



Especialista em Segurança de Aplicações

OWASP/CLASP, Prince II e SDL

ROMULO MARCELLUS DA SILVA NUNES
1223331058



OWASP/CLASP

- **OWASP** - **O**pen **W**eb **A**pplication **S**ecurity **P**roject / Projeto Aberto de Segurança em Aplicações Web

A OWASP, fundada em 2001, é uma organização sem fins lucrativos que gerencia uma comunidade web(www.owasp.org) dedicada a segurança em aplicações web.

A principal finalidade da OWASP é disseminar informação sobre segurança de software de maneira visível, de graça e acessível a todos, facilitando a tomada de decisão no que tange os verdadeiros riscos de segurança em software. Todos, indivíduos ou organizações, são livres para participar da organização, o que torna o projeto atrativo para desde quem está em aprendizado sobre o assunto até gigantes de software.

Para facilitar a divulgação mundial da informação, a OWASP criou os chamados Capítulos, que são grupos locais com objetivo de fomentar os princípios da organização em determinada área. No Brasil, temos capítulos em 19 cidades incluindo o Rio de Janeiro. Na página de cada capítulo os membros interagem com notícias, análises, relatos, pesquisas e marcam reuniões para discutir tópicos de interesse da comunidade.

No Brasil, já foi organizada a conferência OWASP AppSec Brasil em duas ocasiões, 2009 e 2010.

OWASP/CLASP

Projetos famosos:

*WebGoat - O WebGoat é uma aplicação web deliberadamente insegura, que incita o usuário a aprender lições de segurança testando-as conforme as instruções do programa.

*WebScarab - Aplicativo desktop que é configurado como um proxy e analisa todo o tráfego entre o navegador e aplicação. Possibilita alterar requests e assim identificar falhas.

*Top 10 - Documentação web que lista as 10 maiores falhas de segurança web.

*CLASP – Detalhamento no próximo slide.

Alguns contribuintes:



OWASP/CLASP

- **CLASP** - *Comprehensive, Lightweight Application Security Process* / Processo de Segurança de Aplicações Leve e Abrangente

CLASP é uma metodologia de desenvolvimento direcionada a segurança da aplicação, listando uma série de boas práticas consideradas necessárias para obter um software seguro.

A estrutura do processo é dividida em cinco perspectivas, denominadas Visões CLASP. Cada Visão, por sua vez, é dividida em atividades, que contém os componentes do processo

*Visão Conceitual - apresenta como funciona o processo e a interação entre os componentes.

*Visão baseada em Regras - apresenta as responsabilidades dos membros da equipe do projeto, associando-as às atividades propostas.

*Visão de Avaliação de Atividades - descreve os objetivos de cada atividade e os elementos relacionados como custo, aplicação, impacto e análise de riscos.

