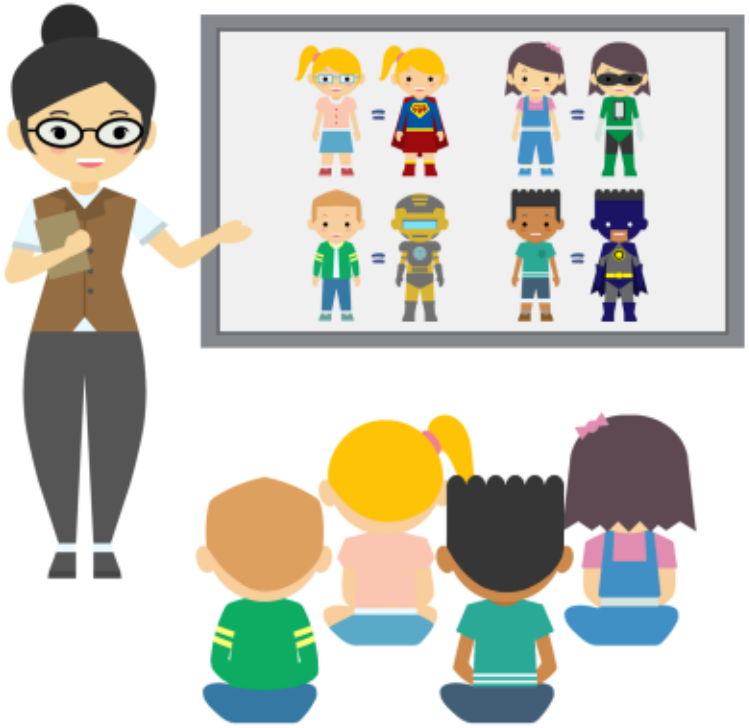
ABC de AppSec

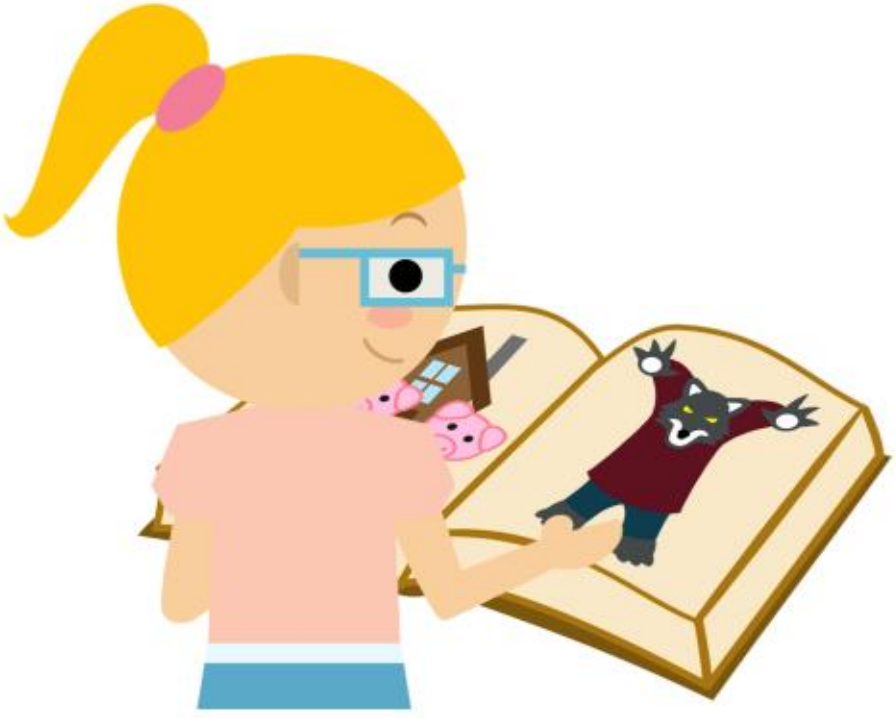
Por Caroline Wong



Todos os dias estamos em contacto com aplicações. Desde o despertador do *smartphone*, à *app* de videochamada que utilizamos para estar em contacto com amigos e família, as aplicações e os programas informáticos são uma parte importante da nossa vida diária.

Como é que te tornas um super-herói da segurança de aplicações?
O que é que necessitas de saber?

Vamos começar por aprender o ABC de AppSec – A Segurança das Aplicações!



