Instituto Politécnico de Setúbal

Escola Superior de Ciências Empresariais

Tendências de implementação e segurança nas redes *wireless* organizacionais

José Humberto Laranjeira Sereno

Dissertação apresentada para cumprimento dos requisitos necessários à obtenção do grau de

MESTRE EM SISTEMAS DE INFORMAÇÃO ORGANIZACIONAIS

Orientador: Professor Doutor José Gaivéo

Setúbal, 2015

Dedicatória

Aqueles que passam por nós, não vão sós, não nos deixam sós. Deixam um pouco de si, levam um pouco de nós — *Antoine de Saint-Exupéry*

A todos aqueles que estiveram comigo neste percurso direta ou indiretamente, mas que deixaram um pouco deles neste trabalho, e como não podia deixar de ser, levaram um pouco dele com eles.

O meu mais profundo agradecimento.

Agradecimentos

Na concretização deste trabalho foi indispensável o apoio e o saber partilhado de diversas pessoas, pelo que, para todas elas, quero aqui deixar claramente expressa a minha gratidão.

Pela motivação, acompanhamento, apoio e orientação que conseguiram transmitir nesta fase da minha vida, agradeço a todos os Professores da parte curricular do Mestrado de Sistemas de Informação, especialmente aos Docentes com quem tive a oportunidade de conhecer e atualizar grande parte do saber depositado no trabalho desenvolvido.

Pela contribuição fundamental que teve para a realização deste trabalho não quero no entanto deixar de agradecer particularmente ao meu orientador, Professor Doutor José Gaivéo, pelo rumo estabelecido mas também pela disponibilidade, compreensão, paciência, assertividade e exigência com que conduziu o mesmo.

E que dizer da Escola Superior de Ciências Empresariais, do Instituto Politécnico de Setúbal, do respetivo corpo docente e não docente, onde fui agradavelmente surpreendido pela paixão ao saber e partilha pelos que procuram saciar essa vontade de conhecimento.

Um muito obrigado ainda por todos aqueles que tiveram paciência em dias menos bons, e à família pela ajuda que direta ou indiretamente me concedeu e pelo facto de ter sido privada da minha presença em muitas circunstâncias.

Por fim, agradeço também aos colegas do primeiro ano de Mestrado, pelo acolhimento e espirito de interajuda neste meu regresso ao ambiente académico.

A todos vós, o meu obrigado

Termino com este pensamento:

Conhecer não é demonstrar nem explicar, é aceder à visão. - Antoine de Saint-Exupéry

Índice

Índice de figuras

Siglas e acrónimos

AAA	*Authentication, Authorization and Accounting*
ACL	*Access Control Lists*
AES	*Advanced Encryption Standard*
AM	*Air Monitor*
AP	*Access Point*
APPS	*Application*
ARM	*Adaptive Radio Management*
ARP	*Address Resolution Protocol*
AS	*Authentication Server*
BSS	*Basic Service Set*
BYOD	*Bring Your Own Device*
CA	*Certification Authority*
CCMP	*Counter mode with Cipher - block chaining Message authentication code Protocol*
DFS	*Dynamic Frequency Selection*
DHCP	*Dynamic Host Configuration Protocol*
DNS	*Domain Name System*
DoS	*Denial Of Service*
DS	*Distribution system*
DWDM	*Dense Wavelength Division Multiplexing*
EAP	*Extensible Authentication Protocol*
EBSS	*Extended Basic Service Set*
ESS	*Extended Service Set*
Gbps	*Gigabits* por segundo
GCM	*Galois / Counter Mode*
GCMP	*Galois Counter Mode Protocol*
GRE	*Generic Router Encapsulation*
HEW	*High-Efficiency WLAN*
HT	*High Throughput*
IBSS	*Independent Basic Service Set*
ICV	*Integrity Check Vector*
IEC	*International Electrotechnical Commission*
IEEE	*Institute of Electrical and Electronics Engineers*
IETF	*Internet Engineering Task Force*
IPS	Instituto Politécnico de Setúbal
IPS	*Intrusion Prevention System*

ISMS	*Information Security Management System*
ISP	*Internet Service Providers*
ISO	*International Standard Organization*
LAN	*Local Area Network*
LLC	*Logical Link Control layer*
MAN	*Metropolitan Area Networks*
Mbps	*Megabit per Second*
Mhz	*Megahertz*
MAC	*Media Access Control*
MIC	*Message Integrity Code*
MIMO	*Multiple Input, Multiple Output*
MPDU	MAC *Protocol Data Unit*
MSDU	MAC *Service Data Unit*
NSA	*National Security Agency*
NIST	*National Institute of Standards and Technology*
OECD	*Organization for Economic Cooperation and Development*
OSI	*Open Systems Interconnection*
PAN	*Personal Area Networks*
PCI-DSS	*Payment Card Industry - Data Security Standard*
PDU	*Protocol Data Unit*
PDU-LLC	*Protocol Data Unit Logical Link Control*
PHY	*Physical Layer*
PNAC	*Port-Based Network Access Control*
PoE	*Power-over-Ethernet*
PSTN	*Public Switched Telephone Network*
PKI	*Public Key Infrastructure*
QAM	*Quadrature Amplitude Modulation*
QoS	*Quality of Service*
RADIUS	*Remote Authentication Dial - In User Service*
RBAC	*Role-Based Access Control*
RC4	*Rivest Ciper - 4*
RF	*Radio Frequency*
RM	*Modelo de Referência*
RSNA	*Robust Security Network Association*
SAN	*Storage Area Networks*
SGSI	Sistema de Gestão de Segurança da Informação
SI	Sistemas de Informação

SSID	*Service Set IDentifier*
STA	*Station*
TAM	*Technology Acceptance Model*
Tbit/s	*1,000,000,000,000 bits per second*
TI /TIC	Tecnologias de Informação e Comunicação
TKIP	*Temporal Key Integrity Protocol*
TPC	*Transmit Power Control*
VPN	*Virtual Private Networks*
VHT	*Very high throughput*
WAN	*Wide Area Networks*
WEP	*Wired Equivalent Privacy*
WIDS	*Wireless Intrusion Detection Systems*
WIPS	*Wireless Intrusion Prevention Systems*
WLAN	*Wireless Local Area Network*
WM	*Wireless Medium*
WPA	*Wi-fi Protected Access*

Resumo

Este trabalho está subordinado aos temas da adoção pelas organizações de *Wireless Local Area Network* (WLAN) e da problemática da segurança da informação e sistemas que estas aportam para o ambiente organizacional.

A notável evolução das redes móveis especialmente as WLAN, tem sido impulsionada pelos requisitos crescentes de velocidade, largura de banda e necessidades dos utilizadores, abrindo uma nova frente para o desenvolvimento das organizações na vertente tecnológica, pois ultrapassaram, em vantagens, como por exemplo mobilidade, alcance da cobertura, facilidade de uso, escalabilidade e baixo custo, as redes fixas infraestruturadas existentes ou a criar.

Neste trabalho pretende-se enquadrar a problemática das WLAN organizacionais, das questões de segurança que são levantadas pela sua adoção em cada vez maior escala, procurando esclarecer os diversos conceitos inerentes a este tipo específico de *networking* e os problemas associados de segurança tecnológica e da informação que nelas circula.

Abordaremos assim ao longo dos capítulos a definição dos conceitos estruturantes das redes *wireless*, passando pelos *standards Institute of Electrical and Electronics Engineers* (IEEE) 802.11 que definem os requisitos básicos específicos do seu funcionamento, segurança e implementação, assim como os novos desafios colocados para as organizações na gestão, necessidade de garantir o seu controlo e resposta ao problema da segurança, da cada vez maior necessidade de mobilidade, sentida pelos genericamente utilizadores.

Depois do enquadramento inicial efetuado, com base na documentação estudada, definir um referencial a observar quando da implementação das WLAN nas organizações. A pertinência do estabelecimento destas regras está relacionada com a dispersão da informação assim como na dificuldade de indicação de uma solução de arquitetura única, pois não existe um modelo único aplicável, mas sim uma decisão ponderada e cuidada do tipo de arquitetura que se quer implementar, do nível de segurança a assegurar, dependente da classificação da informação que circula na WLAN da organização e do tipo de utilização.

Palavras-chave: Arquitetura, Organizações, Segurança, *Standards* 802.11, WLAN.

Abstract

This work is subject to the adoption by organizations of Wireless Local Area Network (WLAN) and the problems of information security and the systems that these contribute to the organizational environment.

The remarkable evolution of mobile networks especially the WLAN, has been driven by the increasing requirements of speed, bandwidth and user needs, opening a new front for the development of organizations in the technological aspect, since surpassed, in advantages, such as mobility, scope of coverage, ease of use, scalability and low cost, fixed networks existing or for create.

In this paper we intend to frame the problem of WLAN security issues, which are raised for their adoption in increasing scale, seeking to clarify the various concepts inherent to this specific type of networking and the associated issues of technological and information security.

We'll cover how throughout the chapters defining the structural concepts of wireless networks, passing by the standards Institute of Electrical and Electronics Engineers (IEEE) 802.11 that defines the basic requirements specific to your operation, security and implementation, as well as new challenges for organizations in management, need to ensure their control and response to the issue of security, the increasing need for mobility, felt by users in General.

After the initial framework, we will, on the basis of the documentation examined, set a benchmark to follow when implementing WLANs in organizations. The appropriateness of the establishment of these rules is related to the dispersal of information as well as the difficulty to indication of a unique architecture solution, because there is no single model, but a weighted decision and cared for the type of architecture that if you want to implement, ensure security level, dependent on the classification of the information that circulates on the Organization's WLAN and the type of use for there.

Keywords: *802.11 Standards, Architecture, Organizations, Security, WLAN*.

1 Introdução

Com a constante evolução observada em todas as áreas tecnológicas, especificamente na área em análise neste trabalho, o da segurança da informação e o das redes infraestruturadas *wireless*, o surgimento de novos *standards*[1] com mais e melhores medidas de segurança, o próprio desenvolvimento da sociedade da informação, que provoca que a partir do século XXI o mundo entre num ciclo acelerado de transformações, a nível económico, cultural, social, tecnológico e organizacional (Santos & Barbosa, 2011).

Assim a capacidade de inovação continuada, apoiada na informação e conhecimento é um dos fatores chave da competitividade das organizações[2], aqui referidas genericamente.

Estas inovações, essencialmente de base tecnológica, levam a que as organizações obtenham como resultado uma redução do ciclo de vida dos produtos, num fluxo constante de novas aplicações e no surgimento de novos mercados (Tan e Mathews, 2010), contribuindo para o surgimento da chamada "convergência digital", que no contexto organizacional se acentua com a convergência de ferramentas que apoiam a gestão da informação e do conhecimento para o aumento da eficiência e eficácia do trabalhador do conhecimento na realização do seu processo produtivo, bem como no desenvolvimento de processos de inovação constantes nas organizações.

As novas necessidades surgidas no ambiente organizacional, considerando a forma como as aplicações de negócio são entregues e ou suportadas nos diversos tipos de estrutura tecnológica de rede e ou dispositivos móveis, leva a que cada vez mais as organizações sejam forçadas a orientar o seu desenvolvimento e renovação tecnológica em determinados sentidos.

Num curto espaço de tempo, relativo, a mobilidade tornou-se uma das maiores tendências tecnológicas. Muito disto advém do interesse dos consumidores, onde diversos dispositivos, como *smartphones* e *tablets*, mudaram a mentalidade em relação à computação e criaram na totalidade, todo um novo sistema de valores (2rd Annual Trends in Enterprise Mobility, 2013).

Mas para as organizações os consumidores apenas parecem constituir metade da equação nesta perspetiva móvel, pois os empregados direcionam e insistem na utilização de tecnologias

[1] De referir que ao longo do trabalho, perante o peso da componente técnica e a perceção explicita destes termos, se utilizarão sempre os termos em inglês pelo enquadramento específico que têm.

[2] Os termos 'organização' e 'organizacional' serão utilizados considerando toda a sua abrangência referenciando genericamente qualquer grupo ou pessoa coletiva ou o seu ambiente.

que lhes dão mais mobilidade e flexibilidade, assim como capacidade de aceder à informação em qualquer local e a qualquer hora.

Do ponto de vista da organização o ecossistema móvel constituído por um conjunto de componentes, como mostrado na figura 1, em conjunto com as ofertas *cloud computing*[3], existentes, representam uma significativa mudança no controlo, forma de fornecer serviços, garantir a segurança da informação e da rede de dados e voz.

De referir que *cloud computing*, onde a palavra nuvem (também formulada como "a nuvem") é usado como uma metáfora para "a Internet", de modo que computação em nuvem significa também "um tipo de computação baseada na Internet", onde diferentes serviços - como servidores, armazenamento e aplicativos - são entregues aos computadores e dispositivos de uma organização através da Internet (Sanaei, Abolfazli, Gani e Buyya, 2014).

