

Especialista em segurança de aplicações

Por que é tão perigoso?

A maior parte dos ataques atualmente, não são contra a infraestrutura organizacional, mas sim contra as aplicações. E se houver falhas em aplicações WEB, muito possivelmente o atacante conseguirá acesso a todo conteúdo existente no servidor onde a aplicação está hospedada.

OWASP – Open Web Application Security Project



Vulnerabilidades mais exploradas em aplicações WEB:

- Injection
- Falha de Autenticação e gerenciamento de sessão
- Cross Site Scripting (XSS)
- Referência Insegura a Objeto direto
- Falhas em configuração de segurança
- Exposição de dados sensíveis
- Falta de Função de controle de Nível de acesso
- Cross-Site Request Forget (CSRF)
- Utilização de componentes com Vulnerabilidades Conhecidas
- Redirecionamentos e Encaminhamentos sem validação

WEBGoat

Ferramenta de aprendizado do funcionamento de vulnerabilidades Web

<http://code.google.com/p/webgoat/>



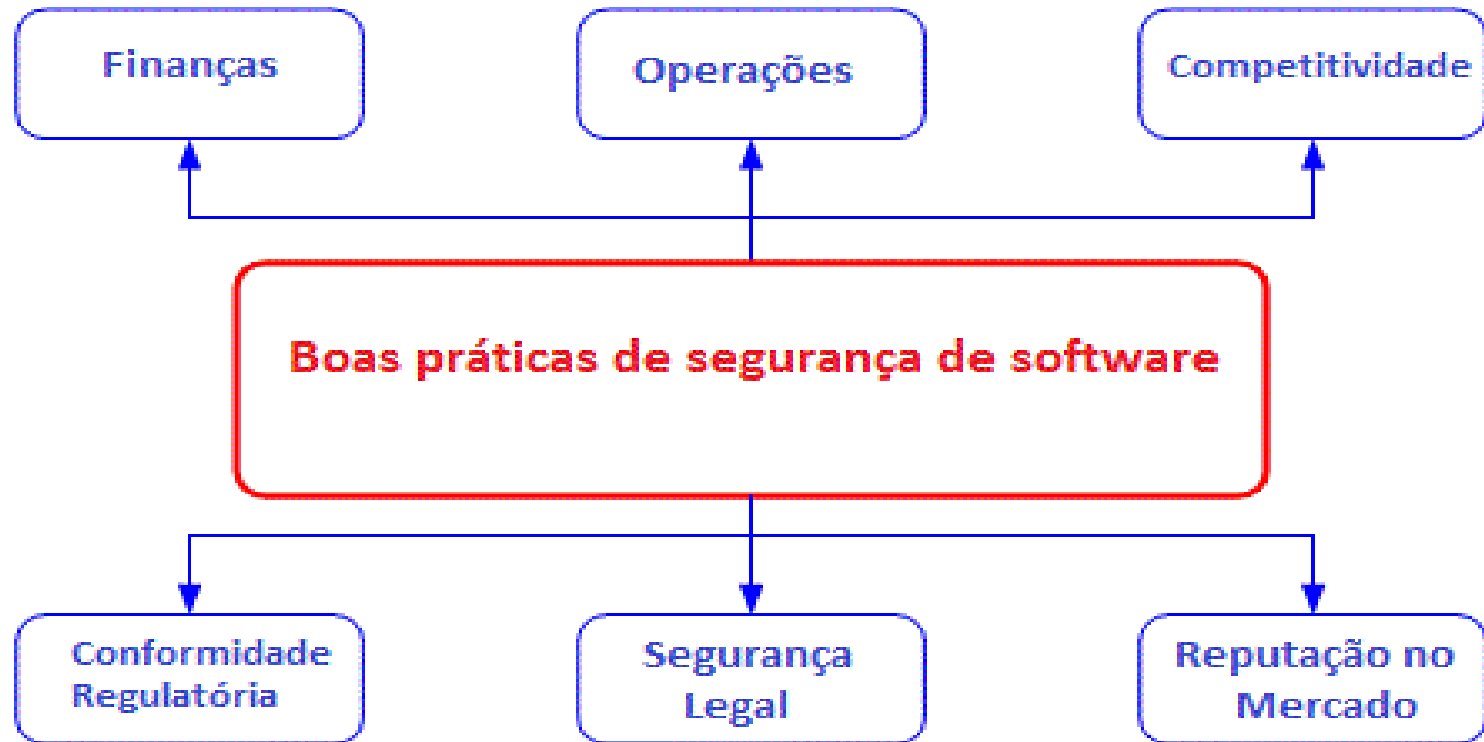
CLASP

Dentro de um projeto de desenvolvimento de software, o CLASP Best Practices é a base de todas as atividades de desenvolvimento de software relacionados à segurança – se o planejamento, concepção ou implementação – incluindo o uso de todas as ferramentas e técnicas que suportam CLASP


Os objetivos do projeto OWASP CLASP estão a fazer estes materiais amplamente disponíveis, bem como proporcionar um fórum para a comunidade a contribuir materiais de volta para apertar para o benefício de todos.

Tendo em vista as consequências de falhas de segurança exploradas , não há alternativa melhor a usar boas práticas de segurança da aplicação o mais cedo possível – e por toda parte – o seu ciclo de vida de desenvolvimento de software.

Panorama de negocios das boas práticas de segurança de software





- O que é o PRINCE2 ?