A

de Ameaça

Uma ameaça é qualquer coisa que tenha o potencial de causar sérios danos numa aplicação ou programa informático.

Na história dos Três Porquinhos, o Lobo é a ameaça.

B de *Backup*

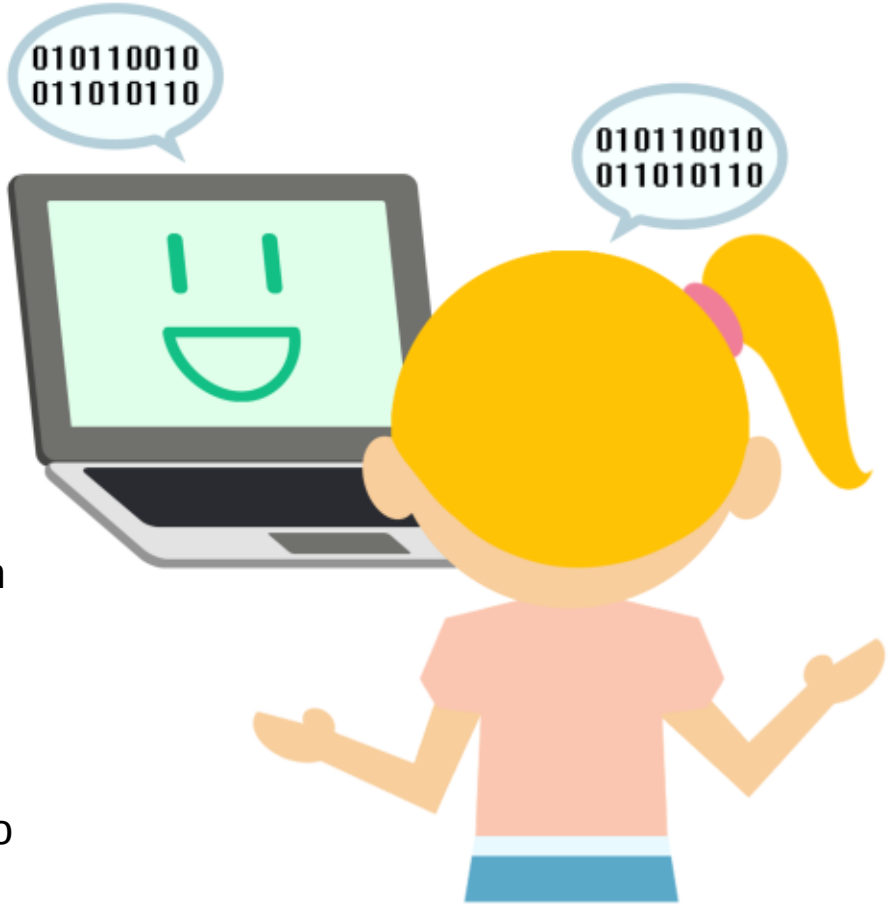
Embora a expressão em português seja “salvaguarda de dados”, toda a gente sabe o que é um *backup*.

É o que fazes quando copias dados importantes para um local diferente para os manter protegidos se houver um incidente no local original.

C

de Código

Chamamos código a um conjunto de instruções, em qualquer linguagem, que seja utilizado para construir programas e aplicações e dizer-lhes o que têm que fazer.



