**Universidade Tecnológica Federal do Paraná**
**Departamento Acadêmico de Informática**
**Curso de Tecnologia em Sistemas para Internet**

**Sandra Maria de Souza Bertoli**

# GUIA DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS: HARDWARE, SOFTWARE E COMPORTAMENTO

**Trabalho de Conclusão do Curso**

**Curitiba**
**2014**

**Sandra Maria de Souza Bertoli**

# GUIA DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS: HARDWARE, SOFTWARE E COMPORTAMENTO

Trabalho de Conclusão do Curso de Tecnologia em Sistemas para Internet, apresentado à Universidade Tecnológica Federal de Paraná como requisito parcial para obtenção do título de Tecnólogo em Sistemas para Internet.

**Orientador**: Prof. Dr. Carlos A. Maziero

**Curitiba**
**2014**

## RESUMO

Esta publicação apresenta boas práticas em segurança da informação, a qualquer pessoa que interaja de alguma forma com dispositivos móveis, desde profissionais de informática envolvidos com segurança de informações até usuários e empresários preocupados em proteger o patrimônio, os investimentos e os negócios de sua organização. O trabalho se refere especificamente a sistemas móveis, seus conceitos e peculiaridades, mas pode auxiliar na segurança contra ameaças intencionais às informações e recursos de qualquer sistema computacional.

BERTOLI, Sandra Maria de Souza. Guia de Segurança para Dispositivos Móveis: Hardware, Software e Comportamento. 2014. XX f. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Sistemas para Internet). Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

**Palavras-Chave:** dispositivos móveis, hardware, software, malware, hacker.

## ABSTRACT

This text presents good pratice of information security, to anyone who interacts in any form with a mobile device, from IT professionals involved with information security to users and entrepreneurs interested in protect their property, investments and organization business. This work specifically refers to mobile devices, their concepts and peculiarities, but can aid in safety against intentional threats to the information and resources of any operating system.

BERTOLI, Sandra Maria de Souza. Guia de Segurança para Dispositivos Móveis: Hardware, Software e Comportamento. 2014. XX f. Trabalho de Conclusão de Curso (Graduação em Tecnologia em Sistemas para Internet). Universidade Tecnológica Federal do Paraná. Curitiba, 2014.

**Key Words:** dispositivos móveis, hardware, software, malware, hacker.

# SUMÁRIO

# 1 INTRODUÇÃO

Atualmente a utilização dos dispositivos móveis *smartphones* e *tablets* cresce nos mais variados âmbitos: pessoais, governamentais e corporativos. A segurança na utilização destes tornou-se imprescindível para o efetivo aproveitamento de todos os benefícios da tecnologia e manutenção da integridade dos dados e informações que trafegam pela Internet. Entretanto, a segurança não deve restringir as potenciais funcionalidades.

Segundo o antropólogo Roderto DaMatta a adoção de novas Tecnologias de Informação e Comunicação (TICs) tem provocado mudanças profundas na sociedade, a ponto de causar impactos significativos no processo de desenvolvimento socioeconômico de nações, organizações e indivíduos.

Por outro lado as empresas que estão diretamente ligadas a estes ramos têm se dedicado a produzir produtos diferenciados que se destaquem para o usuário e superem qualquer lacuna existente em produtos anteriores.

A sociedade usufrui da tecnologia e ao mesmo tempo exige que ela acompanhe o curso das mudanças em direção à maior dependência de tecnologia do ser humano. A evolução dos costumes que vivenciamos resulta da evolução tecnológica dos dispositivos móveis, principalmente *smartphones* e *tablets,* com grande poder de processamento e conectividade.

Apesar do número de dispositivos móveis estar em crescimento, os investimentos em segurança para este segmento não acompanham a curva de vendas. A questão torna-se ainda mais alarmante se considerarmos o crescimento de número de softwares maliciosos infiltrados de forma ilícita, conhecidos como *malwares*, em dispositivos móveis em 135% em 2013, segundo o relatório de tendências de

Tecnologia da Informação realizado pela Kaspersky Lab divulgado em janeiro se 2014. O relatório aponta ainda que o Android é alvo de 99% dos ataques, por sua predominância no mercado de dispositivos móveis.

Cabe ao projeto GUIA DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS: HARDWARE, SOFTWARE E COMPORTAMENTO analisar novas algumas tecnologias disponíveis de hardware e software para *smartphones* e *tablets* com suas funcionalidades e vulnerabilidades, abordando novas técnicas e ferramentas de segurança, considerando a acessibilidade a dados e informações a qualquer tempo e lugar, resultando em um guia para utilização por profissionais da área da tecnologia de informação e leigos.

A motivação para este projeto surge da ampla utilização destes dispositivos por toda a sociedade, seja para uso particular, exemplo das redes sociais, como para fins empresariais, devido à aproximação entre escritórios e departamentos físicos de ambientes corporativos e seus colaboradores em qualquer parte do mundo.

As possibilidades da tecnologia citada criam um movimento de informações e ações que ultrapassam limites físicos e temporais, tornando-se primordial a atenção para a segurança.

Partindo do pressuposto de que a segurança depende igualmente da tecnologia e do usuário, trataremos também do comportamento seguro na operação destas ferramentas.

O trabalho será desenvolvido com embasamento técnico relevante quanto a sistema operacional, rede, hardware e software para desenvolvedores, conhecedores e estudiosos da área da tecnologia de informação e leigos, considerando questões comportamentais para o adequado uso dos dispositivos e tecnologias envolvidas neste conceito.

O assunto será tratado considerando:

- Tipo de dispositivo: *smartphone* e *tablet*;

- Tipo de sistema operacional: iOS e Android;
- Hardware: recursos utilizados para otimizar o poder de poder de processamento, memória e gerenciamento de energia;
- Software: a utilização de aplicativos abertos ou proprietários e de ferramentas de segurança;
- Tipo de rede wireless: EDGE, 3G, 4G, Bluetooth;
- Tipo de atividade: pessoal ou corporativa;
- Vulnerabilidade física do dispositivo: discorrendo sobre as formas de segurança oferecidas por senhas fortes, criptografia, certificação digital, e backup.

O objetivo específico do projeto é criar um guia de orientação sobre os aspectos relacionados à segurança de dispositivos móveis, sugerindo uma política de segurança para os usuários, levando em consideração os seguintes aspetos:

- Evolução histórica dos dispositivos móveis;
- Mecanismos de defesa a ataques cibernéticos.

Este trabalho está dividido em 8 capítulos; o capítulo 2 define os dispositivos móveis de forma a salientar suas peculiaridades; o capitulo 3 conceitua os sistemas operacionais para dispositivos móveis; o capítulo 4 descreve o hardware dos *smartphones* e *tablets*; o capítulo 5 discorre sobre os tipos de rede sem fio (wireless) e protocolos de segurança; no capítulo 6 discorre sobre o ecossistema em que estão inseridos os dispositivos móveis seus produtos; no capítulo 7 são relacionados os principais riscos de ataques, seus tipos e formas de segurança; finalmente o capítulo 8 são relacionadas sugestões de atitudes de segurança a serem adotadas para usuários e empresas.

# 2 OS DISPOSITIVOS MÓVEIS

A mobilidade computacional foi definida por Reza B´Far [REZA B´FAR, 2005] como sistemas computacionais que podem facilmente ser movidos fisicamente ou cujas capacidades podem ser utilizadas enquanto eles estão sendo movidos. Sendo assim, eles normalmente oferecem recursos e características não encontradas em sistemas comuns como:

- Monitoramento do nível de energia e prevenção de perda de dados em caso de pane de energia;
- Armazenamento de dados local e/ou remoto, através de conexão com ou sem fio;
- Sincronização de dados com outros sistemas;

Dispositivo móvel, chamado em inglês de *handheld*, é um computador de dimensões pequenas, equipados com uma pequena tela *(output)* e um teclado em miniatura (*input*). Em alguns aparelhos o *output* e o *input* estão combinados em uma tela tátil (*touchscreen*).

Neste conceito se enquadram os *palmtops*, celulares, *smartphones*, *tablets* e similares, excluindo os notebooks pela necessidade de abrir o equipamento, aguardar carregamento e sua dependência em estabilidade e energia para funcionamento.

A crescente utilização de *smartphones* e *tablets* e a consequente diminuição dos celulares convencionais e computadores desktop estão provocando consideráveis mudanças na sociedade.

Segundo Carlos Américo Perazolo Yamakawa [YAMAKAWA, 2012], algumas vantagens na utilização de dispositivos móveis podem ser mencionadas:

- Reduzir custos de comunicação, já que todas as informações podem estar acessíveis no dispositivo ou sistema;
- Reduzir custos de entrada e processamento de dados, já que as informações poderão ser escritas num formato digital, podendo ser transmitidas para outros dispositivos ou sistemas;
- Otimizar o tempo, já que o sistema poderá enviar e receber informações remotamente, dispensando seu deslocamento para outros locais para receber tais dados;
- Aumentar o faturamento, pois a maior disponibilidade de informações nos momentos de negociação trará resultado mais eficiente.

Uma pesquisa conduzida pela IDC [Internaional Data Corporation, 2011] demonstrou que tem crescido o número de profissionais que utilizam seus dispositivos móveis pessoais para acessar informações relacionadas ao trabalho. No Brasil, por exemplo, 75% dos profissionais que dependem de tecnologia em sua rotina utilizam seus *smartphones* para trabalhar. Outro estudo, realizado pela Proofpoint, mostrou que 84% das companhias aceitam o uso de dispositivos móveis pessoais no ambiente de trabalho. Seguindo esta lógica, cada vez número maior de empresas disponibilizam equipamentos para seus colaboradores, visando otimizar, facilitar e incrementar as transações e troca de informações organizacionais. Os dispositivos móveis passaram a fazer parte do cotidiano das empresas, trazendo diversas vantagens e desvantagens ligadas a esse cenário.

A mobilidade e a liberdade proporcionadas pela tecnologia móvel conferem ao seu usuário maior agilidade, porém pode acarretar maior insegurança pela possibilidade do acesso de conteúdo em qualquer lugar, a qualquer hora além de perda de arquivos. A troca de dados importantes por meio de dispositivos móveis ainda é feita com insegurança, já que os aparelhos são suscetíveis a ataques maliciosos, principalmente quando se trata de um dispositivo de uso também pessoal, sem o controle da empresa e, consequentemente, muito mais vulnerável.

O conceito atual de *smartphone* e *tablet* deve-se sobretudo a evolução tecnológica que ocorreu ao longo dos últimos anos em termos de hardware e software, que permitiu produzir produtos verdadeiramente diferenciados e de destaque no mercado.

Os *smartphones* e *tablets* possibilitam que as pessoas, principalmente jovens e executivos acessem suas informações pessoas e a Internet com maior velocidade e em aparelhos menores, mas com funções semelhantes a um computador.

## 2.1 *Smartphone*

O *smartphone* pode ser definido como um telefone móvel com tecnologias avançadas, incluindo processadores semelhantes aos utilizados nos computadores pessoais, comumente chamados de PC ou Desktop. Esta característica possibilita e execução de um sistema operacional completo associado a diversos outros recursos para diferentes atividades.

Características de um *smartphone:*

- Permitir a instalação de aplicativos.
- Comunicar-se com o PC, seja via USB ou Bluetooth.
- Comunicar-se a Web via GPRS, EDGE ou UMTS (3G).
- Tocar MP3, exibir vídeos e rodar jogos.

Outra denominação frequentemente usada é *feature phone* que permite enquadrar aparelhos intermediários, como os aparelhos NOKIA baseados no S40, os quais permitem a instalação de alguns programas adicionais e incluem micro-navegadores, mas não chegam a ser considerados *smartphones.*

Os principais recursos disponíveis dos *smartphones* são:

- Sistema Operacional: Programa ou conjunto de programas responsável pelo gerenciamento de recursos do sistema.

- Recursos de conectividade: Utilizados para acessar redes wireless como 3G, 4G e Bluetooth.
- Recursos Multimídia: Utilizados para reproduzir arquivos de música e vídeo em diversos formatos.
- Câmera: Utilizado para tirar fotos e gravar vídeos.
- *Global Positioning System (GPS).*
- Jogos.
- Acesso a *e-mail*.
- Acelerômetro: Dispositivo transdutor detector de movimento ou rotação, capaz de responder a um impulso elétrico para uma perturbação induzida pela aplicação de uma força ou gravidade.
- Tela *touchscreen*: Utilizado para os mesmos propósitos de um teclado, através de toques na tela. Popularizado pelo iPhone da Apple e presente na maioria dos s*martphones* do mercado.
- Suporte a aplicativos: A possibilidade de instalação de aplicativos proporciona ao *smartphone* o funcionamento semelhante ao um PC. As lojas *online* dos fabricantes fornecem os aplicativos para *download.* No caso do iPhone a App Store, e do Android o Google Play*,* antigo Android Market.

Os *smartphones* possibilitam que qualquer pessoa possa desenvolver programas, os chamados aplicativos ou *apps*, dos mais variados tipos e para os mais variados objetivos. Um *smartphone* possui características de computadores, como hardware e software, pois são capazes de conectar redes de dados para acesso à Internet, sincronizar dados como um computador, além da agenda de contatos.