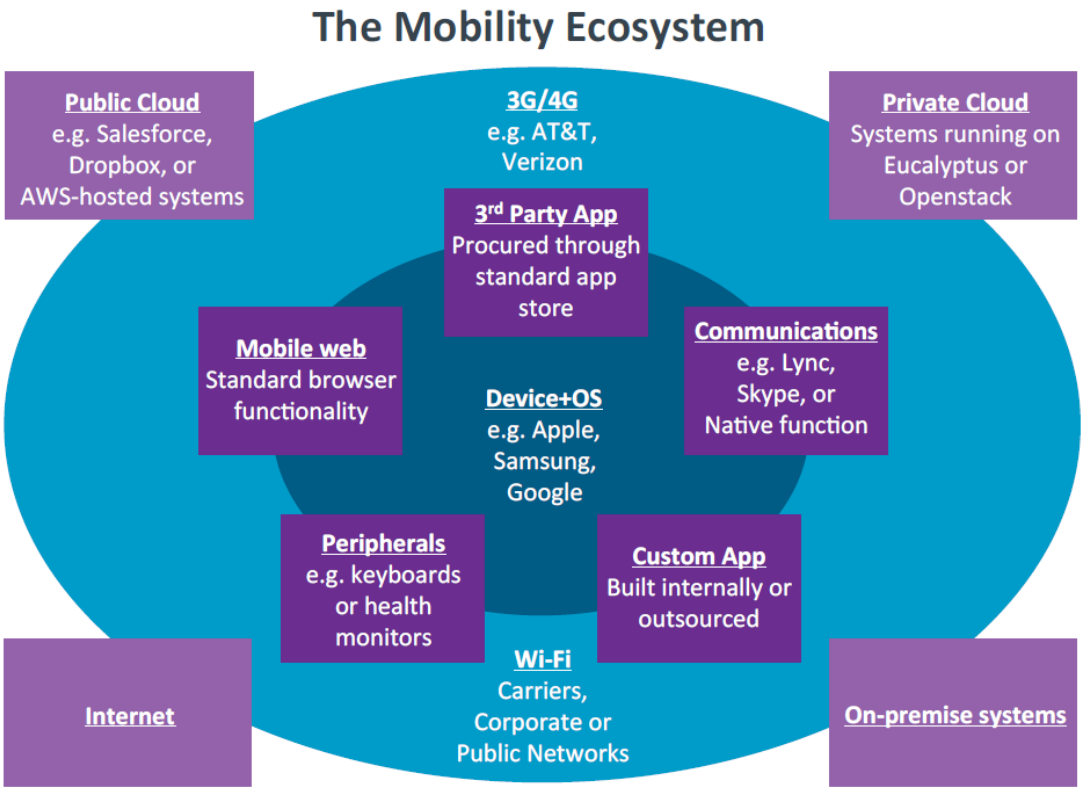

Figura 1 – Ecossistema *móvel*
(3rd Annual Trends in Enterprise Mobility, 2014)

Mais do que ter um controlo apertado sobre toda a experiencia, os arquitetos de infraestruturas tecnológicas[4] usualmente definidos como IT *architects* devem ter em

[3] Computação que se baseia em compartilhar recursos de computação em vez de ter servidores locais ou dispositivos pessoais para lidar com aplicações.
[4] Conjunto de instalações, equipamento e serviços, em tecnologias.

consideração que lidam com dispositivos de duplo propósito, a utilização pessoal e a do negócio, com ligação a sistemas de terceiros. Entre os programadores de aplicações de *software* (*apps*[5]), fornecedores de serviços *cloud*, operadores móveis e WLAN[6], existem muitas partes que podem influenciar as funções, fluxos de trabalho, segurança dos dados e informação.

1.1. Objetivos do trabalho

Num trabalho deste âmbito, perspetivadas as envolventes e os condicionamentos impostos por um conjunto de pressupostos iremos simplesmente focarmo-nos, face às tendências atuais impostas pelos consumidores e pelos utilizadores em geral de sistemas móveis, na evolução que as organizações terão que fazer nas suas infraestruturas de rede adotando sistemas que lhes permitam acompanhar esta evolução e tendência de trabalho dos seus trabalhadores, colaboradores, clientes e fornecedores.

De todo este ecossistema móvel o estudo ir-se-á concentrar nas emergentes redes locais de comunicações *wireless*, mais concretamente as WLAN, nos problemas que aportam às organizações, nomeadamente, em questões de segurança, opções de arquitetura e melhor forma de as criar e/ou integrar com as infraestruturas existentes, analisando o impacto das redes *wireless* infraestruturadas no ambiente organizacional e ainda avaliar o que a sua evolução poderá trazer de vantagem competitiva para esta.

Outro dos objetivos é o de analisar literatura publicada, *standards* de referência destas redes, trabalhos anteriores e *white papers* de diversas organizações reconhecidas internacionalmente, que nos ajudem a enquadrar a análise e o que deve ser tido em atenção na implementação de WLAN, sua integração com a rede infraestruturada da organização e a adoção de políticas que lhes permitam garantir a segurança da informação que circula nelas.

Nos últimos anos, mais e mais organizações criam ambientes WLAN no seu sistema de informação. No entanto, a introdução das WLAN expõe um ponto adicional de vulnerabilidade pelo que potenciais atacantes podem invadir o SI através da vulnerabilidade das WLAN (Liang, et al., 2014). Estudamos os desafios de segurança em WLAN com o fornecimento de um modelo de referência com as boas práticas recomendadas pelos diversos *standards* dedicados à temática de segurança da informação e dos SI e medidas defensivas adequadas.

[5] Sigla utilizada comummente na identificação de aplicativos ou aplicações desenvolvidas para dispositivos eletrónicos móveis.

[6] Para efeitos do presente trabalho assume-se que a referência a WLAN designa redes locais sem fio (wireless) e LAN redes locais com fio.

1.2. Motivações

A amplitude e diversidade de tecnologias usadas pelas organizações permitem identificar duas grandes zonas, que podem ser denominadas:

- Tecnologia central - usada na produção/processamento dos produtos da organização;
- Tecnologia complementar - usada como complemento à tecnologia central e apoio à tarefa principal.

Dentro deste contexto é importante ter a perceção da importância e relevância das tecnologias de transmissão de dados que atualmente ocupam um espaço cada vez mais abrangente e com maiores desafios para as organizações pois são o *core*[7] de toda a sua estrutura tecnológica.

Como tal, a relação entre as organizações e as tecnologias baseiam-se em pressupostos que as levam a adotar essas tecnologias, são aliciantes de um ponto de vista motivacional de análise, de como umas influenciam outras e como as decisões sobre qualquer delas, provocam mudanças na outra.

Esta evolução tecnológica e a necessidade que as organizações tem de olhar e adotar as novas tendências que marcam o mercado, conduziu a um tipo de problema que mistura tecnologia, inovação, atitudes e comportamentos pessoais, estratégia e oportunidades, pelo que as opções por uma evolução tecnológica na área da mobilidade das comunicações se torna premente, para fazer face ao enorme fluxo de informação que dai advém, garantindo acesso fácil e rápido à informação, não descurando as considerações de segurança da informação no ambiente organizacional mas mantendo a operacionalidade desses sistemas.

Com a constatação destas necessidades encontra-se motivação para a análise dos referenciais e soluções tecnológicas que permitam aumentar as interações, mobilidade e portabilidade dos intervenientes no processo, garantindo ao mesmo tempo a segurança e privacidade da informação e simultaneamente dos sistemas e das tecnologias que suportam essa informação, a informação organizacional.

Sendo o *wireless* uma área com inovações recentes, além das implementações dos *standards* do IEEE, onde existem já soluções que permitem substituir efetivamente redes infraestruturadas fixas, pretende-se com este trabalho analisar e verificar as linhas orientadoras

[7] Parte básica e mais importante de algo, neste caso a estrutura de comunicações.

desta evolução, especificamente, nas WLAN do ambiente organizacional, que levaram as organizações a adotá-las.

1.3. Enquadramento

As redes de computadores são atualmente elementos indispensáveis nas organizações por proverem aumento de comunicação entre funcionários, clientes e fornecedores, consequentemente, potenciando também o acesso à informação.

As redes *wireless* são uma das mais populares tecnologias para as comunicações privadas, fazendo hoje parte do nosso dia-a-dia, sendo certo que a sua utilização cresce rapidamente e abrange, já e cada vez mais, o setor organizacional, aparecendo na agenda do dia de cada vez mais organizações.

Associando-se ao papel preponderante que estas redes vão assumindo no desenvolvimento económico e social da sociedade em geral conduz a que as organizações tendam a inovar e a adotar tecnologias que as beneficiem, reduzam os seus custos de exploração ou lhe ofereçam vantagens competitivas.

Do muito que se tem escrito sobre a temática das organizações e das tecnologias adotadas por estas, de forma a obterem vantagens competitivas, julgamos que ainda existe margem para contributos incrementais, que clarifiquem o estado atual das redes de comunicações *wireless*, mais concretamente as WLAN organizacionais, os problemas que aportam às organizações, nomeadamente em questões de segurança, opções de arquitetura e melhor forma de as integrar com as infraestruturas existentes fixas ou não, ou logo desde início como infraestrutura primária de comunicações.

Segundo Dhanalakshmi e Sathiya (2015) nos últimos anos, com o aparecimento de novas tecnologias, as WLANs surgiram como nova proposta para superar limites de alcance e mobilidade das comunicações. Esta nova modalidade de rede gerou vários desafios e ampliou horizontes nas comunicações. O *standard* do IEEE utilizado para este tipo de rede é o da classe 802.11. Este *standard*, com as suas sucessivas correções e alterações, decorre da necessidade de adaptação de requisitos, especificações e eliminação de falhas de segurança existentes constituem a base de toda esta evolução e desenvolvimento. Indicam-se a título de exemplo as alterações supervenientes através dos *standards* IEEE 802.11aa,ad,ae,ac e af, a cuja descrição desenvolvida se procede no Capitulo 2.

Referem os mesmos autores que este tipo de rede foi sendo adotado à medida que a sua velocidade era consideravelmente aumentada com o surgimento de novos *standards* e evolução tecnológica. A cada dia mais utilizadores domésticos e organizações das mais variadas dimensões as utilizam para diversas atividades e fins.

No decorrer dos últimos anos, várias falhas de segurança foram identificadas nos *standards* propostos. Estas falhas demonstram a fragilidade que envolve a questão da segurança neste tipo de rede, sendo que estas fragilidades estão ligadas principalmente, mas não exclusivamente, ao facto de não existirem limites físicos dos sinais transmitidos pelos equipamentos, o que possibilita a interceção da informação que transita entre estações comunicantes, mesmo a uma distância considerável. Com a utilização de equipamento adequado é possível ter acesso aos dados que transitam em uma rede *wireless*, mesmo estando distante dela alguns quilómetros (Alliance, 2012).

Surge assim reforçada a necessidade da análise da segurança da informação que circula neste tipo de infraestrutura pelo que visitaremos os *standards* IEEE da classe 802, 802.11, 802.1X, os *standards* ISO/IEC 27000 a 27002, o 27033, recomendações do *National Institute of Standards and Technology* (NIST) e *Wi-Fi Alliance*[8] para percebermos a forma de assegurar neste tipo de redes disponibilidade, integridade, autenticação e não repudiação da informação.

1.4. Abordagem à investigação

A metodologia é o corpo orientador da pesquisa, que obedecendo a um sistema de normas, torna possível a seleção e a articulação de técnicas, tendo em vista o desenvolvimento do processo de verificação empírica (Pardal e Correia, 1995).

De acordo com Gil (2009), a pesquisa bibliográfica é desenvolvida com base em material já elaborado, constituído principalmente de livros e artigos científicos. Para este autor, a principal vantagem desse tipo de pesquisa reside no facto de permitir ao investigador a cobertura de uma gama maior de fenómenos do que aquela que se poderia pesquisar diretamente.

Sendo o período atual, crítico e difícil tentou-se perceber a complexidade gerada pela adoção de tecnologia de comunicação *wireless*, mais complexa e a forma de garantir a sua compatibilidade com as atuais infraestruturas das organização e com futuros desenvolvimentos.

De acordo com a literatura revisitada e no seguimento do percurso metodológico, foram estabelecidas algumas proposições que irão orientar a investigação com relação aos efeitos percebidos do uso de tecnologias móveis no desempenho organizacional, onde se constatou que, aumenta principalmente a produtividade da empresa, sendo este efeito seguido pela obtenção de novos clientes, aumento das receitas e, por fim, redução dos custos operacionais.

[8] Associação internacional sem fins lucrativos formada em 1999 para certificar a interoperabilidade de produtos de WLAN baseada no IEEE 802.11.

Metodologicamente, para vincular o trabalho aos princípios e requisitos do método científico, optou-se por uma abordagem através de um conjunto de técnicas e ferramentas que se indicam:

- Pesquisa bibliográfica em bases de dados internacionais multidisciplinares como o EBSCO, *Proquest*, *Scielo*, *Scopus*, utilizando-se palavras-chaves relacionadas ao tema.
- Pesquisa documental, procurando na internet ferramentas de levantamento de informações utilizadas nos mais diversos *papers* técnicos para análise, projeção, implementação e segurança de redes organizacionais genérica e especificamente sobre as tecnologias de rede e *wireless*, baseadas nos *standards* 802 e 802.11 do IEEE, os *standards* ISO/IEC 27000 a 27002 e 27033, recomendações do NIST.

Procurou-se sintetizar e concretizar o problema numa questão clara e precisa, empírica, delimitada e passível de solução, isto é, do ponto de vista metodológico e seus critérios, que os temas e os conceitos em análise sejam livres de ambiguidade e dúvidas, observáveis através das técnicas e métodos apropriados e balizados, para evitar complexidade excessiva e dispersão (Gil, 2002; Eco, 2007), de forma a garantir que os pressupostos sejam suportados pelo estudo de documentos, pela análise dos *standards* associados à segurança das WLAN e da informação que nelas transita.

Desta forma, os nossos objetivos específicos concretizam-se se se verificar que os benefícios da tecnologia *wireless* atraem as organizações para implementar as suas WLAN, onde a questão da segurança se tornou cada vez mais importante, validando-se as soluções existentes, adotadas pelos novos *standards* e se garantem efetivamente o nível de segurança necessário e exigido, em conformidade com o definido na organização.

As WLAN apresentam os seus próprios desafios na análise, projeção, implementação e segurança, distintos de organização para organização, quando estas optam pela adoção de tal tecnologia, mas não têm uma solução única e exclusiva, devendo esta implementação ser analisada caso a caso, em conformidade, com os fatores já mencionados, mas não se esgotando nestes.

Neste trabalho faz-se uma revisão da literatura e levantamento de informações utilizadas nos mais diversos documentos técnicos para análise, projeção, implementação e segurança de redes empresariais e muito especificamente as baseadas nos *standards* wireless 802.11 do IEEE, mas também nas recomendações do NIST e *National Security Agency* (NSA) relacionadas com esta temática.

O contexto de pesquisa foi o de tentar perceber o que referiam os autores e organizações sobre este tipo de tecnologia, mais complexa e a forma de implementação com sucesso assim como, garantir a sua compatibilidade com as atuais infraestruturas das organização e com desenvolvimentos futuros.

Como principais limitações a este estudo refere-se a não divulgação pelas organizações de informação sobre as suas opções de implementação das WLAN e estratégias de segurança adotadas, pelo que nesta matéria existem muito poucos estudos sobre esta temática.

1.5. Resultados e contributos

Como resultado deste trabalho pretende-se tipificar e criar um referencial para apoio na implementação de WLAN nas organizações definindo um conjunto de requisitos que deverão ser observados, relacionando-os com os *standards* utilizados, tecnologias e segurança na sua implementação.

Com a crescente importância da tecnologia da informação, há uma necessidade urgente de medidas adequadas de segurança da informação pelo que foi necessário perceber o estado atual dos *standards* de segurança de informação, os *standards* ISO/IEC 27000, 27001 e 27002 que têm vindo a evoluir e sofrem revisões constantes nos últimos anos, a 27000 em 2014, a 27001 e 27002 em 2013 mas esta ultima já com nova revisão agendada ainda para 2015.