D de Dados

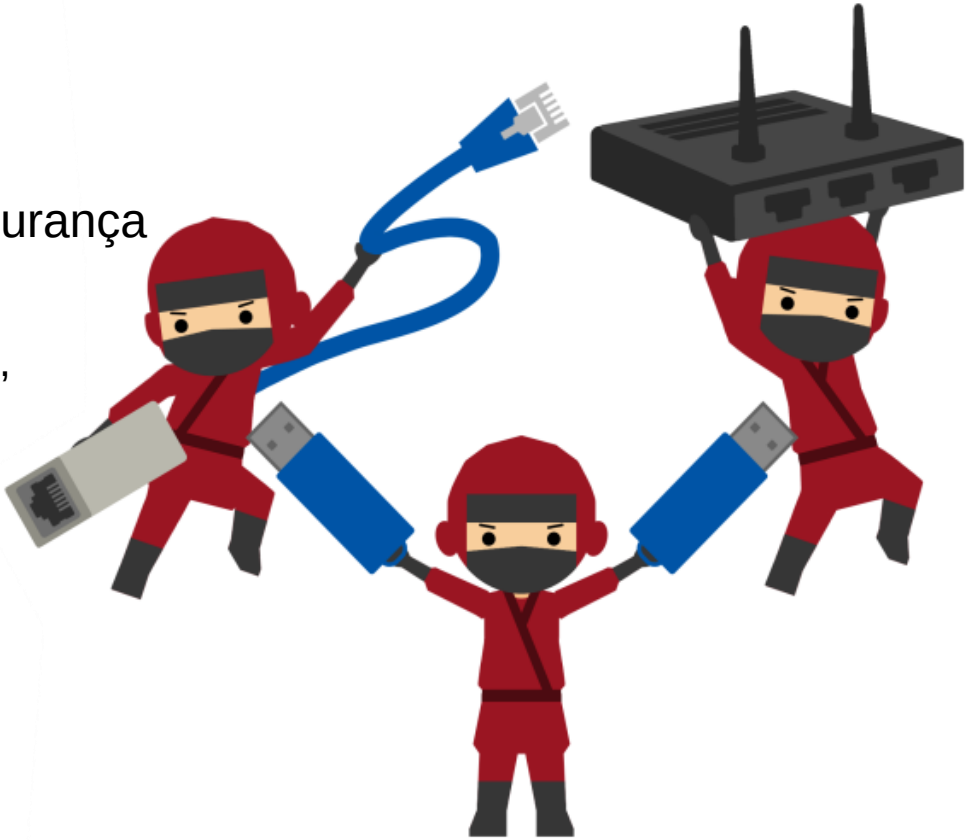
Dados são pedaços de informação ou conhecimento, que podem ser processados por aplicações ou programas informáticos e devem ser protegidos contra acessos não autorizados e alterações maliciosas.

Lembra-te disso quando estiveres a utilizar aplicações ou quando estiveres a programá-las.

E

de Especialista de Segurança

Os especialistas de segurança não são ninjas, mas são profissionais competentes que ajudam a manter as nossas redes, aplicações e dados a funcionar de forma segura.

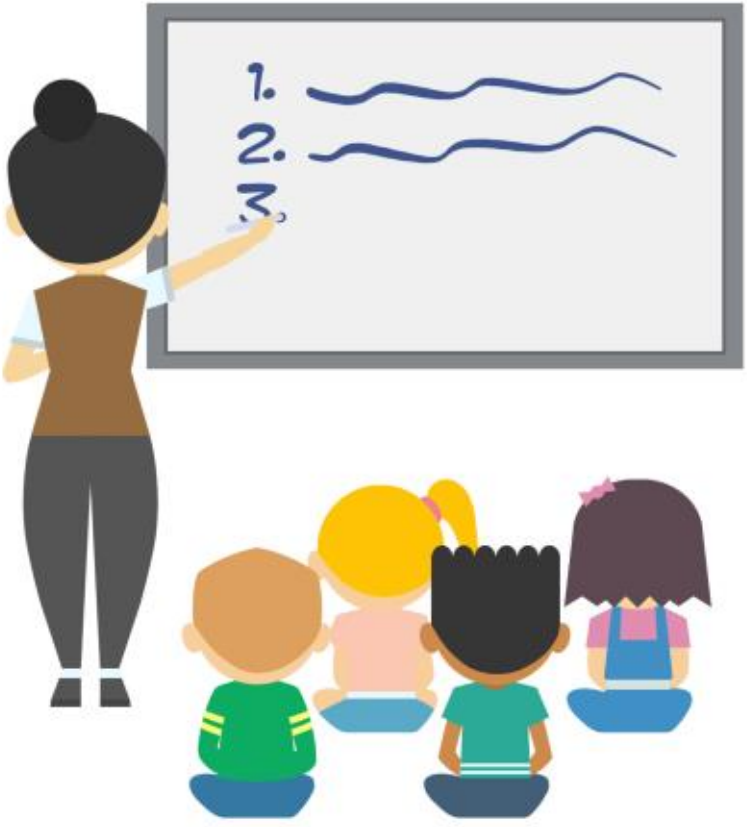


F

de Falso Positivo

Quando as ferramentas que os profissionais de segurança (os *hackers* éticos) identificam problemas que, afinal, não existem, chamamos-lhes Falsos Positivos.