## 2.2 *Tablet*

*Tablet* é um tipo de computador portátil, de tamanho pequeno, com fina espessura, em formato de prancheta que pode ser usado para acesso à Internet,

organização pessoal, visualização de fotos e vídeos, leitura de livros, jornais e revistas e entretenimento com jogos.

Trata-se de um novo conceito, não podendo ser igualado a um computador completo ou um *smartphone*, embora possua funcionalidades de ambos.

É um dispositivo prático, para uso semelhante a um computador portátil convencional, porém usado mais comumente para fins de entretenimento, mas com grande avanço para uso profissional. Possui como dispositivo de entrada principal uma tela sensível ao toque denominada *touchscreen* manuseada com a ponta dos dedos ou caneta.

Algumas das vantagens de um *tablet* comparado aos computadores portáteis:

- Maior duração da bateria;
- Dispensa utilização de teclado ou *mouse*;
- Rapidez e simplicidade na visualização de imagens e outros conteúdos.

Algumas das desvantagens são o elevado preço e algum desconforto para escrever no teclado integrado.

Tornou-se bastante popular após o lançamento do iPad produzido pela empresa Apple Inc. em 2010, muito embora seu conceito seja anterior, trazendo recursos do já popularizado iPhone. Outros concorrentes são o Samsung Galaxy Tab, Motorola Xoom, HP TouchPad, Sony Tablet, etc.

Neste capítulo forma apresentados os principais conceitos relacionados a dispositivos móveis, com seus tipos, peculiaridades, vantagens e desvantagens.

# 3 SISTEMAS OPERACIONAIS

Um sistema operacional é uma coleção de programas que inicializam o hardware do computador, fornecendo rotinas básicas para controle de dispositivos além de gerência, escalonamento e interação de tarefas, sempre mantendo a integridade do sistema.

Existem diversos sistemas operacionais para *smarphones* e *tablets*: Symbian, Blackberry, Windows Mobile, Android e outros. Inclusive, grandes empresas de produtos de e para computadores, como a Apple e a Microsoft estão investindo nos *smartphones*.

As marcas mais conhecidas são o iPhone da Apple, Blackberry da Research In Motion Limited (RIM) e o Android da Google.

## 3.1 Porque da Escolha de Android e iOS

Pesquisas e observações de mercado revelam que quando o assunto é o mundo dos portáteis, especialmente *smartphones* e *tablets*, Google e Apple são os principais atores do cenário. Alguns dos mais comentados produtos de ambas as companhias são, respectivamente, Android e iOS. Esta tendência se confirma desde o lançamento das primeiras versões dos respectivos produtos, com a diferença de que anteriormente o iOS era o mais popular por ser pioneiro no conceito.

Sendo assim, não seria realista falar sobre sistemas operacionais de dispositivos móveis sem focar nestes produtos.

O Android tem alta aceitação por não ser um sistema exclusivo e estar presente em centenas de modelos, facilitando a popularização do sistema.

No entanto, a Apple tem também alta aceitação por ser bem negociado para indústria de equipamentos.

O Android está presente em uma gama maior de dispositivos, como aparelhos da Samsung, Motorola, LG, HTC e diversas outras marcas, assim como o Windows Phone 8 que aparece em mais de uma aparelho como o Nokia, HTC e a própria Samsung, porém em menor proporção que o Android.

O iOS só aparece em aparelhos da própria Apple, porém com gama maior de ferramentas ou serviços específicos para dispositivos móveis, conhecidos como *gadgets*.

Os dispositivos Android lideram na categoria de *smartphones* e *tablets* no Brasil, possivelmente por permitirem maior liberdade e flexibilidade aos usuários, permitindo a personalização muito maior do o iOS.

O sistema da Apple foi projetado para evitar maiores problemas de desempenho dos aplicativos, pois foi desenhado para preservar a vida útil da bateria dos aparelhos.

Segundo o Kantar World Panel, até pouco tempo a Apple possuía a hegemonia do mercado nos Estados Unidos presente em 47% dos aparelhos adquiridos, contra 45% do sistema operacional da Google, porém em 2103 já assumiu a liderança do mercado com 51% contra 43% do iOS, e continua abrindo grande vantagem.

O Windows Phone também apresenta tendência de crescimento, com apenas 2,7% do mercado de 2012, passando para 4,1% em 2013.

O Blackberry detinha 3,6% do mercado e em 2013 chega aos 0,7% e está apenas nos aparelhos Blackberry da Research in Motion ( RIM).

O Symbian, que já foi o grande nome da Nokia, hoje conta com apenas 0,1% do mercado, ainda sendo utilizado apenas neste fabricante. Os outros sistemas operacionais juntos não somam mais de 0,4% de utilização nos dispositivos móveis fabricados atualmente.

A Tabela 1 mostra a participação no mercado dos sistemas operacionais mais utilizados entre 2012 e 2013.

| | 3 mo. ending Feb 12 | 3 mo. ending Feb 13 |
|---|---|---|
| U.S MARKET | *100%* | *100%* |
| iOS | 47.0 | 43.5 |
| Android | 45.4 | 51.2 |
| RIM | 3.6 | 0.7 |
| Windows | 2.7 | 4.1 |
| Symbian | 0.5 | 0.1 |
| Other | 0.8 | 0.4 |

**Tabela 1: Comparativo Sistemas Operacionais 2012/2013**

## 3.2 iOS

O iOS, originalmente chamado iPhone OS, lançado em 29 de junho de 2007, é o sistema operacional desenvolvido pela Apple Inc. para o iPhone e também usado no iPod touch, iPad e Apple TV. É utilizado exclusivamente em produtos Apple. As atualizações, pacotes de segurança, aplicativos melhoria e novas funcionalidades são distribuídos através da loja virtual iTunes.

A interface do usuário é baseada no conceito manipulação direta com movimentos de toque na tela, deslize do dedo e o movimento de pinça utilizado para se ampliar e reduzir a imagem.

Inicialmente as aplicações desenvolvidas por terceiros não eram permitidas sob o argumento do criador Steve Jobs de que os desenvolvedores poderiam criar aplicativos web que se comportassem como aplicações nativas no iPhone.

A versão iOS 6, foi lançada em 11 de junho de 2012 e oferece 200 novas funcionalidades, entre elas a nova aplicação de mapas totalmente independente da Google, seu concorrente direto em vário aspectos, e com navegação *turn-by-turn* (sistema de navegação de GPS orientada por voz).

O sistema operacional iOS é derivado do Mac OS X que por sua vez é baseado em Unix (que serviu de base para o Linux), portanto os dois tem uma certa semelhança conceitual, porém o iOS não é um sistema baseado em Linux e sim o Android.

O iOS consiste em quatro camadas de abstração: a camada Core OS, a camada Core Services, a camada mídia, e a camada Cocoa Touch. O sistema operacional usa aproximadamente 960 MB de armazenamento do dispositivo, que varia para cada modelo.

Em computação, multitarefa é a característica dos sistemas operacionais que permite repartir a utilização do processador entre várias tarefas aparentemente simultaneamente. No iOS o contexto da aplicação é salvo e temporariamente inabilitado, enquanto outra tarefa é processada. Isto faz com que o processo seja temporariamente bloqueado e retomado quando se retorna a ele. Desta forma, o uso da bateria é otimizado, sendo portanto um grande benefício quando se fala em mobilidade e poder de processamento. Porém esta característica deixou iPhones e iPads sempre com hardwares um pouco mais fracos que os concorrentes Android.

O iOS da Apple apresenta-se como altamente fluído, sendo que muito desta experiência deve-se ao fato da multitarefa ser quase inexistente nos aparelhos saídos de fábrica, sem uso da quebra de segurança dos dispositivos nativos, conhecido como *jailbreak.*

*Jailbreak* é um método desenvolvido por *hackers* para desbloquear funções de qualquer dispositivo com restrições de acesso, principalmente o iPhone. Os desenvolvedores especializados em quebra de segurança (*hackers*) instalam aplicativos não oficiais e o utilizam na operadora de telefonia de qualquer, assim o usuário não restringe seu uso apenas a loja oficial de aplicativos, e pode utilizar outros instaladores e habilitar não contidas no sistema operacional original.

A função principal do *jailbreak* é dar liberdade ao usuário e dono do aparelho de utilizá-lo como quiser, mas é uma prática ilegal, pois viola os direitos intelectuais do autor do sistema operacional, além de poder danificar o aparelho. Porém, algumas

organizações afirmam que se o usuário modifica o seu aparelho, não há nada de ilegal nisso, pois o aparelho pertence a quem o comprou.

Além de oferecer liberdade, esta atitude pode acarretar problemas de segurança, como *malwares*, raros no sistema operacional iOS.

A figura 1 mostra a aparência de cada versão do iOS. A versão atual foi lançada em setembro de 2013.


**Figura 1: Versões iOS**

O SO permite ter vários usuários cadastrados, mas somente dois são utilizados: administrador e um usuário convencional.

## 3.3 ANDROID

O sistema operacional Android foi desenvolvido pela Android Inc, uma pequena empresa de Palo Alto (California – USA) de desenvolvimento de plataforma para celulares baseado em Linux, adquirida pela Google em agosto de 2005, com o objetivo de ser flexível, aberta e de fácil migração para os fabricantes.

O Android foi impulsionado pela Google para ser operado nos seus próprios dispositivos móveis e, desta forma, concorrer com outros sistemas operacionais dominantes como o Symbian (dispositivos Nokia), iOS (dispositivos Apple, como iPhone) e Blackberry OS.

Em dezembro de 2006, a Google anunciou o sistema operacional Android como uma plataforma e a criação da Open Handset Aliance (OHA) , conselho com mais de 33 empresas parceiras.

O sistema Android permite a integração dos serviços Google a partir de uma conta Google do usuário e disponibiliza seus aplicativos gratuitamente na loja Google Play.

O primeiro celular a executar o sistema Android foi o T-Mobile G1 (HTC Dream), fabricado pela Google, juntamente com a HTC, em 2008.

Em 2010, a empresa Google, em parceria com a Samsung, lançou a série Nexus, com os modelos Nexus One, Nexus S e Galaxy Nexus.

Android é um sistema operacional que funciona sobre o núcleo Linux e permite aos desenvolvedores escreverem software na linguagem de programação Java controlando o dispositivo via bibliotecas desenvolvidas pela Google. Com o lançamento do SDK, características e especificações são distribuídas após atualizações.

A plataforma é adaptada para dispositivos VGA maiores e os layouts mais tradicionais dos *smartphones.*

O Android suporta grande variedade de tecnologias de conectividade, incluindo Bluetooth, EDGE, 3G, 4G e Wi-Fi.

O Android permite desenvolvimento e execução de programas para dispositivos móveis robusto de fácil utilização.

A infraestrutura é formada por:

- Sistema Operacional baseado em Linux.

- Conjunto de bibliotecas (API) Android Runtime.
- Aplicações pré-existentes e aplicações diversas.

A aplicação Android cria uma instância da Maquina Virtual Dalvik, onde são executados os arquivos, o que requer pouca memória. A Maquina Virtual Dalvik é uma maquina virtual desenvolvida para uso em dispositivos móveis, o que permite que programas sejam distribuídos em formato binário (bytecode) e possam ser executados em qualquer dispositivo Android, independentemente do processador utilizado. Apesar das aplicações Android serem escritas na linguagem Java, não é uma máquina virtual Java, já que não executa bytecode JVM. O sistema suporta formatos de áudio e vídeo como: MPEG-4, H.264, MP3eAAC.

As versões do sistema operacional Android foram lançadas com nomes de doces ou guloseimas, sendo a mais recente versão KitKat, lançado em setembro de 2013.

A figura 2 mostra as denominações de cada versão do sistema operacional Android.


**Figura 2: Versões do Android**

Neste capítulo foram descritos os dois sistemas operacionais de maior utilização na atualidade.

.

# 4 HARDWARE

Os dispositivos móveis mais recentes possuem capacidade de processamento e de armazenamento semelhantes aos computadores pessoais da década de 1990. Esta evolução ocorreu parcialmente por desenvolvimento do hardware com as características descritas a seguir.

## 4.1 Processamento

Atualmente o grande desafio das indústrias de *smartphones* e *tablets* é o paradigma entre o desempenho e a autonomia do aparelho. O maior poder de processamento pelas indústrias esbarra no consumo de energia, limitando as atividades virtuais nestes tipos de dispositivos. Sendo assim, as indústrias se empenham em construir processadores com alto desempenho, esperando que as baterias ofereçam maior autonomia aos novos equipamentos que surgem a cada temporada. As tecnologias avançam e trazem na esteira necessidades muitas vezes inimagináveis

O ritmo de mercado de dispositivos portáteis exige um grande empenho das indústrias de processadores no desenvolvimento de equipamentos mais eficazes e poderosos. As indústrias de geradores de energia (baterias) não têm obtido resultados expressivos na busca de autonomia destes aparelhos.

A capacidade multitarefa implica em maior processamento e uso de memória RAM, mas apresenta como vantagem o fato do usuário poder deixar tarefas sendo executadas em segundo plano enquanto faz outras.

