que ajuda a construir uma reputação de valor no setor.

Compartilhar aprendizados em blogs ou participar de conferências como palestrante também são maneiras de se destacar no mercado.

TER UM MENTOR NA ÁREA PODE ACELERAR

O SEU DESENVOLVIMENTO PROFISSIONAL

Plataformas como o Mentoring Club e programas oferecidos por empresas de segurança facilitam o acesso a profissionais experientes que podem guiar sua carreira numa boa trajetória.

PLANEJAMENTO E GESTÃO DE TEMPO

Organizar seu tempo entre aprendizado, prática e networking é fundamental.

Criar um cronograma que inclua estudo técnico, participação em eventos e desenvolvimento de soft skills ajuda a manter o foco e alcançar metas a longo prazo.

Mas e o desenvolvimento técnico?

Vamos falar de uma ferramenta que é essencial para aprimorar esse aprendizado técnico: as CTFs ou Capture The Flags.

O CTF TEM SUAS RAÍZES NOS JOGOS DE GUERRA MILITARES

Originalmente criados para treinar estratégias de batalha e preparar soldados para diferentes cenários de conflito, em simulações que permitiam testar técnicas de defesa e ataque em ambiente controlados.

Com o avanço das ameaças digitais reais, o conceito foi adaptado para a cibersegurança. Nos anos 1990, o Departamento de Defesa dos EUA começou a realizar simulações no ambiente cibernético, criando o "Capture the Flag" (CTF).



O CTF é uma competição na qual os participantes resolvem desafios, como:

- Vulnerabilidades
- Criptografia
- Análise de código
- Engenharia reversa

Cada desafio contém uma "flag" que representa uma informação ou acesso dentro de sistemas simulados. Os participantes devem encontrar essas flags para vencer.

Ao encontrá-las, os participantes demonstram suas habilidades em detectar e mitigar as ameaças em um ambiente seguro.

O CTF É ESPECIALMENTE ÚTIL PARA RED TEAMS E BLUE TEAMS

Permite que seus membros aprimorem habilidades específicas e identifiquem as áreas de melhoria e oferece um ambiente seguro para testar cenários variados, em que erros podem ser cometidos sem riscos reais para a infraestrutura de TI.

Os desafios também são ajustáveis para diferentes níveis de habilidade, tornando o CTF adequado tanto para iniciantes quanto para profissionais experientes.

Além do desenvolvimento técnico, os CTFs incentivam a colaboração e o trabalho em equipe.

Em um ambiente dinâmico, é possível fortalecer a comunicação e a sinergia entre os membros da equipe, sendo essas habilidades essenciais para uma resposta rápida a incidentes reais. Equipes que participam de CTFs regularmente tendem a se tornar mais rápidas e eficientes na detecção e reação a ataques reais, já que a competição simula cenários intensivos de forma realista.

FIAP + alura

PLATAFORMAS PARA JOGAR CTF

E TREINAR HABILIDADES

Para quem quer praticar, diversas plataformas oferecem desafios variados, permitindo treinar e aprimorar habilidades.



- **Hack The Box**

  Uma plataforma popular com uma ampla gama de desafios, desde exploração de vulnerabilidades até engenharia reversa. Inscreva-se **aqui.**

- **TryHackMe**

  Oferece uma abordagem prática e guiada para iniciantes e profissionais, com laboratórios e desafios de CTF. Acesse **aqui.**

- **CTFTime**

  Um site que lista competições de CTF ao redor do mundo, com oportunidades para participar de eventos online. Confira **aqui.**

- **OverTheWire**

  Focado no ensino básico, esta plataforma permite que você comece com desafios de segurança para construir uma base sólida. Experimente **aqui.**

O CTF NO CENÁRIO ATUAL DA CIBERSEGURANÇA

Com o aumento sem precedentes das invasões virtuais globais, o CTF ganhou muita importância.

Em um cenário em que as ameaças evoluem constantemente, a prática de CTFs e outras simulações é essencial para que as equipes estejam preparadas para enfrentar novos desafios.

O aprendizado prático e a mentalidade proativa são indispensáveis em cibersegurança.

Isso torna o CTF uma ferramenta crucial para a formação de profissionais resilientes, aptos a proteger as organizações contra ataques cada vez mais sofisticados.

Preparado(a) para desafiar suas habilidades e explorar o fascinante universo da cibersegurança? Entre nessa jornada com os CTFs e fortaleça as suas competências de maneira prática e desafiadora.

O segredo de uma carreira de sucesso é o equilíbrio entre o desenvolvimento técnico e as soft skills.

Com isso, você estará preparado(a) para construir uma carreira sólida e enfrentar os desafios do mercado de segurança cibernética de forma eficiente e colaborativa.

CONCLUSÃO

Em resumo, o mercado de cibersegurança exige uma combinação robusta de habilidades técnicas e soft skills. Embora o conhecimento profundo de ferramentas, técnicas e plataformas seja essencial, a capacidade de se comunicar eficazmente, trabalhar em equipe e resolver problemas de maneira criativa pode ser o diferencial que torna um profissional mais completo e eficiente.

Participar de atividades práticas, como CTFs, buscar certificações e investir no desenvolvimento contínuo dessas competências interpessoais são estratégias fundamentais para se destacar no campo.

Ao adotar uma abordagem equilibrada, que integre tanto o aprimoramento técnico quanto o aprimoramento de soft skills, é possível construir uma carreira sólida, resiliente e bem-sucedida, capaz de enfrentar os desafios cada vez mais complexos da cibersegurança.

Fique sempre com a gente para aprender mais.

FIAP + alura

PÓS TECH

Pós-Graduações Tech Intensive em Cyber Sec. Tenha jornadas de aprendizado contínuo, conectadas às mais recentes demandas de um mercado que não para de evoluir.

CURSOS OFERECIDOS

PÓS TECH - ONLINE

DEFENSIVE CYBER SECURITY – BLUE TEAM OPERATIONS

10 MESES - 360 HORAS

SAIBA MAIS

PÓS TECH - ONLINE

OFFENSIVE CYBER SECURITY – RED TEAM OPERATIONS

10 MESES - 360 HORAS

SAIBA MAIS

VEJA OUTROS CURSOS: **POSTECH.FIAP.COM.BR**

FIAP + alura

A FIAP E A ALURA FORMAM O MAIOR
E MAIS EFICIENTE ECOSSISTEMA DE EDUCAÇÃO
EM TECNOLOGIA, NEGÓCIOS, EMPREENDEDORISMO
E PRODUTOS DIGITAIS DA AMÉRICA LATINA, COM
SOLUÇÕES DE EDUCAÇÃO E PRODUTOS DIFERENTES
PARA AS DIVERSAS ETAPAS DE DESENVOLVIMENTO
DAS CARREIRAS DE ALUNOS E ALUNAS. A MISSÃO
DAS DUAS FRENTES É A MESMA: TRANSFORMAR
A REALIDADE DE PESSOAS E EMPRESAS PARA QUE
ELAS SE REALIZEM, POR MEIO DE RESULTADOS,
EM UMA JORNADA DE SUCESSO.

FIAP + alura

PARA MAIS INFORMAÇÕES SOBRE OS CURSOS E FORMAÇÕES
EM CYBER SEC, VISITE NOSSO SITE:

fiap.com.br