É preferível ter um falso positivo do que não identificar os problemas que lá estão.



G

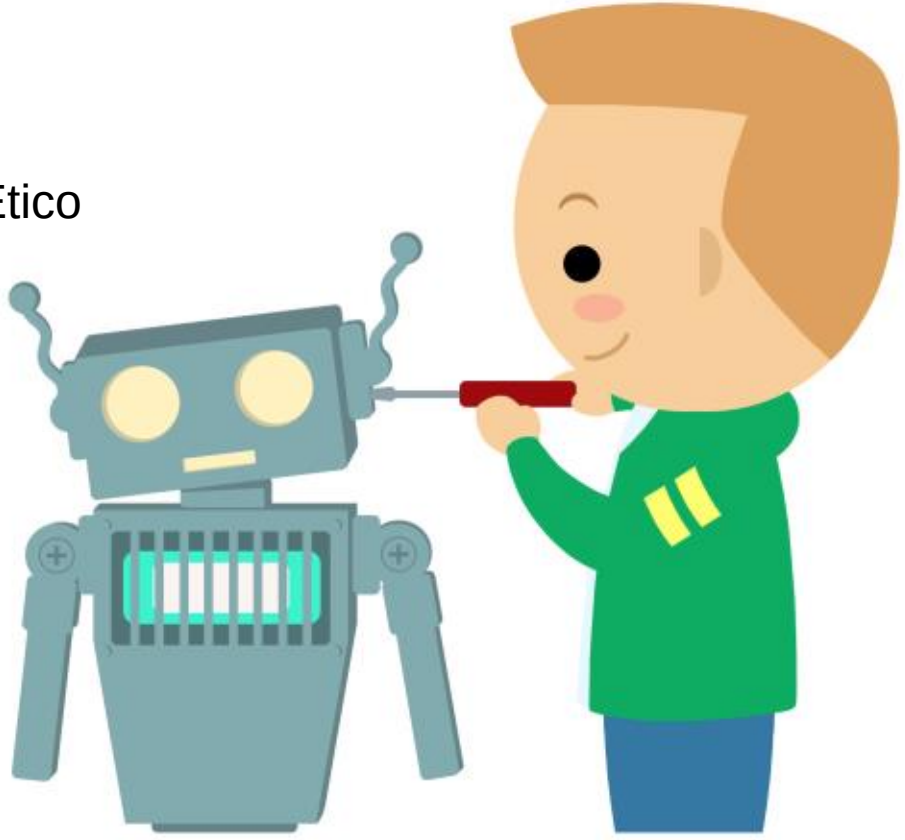
de Governança

Para garantir o funcionamento seguro de uma aplicação, é necessário que existam regras e alguém responsável por garantir que fazem sentido e são bem aplicadas.

H de Hacker Ético

O *hacking* diz-se ético quando estamos autorizados a descobrir falhas em aplicações e programas informáticos.

Depois consertamos de modo a que os criminosos não possam usar a mesma falha para nos prejudicar.



de Incidente de Segurança

Quando alguém tenta quebrar a segurança de uma aplicação e fazer com que deixe de trabalhar ou trabalhe de forma diferente do que é suposto, dizemos que estamos perante um incidente de segurança.

J

de Javascript

Javascript é uma linguagem de programação bastante versátil que pode ser utilizada para vários objetivos – desde construir sítios na Internet até programar robots voadores.

L

de Listagem de Atividades

Quando queres saber o que está a acontecer com a tua aplicação ou programa informático gravas uma listagem das atividades (em inglês: *logs*), onde podes guardar quem teve acesso, que dados leram, e o que fizeram.

É como na escola quando os professores fazem a chamada para saber quem está presente na aula e registam no livro.

M de Malware

Existem vários programas informáticos. Alguns bons que nos ajudam e divertem no dia-a-dia, mas outros são maus e tentam roubar informação ou prejudicar-nos a nós ou a outros.

Os programas maus são conhecidos como *malware*.

N

de Não Autorizado

Quando alguém tenta aceder a informação à qual não tem permissões, diz-se que não está autorizado.

O

de OWASP Top 10

O Pai Natal faz uma lista e verifica-a antes de entregar as prendas.

O OWASP faz uma lista das formas mais comuns que existem para atacar programas e aplicações. Esta lista é a OWASP Top 10.