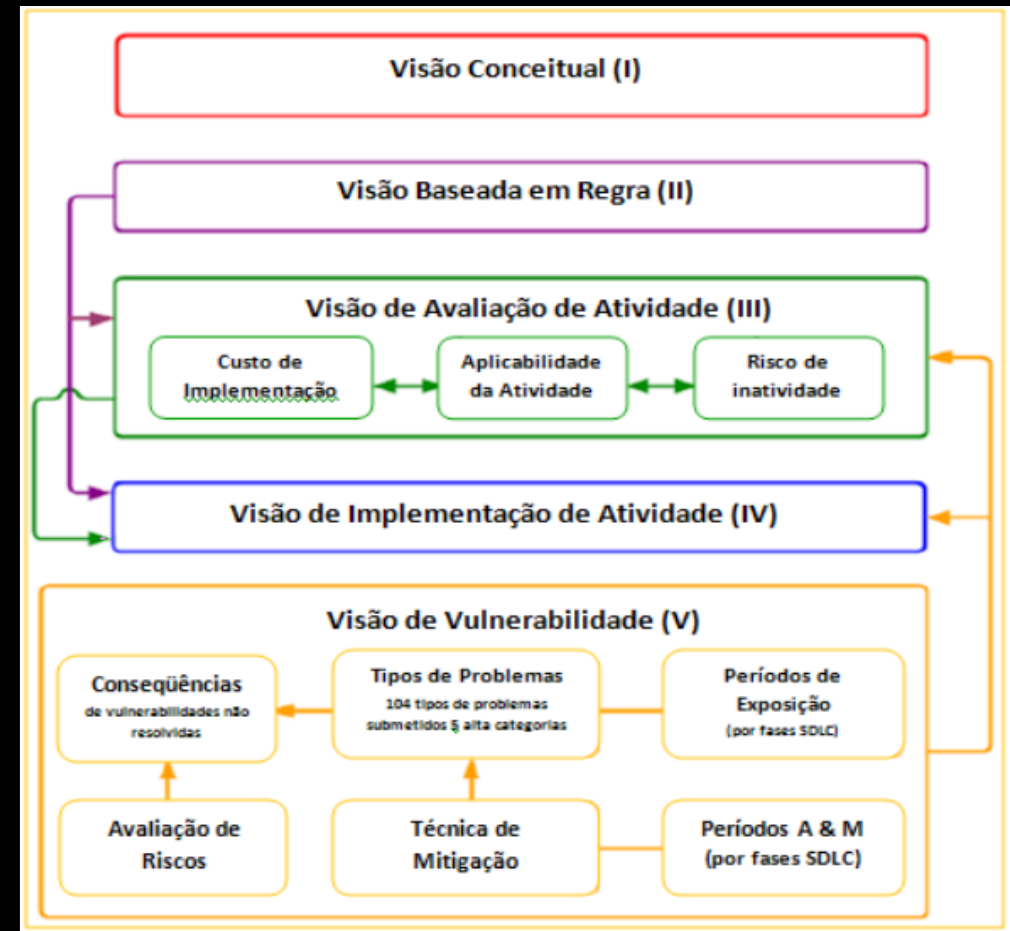
*Visão de Implementação de Atividades - descreve as atividades de segurança envolvidas no CLASP.

*Visão de Vulnerabilidade - descreve os tipos de vulnerabilidades no desenvolvimento de software.

Hoje o CLASP é de responsabilidade da OWASP, fazendo parte de seus projetos mais visados.

OWASP/CLASP

Estrutura das visões:



PRINCE2



- **PRINCE2 - *PR*ojects *IN* Controlled Environments, version 2** / Projetos em ambientes controlados, versão 2

É um método de gestão de projetos adaptável a qualquer tipo ou tamanho de projeto e cobre seu gerenciamento, controle e organização. É padrão para projetos em diversos países, inclusive no Reino Unido(onde foi criado).

No PRINCE2 as áreas do projeto são trabalhadas isoladamente, porém são facilmente integradas pelo método facilitando a criação de uma planta completa e segura do projeto.

É dividido em quatro elementos:

*Princípios - Orientações obrigatórias e boas práticas que determinam se o projeto está sendo genuinamente gerenciado de acordo com o método. Possui sete princípios, como Business Case e gerenciamento por estágios.