Diretamente ligada à segurança da informação em geral mas particularmente à segurança da rede iremos abordar também o *standard* ISO/IEC 27033, que tem sido substancialmente revisto, para se enquadrar na suite ISO27k, cuja última revisão ocorreu em 2015 com a publicação da ISO/IEC 27033-1:2015 que abordaremos também em capítulo próprio.

Como contributo espera-se que o referencial simplifique atividades e identifique desafios na construção de soluções de mobilidade que possam melhorar a conceção, integração, utilização e otimização das WLAN nas organizações.

Associado à adoção das WLAN pelas organizações verificam-se duas tendências significativas e que poderão afetar grandemente a forma como as redes *wireless* são projetados:

- A primeira é a tecnologia *Wi-Fi* de alta velocidade, baseada no protocolo 802.11ac;
- A segunda é a necessidade de personalizar as experiências dos utilizadores das redes móveis para entregar a qualquer hora, em qualquer lugar acessos sem provocar estragos nas operações de rede e controlo de custos.

1.6. Estrutura do trabalho

O presente trabalho está estruturado em 5 capítulos, cada um deles associado a dimensões estruturais diferenciadas a saber:

- Capitulo 1 – Introdução – Contextualização do trabalho proporcionando também uma perspetiva global sobre o tema, sua problemática, pesquisa e forma de abordagem, assim como objetivos e metodologia utilizada;
- Capitulo 2 – Enquadramento – sintetizam-se os diferentes aspetos considerados fundamentais para a realização do trabalho, referindo conceitos, trabalhos e literatura de referência sobre organizações, informação e segurança, infraestruturas tecnológicas, nomeadamente as das WLANs e *standards* destas;
- Capítulo 3 – Caracterização do problema - recorrendo a definições e opiniões dos entendidos, pretende-se fazer uma caraterização/tipificação da situação atual, de adoção de WLANs pelas

organizações, identificação de requisitos, integração com infraestrutura, segurança da informação que nela circula e a sua evolução na organização servindo de ponto de partida para o capítulo seguinte;

- Capítulo 4 – Implementação de redes sem fios - resultante da caraterização e definições provenientes do capítulo anterior, problemas associados e aspetos a considerar numa solução, especificamente para garantir uma implementação com sucesso nas organizações, tentando-se fornecer um modelo base de orientação com definição dos princípios básicos a considerar;
- Capitulo 5 – Referenciais a considerar – onde de uma forma consolidada se estabelece o conjunto de condições e requisitos a considerar na implementação das WLAN na organização estabelecendo o modelo de referencial;
- Finalmente o capítulo 6 – Conclusões – abordam-se e sistematizam-se os resultados e conclusões do trabalho desenvolvido procedendo-se a uma reflexão sobre o tema apresentado, em forma de conclusão. São ainda identificadas linhas orientadoras para estudos futuros de forma a consolidar todo o trabalho desenvolvido;

Esquematicamente podemos perceber o alinhamento na figura 2:

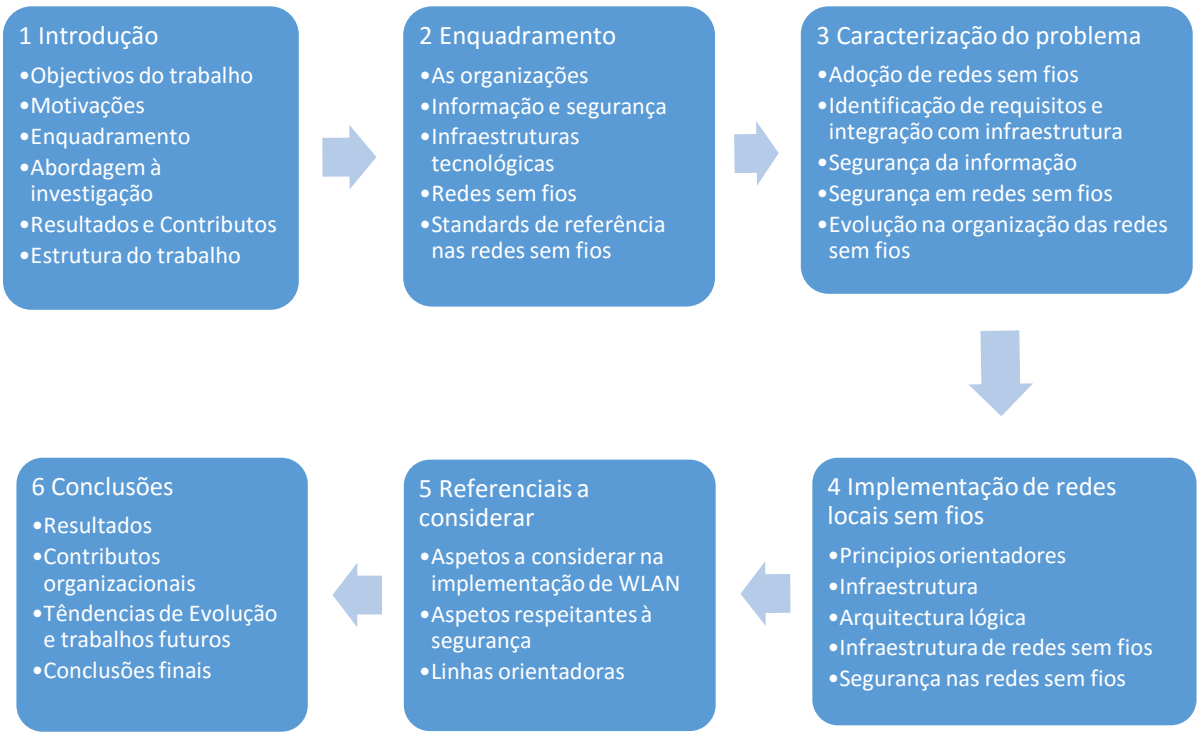

Figura 2 – Estrutura do trabalho

A bibliografia é apresentada no final do documento referenciando globalmente, quer os documentos que serviram de base à pesquisa, quer *standards* e livros de autores de reconhecido mérito na área, que estiveram na base deste trabalho.

2 Enquadramento

Neste capítulo analisam-se aspetos considerados fundamentais para a realização do trabalho, conceitos relacionados com a temática do trabalho, papel inerente às organizações neste contexto, de forma de garantir vantagens competitivas e a sobrevivência das próprias organizações no mercado global atual, assim como desafios colocados ao nível da informação e respetiva segurança.

Na base de tudo isto está a infraestrutura tecnológica adotada pela organização e que faz parte da sua estratégia de desenvolvimento.

Estas novas exigências conduzem muitas vezes à adoção de tecnologia, como as WLAN, pelo impacto positivo que as mesmas trazem ao ambiente organizacional e vantagens competitivas, pela alteração de paradigma, na forma como as aplicações são entregues e ou suportadas nos diferentes tipos de estruturas. O papel desta tecnologia, preponderante no desenvolvimento económico e social da sociedade em geral leva a que as organizações tendam a inovar, adotando novas tecnologias que reduzam os custos de exploração e permitam responder às necessidades de mobilidade dos seus clientes, funcionários e fornecedores.

Assim, ao longo dos diversos capítulos, iremos abordar a temática da organização definindo alguns conceitos seus associados, ligação entre o meio envolvente desta e a mudança, relacionando opções tecnológicas tomadas com a sua estratégia de negócio, a questão da manutenção da segurança da informação, quer pessoal quer organizacional, mas observando as necessidades estratégicas das organizações e as limitações impostas pelas tecnologias adotadas.

Na parte final faz-se uma abordagem aos *standards* que regulamentam e definem as regras associadas às WLAN que garantem a facilidade da conceção, normalização, implementação e segurança em consonância com o estabelecido.

2.1 As organizações

Etimologicamente, organização (do grego, *organon*) significa ferramenta ou instrumento. Organização é um instrumento criado pelo homem para desenvolver tarefas que ele não poderia realizar sozinho (Santos, 2009).

Segundo Maximiano (1992), uma organização é uma combinação de esforços individuais que tem por finalidade realizar propósitos coletivos. Por meio de uma organização torna-se possível perseguir e alcançar objetivos que seriam inatingíveis para uma pessoa. Uma grande empresa ou uma pequena oficina, um laboratório ou o corpo de bombeiros, um hospital ou uma escola são todos exemplos de organizações.

De acordo com Robbins (1990), organização é uma entidade social conscientemente coordenada (liderada), com uma fronteira relativamente identificável, que funciona numa base relativamente contínua para alcançar um objetivo e/ou objetivos comuns. Uma organização é constituída por pessoas – para que ela mude, também as pessoas têm que mudar. No entanto, o ser humano é único e, como tal, cria o seu

próprio pensamento individual, quer por antecipação, quer por reação. A forma como estes pensamentos e correspondentes ações se refletem no contexto organizacional poderá ganhar uma dimensão tal, que torna a reação do sistema imprevisível

Uma organização é formada pela soma de pessoas, máquinas e outros equipamentos, recursos financeiros e outros. De uma forma simples, as organizações podem ser definidas como conjuntos de pessoas que trabalham de forma coordenada para atingir objetivos comuns (Cunha, Rego, Cunha, e Cardoso, 2007).

A teoria das organizações constitui uma disciplina próxima, que tem como domínio específico a construção e testagem de teorias sobre as organizações, os seus membros e a sua gestão, as relações organização-envolvente e os processos organizativos. Os temas da teoria das organizações incluem a escolha estratégica, a dependência e recurso, a ecologia organizacional e a teoria institucional (Cunha et al.,2007).

2.1.1 Estratégia e Tecnologia

Segundo Cunha et al., (2007) a tecnologia tem constituído um dos temas mais importantes nos debates de gestão. Este interesse está relacionado com aspetos tão diversos como as consequências da implementação da tecnologia sobre a conservação ou extinção de postos de trabalho, a mudança na execução do trabalho trazida pela introdução de novas tecnologias.

Por tecnologia deverá entender-se, de acordo com Tushman e Anderson (1986, citado por Cunha et al.,2007), o conjunto das ferramentas, dispositivos e conhecimento que medeiam as entradas (*inputs*) e as saídas (*outputs*) do trabalho.

Segundo Prahalad e Krishnan (2002, citado por Rodrigues e Fernandez,2012) referindo os resultados de sua pesquisa, as organizações relatam frequentemente que a infraestrutura de tecnologia de informação (TI) não acompanha o nível de desejo de inovação, verificando-se que este desalinhamento da TI é, em geral, um empecilho para a implementação de mudanças no negócio.

O papel estratégico dos sistemas de informação (SI) envolve a utilização da TI para desenvolver produtos, serviços e capacidades que confiram a uma organização vantagens estratégicas sobre as forças competitivas que ela enfrenta no mercado mundial.

Referem ainda Rodrigues e Fernandez (2012) que segundo O'Brien (2001, p.282) "este papel gera sistemas de informações estratégicas, os quais apoiam ou moldam a posição e estratégias competitivas de uma empresa" e ajuda a organização a obter vantagem competitiva, reduzir desvantagem competitiva ou alcançar outros objetivos estratégicos.

Uma organização pode sobreviver e ter sucesso a longo prazo se ela desenvolver eficazmente estratégias para enfrentar as cinco forças competitivas de Porter (1980;1985). O rápido crescimento da *Internet*, *intranets*, *extranets* e outras redes globais interconectadas nos anos 90 alterou radicalmente o potencial estratégico dos SI nos negócios. Esta ligação em rede organizacional global, revolucionou a

computação nas organizações e entre elas, consequentemente alterou as comunicações e colaboração que apoiam as operações organizacionais gerando um novo ambiente para os negócios, proporcionando o aumento da escala de uso dos negócios eletrónicos (Castells, 2011).

2.1.2 Meio envolvente e a mudança

Existem grandes adversidades económicas a nível internacional, embora nunca, como agora, se tenha assistido a tamanho nível de complexidade e envolvência sistémica, fruto de uma globalização crescente:

- Pesquisas na área dos SI revelam que inúmeros fatores influenciam a adoção da TI, podendo inclusive mudar em função do tipo de tecnologia e do contexto onde ela está inserida (Kim, Chan, e Gupta, 2007).
- Um dos primeiros modelos estatísticos sobre adoção de tecnologia da informação, o *Technology Acceptance Model* (TAM) desenvolvido por Davis (1989), que demonstrou que, entre tantas variáveis já percebidas na época, duas delas eram extremamente determinantes, a utilidade e a facilidade de utilização, normalmente pela perceção e aceitação:
  - ✓ As pessoas tendem a usar ou não uma tecnologia na medida em que elas acreditam que esta vai ajudá-las a executar melhor seu trabalho;
  - ✓ Mesmo percebendo a utilidade da tecnologia, seu uso será influenciado pela facilidade de utilização.

Modelos como o TAM são adequados para estudos em um contexto organizacional, no qual são diferenciados o consumidor do serviço (organização) e o utilizador da tecnologia.

No entanto, o contexto pode ser um tanto diferente ao investigar o uso da internet móvel (IM) nas organizações, uma vez que apresenta a particularidade de, além de servir aos propósitos organizacionais, também poder ser usada para fins pessoais (Kim et al., 2007). Assim, em muitos casos, os funcionários assumem o duplo papel de utilizadores da tecnologia e de consumidores do serviço. Considerando que há investimentos e despesas para se usar a tecnologia, é lógico pensar que a adoção pode variar em função de quem suporta as despesas, organização ou utilizador.

Outro aspeto a ser considerado é que várias tecnologias implantadas nas organizações são mandatárias, ou seja, os funcionários são obrigados a usar. Nesse caso, o uso da tecnologia para o utilizador pode ser percebido como um sacrifício.

Segundo (Turban, Leidner, McLean, e Wetherbe, 2010), diversos fatores sociotécnicos impulsionam a rápida expansão da utilização dos dispositivos móveis *wireless* para acesso à *Internet*. Como principais fatores referenciam-se:

a) Disseminação – o número de telemóveis cresce exponencialmente em todo o mundo, sendo cada vez mais comum a capacidade de acesso à *Internet* por meio desses dispositivos;

b) Popularização – o uso do telemóvel, *smartphones* e de outros dispositivos móveis *wireless* é um fenómeno social, em praticamente todas as faixas etárias;
c) Redução do preço – o preço dos dispositivos móveis está mais acessível aos compradores, em grande parte devido à redução de custos proporcionada pela escala de produção;
d) Funcionalidade – a introdução de novos recursos nos dispositivos, como também de aplicativos na *Internet*, torna o conjunto cada vez mais útil;
e) Velocidade de transmissão de dados – a largura de banda atual propicia a realização de operações que antes só eram possíveis usando computadores ligados à Internet através de ligações com fios.