 - Resumo histórico;
 - Onde se aplica ?
 - Economia de tempo e dinheiro.
 - Qualidade
 - Relação com : ITIL,ITSM,PMBOK,SCRUM e outras metodologias.
- 

Empresas que utilizam a metodologia:



- Certificações PRINCE2:
Custo £170, ou R\$631,00, ou USD264,76 –
- **PRINCE2 Foundation:** o exame é composto por 75 questões de múltipla escolha, sendo que 5 questões não contam pontuação (durante o exame o candidato não sabe quais são essas questões). Para ser aprovado é necessário acertar 50% da prova, isto é, 35 questões. A prova tem duração de uma hora. Essa certificação não expira.
- **PRINCE2 Practitioner:** o exame conta com 8 questões de múltipla escolha complexa, com 10 pontos por questão, totalizando 80 pontos possíveis. Para ser aprovado são requeridos 44 pontos (cerca de 55% da prova). A prova tem duração de 2h30min. O exame de re-certificação pode ser realizado no período entre 3 e 5 anos a contar da data da primeira certificação.
- **PRINCE2 Professional:** Essa certificação é obtida através de avaliação prática onde o candidato é avaliado pela condução de um projeto.


SDL

Security Development Lifecycle

- Treinamento
- Requisitos
- Design
- Implementação
- Verificação
- Release
- Resposta

Carreira

Dicas para ser um especialista em Segurança de Aplicações

- Faça certificações
 - Tenha conhecimento em controle de aplicações na nuvem
 - Saiba bastante sobre segurança móvel
 - Seja um bom analista
- 

Importância das Certificações

- É com as certificações que se tem credenciais que ressaltam que o especialista passou por teste significativos.



Conhecimento de controle em Aplicações na nuvem

- A gestão da informação de segurança, identidade de acesso na nuvem são uma das grandes preocupações dos Gerentes de TI, que estão implantando softwares de serviços para complementar as aplicações corporativas.