A arquitetura *Advanced RISC Machine* (ARM) de processamento, tecnologia existente desde e década de 80, é atualmente voltada para dispositivos móveis. Muito usada na indústria e na informática, foi desenvolvida visando obter o melhor desempenho possível, com a limitação de ser simples, ocupar pouca área e ter baixo

consumo de energia. É uma arquitetura de processador de 32 bits muito conhecida por sua versatilidade, pois possuem poucas instruções de programação. Usada primeiramente em sistema embarcados é atualmente voltada para dispositivos móveis.

Processadores de dispositivos móveis:

- INTEL: desenvolvimento de processadores para smartphones e outros dispositivos.
- AMD: Atualmente produz processadores gráficos para o mercado de vídeo games.

## 4.2 Hardware do *Smartphone*

Com a evolução das Tecnologias de Informação e Comunicação, os celulares passaram a incorporar funções de outros dispositivos, tornando-se cada vez mais difundidos e utilizados, revolucionando as relações sociais e profissionais.

A possibilidade de acesso a informações remotamente não exige o deslocamento do usuário a um ponto fixo para acesso à Internet. Os dispositivos móveis suprem praticamente todas as necessidade de acesso a informações com mobilidade oferecida antes pelos *desktops* ou *PCs.*

Mesmo os aparelhos mais simples vendidos atualmente utilizam processadores ARM de 300 a 400 MHz e 64 MB ou mais de memória RAM, além da memória flash usada para armazenamento. Ou seja, possuem um poder de processamento superior ao de muitos *PCs* do final da década de 1990.

Com tamanho poder de processamento naturalmente passaram a assimilar funções antes executadas agendas eletrônicas, câmeras digitais, mp3player e GPS.

As restrições com relação ao tamanho e ao consumo fizeram com que o hardware dos *smartphones* evoluísse diferentemente dos *PCs*, com uso de processadores de baixo consumo e chips altamente integrados.

Os chips x86 deram lugar aos processadores RISC de 32 bits, que apresentam uma arquitetura extremamente otimizada, com poucos transistores e consumo elétrico muito baixo.

Os processadores ARM são utilizados em todo tipo de dispositivos eletrônicos, como roteadores, modens ADSL e vídeo games.

Outra característica dos *smartphones* é a integração dos componentes, acompanhada pelo uso de controladores dedicados para diversas funções, diferente do PC onde tudo é feito pelo processador principal. Os controladores dedicados executam suas funções diretamente via hardware, ao invés de via software. Assim as tarefas são executadas com menos transistores e menos ciclos de processamento, o que se traduz em um consumo elétrico mais baixo. Os smartphones atuais possuem diversos destes controladores que ficam desligados a maior parte do tempo e são requisitados para tarefas específicas, como mostra a figura 3.

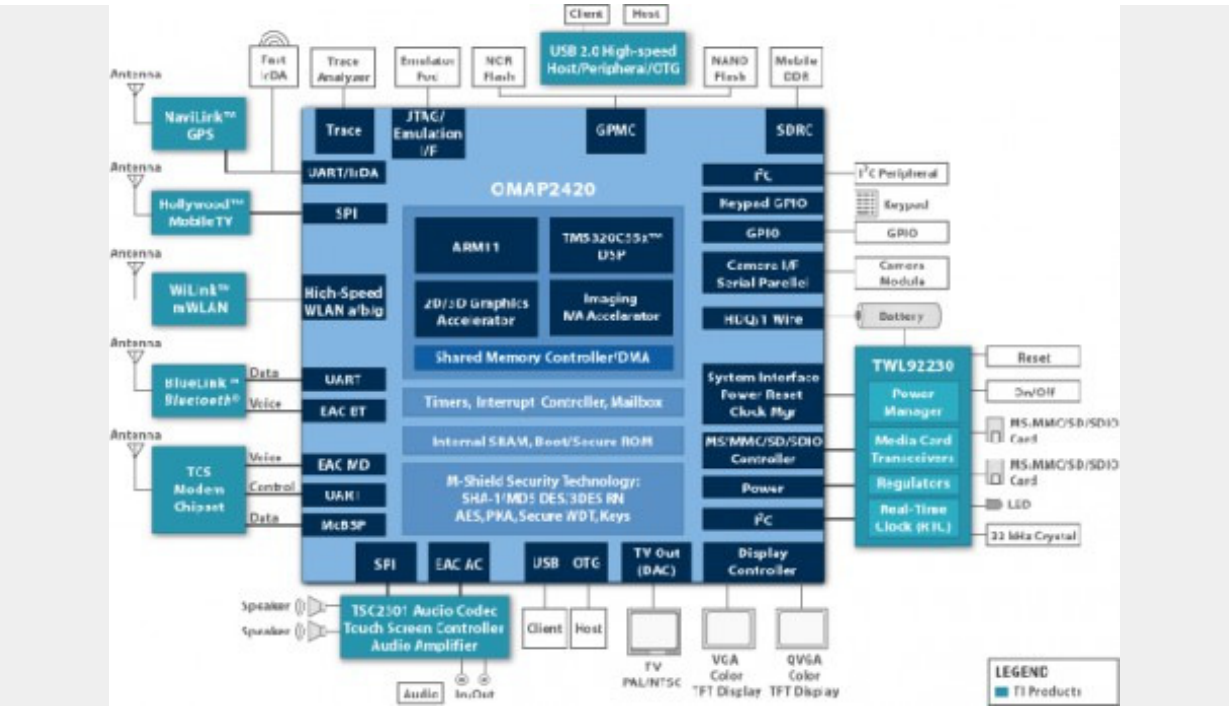


**Figura 3: Diagrama de blocos de um smartphone**

## 4.3 Hardware do *Tablet*

O diagrama de blocos da figura 4 representa a arquitetura convencional de um tablet, como podemos verificar este está dividido em seis núcleos fundamentais que são o processador de aplicações, o núcleo de áudio, núcleo de conectividade, núcleo com os sensores, núcleo do display e o núcleo da gestão de energia

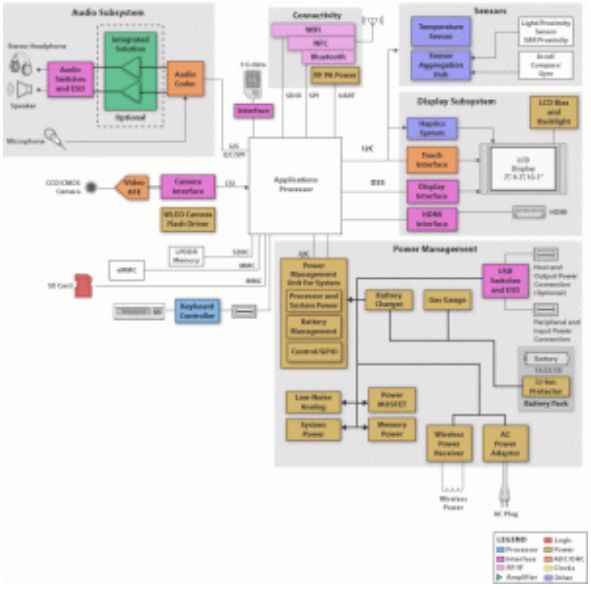

**Figura 4: Diagrama de Blocos do Tablet**

O núcleo do processador de aplicações tem como função a gestão de todas as aplicações que estão a correr no dispositivo, assim como das interfaces de áudio e vídeo.

O núcleo da conectividade proporciona a comunicação do dispositivo com outros dispositivos e com a internet. É composto por uma placa Wi-Fi que permite a ligação à Local Area Network, por um dispositivo Bluetooth para ligação à Personal Area Network e um dispositivo Near Field Communication que permite comunicações via rádio através da tecnologia RFID. Alguns tablets utilizam a tecnologia 3G, que permite uma grande largura de banda para transmissão de dados a longas distâncias.

O núcleo do Display é responsável por todos os elementos que compõem o ecrã do dispositivo, a porta HDMI faz parte desses elementos quando vem integrada no dispositivo. Um dos elementos mais importantes dos tablets é o controlador de touch screen, uma vez que proporciona a funcionalidade de multi-touch ao dispositivo. Os sensores de luminosidade são essenciais para que exista uma constante percepção da luz ambiente, fazendo com que os níveis de luminosidade do ecrã baixe para os mínimos quando assim que seja possível e desta forma há uma optimização do consumo da bateria do tablet.

Os *codecs* de áudio utilizados pela maioria dos tablets são de baixa potência, integram headphone estéreo e *speakers* de class-D para prolongar a vida da bateria. Conseguem alcançar um alto processamento de áudio de forma a melhorar a produção e reprodução de voz e música.

O sistema de sensores é composto por elementos que procuram oferecer sensibilidade, rapidez de resposta e algum contexto ao dispositivo. Componentes como o sensor de temperatura, são importantes para detectar uma eventual sobrecarga no processador.

A autonomia de energia dos *tablets* é um aspecto muito importante para todo o sistema, uma vez que um dos principais objetivos do dispositivo é a mobilidade. O utilizador não precisa estar num ponto fixo com o dispositivo ligado à corrente elétrica através de cabo para conseguir tirar total proveito do equipamento. O núcleo de gestão de energia está encarregado, como o próprio nome indica, de gerir os recursos energéticos do dispositivo.

# 5 REDES WIRELESS

Uma rede sem fio ou *Wireless* refere-se a uma passagem de comunicação sem necessidade de uso de cabos, sejam eles telefônicos, coaxiais ou ópticos, por meio de equipamentos de radiofreqüência ou via infravermelho.

Atualmente seu uso mais comum é em redes de computadores, servindo como meio de acesso à Internet.

Sua classificação é baseada na sua área de abrangência:

- WPAN ou Wireless Personal Area Network: rede que possibilita conexão de vários dispositivos em de curta distância, com baixa potência e pequeno custo e baixas taxas de transferência. Os exemplos são redes *Bluetooth* utiilizados para celulares, impressoras, modems e fones de ouvido sem fio, e infravermelho utilizados em controles remoto para televisão e outros aparelhos.

- WLAN ou Wireless Local Area Network: rede local que usa ondas de rádio para fazer uma conexão Internet ou entre redes, ao contrário da rede fixa ADSL ou conexão TV, que geralmente usa cabos. Serve de opção de conexão nos casos de custo e dificuldade de instalação de cabos para Internet como em edifícios antigos.

- WMAN ou Wireless Metropolitan Area Network: redes com alcance de 4 a 10 Km, o que destina esta tecnologia principalmente a operadoras de telecomunicação. As operadoras de televisão a cabo se utilizam desta rede para oferecer também conexão da Internet.

- WWAN ou Wireless Wide Area Network: redes de longa distância chamadas geograficamente distribuídas, que abrangem países e continentes por

conjuntos de servidores, formando sub-redes com função de transportar os dados entre os computadores ou dispositivos de rede. Os entroncamentos destas redes, chamados *backbones,* se tornaram um mercado promissor para as operadoras de telefonia, principalmente a partir da abertura do mercado brasileiro de telecomunicação, com a oferta da conexão de banda larga para tráfego de voz, dados, imagens e vídeo.

Protocolos de transmissão WAN:

- PPP: protocolo ponto a ponto para acesso à Internet por conxões discadas e dedicadas;
- Rede X.25: arquitetura de rede orientada à conexão para transmissão de dados sobre rede física sujeita a alta taxa de erros;
- Frame Relay: sucessora da X.25 com alta velocidade a maior confiabilidade de transmissão entre nós por meio de cabos ópticos, viabilizando as redes locais. Comumente utilizada por operadoras.
- Rede Asynchronous Transfer Mode (ATM): tecnologia de rede usada para WAN e também para backbones de WLAN, com suporte a transmissão em tempo real de dados de voz e vídeo.
- Digital Subscriber Line (DSL): rede que eprmite tráfego de alta capacidade usando cabo entre o usuário e a central telefônica. Possui 2 modos básicos:

    1. ADSL (Assimetric DSL): compartilha linha de telefone comum usando uma faixa de freqüência de transmissão de voz, com capacidade de transmissão assimétrica, isto é, onde a banda do assinante é projetada para receber maior volume de dados do que pode enviar e utilizada para receber dados da Internet.
    2. HDSL (High-Bit-Rate DSL): a banda do assinante tem a mesma capacidade de envio e recebimento de dados. Serviço mais adequado ao usuário corporativo que disponibiliza dados para outros usuários comuns.

- MPLS (Multi-Protocol Label Switching): mecanismo de transporte de dados caracterizado por inserção de endereço suplementar, o que confere maior velocidade e confiabilidade na transmissão. É normalmente utilizado em empresas de telecomunicações responsáveis por *backbones* que se utilizam de tecnologias avançadas para aumentar sua credibilidade quanto à disponibilidade de seus serviços.

## 5.1 Protocolos de Segurança nas Redes Wireless

A crescente utilização e popularização das redes Wireless, principalmente WLANs, trouxe consigo mobilidade e praticidade, mas também preocupação com a segurança destas. A falta da segurança das conexões wireless é um ponto fraco, por isso protocolos de segurança estão sendo criados, desenvolvidos e atualizados em velocidade cada vez maior.

- WEP (Wired Equivalent Privacy): primeiro protocolo de segurança a ser adotado, utiliza um algoritmo para criptografar os pacotes que estão sendo trocados pela rede na tentativa de garantir confidencialidade e integridade dos dados. Ao final de transmissão é executada função detectora de erros que ao fazer um *checksum* de uma mensagem enviada gera um ICV (Identificador de Circuito Virtual) que deve ser conferido pelo receptor da mensagem, no intuito de verificar se a mensagem recebida foi corrompida e/ou alterada no meio do caminho. Porém vulnerabilidades do método fizeram com que o WEP perdesse credibilidade.