Os paradoxos da tecnologia móvel (Corso, Freitas, e Behr, 2012; Gonçalves e Joia, 2011; Jarvenpaa e Lang, 2005) emergem no processo de ação e experiência dessa tecnologia a partir da perspetiva do utilizador, levando-se em consideração que tais ações e experiências são dependentes de fatores situacionais e contextuais.

No entanto, a maior parte dos estudos ainda é de cunho técnico ou para perceção do comportamento do consumidor (San Martín, López-Catalán, e Ramón-Jerónimo, 2012), mas não de uma perspetiva organizacional de vantagens na adoção de tecnologia móvel.

Estudos desenvolvidos por Balocco, Mogre, e Toletti (2009) e San Martín et al., (2012) são dos poucos que examinam esse fenómeno enfatizando a IM sob a perspetiva da empresa.

Considerando as pesquisas efetuadas, encontram-se como referências ao nível organizacional alguns trabalhos, que se indicam e que analisam alguns fenómenos específicos no contexto de adoção das tecnologias móveis mas que servem para uma perceção mínima da envolvente organizacional e sua utilização:

a) Trabalhos teóricos, como o de Machado e Freitas (2007), propondo um modelo para o planeamento das iniciativas de adoção de tecnologias móveis pelas organizações na interação com seus públicos-alvo; e o de Bento, Martens e Freitas (2013), apresentando um conjunto de elementos decorrentes da adoção de tecnologias móveis em equipas de vendas;
b) Estudos de caso, como o de Saccol e Reinhard (2005), Manica e Saccol (2009), Costa, Saccol e Vieira (2011), visando analisar aplicações de tecnologias móveis e sem fios e decorrências de suas utilizações;
c) Gonçalves e Joia (2011), que analisam os efeitos do uso das tecnologias móveis em profissionais utilizadores de *smartphones*;
d) *Surveys*, como a de Tavares et al (2012), que testa um modelo estrutural para mostrar a influência das tecnologias móveis na inovação em serviços;
e) Estudos utilizando dados secundários, como o de Cappellozza, Sanchez e Albertin (2011), investigando a relação entre infraestrutura de TI e dispositivos móveis;

f) E Klein, Karl e Cunha (2013), pesquisando o conceito de capacidade organizacional para a mobilidade.

Ainda que boa parte desses estudos não utilize explicitamente o termo IM, percebe-se o seu uso nas organizações onde facilitam o acesso aos sistemas corporativos e a ferramentas de produtividade, tais como correio e agendas eletrónicas (Ghose e Han, 2011; Gonçalves e Joia, 2011).

As organizações que fazem uso dessas tecnologias móveis não apenas fornecem aos seus trabalhadores capacidades de computação móvel, mas também reestruturam seus processos de negócio, procedimentos operacionais, estrutura organizacional e sistemas de recompensa em torno das necessidades emergentes de novos modelos de gestão (Chen e Nath, 2008), o que pode resultar na melhoria gradual das práticas de trabalho, permitindo ganhos de eficiência e flexibilidade.

2.2 Informação e segurança

De acordo com Strechie (2014), informação vem do latim *informatio,onis*, ("delinear, conceber ideia"), ou seja, dar forma ou moldar na mente, como em educação, instrução ou treinamento.

A palavra do grego antigo para forma era *μορφή* (*morphe*; cf. morfo) e também *εἶδος* (*eidos*) "tipo, ideia, forma, 'aquilo que se vê', configuração", a última palavra foi usada famosamente em um sentido filosófico técnico por Platão (e mais tarde Aristóteles) para denotar a identidade ideal ou essência de algo.

Informação é o resultado do processamento, manipulação e organização de dados, de tal forma que represente uma modificação (quantitativa ou qualitativa) no conhecimento do sistema (pessoa, animal ou máquina) que a recebe (Amaral, Magalhães, Morais, Serrano e Zorrinho, 2005).

Segundo Jannuzi, Falsarella, e Sugahara (2014) a produção intensa de conhecimento científico e tecnológico vivenciada pela sociedade nos dias atuais dá a esta uma característica que lhe permite a denominação de sociedade do conhecimento. Sob este prisma, esta sociedade tem na informação o alicerce de seu desenvolvimento, pois é ela que viabiliza a aquisição e geração de conhecimentos.

Para estes autores desse modo, seja no âmbito científico, tecnológico, social ou económico, a sociedade faz da informação um fator determinante para orientar suas ações. O reconhecimento do seu valor e da sua influência no funcionamento e no desenvolvimento da sociedade faz da informação um tema de grande interesse nos estudos científicos e tecnológicos. Entretanto a condução desses estudos não se constitui uma tarefa fácil, pois a informação é um conceito que ainda gera diferentes entendimentos, facto este que pode ser amplamente identificado na literatura sobre o tema.

Nos estudos e aplicações relacionados com a informação é possível observar um amplo leque de conceitos sobre o tema, incluindo diversas categorizações em diferentes contextos. Este quadro conceitual resulta das características intrínsecas da informação, mas também do facto desta, enquanto fenómeno, estar presente como parte indissociável do processo de comunicação. Essas inúmeras categorizações da

informação - ou, porque não dizer, significados - podem ser exemplificadas no âmbito das organizações do setor económico.

No ambiente das organizações, bem como nos estudos voltados para o tema informação neste ambiente, é possível identificar termos compostos que procuram atribuir uma identidade - informação operacional, informação financeira entre outras, bem como termos que procuram sistematizar o conjunto de informações – por exemplo sistemas de informações transacionais, sistema de processamento de transações, sistemas de informação de gestão, sistema de apoio executivo, sistemas de apoio à decisão (Falsarella, Beraquet, e Jannuzzi, 2003; Turban, Ranier JR, e Potter, 2007; Cassarro, 2010; Laudon e Laudon, 2010; O'Brien e Marakas, 2013; Rezende e Abreu, 2013).

Para as organizações, que almejam a competitividade no mercado em que atuam, a informação é um insumo deveras importante na condução de seus negócios. Todavia não há como tratar a informação nas organizações sem falar dos SI, mais ainda, dos sistemas de informação baseados em computador (SIBC), pois estes são suportes cada vez mais imprescindíveis ao processo administrativo das organizações. Assim, saber que SI são adequados para as necessidades da organização é facto relevante na gestão de qualquer negócio. Todavia, esse discernimento não se apresenta como uma tarefa fácil diante dos inúmeros tipos de SI.

Por outro lado não podemos falar de informação sem falar em segurança dessa informação, pelo que não devemos esquecer que a informação é um ativo que, como qualquer outro ativo importante, é essencial para os negócios de uma organização e que segundo o *standard* ISO/IEC 27000 (2014):

- Necessita de ser adequadamente protegida no tecido organizacional, pois com o aumento de conetividade, a informação fica exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades;
- A informação pode existir em diversas formas, pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrónicos, apresentada em filmes ou falada em conversas. Seja qual for a forma apresentada ou o meio através do qual a informação é compartilhada ou armazenada, é recomendado que ela seja sempre protegida;
- A Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio;
- A segurança da informação é obtida a partir da implementação de um conjunto de controlos adequados, incluindo políticas, processos, procedimentos, estruturas organizacionais e funções de *software* e *hardware*. Estes controlos precisam ser estabelecidos, implementados, monitorados, analisados criticamente e melhorados onde necessário, para garantir que os objetivos do negócio e de segurança da organização sejam atendidos.

Numa organização torna-se necessário efetuar uma gestão de riscos de segurança da informação, de forma a identificar as necessidades da organização em relação aos requisitos de segurança da

informação e criar um sistema de gestão de segurança da informação (SGSI) que seja eficaz. Convém que esta abordagem seja adequada ao ambiente da organização.

Os esforços de segurança devem lidar com os riscos de uma forma efetiva e no tempo apropriado, onde e quando forem necessários. Convém que a gestão de riscos de segurança da informação seja parte integrante das atividades de gestão da segurança da informação e aplicada tanto à implementação quanto à operação quotidiana de um SGSI.

Com a globalização, as mudanças são mais frequentes e os interesses por informações valiosas, sejam tecnológicas, operacionais ou financeiras, aumentaram significativamente. A Informação assume hoje em dia uma importância crescente (ISO/IEC 27000, 2014; Ward, Griffiths e Whitmore, 1990), fundamental na descoberta e introdução de novas tecnologias, exploração das oportunidades e de investimento de uma organização. As tecnologias da informação e comunicação (TIC)[9] começaram a fornecer base material para uma nova economia informacional e globalizada. Como afirma Castells (2011), essa nova economia é informacional, pois a capacidade para gerar, armazenar, processar e aplicar efetivamente o conhecimento, baseado em informações, determinará a produtividade e competitividade. A garantia da confidencialidade, da integridade e da disponibilidade da informação (ISO/IEC 27002, 2013) passam a ser fatores essenciais para o sucesso das organizações nos dias de hoje.

A segurança, como bem comum, é divulgada e assegurada através de um conjunto de convenções sociais, denominadas medidas de segurança.

A segurança da informação está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização. São características básicas da segurança da informação os atributos de confidencialidade, integridade, disponibilidade e autenticidade, não estando esta segurança restrita somente a sistemas computacionais, informações eletrónicas ou sistemas de armazenamento. O conceito aplica-se a todos os aspetos de proteção de informações e dados. O conceito de segurança informática ou segurança de computadores está intimamente relacionado com o de segurança da informação, incluindo não apenas a segurança dos dados/informação, mas também a dos sistemas em si (ISO/IEC 27002, 2013).

A Gestão de Riscos, por sua vez, fundamental para garantir o perfeito funcionamento de toda a estrutura tecnológica da empresa, engloba a Segurança da Informação, já que hoje a quantidade de vulnerabilidades e riscos que podem comprometer as informações das organizações é cada vez maior.

Ao englobar a Gestão da Segurança da Informação, a Gestão de Riscos tem como principais desafios proteger um dos principais ativos da organização – a informação – assim como a sua marca e reputação, implementar e gerir controlos que tenham como foco principal os objetivos do negócio,

[9] Considerando que alguns autores definem as TIC e as TI no contexto dos SI de forma idêntica, frequentemente usados como sinónimos e uma vez que a separação entre computador e comunicação se dilui cada vez mais, considera-se neste trabalho o termo TI como representante de ambos passando-se a utilizá-lo ao longo do mesmo, atribuindo-se todavia, o mesmo significado a ambos os termos.

promover ações corretivas e preventivas de forma eficiente, garantir o cumprimento de regulamentações e definir os processos de gestão da Segurança da Informação. Entre as vantagens de investir na Gestão de Riscos voltada para a Segurança da Informação estão a priorização das ações de acordo com a necessidade e os objetivos da organização e a utilização de métricas e indicadores de resultados (Cassarro, 2010).

Fazendo o enfoque nas comunicações, verifica-se que as redes de computadores são atualmente elementos indispensáveis nas organizações por incrementarem a comunicação entre funcionários, clientes e fornecedores e consequentemente, aumentando também o acesso à informação. Com o surgimento de novas tecnologias nos últimos anos, as WLAN surgiram como nova proposta para superar limites de alcance e mobilidade. Esta nova modalidade de rede gerou vários desafios e ampliou os horizontes nas comunicações (Stallings, 2013).

Como resultado desse incrível aumento tecnológico, a informação está agora exposta a um crescente número e variedade de ameaças.

Também aqui, apesar da definição de requisitos específicos orientados para a segurança nas redes de comunicação pelos *standards* do IEEE, no decorrer dos últimos anos, várias falhas de segurança foram identificadas nestes.

Estes problemas demonstram a fragilidade que envolve a questão da segurança deste tipo de rede. Estas fragilidades estão ligadas, factualmente, à ausência de limites físicos dos sinais transmitidos pelos equipamentos, possibilitar a aquisição da informação que transita entre as estações comunicantes mesmo a uma distância considerável (Acker, 2010).

Durante o desenvolvimento dos *standards* de segurança a serem utilizados nas redes 802.11 não houve o comedimento necessário para que fossem realizadas análises mais profundas acerca dos algoritmos que seriam empregues, provocando como tal graves lacunas de segurança.

2.3 Infraestruturas tecnológicas

Desde logo, as TI ainda não são um conceito perfeitamente delimitado e as dificuldades em estabelecer uma classificação universal para os produtos e serviços de TI remontam, pelo menos a 1998, quando foram reconhecidas pela *Organisation for Economic Cooperation and Development* (OECD) através do *Working Party on Indicators for the Information Society* (WPIIS)[10]. Um (talvez dos maiores) dos desafios que se coloca relaciona-se com uma característica intrínseca aos produtos ou serviços de alta tecnologia: a mudança e a rapidez com que esta se opera.

Mas há já bastantes autores e entidades que desenvolveram conceitos mais ou menos complexos e abrangentes. Nesse âmbito, o conjunto de tecnologias que suportam os sistemas informáticos e de

[10] Um dos quatro grupos especializados constituídos no seio da OECD, no âmbito do comité para as políticas da Sociedade da Informação e das TI.

comunicações é uma designação genérica por vezes aplicada às TI (ANACOM, 2015). Mais meticulosa é a designação de TIC[11], como sendo uma moderna combinação de tecnologias informáticas e telecomunicações, onde se incluem computadores (*hardware* e *software*), periféricos, redes, outras máquinas e dispositivos tecnológicos que apoiam o processo de armazenagem, agrupamento, distribuição de informação e comunicação na empresa (Whitten e Bentley, 2007).

É comummente aceite que as organizações, que, de forma intensiva, desenvolvem e implementam sistemas e tecnologias de informação, colocando-as ao serviço do planeamento estratégico, terão melhorias significativas na gestão e no processo de tomada de decisão (Shuman, 1982).

Rodrigues e Fernandez (2012) citando Prahalad e Krishnan (2002) referem que as organizações estão em contínua busca do sincronismo da estratégia e da tecnologia da informação porque sabem da vantagem competitiva que ganharão. Porém, é um grande desafio que poucos até o momento conseguem superar.

Quanto mais global e estruturado for o SI, entendido como um conjunto de meios humanos e técnicos, dados e procedimentos, articulados entre si, com vista a fornecer informação útil para a gestão das atividades da organização onde está inserido e quanto melhor representar a organização em funcionamento, mais flexível poderá ser essa organização, na medida em que o SI vai atuar sob a forma de análise da organização e seus sistemas envolventes. O SI vai surgir como um instrumento de mudança estratégica na estrutura organizacional, colocando novos desafios e exigindo a utilização de novas metodologias com a presença das TI, na medida em que estas constituem um potencial de desenvolvimento para as organizações (Jannuzi, Falsarella e Sugahara, 2014).