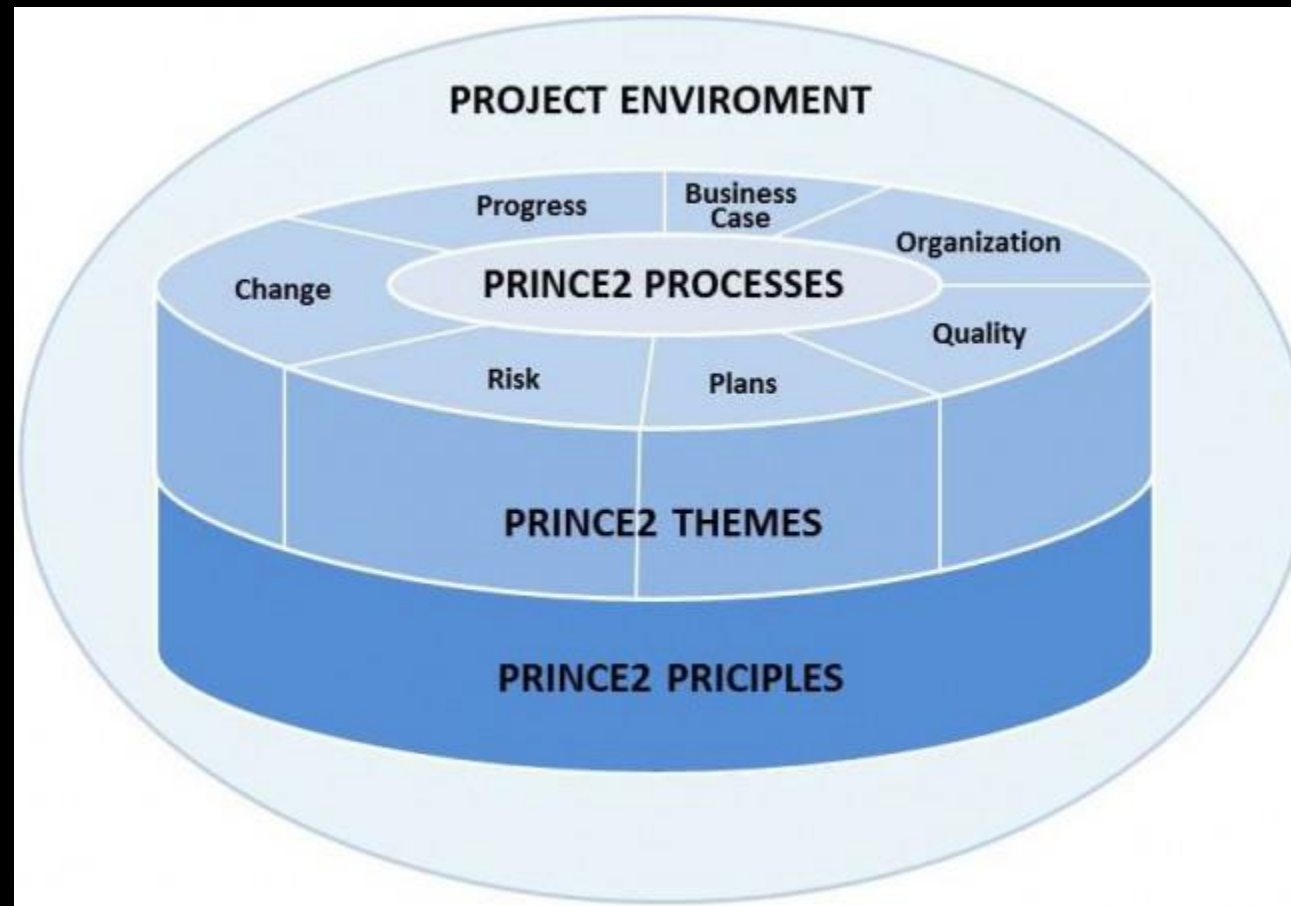
*Temas - Descrevem aspectos do gerenciamento de projeto que devem ser tratados continuamente e em paralelo ao longo de toda a duração do projeto. Também possui sete princípios, como Planos e Qualidade.

*Processos - São percorridos de acordo com as etapas ao longo do ciclo de vida do projeto. Sete princípios, como Início de projeto e Gerenciamento de entrega de produto.

*Ambiente - Trata da adequação do PRINCE2 ao contexto particular do projeto. É aqui que se evidencia a flexibilidade do PRINCE2, podendo se adaptar a ambientes de portes e fins diferentes.

PRINCE2

Elementos do PRINCE2:



PRINCE2

Certificações do PRINCE2:

**PRINCE2 Foundation* - O objetivo deste nível é avaliar se o candidato tem capacidade de agir como um membro informado de uma equipe de gerenciamento de projeto usando o método PRINCE2, em um ambiente de projeto que usa o PRINCE2. R\$780,00

**PRINCE2 Practitioner*: O objetivo deste nível é avaliar se o candidato tem capacidade de aplicar o PRINCE2 à execução e ao gerenciamento de um projeto não complexo em um ambiente de projeto que usa o PRINCE2. O exame de recertificação(R\$850,00) pode ser realizado no período entre 3 e 5 anos a contar da data da primeira certificação. Necessário já haver obtido o nível foundation. R\$ 990,00

**PRINCE2 Professional*: Essa certificação é obtida através de avaliação prática onde o candidato é avaliado pela condução de um projeto. Necessário já haver obtido o nível *practitioner*. Aplicado em eventos e empresas credenciadas.

Vale observar que o PRINCE2 possui a certificação em Gerenciamento de Projetos mais popular do mundo

SDL



- **SDL** - *Security Development Lifecycle* / Ciclo de Vida do Desenvolvimento da Segurança

É um processo que a Microsoft adotou para o desenvolvimento de softwares com objetivo de eliminar problemas de segurança antes da finalização do projeto, assim reduzindo custos de manutenção pós lançamento e aumentando a confiabilidade das aplicações.