- Chaves de 64 e 128 bits estáticas, sendo 24 bits para o Vetor de Incialização, relativamente pequeno;

- Troca de chaves deve ser feita manualmente;

- Colisão de pacotes, devido à reinicialização do contador do Vetor de Inicialização;
- Autenticação somente do dispositivo.
- WPA (Wi-Fi Protected Access): é o melhoramento do protocolo WEP, com autenticação de usuários, porém utiliza chaves compartilhadas, assim como na WEP. Possui vantagens sobre a WEP:
    1. Resolve todas as falhas do WEP;
    2. Chaves dinâmicas de 128 bits + combinação de sessão de logon;
    3. Distribuição de chaves automática.
    4. Autenticação baseada no usuário, com a utilização da arquitetura 802.1x/EAP.

Ainda assim existem vulnerabilidades no sistema:

- Negação de Serviço: Denial of Service (DoS);
- Algoritmo de combinação de chaves;
- Ataques de dicionário.

## 5.2 Redes EDGE, 3G e 4G

As tecnologias de rede denominadas 3G e 4G estão no centro das atenções de usuários e operadores de telefonia celular. As formas e velocidade de transmissão decorrem da evolução nas últimas décadas.

A migração de uma tecnologia para outra tem sido diversa nos diferentes países de acordo com a economia e evolução tecnológica local.

A tecnologia analógica, utilizada na década de 1980, praticamente apenas para trafego de voz, foi gradativamente sendo substituída pela segunda geração. O sistema mais utilizado nesta época era o AMPS (Advanced Mobile Phone System), que aos poucos deu lugar ao sinal digital, ou 2G.

A partir do início da utilização de sinal digital, convencionou-se utilizar a letra G, em citação à geração tecnológica, para definir o patamar de velocidade, que passaria a ser utilizado também para tráfego de dados. Além de permitir múltiplas conexões sem que uma interferisse na outra, a rede 2G, que ainda é padrão no Brasil, também permitia a troca de dados em pequena escala. O padrão brasileiro de 2G sobrevive para dar suporte à conversação via celular, o que deve perdurar por algum tempo, tendo em vista que oferece estrutura necessária para tal, sem maiores problemas, por utilizar principalmente o GSM (Global System for Mobile Communications). Para internet móvel, no entanto, já está bastante defasado.

Para o tráfego de dados, já foram implantados o que foi chamado de 2,5G e 2,75G, padrões de transição para a tecnologia 3G. O 2,5G equivale ao GPRS (*General packet radio service*) e oferece velocidades de até 114 kbps. Já o 2,75G é uma ligeira evolução que utiliza o padrão EDGE (*Enhanced Data rates for GSM Evolution*), que prevê uma média de velocidade de tráfego de 400 Kbps.

A maioria dos usuários de Internet móvel se encontra hoje na tecnologia 3G, inclusive no Brasil. A rede de terceira geração usa principalmente as tecnologias WCDMA ou CDMA e oferece velocidades mínimas de 200 kbps, segundo padrão do IMT-2000,mas promete velocidade muito superior.

A operadoras de celular no Brasil estão se preparando para a implantação da tecnologia 4G até 2014. A quarta geração da Internet móvel promete revolucionar a velocidade de tráfego de dados no país e utiliza a tecnologia LTE, que está sendo implantado na frequencia de 2,5 GHz, mas deve ser ampliada para a de 700 MHz. A tecnologia prevê tráfego de dados em até 100 Mbps.

## 5.3 Bluetooth

O Bluetooth é uma tecnologia de comunicação que oferece uma maneira simples de realizar a comunicação de diversos dispositivos móveis entre si utilizando o menor consumo de energia possível sem a necessidade de cabos.

O Bluetooth foi construído para facilitar a transmissão de informação dentro de uma faixa relativamente pequena, em torno de 10 metros, e trabalha de forma a reduzir o risco de interferências entre os dispositivos.

Uma característica positiva é que automaticamente controla o processo de comunicação entre dois dispositivos, varrendo a área em volta à busca de outros dispositivos Bluetooth, estabelecendo a conexão entre os descobertos. Uma mensagem é criada informando a existência da rede, denominada piconet que se propaga entre os dispositivos criando a comunicação.

Uma combinação de hardware e software é utilizada para permitir que este procedimento ocorra entre os mais variados tipos de aparelhos. A transmissão de dados é feita por meio de radiofreqüência, dentro de um limite de proximidade.

A tecnologia pode ser bastante interessante e útil, mas também pode ser uma grande ameaça à privacidade de seus usuários apesar de contar com serviços de segurança como autenticação, criptografia, qualidade de serviço e outros recursos. No entanto ainda está vulnerável em vários aspectos, permitindo ataques.

Atualmente os usos mais comuns para Bluetooth são:

- Fone de ouvido para celular sem fio.
- Sincronização de informações entre dispositivos.
- Conectividade de impressora, mouse, teclado a um PC.
- Transferência de arquivos entre dispositivos.

A figura 5 mostra uma das funcionalidades do Bluetooth em equipamentos móveis.


**Figura 5: O relógio Sony SmartWatch se comunica com smartphones Android via Bluetooth.**

Neste capítulo foram conceituadas as redes wireless por onde trafegam os dados na infraestutura necessária para a utilização dos dispositivos móveis.

# 6 *CLOUD COMPUTING* E OS DISPOSITIVOS MÓVEIS

Atualmente a possibilidade de acesso remoto às informações via Web traz novas necessidades de serviços que atendam a diferentes demandas. Diante disso os serviços baseados na Internet para sincronização e compartilhamento de arquivos se fazem cada vez mais presente.

A computação nas nuvens vem oferecendo aplicativos baseados na Web para atender desde o usuário comum, passando por pequenas empresas e chegando a governos e multinacionais.

O conceito de compartilhamento de serviços e arquivos advém da década de 60, porém o termo *Cloud Computing* ou Computação nas Nuvens surgiu quando as empresas de telefonia passaram a oferecer o serviço Virtual Private Network (VPN) mencionado em 1997 por Ramnath Chellappa em uma palestra acadêmica.. A metáfora da nuvem foi utilizada para demarcar o limite de responsabilidades do prestador do serviço e do usuário.

Diversos aplicativos baseados neste conceito já fazem parte do cotidiano da Internet há muito tempo, como por exemplo, os serviços de armazenamento de e-mail GMail, Hotmail e Yahoo. Ao acessar a conta, o usuário visualiza as mensagens armazenadas em um servidor remoto, de qualquer computador, a qualquer hora, em qualquer lugar que possua uma conexão com a Internet. Outro exemplo é o aplicativo Google Docs, onde o usuário pode criar editar e compartilhar planilhas, aplicativos de edição de texto e apresentações, sem ter a necessidade de ter o software instalado no computador ou dispositivo móvel.

Em relação aos dispositivos móveis *smartphones* e *tablets,* a utilização de aplicativos armazenados remotamente otimiza seu funcionamento pelos recursos virtuais de ponta como hardware, plataformas de desenvolvimento e serviços.

## 6.1 Ecossistemas dos Dispositivos Móveis

Em 2013 os telefones celulares ultrapassaram os desktops como dispositivos mais comuns para acesso à web em todo o mundo, segundo pesquisas. Esta tendência surgiu com a grande adesão da plataforma móvel da Apple pelos consumidores, que encantados com a mobilidade, impulsionaram o desenvolvimento de tecnologias móveis.

Contudo, isto não significa o abandono do desktop, apenas que as empresas terão que se adequar para oferecer suporte para que os dispositivos móveis sejam utilizados por profissionais cujas funções exigem mobilidade.

O aumento do poder de processamento e conectividade, aliado a grande variedade de aplicativos e serviços transformou os *smartphones* e *tablets* em alvo principal de ataques de segurança. Em vista disso, a segurança anteriormente centralizada em redes e equipamentos deve se tornar descentralizada e individualizada, de modo a tentar restringir os ataques de softwares maliciosos que vem crescendo juntamente com o uso das tecnologias.

Alexandre Melo Braga, Erick Nogueira do Nascimento, Lucas Rodrigues da Palma e Rafael Pereira Rosa citam três aspectos que devem ser abordados quando se estuda a segurança dos dispositivos móveis [Braga et all; Introdução à Segurança de Dispositivos Móveis Modernos, Um Estudo de Caso em Android, 2012].

O aumento dos softwares maliciosos desde 2011 se tornou o próximo desafio de segurança em relação às TICs, motivado pela proliferação de dispositivos com sistema operacional Android. A Google conquistou uma fatia expressiva no mercado, que vem aumentando gradativamente, devendo se tornar dominante ainda em 2013 em relação às outras plataformas móveis como o iOS, da Apple e o RIM, da BlackBerry.

O surgimento de novas tecnologias primeiramente voltadas para o usuário final e somente depois para segmento corporativo denomina-se consumerização. A adoção e utilização destas tecnologias se tornou intensa nas atividades pessoais a ponto de

alterar os processos corporativos com o fenômeno comportamental chamado BYOD (*Bring Your Own Device*). Assim, os indivíduos passaram a utilizá-los no ambiente corporativo de modo a obrigar as empresas a adotar estas tecnologias e tratar as questões de segurança de forma descentralizada, pela indefinição dos limites de rede e perímetro de segurança nos equipamentos móveis utilizados em atividades tanto pessoais como profissionais.

O terceiro aspecto se refere à ineficácia dos controles de segurança aplicados a redes internas, *desktops* e outros ativos de infraestrutura pelos fenômenos de consumerização e BYOD. A proliferação de softwares maliciosos não se dá por transferências diretas entre dispositivos, mas por meio de lojas virtuais de aplicativos e sites de terceiros potencialmente não confiáveis, tornando estrutura corporativa vulnerável.

Além do ecossistema envolvendo os dispositivos móveis em relação à Internet e *Cloud Computing*, cada empresa criou seu próprio ambiente de forma a conectar suas tecnologias e plataformas.

### 6.1.1 Google

A Google Inc. é uma empresa multinacional de serviços online e software dos Estados Unidos que hospeda e desenvolve uma série de serviços e produtos baseados na Internet, gerando lucro principalmente através de publicidade pelo AdWords. A empresa foi fundada pelos alunos de doutorado da Stanford University Larry Page e Sergei Brin em 1998 com a missão declarada de "organizar a informação mundial e torná-la universalmente acessível e útil".

O rápido crescimento da Google culminou em uma cadeia de produtos, aquisições e parcerias que vão muito além do produto inicial, o sistema de buscas Google executado através de mais de 1 milhão de servidores em *datacenters* ao redor do mundo e processa mais de 1 bilhão de solicitações de pesquisa e 20 petabytes de

dados gerados por usuários todos os dias. A empresa oferece ainda softwares de produtividade online, como software de e-mail Gmail, e ferramentas de redes sociais, inlcuindo o Orkut, o Google+ e o descontinuado Goolgle Buzz. Os produtos se estendem à área de trabalho, com aplicativos como o navegador Google Chrome, o programa de organização e edição de fotografias PICASA e o aplicativo de mensagens instatâneas GTalk. Notavelmente, a Google também lidera o mercado com o desenvolvimento do sistema operacional móvel Android para *smartphones* e *tablets*..

A Google é um apoiante notável da neutralidade da rede. Segundo o Guia da Neutralidade da Rede da Google:

Neutralidade da rede é o princípio de que os usuários da Internet devem estar no controle do conteúdo que eles vêem e de quais aplicações eles usam na internet. A Internet tem operado de acordo com este princípio de neutralidade desde seus primeiros dias... Fundamentalmente, a neutralidade da rede é a igualdade de acesso à Internet. Em nossa opinião, as operadoras de banda larga não devem ser autorizadas a usar seu poder de mercado para discriminar candidatos ou conteúdos concorrentes. Assim como as empresas de telefonia não estão autorizadas a dizer aos consumidores para quem eles devem ligar ou o que eles podem dizer, as operadoras de banda larga não devem ser autorizadas a utilizar seu poder de mercado para controlar a atividade online.

A política de privacidade da empresa é controversa e tem gerado várias contendas judiciais.

Em 2009, o CEO Erich Schmidt declarou após especulações sobre as preocupações com a privacidade dos usuários do Google: "Se você tem algo que você não quer que ninguém saiba, talvez você não devesse estar fazendo isso em primeiro lugar. Se você realmente precisa desse tipo de privacidade, a realidade é que os motores de busca - inclusive o Google - não guardam esta informação há algum tempo e é importante, por exemplo, que todos nós estamos sujeitos nos Estados Unidos ao Patriot Act e é possível que todas as informações que podem estar disponíveis às autoridades." Na conferência Techonomy de 2010 Eric Schmidt previu que "a

verdadeira transparência e sem anonimato" é o caminho a seguir na internet: "Em um mundo de ameaças assíncronas é muito perigoso que não que haja alguma maneira de identificá-lo. Nós precisamos de um serviço de nomes das pessoas. Os governos vão exigir isso."

O Privacy International classificou a Google como "hostil à privacidade", a sua classificação mais baixa em seu relatório, fazendo da Google a única empresa na lista a receber essa classificação.