As TI impulsionam o progresso, conduzem a inovações, aumentam a riqueza e atraem novos investimentos. Em simultâneo, permitem um aumento da eficiência e a redução dos preços, bem como melhoram os serviços ao cliente, a qualidade e a variedade dos produtos.

A introdução de SI/TI numa organização irá provocar um conjunto de alterações, nomeadamente ao nível das relações da organização com o meio envolvente (analisado em termos de eficácia, nomeadamente em termos de cumprimento da missão da organização) e ao nível de impactos internos na organização (analisados através da eficiência organizacional em termos de opções estratégicas) (Reisswitz, 2008).

As TI são um recurso valioso e provocam repercussões em todos os níveis da estrutura organizacional (Reisswitz, 2008):

- Ao nível estratégico, quando uma ação é suscetível de aumentar a coerência entre a organização e o meio envolvente, que por sua vez se traduz num aumento de eficácia em termos de cumprimento da missão organizacional;

[11] Como referido anteriormente para efeitos deste trabalho adotar-se-á exclusivamente o termo TI.

- Aos níveis operacional e administrativo, quando existem efeitos endógenos, traduzidos em aumento da eficiência organizacional em termos de opções estratégicas.

No entanto, ao ser feita esta distinção, não significa que ela seja estanque, independente, pois existem impactos simultâneos aos vários níveis, estratégico, operacional e tático.

Nas últimas décadas as redes de computadores tem feito parte do nosso dia-a-dia em todas as vertentes desde a vertente empresarial até nossa casa, no acesso à Internet, bancos, hospitais e tudo o mais que possamos imaginar tem como base uma rede de computadores.

Já nas organizações os computadores estão ligados para partilha de recursos, capacidade de processamento e interligação pelas mais diversas razões, desde a facilidade de cooperação entre todos os utilizadores, a partilha de ficheiros, as mensagens de correio eletrónico, o acesso a aplicações, partilha, gestão de dados e bases de dados.

Mas estas redes são complexas misturando um número de disciplinas autossuficientes da ciência e engenharia como telecomunicações, computação, tecnologia da informação e/ou engenharia da computação na criação e otimização dos seus sistemas.

Os sistemas de computadores estão ligados simplesmente através de telecomunicação. As telecomunicações, por sua vez, podem ser operadas com sistemas de computador.

O desenvolvimento das redes de computadores atuais pode ser datado desde o meio do século passado com iniciativas de ligação entre dois equipamentos remotamente.

Segundo Monteiro e Boavida (2011), uma rede de comunicação pode ser classificada segundo um ou mais critérios. Os critérios mais comuns/frequentes são:

- Débito (baixo, médio, alto, muito alto);
- Topologia (*bus*, anel, estrela, híbrida);
- Meios físicos (cobre, fibra ótica, micro-ondas, infravermelhos por exemplo);
- Tecnologia de suporte (por exemplo comutação de pacotes, comutação de circuitos, assíncronas, plesiócronas, síncronas);
- Ambiente ao qual se destinam (redes de escritório, redes industriais, redes militares, redes de sensores por exemplo)

No entanto, a classificação mais frequente baseia-se na área (geográfica ou organizacional), e aí entram os termos que normalmente ouvimos:

- ✓ LAN (*Local Area Networks*) – também designadas de redes locais, são o tipo de redes mais comuns uma vez que permitem interligar computadores, servidores e outros equipamentos de rede, numa área geográfica limitada (ex. sala de aula, casa, espaço Internet);
- ✓ MAN (*Metropolitan Area Networks*) – permitem a interligação de redes e equipamentos numa área metropolitana (ex. locais situados em diversos pontos de uma cidade);

- ✓ WAN (*Wide Area Networks*) – permitem a interligação de redes locais, metropolitanas e equipamentos de rede, numa grande área geográfica (ex. país, continente);
- ✓ PAN (*Personal Area Networks*) – também designadas de redes de área pessoal, são redes que usam tecnologias de rede *wireless* para interligar os mais variados dispositivos (computadores, *smartphones* por exemplo) numa área muito reduzida;
- ✓ SAN (*Storage Area Networks*) – também designadas de redes de armazenamento, têm como objetivo a interligação entre vários computadores e dispositivos de *storage* (armazenamento) numa área limitada. Considerando que é fundamental que estas redes tenham grandes débitos (rápido acesso à informação), utilizam tecnologias como por exemplo *Fiber Channel*[12].

2.4 Redes sem fios

Comunicação *wireless* é a transferência de informações entre dois ou mais pontos que não estão ligados por um condutor elétrico.

Os diferentes tipos de tecnologias de comunicação *wireless* incluem (Dhanalakshmi e Sathiya, 2015):

- ➢ Comunicação por infravermelhos (IR);
- ➢ *Bluetooth;*
- ➢ *Wi-fi*[13]*;*
- ➢ Rádio;
- ➢ Telefone móvel ou celular.

O Wi-Fi *Alliance* define *Wi-Fi*, como qualquer rede de área local *wireless* (WLAN), de produtos baseados nos *standards* 802.11 do IEEE.

No entanto, como a maioria dos WLAN modernas são baseados sobre esses *standards*, o termo "*Wi-Fi*" é usado, como um sinónimo para "WLAN", não se aplicando neste trabalho onde se utiliza a expressão em conformidade com a sua aplicação.

Segundo diversos autores, as WLAN são um sistema de comunicação de dados extremamente flexíveis, podendo ser empregues como extensão ou alternativa para as redes fixas em ambientes locais como a LAN, sendo uma tecnologia que combina conectividade de dados com mobilidade através do uso de *Radio Frequency* (RF) (Garber, 2012; Sanaei, Abolfazli, Gani e Buyya, 2014; Stallings e Beard, 2015).

[12] Tecnologia para transmissão de dados entre dispositivos de computador a taxas de até 10 *Gbps* de dados.

[13] Comunicação *Wi-Fi*, também escrita *Wi-Fi* ou *WiFi*, é uma tecnologia popular que permite que um dispositivo eletrónico efetue troca de dados ou se ligue à internet *wireless* através de ondas de rádio. O nome é um nome de marca e foi indicado para ser uma brincadeira com o termo audiófilo *Hi-Fi*.

Além disso segundo os mesmos autores, representam ou podem representar (conforme a solução adotada) um *gateway*[14], separar domínios de colisão, ou mesmo traduzir protocolos entre os dispositivos *wireless* e uma LAN infraestruturada organizacional.

As WLAN, inicialmente, tentavam simplesmente imitar a estrutura das LAN, usando outro meio para transferir dados, ao invés de cabos, sendo que este meio poderá ser o das ondas eletromagnéticas de RF ou de IR. Como qualquer rede, necessita de *hardware* que permita esta conectividade assim como protocolos que estabeleçam as regras deste funcionamento.

Na base deste sistema estão os *standards* 802.11 desenvolvidos pelo IEEE desde 1997 para definição das regras de performance e segurança das WLAN, que foram estabelecendo e consolidado a tecnologia, em conformidade com as necessidades dos utilizadores e a evolução tecnológica.

A estrutura básica de uma WLAN é chamada de *Basic Service Set* (BSS), em que a rede consiste habitualmente de um *Access Point* (AP)[15] e vários dispositivos *wireless*. Quando esses dispositivos tentam comunicar entre si, propagam os seus dados através do AP. A fim de formar a rede, o AP continua transmitindo o seu *Service Set IDentifier* (SSID) para permitir que outros equipamentos se juntem à rede.

O IEEE 802.11 define dois modos de funcionamento para as WLAN, o *Infrastructure mode* e o *Ad-hoc mode*, mas em ambos os modos de funcionamento, um SSID, identifica-as.

O SSID é um nome configurado no AP (para o *Infrastructure mode*) ou num cliente *wireless* inicial (para o modo *ad-hoc*) que identifica a WLAN. O SSID é periodicamente anunciado pelo AP ou o cliente *wireless* inicial, usa uma *frame*[16] especial de gestão MAC[17] 802.11 conhecida como *beacon frame*[18].

As WLAN baseiam-se principalmente em dois grupos conjunturais:

- Clientes ou dispositivos de utilizador final - Os clientes estão equipados com dispositivos que permitem que o utilizador utilize o meio de RF para comunicar com outros dispositivos *wireless*;
- AP - funcionam como um *switch* ou *router* normal em uma LAN para os dispositivos wireless. Além disso, representam ou podem representar (conforme a solução adotada) um *gateway* entre os dispositivos *wireless* e uma LAN infraestruturada organizacional.

A família de *standards* 802.11 dispõe neste momento de um conjunto de sub-*standards* alargados do 802.11, com diferentes especificações para largura de banda, frequências e tecnologias de transmissão, tendo sido ratificado por último o 802.11ac com grandes alterações para as WLAN. Indo-se analisar no

[14] Ponte de ligação - equipamento intermédio geralmente destinado a interligar redes.
[15] Dispositivo em uma rede *wireless* que realiza a interligação entre todos os dispositivos móveis.
[16] Estrutura.
[17] *Media Access Control*
[18] É uma das *frames* de gestão das WLAN baseadas no IEEE 802.11. Contém todas as informações sobre a rede e são transmitidos periodicamente pela mesma.

capítulo seguinte de forma resumida, mas com mais enfase, aqueles que se entendam importantes para o desenvolvimento deste trabalho.

Esta última ratificação de alterações coloca em destaque, num relativamente curto espaço de tempo, a mobilidade no acesso às redes, que se torna uma das maiores tendências na tecnologia wireless, que com o aparecimento da 5ª geração de *Wi-Fi* através do *standard* 802.11ac *Wave* 2 aumenta, pois é mais rápida e escalável que qualquer outra, reunindo a liberdade do *wireless* com as capacidades das redes *ethernet*[19] a *gigabit*[20]. Esta especificação significa não só muito mais velocidade, quase até aos 7 Gbps[21], mas também afeta o papel que as WLAN desempenharão nas organizações.

Os *sites* WLAN 802.11ac terão significantes melhorias no número de clientes suportados por AP e uma melhor experiencia para cada um deles, assim como, mais largura de banda disponível para um número mais elevado de *streams*[22] paralelos de vídeo, o que é conseguido por melhorias em 3 diferentes dimensões (Cisco Systems, 2014):

- Mais ligações por canal, aumentando de um máximo de 40 Mhz[23] no 802.11n para 80 ou 160Mhz (aumentando a velocidade para 117 ou 333 por cento, respetivamente);
- Mais *Multiple Input*, *Multiple Output* (MIMO), enquanto o 802.11n apenas admite quatro fluxos espaciais, o 802.11ac permite até oito (outro aumento de velocidade de 100 por cento);
- Modulação mais densa, agora com 256QAM (*Quadrature Amplitude Modulation*), acima dos 64QAM em 802.11n (aumento de velocidade de 33 por cento a curto prazo, mas ainda utilizável nas frequências atuais).

Como se pode verificar na figura 3 os produtos baseado nos *standards* 802.11 têm percorrido um longo caminho na última década, aumentando constantemente as taxas de transmissão de dados máximas, bem como a capacidade total proporcionada por cada AP.

[19] Arquitetura de interligação de LAN baseada no envio de pacotes.
[20] Unidade de armazenamento de informações ou dados de computadores. Normalmente ele é abreviado por Gb e corresponde a 1.000.000.000 bits.
[21] *Gigabits* por segundo, uma medida da velocidade de transferência de dados para redes de alta velocidade tal como *Ethernet* a *Gigabit.*
[22] Fluxo de dados num sistema informático.
[23] *Megahertz* - Unidade de medida de frequência e representa um milhão de ciclos por segundo.

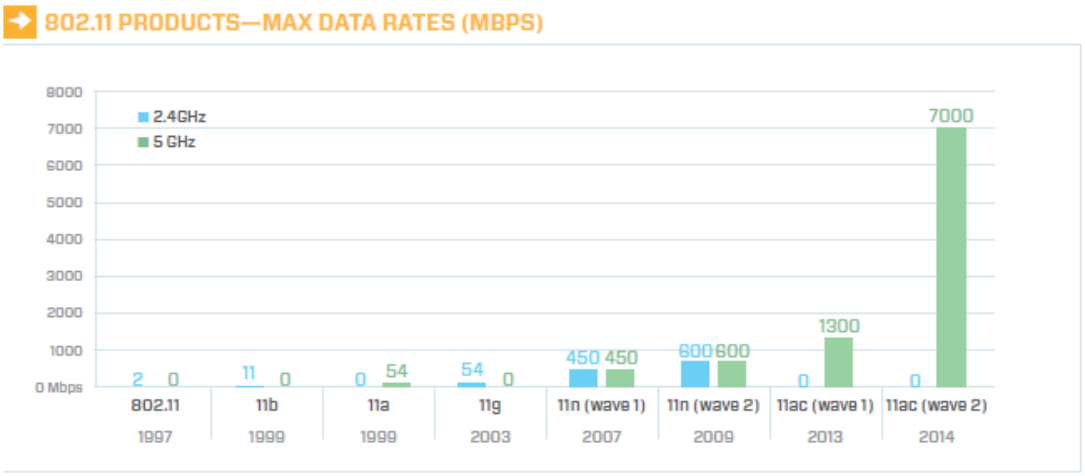

Figura 3 - Evolução das taxas de transmissão
(Phifer, 2014)

2.5 *Standards* de referência nas redes sem fios

A definição de *standards* de performance e segurança para as WLAN foi desenvolvida pelo IEEE em 1997 constituindo a versão base do *standard* 802.11, que é um conjunto de especificações sobre MAC e *Physical Layer* (PHY) para implementação de WLAN e comunicação entre computadores nas bandas de frequência de 2.4, 3.6, 5 e 60 GHz, que posteriormente foi desenvolvida. O *standard* e as suas alterações subsequentes, que melhoram algumas fragilidades no 802.11 original, fornecem a base para os dispositivos *wireless* usando a "marca" *Wi-Fi*. Embora cada alteração (melhoramento) esteja oficialmente revogada, quando incorporada na versão mais recente do *standard*, o mundo corporativo, no mercado, para destacar os recursos de seus produtos destaca as revisões que inclui no respetivo produto. Como resultado, no circuito comercial, cada revisão tende a tornar-se o seu próprio "*standard*".