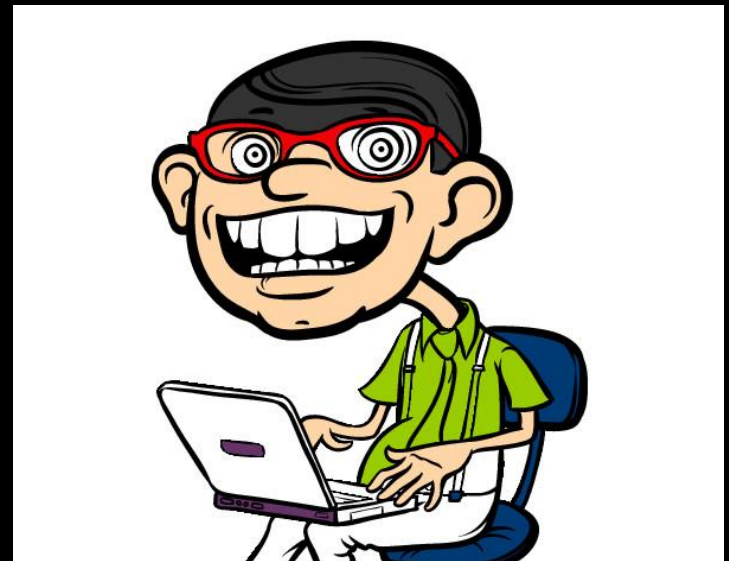
Conhecimento em Segurança para dispositivos móveis

- Muitas organizações estão sendo desafiadas a criar políticas para dispositivos móveis. Elas precisam proteger informações armazenadas em uma variedade de dispositivos.



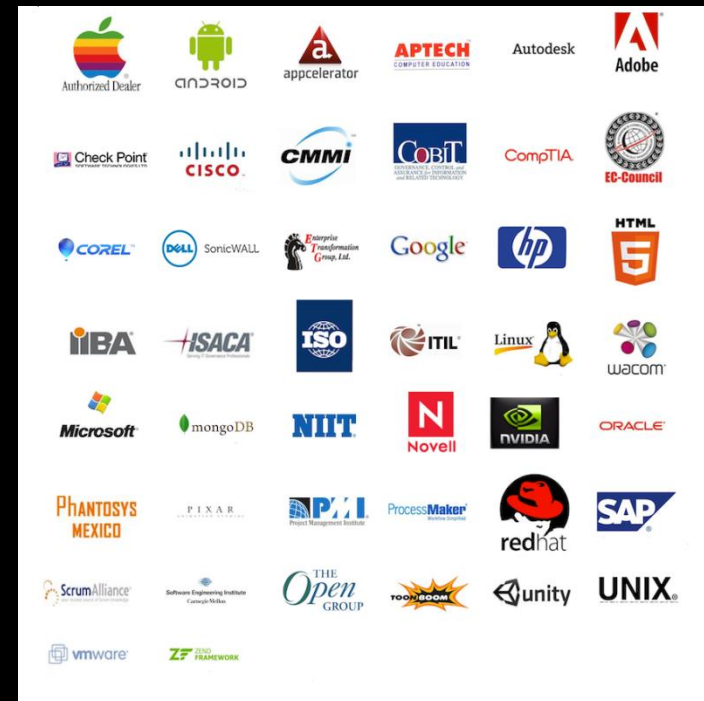
Ser um bom analista

- Os especialistas em segurança cibernética são mestres em encontrar agulhas em palheiros. Eles precisam lidar com grandes volumes de dados coletados por meio de dispositivos de segurança e encontrar anomalias que indicam falhas.



CERTIFICAÇÕES

- CompTia Security+
- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)
- Certified Information Security Systems Professional (CISSP)



O que é certificação?

A certificação nada mais é do que a confirmação de que um profissional está apto a cumprir determinada função. É a garantia de que ele é totalmente capacitado para realizar as tarefas e agir conforme prega o manual desde os momentos mais corriqueiros até os mais complexos referentes àquela atividade.



A Certificação CompTIA Security+ é uma credencial independente, sem a inclusão de Tecnologia específica de nenhum fabricante.