Durante o período compreendido entre os anos de 2006 e 2010, os carros com câmeras acopladas do Google Street View recolheram cerca de 600 gigabytes de dados de usuários de redes sem fio sem criptografia em empresas públicas e privadas em mais de 30 países. A não divulgação e nem uma política de privacidade foi oferecida para as pessoas afetadas e nem para os proprietários das estações de sem fio. Um representante da Google afirmou que eles não estavam conscientes de suas atividades de coleta de dados privados, até um inquérito de agência reguladora alemã ter sido enviado e que nenhum destes dados foi utilizado no motor de busca da Google ou em outros serviços da empresa. Um representante da Consumer Watchdog respondeu: "Mais uma vez, a Google tem demonstrado uma falta de preocupação com a privacidade." Em um sinal de que as sanções legais podem ter algum resultado, a Google afirmou que não irá destruir os dados até ser permitido pelos reguladores.

### 6.1.2 Apple

A empresa multinacional norte-americana fundada em 1976 por Steve Wozniak, Steve Jobs e Ronald Wayne, projeta e comercializa produtos eletrônicos de consumo, software de computador e computadores pessoais. Entre os produtos mais conhecidos da empresa estão a linha de computadores Mac, seu sistema operacional Mac OSX e a linha iPhone de *smartphones* e IPads de *tablets*, incluindo o sistema operacional para dispositivos móveis iOS.

Por uma variedade de razões, desde sua filosofia de design às suas raízes *indie*, assim como suas campanhas publicitárias, a Apple construiu uma reputação distinta na indústria de informática e eletrônicos e cultivou uma base de consumidores que é devotada de modo incomum à empresa e à sua marca.

Atualmente dirigida por Tim Cook, gerencia seus produtos através da loja virtual App Store.

## 6.2 Plataformas para Distribuição Digital

A Internet no Brasil continua crescendo exponencialmente, principalmente em ambientes móveis. Os usuários encontram na Internet uma fonte inesgotável de informações e conteúdos, bem como um ambiente de convívio através das redes sociais. Os países buscam fortemente desenvolver políticas de massificação da infra-estrutura de acesso à rede em alta velocidade, com o movimento de inclusão digital.

A inclusão digital consolidou a presença de usuários de praticamente todos os perfis sociais e culturais. Desta forma, o mercado virtual obteve espaço para comercialização de produtos e serviços diversos.

Dentro deste conceito, as empresas de tecnologia criaram seus próprios canais para distribuição digital de aplicativos, jogos, músicas, filmes e os mais variados conteúdos através das lojas virtuais, ditando uma nova forma de interação de mercado e pessoal, pois os aplicativos podem ser desenvolvidos por terceiros, criando um novo mercado de desenvolvimento de tecnologia.

Cada empresa determina a sua forma de captação e distribuição dos aplicativos.

Os fabricantes de *smartphones* e *tablets* determinam os sistemas que utilizam. O sucesso ou fracasso dos sistemas operacionais tem sido medido pelo número de

aparelhos vendidos.

A integração dos serviços do desenvolvedor do sistema operacional com o fabricante dos dispositivos torna o produto específico, diferentemente de qualquer aparelho eletrodoméstico ou de uso pessoal.

Por isso, o mercado de tecnologia de dispositivos móveis é único, e com surpresas a cada lançamento, normalmente repletos de suspense e campanhas de marketing.

A empresa que distribui seu sistema operacional para poucos fabricantes, com vendas modestas, será pouca participação no mercado. O conjunto dispositivo-sistema operacional é resultado de transações comerciais, não dando ao usuário total liberdade de escolha em separado.

### 6.2.1 Google Play

Google Play é a loja virtual online da empresa de comunicações Google, com as aplicações totalmente voltadas para o sistema operacional Android. A loja foi criada em 2008 com o nome Android Market.

Os novos dispositivos vêm com o aplicativo Google Play instalado, de onde pode ser acessado todo o conteúdo disponível em caráter gratuito ou mediante pagamento.

Os desenvolvedores interessados em distribuir aplicativos via Google Play devem inscrever-se no Console do Desenvolvedor do Google Play, onde as informações de acesso, privilégios e política de conteúdo. O registro poderá ser realizado após a aceitação do Contrato de Distribuição do Desenvolvedor do Google Play, desde que o desenvolvedor seja morador dos países aceitos e efetue pagamento de US $25.

Sendo a loja ser baseada em *cloud computing*, os projetos são publicados

diretamente para usuários também registrados.

O Google Play tem políticas de privacidade rigorosas para desenvolvedores, além de políticas de conteúdo, oferecendo certo nível de segurança aos usuários. Porém os aplicativos não são analisados antes da publicação, o que difere da loja da Microsoft. No caso de violação dos Termos do Desenvolvedor, aceito no ato do registro, o aplicativo é suspenso.

Os anúncios são parte importante do conteúdo, portanto seguem também normas segundo a classificação de conteúdo.

### 6.2.2 Apple Store

A Apple Store é uma cadeia de lojas de varejo de propriedade e operação da Apple Inc., que comercializa de computadores eletrônicos.

Da mesma forma que a Google Play, a Apple Store aceita aplicativos desenvolvidos por terceiros ou empresas, desde que registrados no iOS Developer Enterprise Program. Equipes podem ser registradas e devem seguir termos aceitos previamente.

Diferentemente da Google, a Apple testa os aplicativos antes da distribuição através da loja online.

Neste capítulo foi apresentado o desenvolvimento das empresas e seus produtos em um mercado incipiente e em constante evolução, dentro de novos conceitos de comunicação, compartilhamento e relações sociais e econômicas.

# 7 SEGURANÇA NOS DISPOSITIVOS MÓVEIS

O crescente uso da tecnologia móvel gerou a necessidade de reavaliação dos conceitos da segurança em sistemas computacionais na vida pessoal e empresarial.

Sendo a informação um diferencial competitivo e um patrimônio pessoal, deve ser considerada como recurso mais crítico e merecedor de atenção de usuários e responsáveis pela gestão das informações nas empresas. Sendo assim, a segurança deixou de ser um item suplementar para qualquer atividade, tornando-o de sobrevivência, principalmente das empresas.

Considera-se informação todo recurso disponível em um sistema, compreendendo registros de banco de dados, arquivos, áreas de memória, portas de entrada/saída, conexões de rede, configurações, além de dados pessoais dos usuários como senhas de bancos, emails e sites, números de cartões de crédito, documentos pessoais, declarações de imposto de renda, endereços, passatempos e interesses diversos, preferências individuais e informações profissionais.

A segurança abordada neste capítulo está relacionada à garantia das propriedades fundamentais destes recursos [STANTON et all, 2003]:

- Confidencialidade: propriedade que limita acesso à informação tão somente às entidades legítimas, ou seja, àquelas autorizadas pelo proprietário da informação;
- Integridade: propriedade que garante que a informação manipulada mantenha todas as características originais estabelecidas, pelo proprietário da informação, incluindo controle de mudanças e garantia do seu ciclo de vida (nascimento, manutenção e destruição);

- Disponibilidade: propriedade que garante que a informação esteja sempre disponível para o uso legítimo, ou seja, por aqueles usuários autorizados pelo proprietário da informação;
- Autenticidade: propriedade que garante que a informação e seus dados associados são verdadeiros e correspondem as informações reais às quais representam, como identidades dos usuários, origem dos dados de um arquivo, etc.;
- Irrefutabilidade: propriedade que garante a autoria da criação e de todas as ações realizadas no sistema.

A responsabilidade primária da segurança dos dados e recursos de um equipamento computacional é do sistema operacional, porém atitudes do usuário podem dirimir o risco de ataques maliciosos.

A casuística de incidentes de segurança demonstra a maior ocorrência de violações em decorrência de:

- Fatores comportamentais do usuário influenciados pela engenharia social;
- Erros de utilização do sistema pelo usuário;
- Erros de desenvolvimento ou utilização de software;
- Ações praticadas por indivíduo sem acesso autorizado com objetivos de uso malicioso ou deletério ao usuário ou ao sistema.

Paralelamente ao impulso na demanda de atividades digitais e produtos tecnológicos, aumentou a prática de ilícitos, tais como obtenção indevida de dados, propagação maliciosa de vírus e diversos tipos de estelionatos.

Com o objetivo de diminuir o nível de insegurança dos dados presentes na rede, torna-se crucial a busca por melhores práticas para prevenir ocorrências indesejáveis de crimes praticados contra empresas e indivíduos por meio de canais tecnológicos.

## 7.1 Ameaças, Ataques e Vulnerabilidades

Qualquer dispositivo, móvel ou não, conectado a uma rede ou Internet, é potencialmente vulnerável a uma ação externa com fins desconhecidos pelo administrador ou usuário do sistema, geralmente com objetivos prejudiciais.

Vulnerabilidade á um fator intrínseco ao sistema que permite a ação de agentes externos influenciando negativamente no seu funcionamento.

Ameaça é um agente ou ação externa, espontâneo ou proposital, que se aproveita da vulnerabilidade de um sistema para conseguir seu intento.

Quando existe simultaneamente a vulnerabilidade e a ameaça, ocorre o que se chama em segurança de informação de risco.

O risco pode ser minimizado corrigindo-se as vulnerabilidades e ameaças com medidas preventivas ao sistema computacional ou atitudes de segurança dos usuários.

Ataque consiste em tentativa de causar dano a ativos valiosos, normalmente tentando explorar uma ou mais vulnerabilidades. Caso o ataque seja bem sucedido, caracteriza-se uma invasão.

São consideradas ameaças de segurança situações que possam comprometer a confidencialidade, integridade e disponibilidade de dados e serviços utilizados pelos usuários da infraestrutura de computação.

As principais ameaças podem ser assim relacionadas:

- Vulnerabilidades frequentes;
- Códigos maliciosos explorando essas vulnerabilidades, em curto espaço de tempo;
- Ferramentas automatizadas de ataque;

- Atacantes e *Spammers*;
- Ataques de força bruta;
- Redes mal configuradas sendo abusadas para realização de todas estas atividades sem o conhecimento dos proprietários dos dados;
- Botnets: usados para envio de *scams*, *phishing*, invasões, DoS, esquemas de extorsão;
- Alvo migrando para usuários finais;
- Fraudes, *scams*, *phishing*;
- Crime organizado com aliciamento de *spammers* e invasores, estimulando economia ilícita;

## 7.2 Tipos de Ameaças

- *Buffer Overflow*: trata-se de uma vulnerabilidade do software causado por falha na programação, resultado do armazenamento de um *buffer* de uma quantidade maior de dados que sua capacidade. A solução mais adequada para evitar este tipo de vulnerabilidade é a utilização pelos programadores de funções de biblioteca de linguagens de programação que não apresentem problemas relacionados a buffer overflow. Exemplos de softwares conhecidamente vuneráveis a *buffer overflow*: Sendmail, módulos do Apache, alguns produtos da Microsoft como Internet Information Servces(IIS) e OpenSSH.
- *Clickjacking*: Podendo ser traduzida como "furto de *click*" é a técnica de informática fraudulenta em que áreas clicáveis são sobrepostas na página para extrair ou injetar dados do usuário. O mau uso de algumas

características das linguagens HTML e CSS combinados com a forma como os browsers interpretam a interação do usuário com os elementos da página podem facilitar este ataque. Para os desenvolvedores a forma de proteção passa da implementação correta de cada linguagem de programação à atualização frequente da própria página. Para os usuários basta a atualização dos browsers e não acesso a websites de procedência desconhecida. É possível também desativar o Javascript para quebrar o ataque, porém a técnica mais utilizada para defender os usuários utiliza a mesma linguagem de programação, ou seja, o usuário estaria desativando sua própria proteção em alguns casos.

- *Race Condition*: Trata-se de uma falha no sistema ou processo em que o resultado do processo depende do gerenciamento de concorrência entre processos teoricamente simultâneos. Processos em execução simultânea dependem de estado compartilhado, e o resultado depende de escalonamento (sequência ou sincronia) de processos. Exemplos: acesso e modificação de sistema de arquivos compartilhado podem acarretar corrupção de dados; conversas em rede (chats) podem ter conflitos de privilégios de operação do canal quando utilizados em servidores diferentes. Uma "condição de corrida" explora a pequena janela de tempo entre um controle de segurança a ser aplicado e quando o serviço é usado.

- *Cross-site scripting* (XSS): É a vulnerabilidade de um sistema encontrada nas aplicações web que ativam ataques maliciosos ao injetarem códigos dentro das páginas acessadas pelo usuário. *Cross-site scripting* usa vulnerabilidades conhecidas em aplicações baseadas na web, seus servidores ou sistemas de plug-ins nos quais eles dependem. Explorando um destes, inserem conteúdo malicioso no conteúdo a ser entregue a partir do site comprometido. Quando o conteúdo combinado resultante chega ao navegador do lado do cliente, tudo tem sido entregue a partir da fonte confiável e, portanto, atua de acordo com as permissões concedidas a esse sistema. Ao encontrar maneiras de injetar scripts maliciosos em páginas

web, um atacante pode obter acesso com privilégios elevados para o conteúdo crítico da página, *cookies* de sessão, e uma variedade de outras informações mantidas pelo navegador em nome do usuário. Sites proeminentes foram afetados no passado incluindo sites de redes sociais Twitter, Facebook, MySpace, YouTube e Orkut. Nos últimos anos falhas de *cross-site scripting* superaram o transbordamento de dados para se tornar a vulnerabilidade de segurança mais comum relatada.