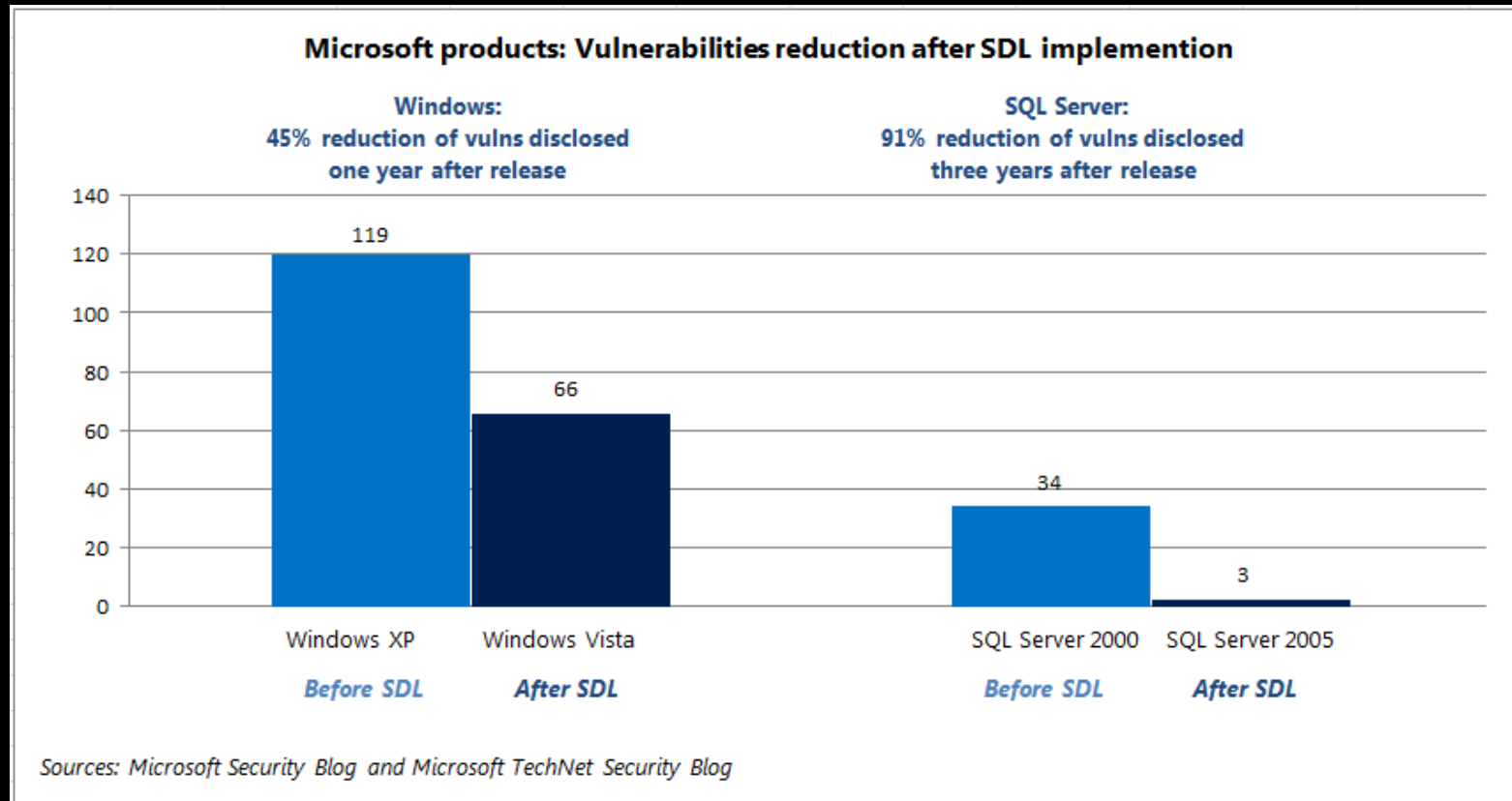
O processo engloba a adição de uma série de atividades e produtos concentrados na segurança em cada fase do processo de desenvolvimento de software da Microsoft. Essas atividades e esses produtos incluem o desenvolvimento de modelos de ameaças durante o design do software, o uso de ferramentas de verificação de código de análise estática durante a implementação e a realização de revisões de código e testes de segurança durante um "esforço de segurança" direcionado.