P de Privacidade

Os nossos dados podem ser um tesouro de informação para pessoas maliciosas.

Lembra-te de assegurar a privacidade dos dados quando estiveres a programar e a utilizar as tuas aplicações.

Q

de Quebra de Segurança

Uma quebra de segurança acontece quando informação privada é acedida ou roubada por alguém que não deveria ter acesso a essa informação.

R de Ransomware

Ransomware é o nome que se dá aos tipos de programa que atacam os nossos dispositivos e nos impedem de aceder à nossa informação, a menos que se pague um resgate aos criminosos.

S

de Segurança de Aplicações

Segurança de Aplicações (em inglês: *AppSec*) é a prática de prevenir, encontrar, e corrigir erros que possam colocar em causa as nossas aplicações e programas informáticos.

T

de Testes de Segurança

Os testes de segurança são realizados por especialistas (os *hackers éticos*) que identificam problemas em aplicações e programas informáticos para que sejam corrigidos antes que os criminosos se possam aproveitar destas situações para prejudicar os utilizadores.

U de Utilizador Autorizado

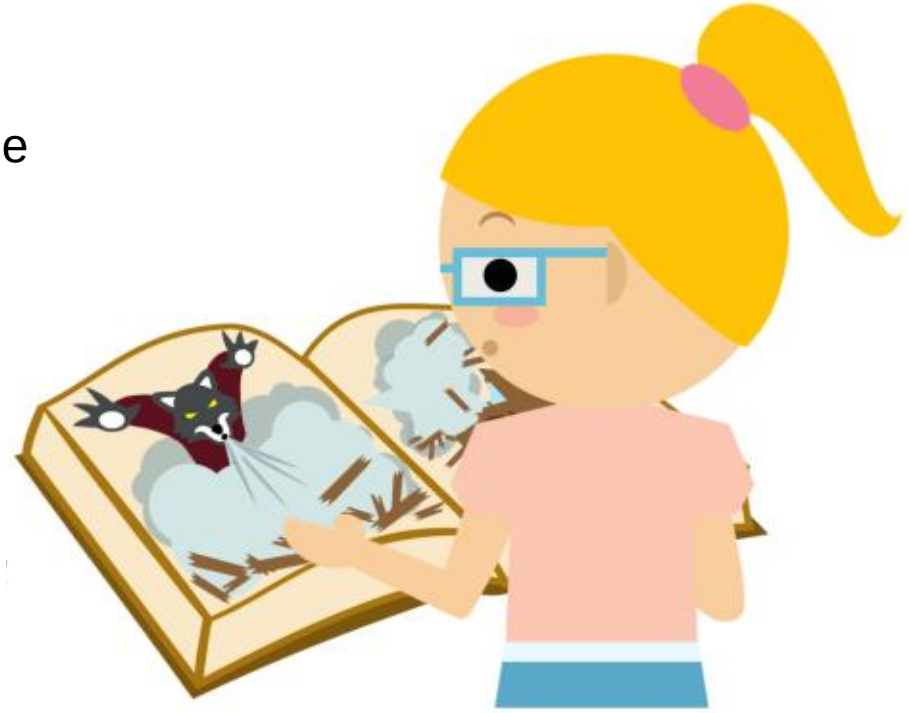
As aplicações e programas informáticos apenas devem estar disponíveis para utilizadores autorizados.

Não queremos estranhos a aceder à nossa informação.

V de Vulnerabilidade

Uma vulnerabilidade é uma fraqueza nas aplicações e programas informáticos que pode ser aproveitada por alguém mal intencionado.

Na história dos Três Porquinhos as casas de palha e de gravetos são vulneráveis ao Lobo pela sua má construção.



X de XSS

O XSS (em inglês: *cross site scripting*) é um tipo de vulnerabilidade que permite a um atacante alterar a informação que está a ser vista no navegador de um utilizador, sem que este se aperceba.

Z de Zero

Uma vulnerabilidade “dia Zero” (em inglês: *zero day)* é um problema de segurança nas aplicações e programas informáticos que sabemos que existe mas ainda não tem solução.

Agora que já sabes o ABC de AppSec já estás no caminho certo para seres um super-herói da segurança.

Apoiado por:

Texto original por Caroline Wong

Ilustrações por Mike Smith

Direção Artística por Julie Kuhrt

Editado por Chris Tilton

Adaptado para português por AP2SI