- *Cross-site Request Forgery* (XSRF): A "Falsificação de solicitação entre sites" é um tipo de exploração maliciosa de um website pelo qual comandos não autorizados são transmitidos de um usuário que confia no website. Ao contrário do *cross-site scripting* (XSS), que explora a confiança de um usuário para um site particular, o CSRF explora a confiança que um site tem do navegador do usuário. Ocorrências deste ataque foram registradas em 2008 no site de leilões eBay, quando cerca de 18 milhões de usuários perderam informações pessoais na Coréia do Sul e clientes de um banco no México forma atacados com uma *tag* na imagem do e-mail. O link da *tag* da imagem mudou a entrada DNS para o banco em seu roteador ADSL para apontar para um site malicioso, representando o banco.

- *Denial of Service* (DoS): Os "ataques de negação de serviço" têm por objetivo torná-lo indisponível, diferentemente dos outro tipos de ataque. Pode ser lançado contra qualquer equipamento conectado à Internet, não sendo necessário que sejam serviços com vulnerabilidade de segurança, o que torna a ameaça mais preocupante. O mecanismo de ação é enviar grande volume de requisições, aparentemente válidas, para acesso às páginas hospedadas. Caso o servidor não possua nenhum tipo de filtro ou regra de *firewall* que limite o volume de páginas servidas a um único endereço, ele passará a simplesmente tentar responder a todas as requisições, o que saturará o *link* ou consumirá todos os recursos do servidor, fazendo com que ele deixe de responder a requisições de usuários válidos. O tipo mais famoso de ataque DoS é o DDoS, ou "*Distributed Denial of Service*" (ataque

distribuído de negação de serviço), onde o ataque é lançado usando centenas ou milhares de destinatários (situados em locais diferentes) simultaneamente. Nesse caso, o ataque é especialmente difícil de conter, pois é necessário bloquear as requisições provenientes de cada um dos endereços usados antes que cheguem ao servidor. Ou seja, o bloqueio precisa ser feito pela empresa que administra os links de acesso e não no servidor propriamente dito.

- *Directory Traversal*: Ataque realizado através de manipulação de URL, permitindo que uma aplicação web acesse um arquivo sem verificação e autenticação de usuário.

- *Drive-by download*: Tipo de ataque em que uma página maliciosa induz o usuário a baixar arquivos de forma diferente do padrão, facilitado por configuração insegura do navegador. Este procedimento é realizado de forma lícita pelos *applets* ClickOnce e ActiveX para facilitar o processo de download.

- Elevação de Privilégio: Falhas em componentes importantes do sistema operacional podem permitir leitura de arquivos ou execução de comandos sem autorização adequada. O Windows apresentou esta falha, denominada *shatter*, a qual foi corrigida no sistema operacional Windows Vista.

- Envenenamento do cache DNS: Ataque complexo que consiste em enviar uma resposta falsa para um servidor de DNS, redirecionando a requisição para uma página clonada. O modo de ação é a tradução maliciosa do endereço IP, permitindo que o usuário insira dados e informações sigilosas em páginas falsas. Exemplos do ataque foram percebidos em sites de bancos e no Google AdSense.

- *Man in the Middle* (MITM): Tipo de ataque em que o atacante se infiltra entre a conexão do usuário e o site legítimo acessado, permitindo a leitura ou alteração das informações enviadas pelo usuário.

- *Pharming e drive-by pharming*: Denomina-se *pharming* o redirecionamento de um site em sequência a outro tipo de ataque, normalmente envenenamento de chache DNS ou alteração de arquivos de host da vítima. O ataque *drive-by-pharming* acontece com a utilização de erros de configuração em modens ADSL e roteadores para alterar a configuração de servidores DNS a partir de uma página web por meio de ataques de XSRF e *clickjacking*.

- *Phishing*: *Phising* é uma das principais preocupações de segurança informática que se baseia no envio de um email fraudulento com o objetivo de obter códigos de acesso e dados financeiros. O email pode conter um link direcionando para um formulário onde se requer dados confidenciais ou para uma página contendo programas maliciosos, que se auto-instalam no computador.

- *Remote File Inclusion/Injection* (RFI): Tipo de ataque que indica remotamente arquivos maliciosos para inclusão na montagem da página web pelo servidor.

- *Sniffing*: Monitoramento da rede pelo atacante para captação de dados e informações.

- *Spoof*: O ataque forja endereços MAC, ARP e IP falsos.

- *SQL Injection*: O ataque permite alterar de forma maliciosa os comandos passados ao banco de dados com linguagem SQL.

## 7.3 Recursos de Segurança

### 7.3.1 Controles de Acesso

O controle de acesso físico ou lógico às informações ou dados têm por objetivo proteger equipamentos, aplicativos e arquivos de dados contra perda, modificação ou divulgação não autorizada. Os sistemas computacionais, bem diferentes de outros tipos de recursos, não podem ser facilmente controlados apenas com dispositivos físicos, como cadeados, alarmes ou guardas de segurança.

Os controles de acesso lógicos são um conjunto de procedimentos e medidas com o objetivo de proteger dados, programas e sistemas contra tentativas de acesso não autorizadas feitas por pessoas ou por outros programas de computador.

O controle de acesso lógico pode ser viabilizado de duas formas diferentes:

- A partir do recurso computacional que se quer proteger;
- A partir do usuário a quem serão concedidos privilégios de acesso aos recursos.

A proteção aos recursos computacionais inclui desde aplicativos e arquivos de dados até utilitários e o próprio sistema operacional.

A implantação de controles de acesso tem por objetivo:

- Garantir que apenas usuários autorizados tenham acesso aos recursos;
- Garantir que os usuários tenham acesso apenas aos recursos necessários para a execução de suas tarefas;
- Garantir que o acesso a recursos críticos seja bem monitorado e restrito a poucas pessoas;
- Garantir que os usuários estejam impedidos de executar transações incompatíveis com sua função ou além de suas responsabilidades.

Sendo assim, as funções do controle de acesso podem ser assim definidas:

- Identificação e autenticação de usuários;

- Alocação, gerência e monitoramento de privilégios;
- Limitação, monitoramento e inabilitação de acessos;
- Prevenção de acessos não autorizados.

Recursos do sistema computacional a serem protegidos:

- Aplicativos: O acesso não autorizado ao código fonte dos aplicativos e objeto pode ser usado para alterar suas funções e a lógica do programa, como por exemplo, um aplicativo bancário que pode ser alterado para desvio de valores.
- Arquivos de dados: Bases de dados, arquivos ou transações de bancos de dados devem ser protegidos para evitar que os dados sejam apagados ou alterados sem autorização, como, por exemplo, arquivos com a configuração do sistema, dados da folha de pagamento, dados estratégicos da empresa.
- Utilitários: O acesso a utilitários, como editores, compiladores, softwares de manutenção, monitoração e diagnóstico deve ser restrito, já que essas ferramentas podem ser usadas para alterar aplicativos, arquivos de dados e de configuração do sistema operacional.
- Sistema operacional: O sistema operacional é um alvo muito visado, já que sua configuração é o ponto chave de todo sistema de segurança. A fragilidade do sistema operacional compromete a segurança de todo conjunto de aplicativos, utilitários e arquivos.
- Arquivos de senha: A falta de proteção adequada aos arquivos que armazenam as senhas pode comprometer todo o sistema, pois um usuário não autorizado ao obter o identificador (ID) e senha de um usuário privilegiado, pode, intencionalmente, causar danos ao sistema. Este tipo de ataque dificilmente será detectado por qualquer controle de segurança instalado, já que simula a atividade de um usuário credenciado.
- Arquivos de *log*: Os arquivos de log são usados para registrar ações dos

usuários, constituindo-se em ótimas fontes de informação para auditorias futuras. Os logs registram os acessos aos recursos computacionais, aplicativos, arquivos de dados e utilitários, quando foi feito o acesso e que tipo de operações foram executadas.

### 7.3.2 Políticas de Segurança

A política de segurança de informações é um conjunto de princípios que norteiam a gestão de segurança de informações e deve ser observada pelo corpo técnico e gerencial da organização, além de seus usuários internos e externos. As diretrizes estabelecidas nesta política determinam as linhas mestras que devem ser seguidas pela organização para que sejam assegurados seus recursos computacionais e suas informações.

A elaboração e implementação de políticas de segurança em sistemas operacionais visa garantir a integridade, confidencialidade, autenticidade e disponibilidade das informações processadas por uma organização.

O processo de elaboração da política de segurança deve ser conduzido pela área responsável pelas informações, além de coordenar sua implantação, aprová-la e revisá-la e designar funções de segurança. A alta administração e os diversos gerentes e proprietários dos sistemas informatizados devem igualmente participar da elaboração da política. Sendo assim, a política deve extrapolar o escopo abrangido pelas áreas de sistema de informações e pelos recursos computacionais integrando-se à visão, à missão, ao negócio e às metas institucionais, bem como ao plano estratégico de informática e às políticas da organização no que concernem à segurança em geral.

Para o alcance de resultados consistentes a partir de uma política de segurança, a estratégia deve incluir a integração de três elementos essenciais no planejamento:

- Pessoas: definir o grupo de segurança com participação de todos os

profissionais envolvidos no processo de melhoria da segurança;

- Tecnologias: adotar ferramentas eficientes para excução de testes de avaliação e uso nos dispositivos, aplicações e servidores;
- Metodologia: definir os ambientes s serem monitorados, análise de resultados e acompanhamento de melhorias.

Vale lembrar que o comportamento do usuário consiste no elo mais fraco da cadeia de eventos a seguir para o aumento da segurança em sistemas computacionais.

## 7.4 Ferramentas de Segurança

Na utilização de sistemas computacionais, ligados a redes internas ou Internet, o indivíduo está exposto a diversas formas de insegurança. Todos os tipos de *malwares*, ameaças e vulnerabilidades colocam sua privacidade em risco inexoravelmente.

Os softwares de segurança constituem-se em manobra importantíssima na redução dos riscos relacionados à atividade virtual para todos os usuários individuais ou organizações.

### 7.4.1 Para administradores de sistemas e redes

Os administradores de sistemas e redes devem estar constantemente atualizados quanto aos principais recursos disponíveis para buscar a implementação de um ambiente seguro, com algum grau de proteção contra os perigos mais comuns existentes em redes de computadores. O primeiro passo é obter um sistema simplificado, disponibilizando apenas os serviços necessários e limitando o número de opções e facilidades.

Muitas ferramentas auxiliam na manutenção da segurança de um sistema e podem ser classificadas quanto ao seu escopo ou função.

Quanto ao escopo:

- Ferramentas de segurança de *hosts*: voltadas para análise, correção, e implementação de novos controles em sistemas computacionais. Um exemplo é o *crack*, para verificação de senhas.

- Ferramentas de segurança de rede: direcionadas para a verificação e implementação de controles sobre o tráfego de uma rede. Como exemplo pode-se citar o filtro de pacotes.

Quanto à função:

- Verificação de integridade e vulnerabilidade: programas que analisam a situação de um ou mais sistema, relacionando os serviços disponíveis, os erros de permissão de arquivos, mudanças em programas, acesso a serviços, etc.

- Autenticação: ferramentas relacionadas á identificação de usuários de um sistema (senhas de acesso).

- Privilégios: relacionadas com um ambiente de operação, restringindo os privilégios de usuários ao mínimo necessário para a execução das tarefas.

- Criação de programas seguros: bibliotecas com novas funções para a elaboração de programas resistentes às técnicas mais comuns de quebra de segurança.

Existem várias ferramentas a serviço dos administradores de redes para segurança de dados e recursos:

- Tcp_wrapper

Sua função é interceptar, filtrar e aumentar o nível de detalhamento de *logs* para os serviços iniciados. Sua ativação ocorre ao receber a solicitação de um serviço, quando um módulo executa um programa de controle em vez do servidor original. Este programa atua como protetor do programa original, verificando a origem da conexão, registrando o acesso e tomando ações pré-definidas.

- Crack

O objetivo deste programa é quebras as senhas escolhidas pelos usuários antecipadamente. Assim, o administrador terá condições de solicitar a mudança de senha, avaliar o estado de atenção de seus usuários para o problema e verificar a necessidade de utilização de alguma outra ferramenta para exigir a utilização de senhas mais fortes.

- Tripwire

Ferramenta de verificação de integridade de arquivos, detectando mudanças não autorizadas ou não esperadas nos principais arquivos do sistema.

- Tiger

Ferramenta desenvolvida para auditoria em sistemas UNIX, tentando localizar potenciais problemas na configuração do sistema, examinando contas, senhas, permissão de acesso a arquivos, PATHS atribuídos, mudanças em arquivos, NFS e binários desatualizados entre outros pontos.

O Tiger é semelhante ao conhecido COPS, porém com abordagem um pouco diferente.

- Swatch

O programa realiza verificação sistemática de determinadas ocorrências, como tentativa de *logins*, e a tomada de ações, como envio de email ou interrupção de algum serviço. Essa busca é feita nos arquivos de *log* do sistema, simultaneamente ou após a coleta dos registros.