Antes que o software sujeito ao SDL possa ser lançado, ele deve passar por uma Revisão final de segurança feita por uma equipe independente de seu grupo de desenvolvimento.

Quando comparado a um software que não foi submetido ao SDL, o software que passou pelo SDL apresentou uma taxa significativamente reduzida de descobertas externas de vulnerabilidades de segurança.

SDL

Exemplo comparativo pré e pós SDL:



SDL

○ SDL possui 7 fases de desenvolvimento:

- *Treinamento – Informativo sobre o básico em segurança e tendências recentes em segurança e privacidade.

- *Requerimentos– Análise de riscos e definição de padrões de qualidade

- *Design – Modelagem de ameaça, análise de ataque.

- *Implementação – Especificação de ferramentas aprovadas, depreciação de funções menos seguras

- *Verificação – Fuzzing

- *Lançamento – Plano de resposta a incidentes, análise de segurança final

- *Resposta – Executar plano de resposta

O Profissional em Segurança de Aplicações

- Segurança da informação:

Segundo a ABNT, a Segurança da Informação consiste na “proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio”.

Para que isso seja alcançado existem formas de controlar o trâmite desse conteúdo. De acordo com a norma citada anteriormente, estão inclusos nesses conjuntos de ferramentas gerenciais a definição de políticas de acesso, a estipulação de processos e procedimentos que resguardecam a integridade dos dados armazenados, consolidação de estruturas organizacionais bem definidas e implementação de funções de software e hardware.

- Segurança de aplicações:

Promove serviços de segurança como técnicas de criação de código seguro, análises, treinamento e percepção, testes de segurança e guiar em geral os passos de desenvolvimento interno de projetos de software.

O Profissional em Segurança de Aplicações

- Certificações - Existem dezenas de certificações relacionadas a segurança em TI, abrangendo as mais diferentes áreas. Abaixo seguem alguns dos principais exemplos:

*CompTIA Security+ - É o primeiro passo para todas as áreas de Segurança da Informação. Ela é o passo inicial para os profissionais da área de Segurança da Informação, pois aborda conceitos básicos de Segurança da Informação, tais como: Segurança de Redes; Conformidade e Segurança Operacional; Ameaças e Vulnerabilidades; Segurança de Aplicações, Dados e Estações; Controle de Acesso e Gerência de Identidade; e Criptografia.

*CEH (Certified Ethical Hacker) - Tem sido amplamente utilizado pelo Pentágono a fim de treinar os profissionais que atuam na área de defesa de redes e também uma das selecionadas pelo DSIC(Departamento de Segurança da Informação e Comunicações) do Gabinete de Segurança Institucional da Presidência da República.

*EC-Council Certified Security Analyst (ECSA) - Complementa a certificação Certified Ethical Hacker (CEH) com foco na análise dos dados obtidos em um teste de invasão.

*CHFI (Computer Hacking Forensic Investigator) - Certificação que prepara o profissional para detectar ataques e extrair adequadamente as evidências para a comprovação do crime cibernético, assim como a condução de auditorias que visam prevenir futuros incidentes. Computer forensics é simplesmente a aplicação de investigações cibernéticas e técnicas de análises com o fim de determinar a evidência legal. A evidência pode ser classificada dentro de uma ampla gama de crimes digitais, incluindo, dentre outros, o roubo de segredos comerciais, espionagem corporativa, destruição ou uso indevido de propriedade intelectual, sabotagem, fraude e mau uso de programas e sistemas.