De referir que apesar da especificidade do 802.11, para aplicação nas WLAN, não se pode ignorar o *standard* 802 (cuja ultima versão foi aprovada e publicada em 2014) que estabelece modelos de referência para as camadas superiores das redes e estrutura de endereços, servindo de base para a família de *standards* IEEE 802, ratificado para aplicação nas LAN, que se descreve mais pormenorizadamente abaixo, apesar de não diretamente ligada ao WI-FI.

Obviamente as necessidades de segurança nos diversos tipos de redes varia e atingem graus de criticidade diferentes em conformidade com a utilização e confidencialidade dos dados que lá passam.

A família de *standards* 802.11 vai sendo desenvolvida pelo IEEE à medida que o interesse pelo *wireless* aumenta e o desenvolvimento das suas aplicações vai abrangendo outros domínios, sendo que, neste momento dispõe de um conjunto de *sub-standards* alargados do 802.11 com diferentes especificações para larguras de banda, frequências e tecnologias de transmissão.

De entre este conjunto de *standards* serão somente referenciados os que forem identificadas como essenciais para o desenvolvimento do trabalho, cuja síntese estrutural se apresenta de seguida. O destaque

a dar a qualquer dos *standards* terá em atenção o seu enquadramento com as questões a que este trabalho pretende responder, pelo que se identificam especificamente:

- IEEE 802®-2014 - IEEE *Standard for Local and Metropolitan Area Networks: Overview and Architecture*;
- IEEE 802.11™-2012 - *IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks -Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*;
- IEEE 802.11aa™-2012 - IEEE *Standard for Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 2: MAC Enhancements for Robust Audio Video Streaming*;
- IEEE 802.11ad™-2012 - IEEE *Standard for Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band*;
- IEEE 802.11ae™-2012 - IEEE *Standard for Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Prioritization of Management Frames*
- IEEE 802.11ac™-2013 - IEEE *Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz*;
- IEEE 802.11af™-2013 - IEEE *Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Television White Spaces (TVWS) Operation*
- NIST SP 800-153 - *Guidelines for Securing Wireless Local Area Networks (WLANs);*
- NIST SP 800-124r1 - *Guidelines for Managing the Security of Mobile Devices in the Enterprise;*
- ISO/IEC 27033-4:2014: *Securing communications between networks using security gateways;*

As especificações e requisitos destes *standards* estão assim na base de todo o trabalho desenvolvido e das opções tomadas posteriormente no capitulo 4 pelo que se efetua de seguida uma descrição sintética do seu conteúdo.

2.5.1 IEEE 802

Este *standard* designado como IEEE *Standard for Local and Metropolitan Area Networks: Overview and Architecture* publicado em 2014 fornece uma visão geral da família de *standards* IEEE 802, sendo a terceira grande revisão da arquitetura e visão geral de IEEE 802.

Esta revisão integra duas alterações anteriores, o *standard* IEEE 802a -2003 (cobrindo *Ethertypes*[24] para protótipos e desenvolvimento específico de protocolo de fornecedores) e o *standard* IEEE 802b - 2004 (registro de identificadores de objeto), a grande revisão anterior do *standard publicado em 2001*. Desde a revisão de 2001 deste *standard* publicado pela primeira vez em 1990, os *standards* IEEE 802 e seus grupos de trabalho sofreram muitas mudanças, por exemplo o *standard* IEEE 802.5 foi retirado, portanto, as referências a ele foram também retiradas desta revisão.

O *standard* IEEE 802 também tem sido ampliado para incluir uma variedade de *standards* de *wireless*, portanto, foi adicionado um novo anexo informativo para endereçar esta variedade de *standards* IEEE 802 que constam no seu anexo D. As taxas de transferência de dados para os *standards* IEEE 802 variam agora de dezenas de *kilobits* por segundo a centenas de *gigabits* por segundo e englobam cobre, fibra ótica, *wireless* e *free-space optical media*[25].

Descreve modelos de referência para os mesmos, explicando a relação destes *standards* com os protocolos das camadas superiores dos modelos; proporciona um modelo para a estrutura de endereços MAC do IEEE 802, assim como, fornece um modelo para identificação de protocolos públicos, privados e protótipos; especifica ainda a hierarquia do identificador de objeto usado no IEEE 802 para alocação uniforme de identificadores de objetos usados na família de *standards* IEEE 802 assim como um método para identificação em protocolos de camadas mais elevadas.

Algumas tecnologias IEEE 802, em particular as baseadas em tecnologias *wireless*, são sistemas inerentemente de comunicação de mídias compartilhada. Eles também têm sido aumentados ao longo do tempo. Muitas WLAN suportam a mobilidade com nós móveis e portanto topologias dinâmicas, Estas facilidades adicionais podem, dependendo da tecnologia de IEEE 802 em utilização, restringir interligações LAN para os nós de topologia estáticos dentro da parte *wireless* de uma LAN de tecnologia heterogénea.

Contém ainda descrições das regras publicadas pelo IEEE para redes de dados com base em *frames*, bem como um modelo de referência (RM) para *standards* de protocolos e serve como base para a família de *standards* IEEE 802, publicados pelo IEEE para LAN, MAN, PAN e RAN.

[24] Campo de dois octetos numa *frame Ethernet*. É usado para indicar que protocolo é encapsulado na área de carregamento de dados de uma *frame Ethernet*. Este campo foi definido pela primeira vez pelo *standard* de rede *Ethernet* II, e, mais tarde adaptado para o *standard* de rede *Ethernet* IEEE 802.3.

[25] Tecnologia de comunicação ótica que utiliza luz propagando-se no espaço livre para transmissão *wireless* de dados para telecomunicações ou redes de computadores. "Espaço livre" significa ar, espaço sideral, vácuo ou algo semelhante.

2.5.2 IEEE 802.11

Este *standard*, cuja versão original foi publicada em 1999 e reafirmada em 2003, designado como *IEEE Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks -Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications foi* publicado em 2012, revê a publicada em 2007, que incorporou na edição de 1999 as alterações ratificadas pelos: IEEE 802.11a-1999, IEEE 802.11b-1999, IEEE 802.11b-1999/*Corrigendum* 1-2001, IEEE 802.11d-2001, IEEE 802.11g-2003, IEEE 802.11h-2003, IEEE 802.11i-2004, IEEE 802.11j-2004 e o IEEE 802.11e-2005.

Esta revisão do IEEE 802.11, de 2012, incorpora as seguintes alterações para a revisão de 2007:

- IEEE 802.11k™-2008: *Radio Resource Measurement of Wireless LANs (Amendment 1)*;
- IEEE 802.11r™-2008: *Fast Basic Service Set (BSS) Transition (Amendment 2);*
- IEEE 802.11y™-2008: *3650–3700 MHz Operation in USA (Amendment 3);*
- IEEE 802.11w™-2009: *Protected Management Frames (Amendment 4);*
- IEEE 802.11n™-2009: *Enhancements for Higher Throughput (Amendment 5);*
- IEEE 802.11p™-2010: *Wireless Access in Vehicular Environments (Amendment 6);*
- IEEE 802.11z™-2010: *Extensions to Direct-Link Setup (DLS) (Amendment 7);*
- IEEE 802.11v™-2011: IEEE 802.11 *Wireless Network Management (Amendment 8);*
- IEEE 802.11u™-2011: *Interworking with External Networks (Amendment 9);*
- IEEE 802.11s™-2011: *Mesh Networking (Amendment 10).*

O seu âmbito é a definição do MAC e várias especificações para a PHY, para ligação dentro de uma WLAN, de estações fixas, portáteis e móveis (STA).

Oferece também aos organismos reguladores, meios para normalização de acessos a uma ou mais faixas de frequências para comunicação em WLAN.

Especificamente este *standard* descreve (IEEE 802.11, 2012):

- Funções e serviços requeridos para dispositivos, compatíveis com o *standard* IEEE 802.11, operarem tanto dentro de redes a funcionar em *infrastructure mode* ou *ad-hoc mode*, bem como, nos aspetos relativos à mobilidade STA (de transição) dentro dessas redes;
- Funções e serviços que permitem que um dispositivo, compatível com o IEEE 802.11, comunique diretamente com qualquer outro dispositivo fora de uma rede *ad-hoc* ou *infrastructure mode*;
- Requisitos e procedimentos para garantir a confidencialidade dos dados de informação do utilizador e informações de gestão MAC transferidos através do *wireless medium* (WM) e autenticação dos dispositivos conformes com o IEEE 802.11.

Para alguns serviços define também um conjunto de aspetos fundamentais como (IEEE 802.11, 2012):

- Procedimentos MAC para suportar serviços de MAC S*ervice Data Unit* (MSDU);
- Várias técnicas de sinalização PHY e funções de interface que são controlados pelo IEEE 802.11 MAC;
- Funcionamento de um dispositivo, conforme com o IEEE 802.11, dentro de uma WLAN, que pode coexistir com múltiplas WLANs IEEE 802.11 sobrepostas;
- Mecanismos para a *Dynamic Frequency Selection* (DFS) e *Transmit Power Control* (TPC) que podem ser utilizados para satisfazer os requisitos normativos para funcionar em qualquer banda;
- Procedimentos MAC para suportar aplicações de LAN, com requisitos de *Quality of service* (QoS), incluindo o transporte de voz, áudio e vídeo;
- Mecanismos e serviços, para gestão na WLAN, de STAs que incluem a gestão da transição BSS, utilização do canal e coexistência, relatórios de interferência colocados, diagnóstico, diagnóstico de *multicast* e relatório de eventos, *multicast* flexível, mecanismos eficientes de *beacon*, anúncio de *proxy* de *Address Resolution Protocol* (ARP), localização, medição de sincronismo, *multicast* dirigido, modos de repouso estendidos, filtragem de tráfego e notificações de gestão;
- Funções e procedimentos auxiliando a descoberta de rede e seleção por STA, transferência de informações a partir de redes externas usando mapeamento de QoS, e um mecanismo genérico para a prestação de serviços de emergência;
- Procedimentos MAC que são necessários para a comunicação *wireless multi-hop* suportar WLAN com topologia *mesh*[26].

2.5.3 IEEE 802.11ad

Esta alteração designada como IEEE *Standard for Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band*, publicada em 2012, define modificações *standardizadas* para as PHYs e para a camada MAC do IEEE 802.11 de forma a permitir operações em frequências à volta dos 60 GHz, capazes de elevadas taxas de transferência.

Altera a descrição das funções e os serviços necessários por um dispositivo, conforme com o IEEE 802.11, operar dentro de redes *ad-hoc*, pessoais e de *infrastructure mode*, bem como os aspetos da transição entre STA, dentro dessas redes.

[26] Topologia de rede em que os dispositivos são ligados com muitas interligações redundantes entre os nós de rede.

Define a sinalização PHY, MAC, e os procedimentos requeridos para a operação de formação do feixe com padrões de antenas direcionais.

2.5.4 IEEE 802.11ae

Esta alteração designada como IEEE *Standard for Information technology -Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Prioritization of Management Frames*, publicada em 2012, estabelece regras de priorização para as *frames* de gestão, fazendo alterações para as especificações nas camadas PHY e MAC do IEEE 802.11 relacionadas com QoS para a Gestão de *Frames*.

2.5.5 IEEE 802.11ac

Esta alteração designada como IEEE *Standard for Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz*, publicada em 2013, baseia-se no *standard* IEEE 802.11 - 2012, considerando as alterações dos *standards* IEEE 802.11ae - 2012, IEEE 802.11aa - 2012 e IEEE 802.11ad – 2012

O seu objetivo é melhorar a experiência do utilizador das WLAN, baseadas no *standard* IEEE 802.11, fornecendo um aumento significativo nas taxas de transferência do BSS para as áreas aplicacionais das WLAN existentes e para permitir novos segmentos de mercado para operações abaixo de 6 GHz, incluindo distribuição de múltiplos fluxos de dados multimédia.

Para além disso altera as especificações para estabelecer *Robust Security Network Association* (RSNA**)** no *Distribution System* (DS) definindo um conjunto de caraterísticas de segurança além de *Wired Equivalente Privacy* (WEP) e autenticação IEEE 802.11. Esses recursos incluem os seguintes:

- ✓ Mecanismos de autenticação reforçada para STA;
- ✓ Algoritmos de gestão de chaves;
- ✓ Estabelecimento de chaves criptográficas;
- ✓ Reforço de mecanismos de encapsulamento criptográfico de dados, tais como *Counter mode with Cipher-block chaining Message authentication code Protocol* (CCMP), Galois Counter Mode Protocol (GCMP) e, opcionalmente, *Temporal Key Integrity Protocol* (TKIP);
- ✓ Mecanismo rápido de transição de BSS;
- ✓ Reforço de mecanismos de encapsulamento criptográfico para gestão de *frames* robustas.

Estabelece ainda as alterações de requisitos para *Very High Throughput* (VHT) STA do IEEE 802.11 especificando as principais características PHY e MAC para atingir taxas altas de transferência de dados.

A maioria das características VHT, entre outros benefícios, aumentam a taxa de transferência máxima viável entre dois VHT STA, além das já conseguidas, usando simplesmente as características *High-Throughput* (HT), estabelecendo suporte obrigatório e/ou opcional para um conjunto de especificações nas diversas cláusulas que a compõem.

2.5.6 NIST SP 800-153

O objetivo desta publicação de 2012 designada como NIST SP 800-153 - *Guidelines for Securing Wireless Local Area Networks (WLAN)* é proporcionar às organizações recomendações para melhorar a configuração de segurança e monitorização de suas WLAN baseadas no *standard* IEEE 802.11 e dos dispositivos ligados a essas redes.

Está limitada no seu âmbito a WLAN e instalações não classificadas, dentro do alcance das já referidas WLAN.

Esta publicação complementa outras publicações NIST, tais como a NIST SP 800-53, 800-114 e 800-124, consolidando e fortalecendo as suas principais recomendações, indicando as publicações NIST apropriadas para obter informações adicionais e fornecendo recomendações para a configuração de segurança nas WLAN, incluindo a conceção de configuração, implementação, avaliação e manutenção destas redes.

Apresenta uma visão geral da monitorização de segurança a efetuar nas WLAN e estabelece recomendações relacionadas, incluindo critérios para a seleção de ferramentas de monitorização e orientações para determinar com que frequência se deverá realizar essa monitorização.

2.5.7 NIST SP 800-124r1

Este standard foi definido em 2013 pela NIST com a designação de SP 800-124r1 - *Guidelines for Managing the Security of Mobile Devices in the Enterprise* e fornece recomendações para proteger tipos específicos de dispositivos móveis, como smartphones e tablets.