- Strobe

Esta ferramenta realiza uma verificação de portas, listando todos os serviços TCP disponíveis em um sistema. Rapidamente ele é capaz de identificar as portas abertas, permitindo a identificação pelo administrador do sistema de caminhos que podem ser utilizados pra um possível ataque.

- ISS

O *Internet Security Scanner* é um programa que busca vulnerabilidades mais comuns nos serviços de rede smtp, finger, FTP, etc.

- Gabriel

O Gabriel é um detector de *scanners,* cuja função é detectar atividades intensas realizadas em curto espaço de tempo, sobre os serviços de rede. Um programa semelhante é o Courtney.

### 7.4.2 Para usuários

- Antivírus

O antivírus é a primeira ferramenta a ser instalada para a segurança de um computador, porém não dever ser o único responsável. Os bons *softwares* de proteção podem ser gratuitos ou pagos que oferecem amplo suporte.

- Firewall

O *firewal*l trabalha juntamente com o antivírus, uma vez que é responsável em expulsar o que é de caráter duvidoso antes de entrar na máquina.

- Antispyware

Os antispyware são responsáveis por executar varreduras no computador com o objetivo de eliminar do sistema spywares – programas deixados pelos *hackers* no computador com o intuito de recolher informações confidenciais.

Neste capítulo forma conceituadas as propriedades fundamentais da informação ou recurso a ser protegido, bem como as formas e ferramentas para proteção.

# 8 COMPORTAMENTO DE SEGURANÇA

Pela crescente utilização dos dispositivos móveis para executar grande parte das ações realizadas em computadores pessoais, como navegação Web, *Internet Banking* e acesso a e-mails e redes sociais, os riscos de ataques aumentam significativamente.

O comportamento do usuário pode determinar o maior ou menor grau de segurança nestes e em qualquer outro dispositivo.

A engenharia social foi definida como estratégia utilizada para explorar o lado mais fraco ou sensível do ser humano no intuito de obter informações relevantes. A segurança da informação é muito importante no dia a dia das pessoas, principalmente com o surgimento da tecnologia onde o cenário torna-se ainda mais vulnerável.

Por isso o cuidado é essencial, seja no comportamento como no gerenciamento de informações.

A facilidade, mobilidade e disponibilidade podem tornar-se vulnerabilidades, pois os meios de comunicação são utilizados sem as devidas precauções.

A engenharia social é aplicada em diversos setores da segurança da informação independente de sistemas computacionais, *software* e ou plataforma utilizada, o elemento mais vulnerável de qualquer sistema de segurança da informação é o ser humano, o qual possui traços comportamentais e psicológicos que o torna suscetível a ataques de engenharia social. Dentre essas características, pode-se destacar:

- Vaidade pessoal e/ou profissional: O ser humano costuma ser mais receptivo à avaliação positiva e favorável aos seus objetivos, aceitando basicamente argumentos favoráveis a sua avaliação pessoal ou

profissional ligada diretamente ao benefício próprio ou coletivo de forma demonstrativa.

- Autoconfiança: O ser humano busca transmitir em diálogos individuais ou coletivos o ato de fazer algo bem, coletivamente ou individualmente, buscando transmitir segurança, conhecimento, saber e eficiência, buscando criar uma estrutura base para o início de uma comunicação ou ação favorável a uma organização ou individuo.

- Formação profissional: O ser humano busca valorizar sua formação e suas habilidades adquiridas nesta faculdade, buscando o controle em uma comunicação, execução ou apresentação seja ela profissional ou pessoal buscando o reconhecimento pessoal inconscientemente em primeiro plano.

- Vontade de ser útil  O ser humano, comumente, procura agir com cortesia, bem como ajudar outros quando necessário.

- Busca por novas amizades: O ser humano costuma se agradar e sentir-se bem quando elogiado, ficando mais vulnerável e aberto a dar informações.

- Propagação de responsabilidade: Trata-se da situação na qual o ser humano considera que ele não é o único responsável por um conjunto de atividades.

- Persuasão: Compreende quase uma arte a capacidade de persuadir pessoas, onde se busca obter respostas específicas. Isto é possível porque as pessoas possuem características comportamentais que as tornam vulneráveis a manipulação.

A segurança na utilização da Internet deve ser abordada sob dois aspectos: a informação e conscientização do usuário final e uma política de segurança

disponibilizada pela empresa que se dispõe a oferecer esta tecnologia aos funcionários na busca de resultados estratégicos.

Sendo assim abordaremos os principais mecanismos de segurança distintamente para usuários e organizações.

## 8.1 Para Usuários

As redes sociais são no momento o ponto mais crítico na segurança da informação pessoal, principalmente no Brasil onde 87,6% dos usuários internautas participam. A ferramenta que traz a informação compartilhada como foco principal permite a ocorrência de golpes, onde os indivíduos se aproveitam de deslizes ou inocência dos usuários, utilizando a engenharia social. A precaução mais plausível para estas situações sé a não divulgação de dados pessoais, como local de moradia, números de telefone, nomes de pessoas da família, números de documentos, empresa em que trabalha, cargos que ocupa, projetos em elaboração, enfim, informações que podem fazer com que indivíduos mal intencionados utilizem estas informações para obtenção de dados ou vantagens pessoais.

Pela facilidade de transporte os celulares, *smartphones* e *tablets* tornam-se produtos visados para roubo, consequentemente facilitando a obtenção de dados pessoais por meio de aplicativos como redes sociais, emails logados, possibilitando ainda fraudes e roubos.

Pesquisa realizada pela empresa de segurança da informação F-Secure em 2012 em 14 países sobre percentual de roubos ou perdas de dispositivos móveis mostrou o Brasil em segundo lugar, com total de 25% dos participantes brasileiros. Comparativamente ao ranking mundial com 11%, o percentual é alto e demonstra a falta de segurança no país.

Algumas orientações para evitar roubos e fraudes em dispositivos móveis:

- Não registrar informações pessoais.
- Não manter aplicativos logados.
- Ocultar senhas.
- Evitar gravar contatos no telefone mencionando o grau de parentesco.

- Configurar o celular para desbloqueio com senha.

## 8.2 Para Organizações

A abordagem para a busca de maior segurança pode ser por duas vertentes: empresarial ou individual, embora estas, em muitas ocasiões, estejam interligadas.

Com as mudanças tecnológicas e com o uso de computadores de grande porte e dispositivos móveis, a estrutura de segurança tornou-se mais complexa, englobando controles lógicos, porém ainda centralizados. Com o advento dos computadores pessoais e das redes que conectam o mundo inteiro, os aspectos de segurança atingiram tamanha complexidade que há a necessidade de desenvolvimento de equipes e de métodos de segurança cada vez mais sofisticados. Paralelamente, os sistemas de informação também adquiriram importância vital para a sobrevivência da maioria das organizações modernas, já que, sem computadores e redes de comunicação, a prestação de serviços de informação pode se tornar inviável.

Mais complexa ainda a questão se torna com os dispositivos móveis sendo utilizados para as atividades empresariais e pessoais, seja pelo comportamento BYOD ou pela disponibilização destes pelas empresas para seus funcionários na realização das atividades corporativas. Um comportamento inseguro em qualquer situação poderá

colocar em risco todos os dados relativos ao indivíduo ou empresa.

Todas as instituições e indivíduos que utilizam a informática como meio de geração, armazenamento e divulgação de informações, devem criar meios para prover segurança de acesso a essas informações.

A crescente demanda por ferramentas acessíveis de segurança de TI e o conceito de comoditização de segurança tornaram mais difícil escolher a solução de segurança correta para redes organizacionais de qualquer tamanho.

A primeira estratégia deve ser a criação de um ambiente de trabalho com políticas adequadas e procedimentos tecnológicos considerando os seguintes aspectos:

- Desenvolvimento de estratégia empresarial para segurança móvel, não para limitar a utilização dos dispositivos, mas para aceitar que eles são um modo de vida. Eles aumentam a eficiência dos funcionários, tal como a flexibilidade e velocidade na implantação de novos aplicativos;

- Auditorias para definição dos locais onde notebooks e outros dispositivos móveis são utilizados dentro da empresa. A auditoria ajuda a entender o nível de risco e as tecnologias que limitam o acesso ou a transferência de informações confidenciais;

- Classificação dos funcionários de dados sensíveis: eles podem ser classificados da seguinte forma, dados regulamentados (cartões de crédito, dados de saúde), não-regulamentados (histórico de compras, navegação), dados dos funcionários e não-regulamentados confidenciais de negócios (IP, financeiro);

- Criação de política global que aborde riscos associados a cada dispositivo e os procedimentos de segurança que devem ser seguidos;

- Definição de práticas de monitoramento rigoroso e implementação de tecnologias de base para assegurar que as políticas e diretrizes sejam cumpridas;

- Definição de configurações de segurança, impedindo *jailbreaking*: pesquisas mostram que os funcionários desligam os recursos de segurança de seus dispositivos móveis, causando problemas para a segurança das informações;

- Determinação de responsabilidades organizacionais: a empresa tem a responsabilidade de determinar políticas, procedimentos e tecnologias necessárias para a segurança dos dispositivos móveis, e os funcionários devem estar cientes de suas responsabilidades e da importância do uso responsável dos dispositivos.

Algumas atitudes podem ser tomadas para prevenir ocorrências indesejáveis de crimes praticados contra empresas por meio de canais tecnológicos.

- Escolha de equipamentos adequados à atividade da empresa com a aquisição de equipamentos de renome e qualidade. A adoção de um plano estratégico associado a um plano tecnológico de aquisições e treinamentos;

- A aquisição de produtos tecnológicos deve ser realizada por fornecedores confiáveis de assistências técnica e manutenção;

- Escolha de softwares que possam suprir as necessidades da empresa sendo customizados, especialmente desenvolvidos ou de mercado;

- Controle de patrimônio tecnológico: os bens da empresa devem ser devidamente inventariados, tornando-se possível o acompanhamento total dos incidentes na vida útil dos equipamentos, atualizações e nível de obsolescência.

- Após o término da vida útil do equipamento é essencial que se realize a formatação completa das máquinas, preferencialmente com softwares especializados em apagar dados definitivamente antes de se proceder a

destinação final.

Alguns princípios básicos de segurança devem ser seguidos, como descrito a seguir:

## 8.3 Senha

A maioria da fraudes mundiais por meio eletrônicos acontecem por meio de compartilhamento ou obtenção de senhas por meios indevidos. Sendo assim o gerenciamento de senhas merece atenção especial desde sua formulação, concessão e bloqueio.

Algumas atitudes podem minimizar os riscos relacionados a senhas:

- Definição de regras de formulação de senhas, exigindo variedades de tipos de caracteres com letras, números e símbolos;
- Monitoramento ostensivo da política de segurança para funcionários e colaboradores, com regras obviamente proibitivas e punitivas, relacionadas ao compartilhamento de senhas com terceiros, ainda que da própria empresa;
- Estabelecer validade temporal das senhas, que devem ser obrigatoriamente alteradas em um período razoavelmente curto de tempo.

## 8.4 E-mail e spam

Se, por um lado, a captação de senhas é o início de uma fraude, a propagação é estabelecida por meio de e-mails, incluindo mensagens eletrônicas abusivas e não solicitadas de cunho comercial (spam). Os fraudadores enviam arquivos para captação

de senhas, disseminadores de vírus e outros artifícios para obter informações sigilosas da empresa. Algumas ações simples podem evitar ou minimizar a situação:

- Nunca abrir anexos de mensagens de pessoas desconhecidas;
- Analisar cuidadosamente a possibilidade de não abrir anexos, se possível, mesmo de pessoas conhecidas;
- Nunca efetuar ou preencher cadastros de pesquisas enviadas anexas a e-mails;
- Excluir e-mails supostamente enviados por instituições bancárias. Bancos de renome não enviam comunicação por e-mail;
- Ao clicar em *links* enviados por e-mail, confirmar na barra de endereço se está sendo direcionado para o local efetivamente desejado, pois *links* falsos direcionam para sites fraudulentos;
- Criar política interna de utilização de e-mails corporativos, com regras claras, objetivas e com possibilidade de imposição de penalidades em caso de inobservância;
- Utilizar ferramentas legais de monitoramento dos e-mails corporativos da empresa, com ampla divulgação desta estratégia aos funcionários;
- Instalar filtros *antispam* e atualizar com regularidade;
- Manter os sistemas operacionais sempre atualizados e originais de seus fabricantes.

## 8.5 Antivírus, firewalls e bloqueio de sites

Diante da importância dos dados e cadastros das empresas, sua perda ou divulgação pode significar danos irreversíveis ao negócio. Por isso, a proteção dos

equipamentos tecnológicos da empresa contra ameaças de invasão ou vírus também merece adoção de medidas preventivas importantes.

O objetivo principal do antivírus é evitar a contaminação do computador por *malwares*, onde o mercado oferece uma gama de soluções a baixo custo. Para a escolha deste software, a avaliação do profissional de tecnologia é crucial, já que para a aquisição de uma solução tecnológica seja eficaz, é preciso definir quais são os tipos de riscos a que determinada empresa está sujeita, de acordo com as suas atividades e modalidades de equipamentos utilizados.