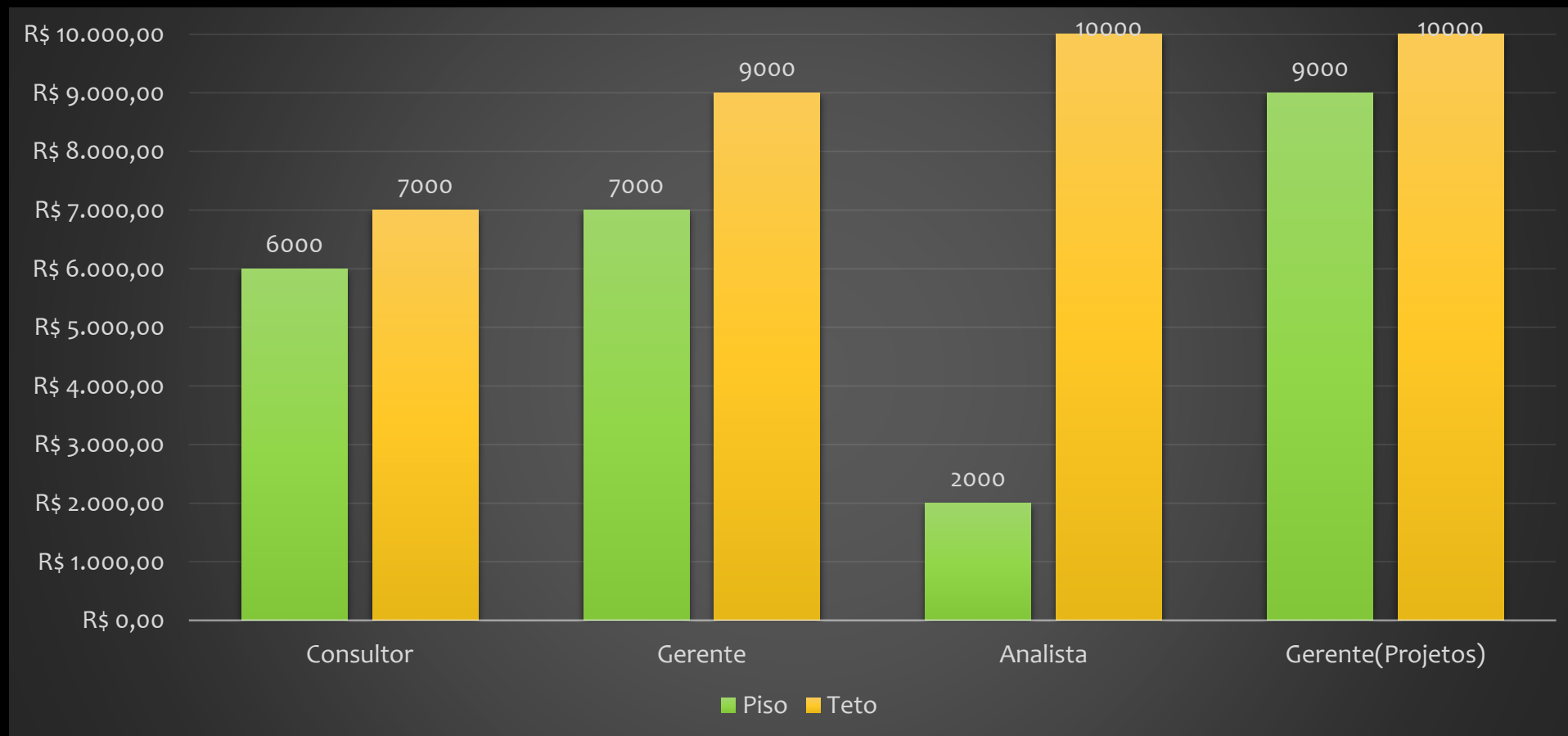
*CISM (Certified Information Security Manager) - É uma das principais da área de Segurança da Informação, por ser destinada especificamente aos profissionais que visam atuar ou já atuam na gestão de segurança da informação. Ela é para profissionais que projetam, dirigem e avaliam os programas de segurança de informação de corporações.

*CASP (CompTIA Advanced Security Practitioner) - Abrange conhecimentos técnicos e habilidades necessárias para projetar, conceituar e aplicar soluções de segurança em ambientes corporativos complexos.