Os dispositivos móveis, como *smartphones* e *tablets*, tipicamente precisam suportar múltiplos objetivos de segurança: confidencialidade, integridade e disponibilidade. Para atingir estes objetivos, os dispositivos móveis devem ser protegidos contra uma variedade de ameaças. O objetivo desta publicação é ajudar as organizações a fazer a gestão centralmente da segurança de dispositivos móveis[27].

Fornece ainda recomendações para a seleção, implementação e utilização de tecnologias de gestão centralizada, explica os problemas de segurança inerentes à utilização de um dispositivo móvel e fornece recomendações para a proteção de dispositivos móveis em todo seu ciclo de vida.

[27] Os *Laptops* estão fora do âmbito desta publicação, assim como os dispositivos móveis com capacidade de computação mínimo, tais como telefones celulares básicos.

O seu âmbito inclui proteger, tanto os dispositivos móveis fornecidos pela organização como os de propriedade pessoal, que seguem um conceito recente, o *Bring Your Own Device* (BYOD)[28].

2.5.8 ISO/IEC 27033-4

Este *standard* da ISO, designado como ISO/IEC 27033-4 *Securing communications between networks using security gateways*, publicado em 2014, fornece orientações sobre como proteger as comunicações entre redes que utilizam *gateways* de segurança[29] de acordo com uma política dos *gateways* de segurança, incluindo a segurança da informação documentada:

- Identificar e analisar as ameaças de segurança de rede associados com *gateways* de segurança;
- A definição de requisitos de segurança de rede para *gateways* de segurança com base em análise de ameaças;
- Introdução de técnicas de *design* para atingir uma arquitetura técnica de segurança de rede capaz de enfrentar as ameaças e aspetos de controlo associados com cenários típicos de rede;
- Abordagem das questões associadas à implementação, operação, monitorização e revisão de controlos de segurança de rede com *gateways* de segurança;

Verifica-se assim que os *standard* publicados pelas organizações internacionais com responsabilidade nesta área refletem um conjunto de análises e recomendações associadas a questões que se impõe salvaguardar, estabelecendo também soluções e sugestões para caraterizar o problema da segurança da informação, redes *wireless* e forma de salvaguarda dessa informação que irá ser efetuado no capítulo 3 de caraterização do problema.

A construção de um referencial para implementação de WLAN nas organizações garantindo a segurança da informação e da tecnologia utilizada será concebido com base em referenciais obtidos através quer da revisão da literatura e do *standards* considerado adequado ao estudo desta problemática.

[28] Corresponde à política de permitir que funcionários levem e utilizem os seus dispositivos móveis pessoais (*laptops*, *tablets* e *smartphones* e, cada vez mais, *notebooks* e *PCs*) para o seu local de trabalho, usando-os para aceder a informações privilegiadas e aplicações da organização.

[29] F*irewall*, *firewall* aplicacional, *Intrusion Prevention System* (IPS), etc.

3 Caracterização do problema

Neste capitulo vai-se fazer uma caraterização e/ou tipificação atual da situação das redes *wireless* e utilização no âmbito das organizações recorrendo-se a quatro capítulos diferenciados para contextualização do tema, nomeadamente o aparecimento das WLAN na esfera da dinâmica das organizações, requisitos e forma de integração com infraestrutura de rede fixa existente ou a criar, problemas de segurança que este tipo de rede cria e a possibilidade de evolução na organização, servindo depois de base para o capitulo seguinte onde se pretende estruturar os conceitos essenciais para implementações que garantam a segurança e o sucesso das WLAN.

Atualmente, a maioria das organizações, comerciais, governamentais, com ou sem fins lucrativos têm seus sistemas de informação ligados através de redes interligadas, conforme exemplificado na figura 4, estabelecendo comunicação entre elas e ou para o exterior, tipicamente em conformidade com um ou mais dos seguintes tipos:

- Dentro da organização;
- Entre diferentes organizações;
- Entre a organização e o público em geral.

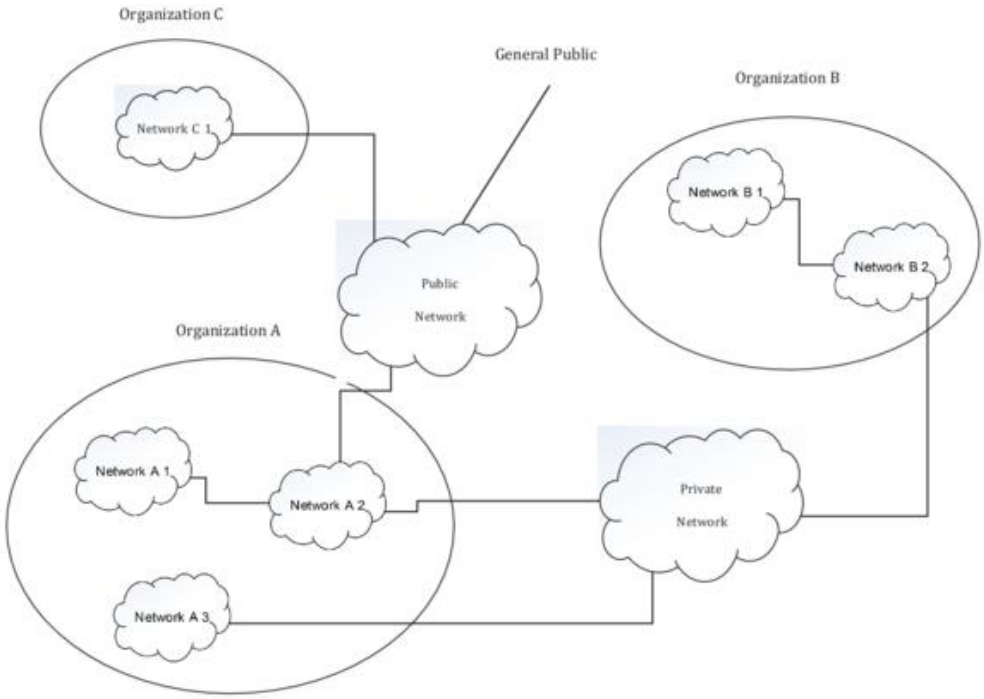

Figura 4 - Grandes tipos de ligação de rede
(ISO/IEC 27033-1, 2015)

Com a rápida evolução na tecnologia de rede, publicamente disponível (em particular com a *Internet*), oferecendo oportunidades de negócio significativo, as organizações vão cada vez mais realizando negócios eletrónicos em escala global e prestação de serviços públicos em linha. Estas oportunidades incluem a aquisição de comunicações de dados, a custo reduzido, usando a *Internet*

simplesmente como um meio de conexão global, através de serviços mais sofisticados fornecidos pelos *Internet Service Providers* (ISP).

No entanto, enquanto este ambiente facilita benefícios de negócio significativos, há novos riscos de segurança a serem geridos. Com as organizações a depender fortemente do uso da informação e das redes associadas para realizar seus negócios, a perda de confidencialidade, integridade e disponibilidade da informação e serviços pode ter impactos adversos significativos sobre as operações de negócios.

Assim, há um requisito importante para proteger adequadamente as redes, suas informações e sistemas de informação relacionados. Em outras palavras: implementação e manutenção da segurança de rede adequada são absolutamente críticos para o sucesso das operações de negócios de qualquer organização (ISO/IEC 27033-1, 2015).

Nas últimas décadas as redes de computadores tem feito parte do nosso dia-a-dia em todas as vertentes, desde a empresarial à privada, no acesso à internet, bancos, hospitais e tudo o mais que possamos imaginar tem como base essas redes de computadores.

Sendo o período atual crítico e difícil tentou-se perceber a complexidade gerada pela adoção de nova tecnologia de redes *wireless* nas organizações, mais complexa, forma de garantir a sua compatibilidade com as atuais infraestruturas de rede e com os futuros desenvolvimentos da tecnologia *wireless*.

Com relação aos efeitos percebidos do uso de tecnologias móveis no desempenho organizacional, constatou-se que aumenta principalmente a produtividade da empresa, sendo este efeito seguido pela obtenção de novos clientes, aumento das receitas e, por fim, redução dos custos operacionais.

Em termos económicos, a globalização, que nos impele para mais longe, tal como, aos mais distantes, os aproxima de nós, nos impede de retroceder ou, sequer, perder tempo a contemplar o passado, mas as consequências que daí resultam não têm que ser fatais, pelo menos, para organizações atentas à realidade e que, antevendo o futuro, curem de planear de forma avisada e atuem proactivamente (Hirst, Thompson, e Bromley, 2015).

As WLAN apresentam os seus próprios desafios de análise, projeção, implementação e segurança, para as organizações que optam por tal tecnologia, distintos de organização para organização, mas não tem uma solução única e exclusiva, devendo ser analisada caso a caso em conformidade com os fatores já mencionados, mas que não se esgotam nestes.

3.1 Adoção de redes sem fios

Segundo Stallings (2013) as décadas de 1970 e 1980 viram uma fusão tal, dos campos das ciências de computação e do de comunicação de dados, que mudou profundamente a tecnologia, os produtos e as organizações, da indústria de computadores e comunicações agora completamente interligada.

O mesmo autor refere ainda que a revolução das comunicações nas TI tem produzido vários factos notáveis:

- Não há nenhuma diferença fundamental entre o processamento de dados (informática) e comunicações de dados (equipamento de comutação e transmissão);
- Não existem diferenças fundamentais entre dados, voz e comunicação vídeo;
- As distinções entre computadores com processadores únicos, multiprocessadores, LAN, MAN e WAN esbateram-se quase completamente.

Um efeito destes factos tem sido uma crescente sobreposição das indústrias de computadores, de comunicações, do fabrico de componentes à integração de sistemas.

Outro resultado, desta sobreposição, é o desenvolvimento de sistemas integrados que transmitem e processam todos os tipos de dados e informações. A tecnologia e as organizações que gerem as ratificações de *standards* técnicos, estão direcionando as suas orientações para sistemas públicos integrados, que tornam, praticamente, todas as fontes de dados e informações ao redor do mundo fácil e uniformemente acessíveis. (Stallings, 2013).

Os computadores ficavam atrás na corrida ao *wireless* por causa de necessidades intrínsecas de maior largura de banda para a transmissão de dados e informação comparativamente a outros equipamentos *wireless* (televisão, telemóveis por exemplo). Mas há alguns anos atrás avanços nas tecnologias dos *chips wireless* aumentaram as taxas de transferência de dados através destas ligações, fazendo que a ligação *wireless* entre computadores fosse uma realidade.

Usando ondas eletromagnéticas, as WLAN transmitem e recebem dados através do ar, minimizando as necessidades de ligações através das LAN. Com a tecnologia atual as WLAN são altamente escaláveis, de confiança e fáceis de implementar, permitindo aos utilizadores móveis o acesso a informação em tempo real, ganhando cada vez mais popularidade. As WLAN são atualmente uma das mais populares tecnologias para as comunicações privadas, fazendo hoje parte do nosso dia-a-dia, sendo certo que a sua utilização vai crescendo rapidamente e abrange já e cada vez mais o setor organizacional, estando na agenda do dia das organizações, pelas perspetivas de aumento de competitividade que poderão aportar (3rd Annual Trends in Enterprise Mobility, 2014).

Equipamentos ligados através de tecnologia *wireless* providenciam mobilidade acrescida requerendo menos infraestruturas que as tradicionais LAN (Dhanalakshmi e Sathiya, 2015).

3.1.1 Pressupostos

Segundo Lunardi, Dolci, e Maçada (2010) as TI no meio organizacional podem fornecer um conjunto bastante rico de resultados e, inclusive, teorias que possam ser aplicadas diretamente para compreender melhor o impacto de sua utilização, identificando também fatores relacionados ao sucesso e ao fracasso de sua implementação. Estes autores, considerando o referido anteriormente por outros, assinalam outros fatores importantes, como:

- Necessidade interna (Prates e Ospina, 2004);
- Ambiente organizacional (Cragg e King, 1993);
- Pressões externas (Cragg e King, 1993; Grandon e Pearson, 2004);
- Utilidade percebida (Davis, 1989; Grandon e Pearson, 2004); reforçado com o defendido por Oliveira, Martins, e Lisboa (2011).

Estes fatores que têm levado as organizações a adotarem diferentes TI em conformidade com:

- Necessidade interna – quando a organização adota a tecnologia em função de seu crescimento ou para melhor atender as suas necessidades, garantindo, dessa forma, o seu bom funcionamento;
- Ambiente organizacional – quando a organização adota a tecnologia porque percebeu que possuía um ambiente favorável à sua utilização, com funcionários em condições de utilizá-la e com uma estrutura organizacional adequada;
- Pressões Externas – quando a organização adota a tecnologia em função de grande concorrência existente, porque os concorrentes diretos têm adotado ou ainda por influência de clientes, fornecedores ou do próprio governo;
- Utilidade Percebida – quando a organização adota a tecnologia porque percebeu que seria útil no seu dia-a-dia, melhorando a realização de tarefas e suas atividades, aumentando a segurança, o controle e o atendimento aos clientes.

Tornatzky e Fleischer (1990, como citado em San Martín et al., 2012), ao desenvolverem um modelo genérico para adoção de novas tecnologias, sugerem três fatores-chave que influenciam essa adoção:

- O contexto tecnológico (definido pela competência tecnológica da organização);
- O contexto organizacional (que abrange fatores como: adequação, tamanho ou formalização);
- E o contexto ambiental (impactado por diferentes pressões competitivas).

Nesse sentido, percebe-se que as pressões competitivas existentes no contexto ambiental atuam como mais um fator que incentiva o crescimento e a disseminação das tecnologias móveis (Shankar, Venkatesh, Hofacker, e Naik, 2010).

Estas refletem-se, para as organizações, num conjunto de pressões externas, tais como: concorrência, mudança de necessidades dos clientes, regulamentações governamentais e surgimento de novas tecnologias (Ungan, 2004). As pressões externas dos concorrentes, por exemplo, podem levar uma empresa a adotar uma inovação mesmo quando ela não percebe muitas vantagens nesta tecnologia. Diferentes pressões competitivas podem influenciar uma empresa a adaptar suas estratégias a uma nova situação (Grant, 2003), particularmente em setores nos quais existe grande rivalidade e incerteza quanto ao que os concorrentes estão fazendo (Pavlou e El Sawy, 2010).

Assim, como tentativa de enfrentar essas pressões, as organizações procuram adotar a melhor solução possível (Ungan, 2004), ainda que em muitos casos não tenham certeza sobre o impacto que a solução adotada terá.

Competência técnica para lidar com essa tecnologia é essencial para a sua adoção e principalmente para garantir o sucesso da sua utilização (Kuan e Chau, 2001).