O *firewall* é uma ferramenta de bloqueio de acessos não autorizados. Para sua aquisição, é aconselhável que haja análise prévia de um profissional da TI, para que sua implementação seja estudada em conjunto com a utilização de todas as demais ferramentas de segurança da informação existentes na empresa.

A variedade de soluções adotadas determina o nível de segurança. Sendo assim, deve ser considerado ainda o bloqueio, no ambiente de trabalho, de determinados sites ou funcionalidades que potencialmente podem trazer prejuízos. Entre eles aqueles que oferecem *downloads* de programas e conteúdos, redes sociais em geral e troca de mensagens, entre outros.

O bloqueio de acesso a e-mails particulares deve ser considerado, se as informações veiculadas nas máquinas forem de cunho confidencial, bem como a possibilidade de cópia de arquivos das máquinas móveis, como *pendrive* ou HD externo.

A criação e o gerenciamento de redes internas devem ser criteriosos e sob constante monitoramento, já que se, sob certo aspecto, facilitam o acesso a arquivos e informações de interesse comum, sob outro pode causar estragos coletivos caso haja contaminação por vírus e outras ações criminosas em geral.

Uma alternativa a ser avaliada com cuidado, é a solução de *Cloud Computing.* Estas soluções ficam armazenadas e sistemas profissionais e os usuários só necessitam de conexão à Internet para acesso.

## 8.6 Backups e Revisões Periódicas

A verificação e manutenção das condições do parque de máquinas das empresas são extremamente importantes para melhorar o nível de segurança de dados das empresas. A substituição de máquinas antigas, não necessariamente obsoletas, a aquisição de equipamentos atualizados e constante busca pela modernização a atualização de todo o sistema, certamente auxiliam na diminuição dos riscos. Por outro lado, também é medida fundamental que periodicamente se realiza cópia de segurança (*backup*) de todos os dados do sistema, dependendo do grau de relevância das informações.

Este capítulo foi dedicado ao ponto mais crítico da segurança: o comportamento do usuário, seja ele leigo, profissional, individual ou organizacional.

# 9 CONCLUSÕES

O objetivo principal do GUIA DE SEGURANÇA PARA DISPOSITIVOS MÓVEIS: HARDWARE, SOFTWARE E COMPORTAMENTO, foi esclarecer e orientar leigos e profissionais na melhor escolha e uso de seus aplicativos, pessoais ou corporativos.

Este produto pode ser customizado e utilizado por qualquer tipo de organização que faça uso desta tecnologia ou para cidadãos interessados em adquirir conhecimento dos benefícios e riscos que a atividade virtual possibilita.

No decorrer deste trabalho foi possível perceber que a segurança da informação é algo que merece atenção especial de indivíduos e empresas, principalmente em uma realidade de negociações, transações e aquisições em todas as esferas no meio virtual.

Transações bancárias, *e-commerce* e relações pessoais através das redes sociais, permitem formas de ataques e situações indesejáveis a qualquer usuário.

As sugestões de mecanismos de segurança abordados neste trabalho podem e devem ser periodicamente reavaliadas, diante da constante mutação de tecnologias e comportamentos a que estamos expostos diariamente.

No decorrer do trabalho, restou claro que a responsabilidade da segurança da informação recai sobre todos os participantes da cadeia de eventos que é a Internet: desde desenvolvedores de softwares, administradores de redes e sistema, organizações que disponibilizas estes recursos a sues colaboradores e usuários finais.

## 10 REFERÊNCIAS

BARBOSA, André Sarmento: Fundamentos de Sistemas de Segurança da Informação. Disponível em: <http://www.land.ufrj.br/~verissimo/cos871/bibref/biblio02.pdf>. Acesso em: 18 ago 2013.

B'FAR, Reza; Mobile Computing Principles: Designing and Developing Mobile Applications with UML and XM Reza B'Far, Cambridge University Press, 2005.

BLOG Administradores. Disponível em:

<http://www.administradores.com.br/noticias/tecnologia/7-dicas-de-seguranca-para-dispositivos-moveis/76801/>. Acesso em 18: ago 2013.

BLOG Administradores. Disponível em:

<http://www.administradores.com.br/artigos/tecnologia/seguranca-da-informacao-gerenciamento-das-informacoes-comportamento-e-internet/69468>. Acesso em: 18 ago 2013.

BLOG Canal Tech. Disponível em: <http://canaltech.com.br/analise/mobile/Os-numeros-nao-mentem-Android-ou-iOS-qual-e-o-melhor/>. Acesso em 25 set 2013.

BLOG Canal Tech. Disponível em:

<http://canaltech.com.br/dica/seguranca/Dicas-de-seguranca-corporativa-para-dispositivos-moveis/>. Acesso em: 18 ago 2013.

BLOG DClickHolmes. Disponível em: <http://www.dclickholmes.com/blog/dispositivos-moveis-uma-nova-realidade/>. Acesso em: 23 set 2013.

BLOG Devmedia. Disponível em: <http://www.devmedia.com.br/mobilidade-em-analise/3309>. Acesso em 14 out 2013.

BLOG EXAME INFO. Disponível em: <http://info.abril.com.br/noticias/seguranca/90-dos-novos-virus-de-celular-sao-para-android-25052013-5.shl>. Acesso em: 12 ago 2013.

BLOG Guia do hardware. Disponível em: <http://www.hardware.com.br/dicas/smartphones-uma-introducao.html>. Acesso em: 23 set 2013.

BLOG Guia do hardware. Disponível em: <http://www.hardware.com.br/guias/smartphones/>. Acesso em 18 set 2013.

BLOG Guia do hardware. Disponível em: <http://www.hardware.com.br/livros/smartphones/capitulo-entendendo-arquitetura.html>. Acesso em 23 set 2013.

BLOG Infowester. Disponível em: <http://www.infowester.com/bluetooth.php>. Acesso em 12 out 2013.

BLOG Kioskea. Disponível em: <http://pt.kioskea.net/faq/11106-sistemas-operacionais-para-celulares-e-dispositivos-moveis>. Acesso em 28 out 2013.

BLOG Mania de Celular: Disponível em: <http://www.maniadecelular.net/voce-sabe-a-diferenca-entre-as-redes-2g-3g-e-4g/>. Acesso em: 23 set 2013.

BLOG Oficina da Net. Disponível em: <http://www.oficinadanet.com.br/artigo/2239/google_android_o_que_e#ixzz2aMEgiRQ7>. Acesso em: 7 jul 2013.

BLOG Olhar Digital: Disponível em: <http://olhardigital.uol.com.br/noticia/conhe-a-as-diferen-as-entre-1g-2g-3g-e-4g/34225>. Acesso em: 18 ago 2013.

BLOG Processadores Dispositivos Móveis. Disponível em: <http://procdispositivosmoveis.blogspot.com.br/2012/06/o-processador-e-o-cerebro-do-micro.html>. Acesso em: 14 ago 2013.

BLOG Smart and Tablets. Disponível em: <http://smartsandtablets.wordpress.com/2012/08/21/hardware-e-o-multitarefa-em-dispositivos-moveis/>. Acesso em: 30 set 2013.

BLOG SUCESU-MT. Disponível em: <http://www.sucesumt.org.br/mtdigital/anais/files/RedesWirelessWEP.pdf>. Acesso em 12 ago 2013.

BLOG Tableless. Disponível em: <http://tableless.com.br/mobile-first-a-arte-de-pensar-com-foco/#.UdiImzvqln0>. Acesso em: 27 set 2013.

BLOG Techmundo. Disponível em: <http://www.tecmundo.com.br/amd/4640-amd-versus-intel.htm#ixzz2aNwFiidA http://insecure.org/tools/tools-pt.html>. Acesso em 20 set 2103.

BLOG Techmundo. Disponível em: <http://www.tecmundo.com.br/qualcomm/7708-por-que-os-processadores-arm-podem-mudar-o-rumo-dos-dispositivos-eletronicos-.htm>. Acesso em: 18 out 2013.

BLOG Tudo em Tecnologia. Disponível em: <http://www.tudoemtecnologia.com/2013/04/iphone-perde-terreno-para-android-no-mercado-norte-americano.html>. Acesso em 25 ago 2013.

BRAGA, Alexandre Melo, NASCIMENTO,Erick Nogueira do,PALMA, Lucas Rodrigues da, ROSA,Rafael Pereira Rosa: Introdução à Segurança de Dispositivos Móveis Modernos – Um Estudo de Caso em Android . Disponível em: <http://dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/ceseg:2012-sbseg-mc2.pdf >. Acesso em: 13 ago 2013.

Cartilha Segurança da Informação – FECOMÉRCIO São Paulo. Disponível em:

<http://www.fecomercio.com.br/arquivos/arquivo/cartilha_seguranca_da_informacao_-_conselho_de_tecnologia_da_informacao_8mdaoaahah.pdf>. Acesso em: 22 ago 2013.

CARVALHO, Mauricio; ABREU, Patricia, VASQUES, Leonardo Felipe Serra: Dispositvos Móveis, Uma visão Geral sobre História e Tecnologia para Dispositivos Móveis. Disponível em: <http://www.slideshare.net/MauricCarvalho/dispositivos-mveis-15375049>. Acesso em: 27 set 2013.

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil- CERT-Br. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 23 set 2013.

Departamento de Engenharia Química – UFRS. Disponível em: <http://www.enq.ufrgs.br/files/Engenharia%20Social.pdf>. Acesso em: 28 jan 2013.

Grupo de Resposta a Incidentes de Segurança. Disponível em: <http://www.gris.dcc.ufrj.br/news/dicas-de-seguranca-para-android>. Acesso em: 10 jul 2013.

International Data Corporation. Disponível em: <http://www.idc.com/getdoc.jsp?containerId=prUS24628914>. Acesso em: 19 jan 2014.

Kantar Worldpanel. Disponível em: <http://www.kantarworldpanel.com> Acesso em: 18 jun 2013.

Kaspersky Lab. Disponível em: <http://www.kaspersky.com/pt/about/news/virus/2014/Malware_movel_cresceu_135_por_cento_em_2013#>. Acesso em 15 de jan 2014.

MAIA, Luiz Paulo. Arquitetura de redes de computadores. Rio de Janeiro, RJ: LTC, 2009.

MAZIERO, Carlos Alberto; Sistemas Operacionais: Conceitos e Mecanismos. Disponível em: <http://dainf.ct.utfpr.edu.br/~maziero/lib/exe/fetch.php/so:so-cap08.pdf> Acesso em: 18 ago 2013.

National Vulnerability Database. Disponível em: <http://nvd.nist.gov/>. Acesso em: 15 set 2013.

OLIVERIO, Márcio Araujo. Cloud Computing: Mobilidade no Compartilhamento e Acesso Remoto de Arquivos e Serviços. Disponível em: <http://www.academia.edu/426839/Cloud_Computing_mobilidade_no_compartilhamento_e_acesso_remoto_de_arquivos_e_servicos> Acesso em: 6 jul 2013.

PINHEIRO, Carlos Augusto Campana. Disponível em: <http://www.rnp.br/newsgen/9711/seguranca.html> Acesso em: 6 jul 2013.

Proofpoint. Disponível em: <http://www.proofpoint.com/support/training-programs.php>. Acesso em: 21 jan 2014.

RODRIGO, João. Disponível em: <http://web.ist.utl.pt/joao.rodrigo/CM/>. Acesso em: 8 jul 2013.

RUFINO, Nelson Murilo de O. Seguranca em redes sem fio: aprenda a proteger suas informacões em ambientes Wi-fi e Bluetooth. 2. ed. São Paulo: Novatec, 2007.

STANTON, Jeffrey; Analysis of end user secutity behaviors, Jeffrey M. Stanton, Kathryn R. Stam, Paul Mastrangelo, Jeffrey Jolton, 20003.

TANENBAUM, Andrew S. Organização estruturada de computadores. 5. ed. São Paulo: Pearson Prentice Hall, c2007.

TANENBAUM, Andrew. Redes de computadores. Rio de Janeiro: Elsevier, 2003.

Tribunal de Contas da União: Boas práticas em Segurança da Informação. Disponível em: <http://portal2.tcu.gov.br/portal/pls/portal/docs/2059162.PDF>. Acesso em: 22 set 2013.

USIGIO Bruno Paulo Kovacs; MONTEIRO, Vanesa de Freitas:Um estudo prático das ameças de segurança em dispositivos portáteis com Windows Mobile. Disponível em: <http://www-di.inf.puc-rio.br/~endler/projects/Anubis/Ameacas.pdf >. Acesso em: 22 ago 2013.

VELTE, Anthony T. Cloud computing: computacão em nuvem, uma abordagem pratica . Rio de Janeiro, RJ: Alta Books, 2012.

Wikipedia. Disponível em: <http://pt.wikipedia.org/wiki/Tablet> Acesso em: 13 fev 2013. Acesso em: 22 ago 2014.

YAMAKAWA, Carlos Américo Perazolo, 2012; Garantia de Qualidade em Páginas Web para Dispositivos Móveis: Acessibilidade e Restrições de hardware. Disponível em <http://repositorio.cbc.ufms.br:8080/jspui/bitstream/123456789/1641/1/Carlos%20Americo%20Perazolo%20Yamakawa.pdf> . Acesso em 12 nov 2013.