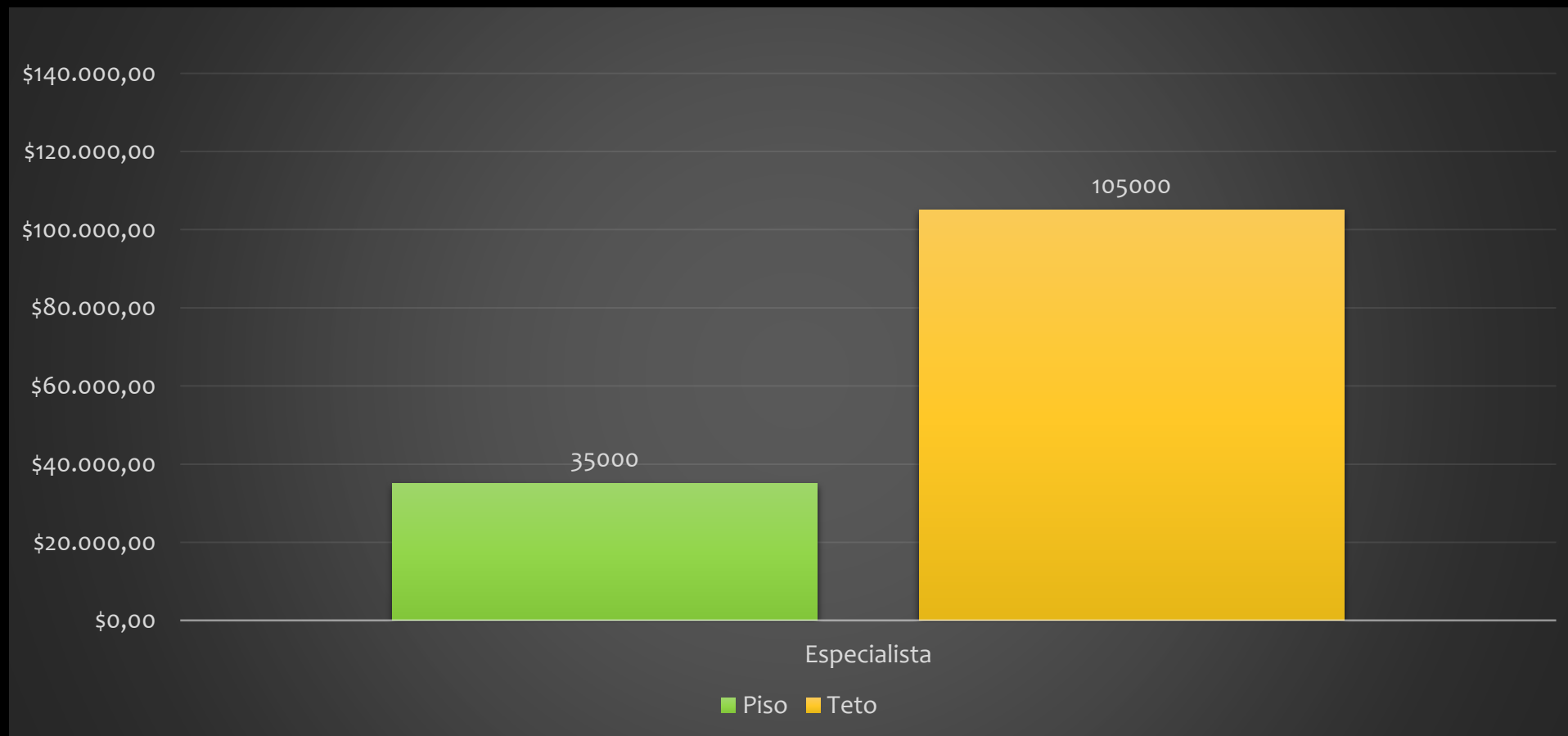
*CISSP (Certified Information Systems Security Professional) - Um CISSP é um profissional de segurança da informação que define a arquitetura, design, gestão e/ou controles que garantem a segurança de ambientes corporativos. A vasta amplitude de conhecimentos e experiências necessários para aprovação no exame é o que diferencia um CISSP. A credencial demonstra um nível reconhecido globalmente de competência fornecido pelo CBK® do (ISC)2®, que cobre tópicos críticos em segurança atual, incluindo computação em nuvem, segurança móvel, segurança no desenvolvimento de aplicativos, gestão de riscos, e outros.

*CSSLP (Certified Secure Software Lifecycle Professional) - A CSSLP foi uma das primeiras certificações no mundo a abordar o desenvolvimento seguro. Possui como requisito 4 anos de experiência, no mínimo, em desenvolvimento seguro. Certifica proficiência em: desenvolvimento de um programa de segurança de aplicações na organização; redução de custos de produção, vulnerabilidades em aplicações e atrasos de entrega; melhoria da credibilidade da organização e da sua equipe de desenvolvimento; redução de perda financeira devido a violação de softwares inseguros

Salários em segurança da informação e área de projetos:



Salário na área de segurança de aplicações:



The background of the slide is a light gray circuit board pattern with various traces and circular components. A solid black horizontal bar spans the middle of the image, serving as a background for the text.

FIM

}

ROMULO MARCELLUS DA SILVA NUNES
1223331058