O exame CompTIA Security+ é uma forma de validação reconhecida internacionalmente, de habilidades e conhecimento do nível de fundamentos de segurança da informação e é utilizada por organizações e profissionais de segurança em todo o mun



A Certificação CompTIA Security+ é voltada a um profissional de segurança de TI que tenha:

- No mínimo 2 anos de experiência em administração de TI com foco em segurança.
- Experiência cotidiana de técnicas de segurança de informação.
- Amplo conhecimento dos interesses e implementações envolvendo segurança da informação



Como obter o CompTIA Security+

O teste, disponível em português, reúne até 100 questões de múltipla escolha e de desempenho, e o candidato tem 90 minutos para finalizá-la. A pontuação mínima para aprovação é de 750, em uma escala de 100 a 900.

A CompTIA possui uma rede de parceiros autorizados que fornecem treinamento e materiais recomendados para o teste. Os custos das aulas variam entre 2 e 3 mil reais.



- **Público Alvo:**

Profissionais da área de Segurança da Informação e Tecnologia da Informação que buscam uma certificação renomada na área de Segurança da Informação.

- **Certificação**

O exame de certificação possui 200 questões objetivas distribuídas entre os tópicos:

- Information Security Governance (24%)
- Information Risk Management and Compliance (33%)
- Information Security Program Development and Management (25%)
- Information Security Incident Management (18%)

- **Pré requisito**

Além de bom inglês para leitura, mais de 3 anos de conhecimento na área de gestão e gerenciamento em Segurança da Informação.



Público Alvo

Profissionais da área de Segurança da Informação com um mínimo de cinco anos de experiência em auditoria de Segurança da Informação, controle, garantia e segurança.

Certificação

- O aluno poderá realizar o exame oficial CISA da ISACA, que contém 200 questões distribuídas entre os tópicos:
- O processo de auditoria de Sistemas de Informação (14%)
- Governança e gestão de TI (14%)
- Aquisição de Sistemas de Informação, desenvolvimento e implementação (19%)
- Operação de Sistemas de Informação, manutenção e suporte (23%)
- Proteção de ativos de informação (30%)

Pré requisito

Além de bom inglês para leitura, mais de 5 anos de experiência em auditoria de Segurança da Informação, controle, garantia e segurança.



CISSP – Certified Information Security Systems Professional – é uma certificação na área de Segurança da Informação que reconhece o nível de conhecimento do profissional em um conjunto de melhores práticas que foram condensadas em 10 domínios, vale lembrar que a CISSP foi a primeira credencial na área da informação a atender aos rigorosos requisitos da Norma ISO/IEC 17024. CISSP não é apenas uma medida de excelência, mas também um padrão de conquista com reconhecimento mundial.

- Sistemas de controle de acesso
- Segurança de telecomunicações e redes
- Governança de Segurança da Informação e Gerenciamento de riscos
- Desenvolvimento seguro de software
- Criptografia
- Arquitetura de segurança e design
- Segurança de operações
- Plano de continuidade de negócios e recuperação de desastres;
- Leis, regulamentos, investigação e conformidade
- Segurança física



Certificação

Até 2010 a prova era em inglês mas hoje em dia existe a opção de se fazer no idioma português. No entanto, vale ressaltar que os materiais de estudo são apenas em inglês. O exame consiste em 250 questões de múltipla escolha com 4 alternativas cada e deve ser concluído em até 6 horas.

Pré Requisitos

Para realizar o exame, o candidato deve afirmar que ele ou ela possui um mínimo de cinco anos de experiência profissional na área de segurança da informação ou quatro anos de experiência além de um diploma universitário.

SALÁRIO

PROFISSIONAIS DE SEGURANÇA DA INFORMAÇÃO

Analista de segurança da informação júnior	R\$ 4.934,72
Analista de segurança da informação pleno	R\$ 5.600,00
Analista de segurança da informação sênior	R\$ 7.266,93
Analista segurança de sistemas júnior	R\$ 4.890,00
Analista segurança de sistemas pleno	R\$ 6.720,00
Analista segurança de sistemas sênior	R\$ 7.840,00
Gerente de segurança júnior	R\$ 11.060,00
Gerente de segurança pleno	R\$ 12.192,00
Gerente de segurança sênior	R\$ 14.333,00