Similarmente, Cappellozza et al. (2011) evidenciam a infraestrutura das TI com o relacionamento significante aos dispositivos móveis nas organizações do setor de serviços. Como ocorre com qualquer outra tecnologia recente, há muitos fracassos de aplicações nas organizações que investiram nessa tecnologia (Turban et al., 2010). Ainda assim, a presença de ferramentas onde o utilizador não precise realizar grande esforço na sua utilização pode prevenir o problema de subutilização dessa tecnologia, apresentando uma plataforma amigável e de fácil aprendizagem (Lin, 2011).

3.1.2 As redes sem fios na organização

Com a emergência de novas tecnologias associadas às WLAN, novas alterações aos *standards* que permitem mais velocidade e melhor segurança neste tipo de redes de comunicações, com uma maior perceção da sua utilidade prática, os custos reduzidos e a rapidez de implementação são motivação para cada vez mais organizações as adotarem, com as mais diversas funcionalidades. Assim começam a tornar-se na rede primária do ambiente organizacional com as vantagens e desvantagens que as caraterizam, em complemento ou não, de infraestruturas já existentes.

À medida que as WLAN vão crescendo e adotando o papel de rede primária do ambiente organizacional os administradores começam a considerar, quer as aplicações que fazem parte desse ambiente, quer o ambiente no qual essa aplicações estão apoiadas.

Apesar da grande evolução sofrida nos últimos anos, mantêm-se atual o defendido por alguns autores (San Martín, López-Catalán e Ramón-Jerónimo, 2012; Zhang, Zhu e Liu, 2012) de que a utilização das redes *wireless* e dos dispositivos móveis nas organizações, embora crescente, ainda está em seu estágio inicial em termos de conhecimento científico.

Pode-se assim verificar que já em 2004 se perspetivava uma grande evolução na convergência entre dados e voz no ambiente *wireless* organizacional à medida que as tecnologias fossem estabelecendo novos parâmetros para funcionamento, conforme indicado na figura 5.

Estes parâmetros, com a alteração de paradigma das aplicações orientadas a dados para as aplicações que integram voz e dados, convergência entre o *Wi-fi* e redes celulares por exemplo implicam necessidades de aumento da capacidade de transmissão de dados e uma integração global das infraestruturas.

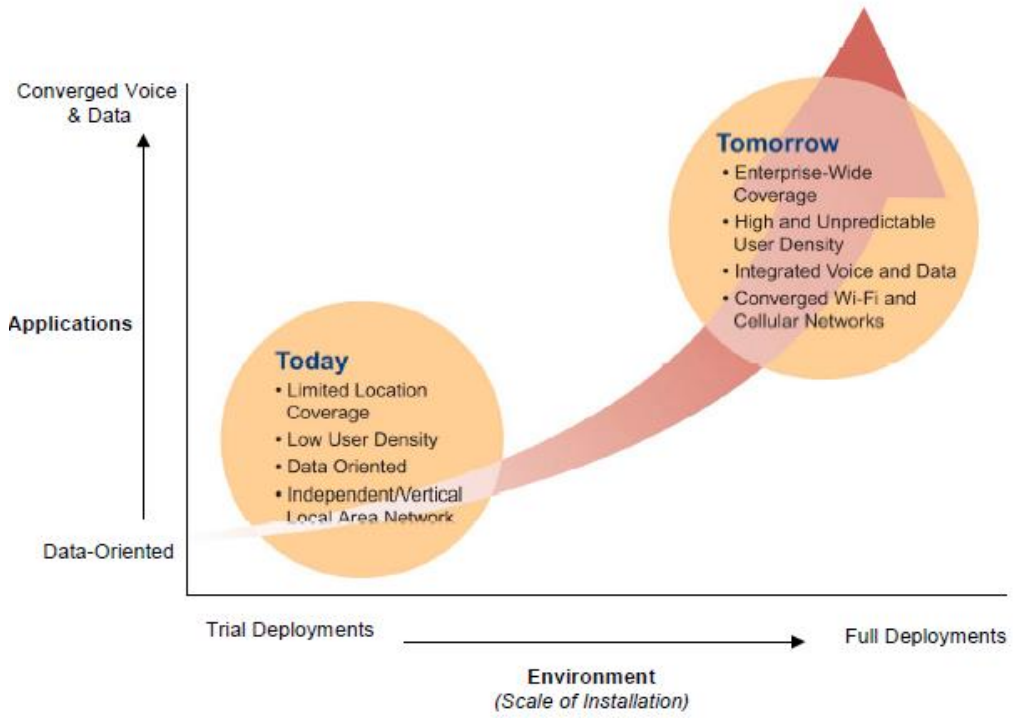

Figura 5 - Evolução do *WI-FI* na organização

(Wi-Fi in the Enterprise, 2004)

3.2 Identificação de requisitos e integração com infraestrutura

Segundo Stallings (2013) infraestruturas de rede e comunicações de dados eficazes e eficientes são vitais para qualquer organização. A arquitetura e a evolução das infraestruturas de comunicações e redes de dados têm sido impulsionadas por três diferentes forças de forma consistente, o crescimento do tráfego, o desenvolvimento de novos serviços, e os avanços na tecnologia.

Refere o mesmo autor que o tráfego de comunicações, locais (dentro de um edifício ou complexo de edifícios) ou de longa distância, de voz ou dados, tem vindo a crescer a um ritmo elevado e constante ao longo de décadas. A crescente ênfase na automatização e automação do escritório, acesso remoto, transações *on-line* e outras medidas de produtividade significam que esta tendência, de aumento de tráfego, é mais que provável que continue.

Assim, os gestores estão lutando constantemente, para maximizar a capacidade e minimizar os custos de transmissão das comunicações. Como as organizações dependem cada vez mais das TI e a gama de serviços se expande, aumenta também a procura de estruturas de redes e de transmissão de alta capacidade (Stallings e Beard, 2015).

Por sua vez, o crescimento contínuo da oferta de rede de alta velocidade com a queda contínua dos preços encoraja a expansão dos serviços pelo que o crescimento em serviços e o crescimento da capacidade de tráfego andam de mãos dadas. A Figura 6 apresenta alguns exemplos de serviços baseados na informação e taxas de dados necessários para apoiá-los (Stallings, 2013).

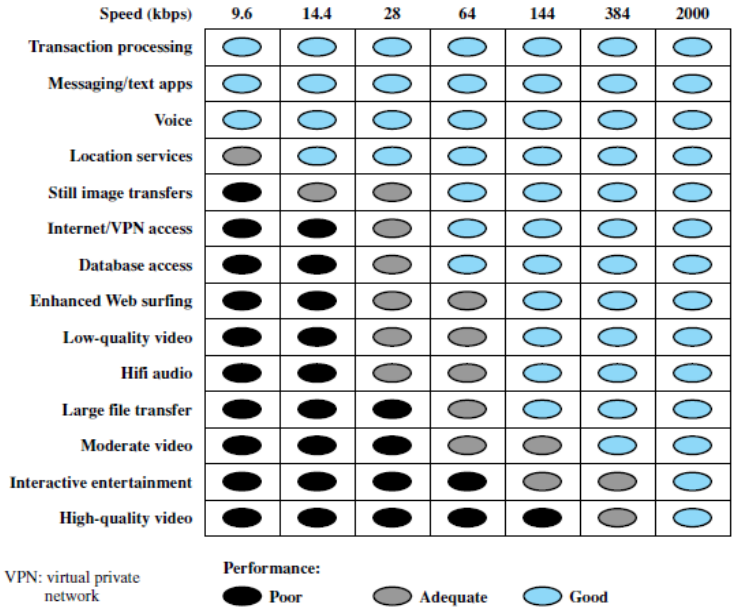

Figura 6 - Serviços versus taxas de transferência (Stallings, 2013)

Finalmente, as tendências em tecnologia possibilitam o fornecimento de capacidade de tráfego crescente com apoio de uma grande gama de serviços.

De acordo com Stallings (2015) quatro dessas tendências tecnológicas são particularmente notáveis:

1. A tendência para mais rápido e mais barato, tanto em informática como em comunicações, contínua o que representa que:
   - Em termos de computação, isso significa que computadores mais potentes e *clusters* de computadores são capazes de suportar aplicações mais exigentes, tais como aplicações multimédia;
   - Em termos de comunicações, a crescente utilização de fibra ótica tem reduzido os preços de transmissão e aumentado consideravelmente a capacidade. Por exemplo, para telecomunicação de longa distância e ligações de rede de dados, ofertas recentes da *Dense Wavelength Division Multiplexing* (DWDM)[30] permitem capacidades de muitos Tbit/s[31]. Nas LAN muitas organizações agora têm redes de *backbone Gigabit Ethernet* e algumas estão começando a implementar a *Ethernet* de 10 Gbps;
2. Ambas as redes de telecomunicações, orientadas para voz, como a *Public Switched Telephone Network* (PSTN), e as de redes de dados, incluindo a Internet, são mais "inteligentes" do que nunca. Duas dessas áreas de inteligência são notáveis:

[30] Tecnologia que coloca dados de fontes diferentes, em conjunto, sobre uma fibra ótica, com cada sinal sendo transportado ao mesmo tempo sobre o seu próprio comprimento de onda de luz separado.

[31] *Terabits* por segundo – unidade de taxa de transferência equivalente a 1000 *gigabits* por segundo já anteriormente definido.

- Em primeiro lugar, as redes de hoje podem oferecer diferentes níveis de QoS, que incluem especificações para atraso máximo, taxa de transferência mínima e assim por diante;
- Em segundo lugar, as redes de hoje oferecem uma variedade de serviços personalizados nas áreas de gestão de rede e segurança;

3. A *Internet*, a *Web* e aplicações associadas surgiram como características dominantes, tanto do mundo organizacional como do pessoal, abrindo muitas oportunidades e desafios para os gestores. Além de explorar a *Internet* e a *Web* para atingir os clientes, fornecedores e parceiros, as organizações têm formado *intranets* e *extranets* para isolar a sua informação, de propriedade livre, do acesso indesejado.
4. Tem havido uma tendência de mobilidade crescente por décadas, libertando os trabalhadores dos confins da organização física. As inovações incluem correio de voz, acesso a dados remotos, fax, *e-mail*, telefones *wireless*, telemóveis, *smartphones*, redes celulares e portais de *Internet*. O resultado é a capacidade dos empregados para levar seu contexto de negócio com eles, quando se movem. Estamos vendo o crescimento de acesso *wireless* de alta velocidade, o que mais aumenta a capacidade de usar recursos de informações da organização e serviços em qualquer lugar.

O *standard* IEEE 802.11 estabelece as especificações para a tecnologia de acesso de rede que estabelece ligação entre STA *wireless* e infraestruturas LAN.

Com a implementação de redes IEEE 802.11 e tecnologias associadas, o utilizador móvel pode deslocar-se através dos diversos espaços da organização sem perder conetividade — salas de reuniões, vestíbulos, corredores, refeitórios, salas de aula e assim por diante — e manter o acesso aos seus dados em rede. Também, além do ambiente de trabalho corporativo, permite o acesso à Internet e até mesmo aos *sites* corporativos.

A utilização de tais especificações permite a integração destas tecnologias emergentes com as redes fixas estruturadas existentes, com infraestruturas *wireless* baseadas em protocolos mais antigos, que são o *core* destas e garante a sua interoperabilidade, não esquecendo os SI herdados[32], resultando no desenvolvimento de novos produtos, aplicações e soluções para fazer face a estes desafios. Como resultado, isto reflete-se desde logo no desempenho organizacional, com o aumento, principalmente, da produtividade da empresa, sendo seguido pela obtenção de novos clientes, aumento das receitas e, por fim, pela redução dos custos operacionais. Usado em conjunto com outra tendência, a dos equipamentos móveis – como *notebook*, *smartphones* e *tablets* –, é possível atingir níveis de conetividade com mobilidade nunca antes experimentados.

[32] Sistema informático crítico em utilização há determinado tempo, desenvolvido com tecnologia supostamente ultrapassada.

3.2.1 Requisitos de capacidade de rede e de transmissão de dados

Mudanças significativas na forma como as organizações fazem negócios e processam informações foram impulsionadas por mudanças na tecnologia de rede e ao mesmo tempo têm impulsionado essas mudanças. É difícil separar a origem e o resultado destas mudanças.

Da mesma forma, o uso da Internet por organizações e indivíduos reflete essa dependência cíclica: a disponibilidade de nova imagem baseada em novos serviços na *Internet* (ou seja, a *Web*) resultou em um aumento no número total de utilizadores e o volume de tráfego gerado por cada utilizador. Este, por sua vez, resultou numa necessidade de aumentar a velocidade e eficiência da *Internet*. Por outro lado, é só este aumento de velocidade que torna o uso de aplicações baseadas na *Web* apetecíveis para o utilizador final (Castells, 2011).

3.2.2 O surgimento de redes de alta velocidade

Computadores pessoais, estações de trabalho e microcomputadores começaram a alcançar uma aceitação generalizada em informática no início de 1980 e agora alcançaram praticamente o *status* de ferramenta essencial e indispensável para os trabalhadores das organizações.

Até alguns anos atrás, as LAN nas organizações forneciam serviços de conetividade básica — ligando computadores pessoais, terminais para *mainframes*, sistemas intermédios que executavam aplicações corporativas e fornecendo conetividade de grupo de trabalho a nível departamental ou divisional. Em ambos os casos, os padrões de tráfego eram relativamente leves, com ênfase na transferência de arquivos e correio eletrónico. As LAN que estavam disponíveis para este tipo de carga de trabalho, principalmente a *Ethernet* e *Token Ring*[33], eram bem adaptados a este ambiente (Stallings, 2013).

Segundo o mesmo autor, na década de 1990, duas tendências significativas alteraram o papel do computador pessoal e, portanto, os requisitos nas LAN:

1. A velocidade e o poder computacional dos computadores pessoais continuou a desfrutar dum crescimento explosivo. Essas plataformas mais poderosas suportam aplicações intensivas em gráficos e cada vez mais, elaboradas interfaces gráficas, do utilizador para o sistema operativo;
2. Os SI de gestão das organizações reconheceram a LAN como uma plataforma de computação essencial e viável, resultando no foco da computação de rede. Esta tendência começou com a arquitetura cliente/servidor de computação, que se tornou uma arquitetura dominante no ambiente corporativo nessa década, ao que se juntou a tendência de intranet focada na *Web*. Ambas estas abordagens envolvem a transferência frequente de, potencialmente, grandes volumes de dados em um ambiente orientado a transação.

[33] Arquitetura de rede com uma topologia lógica em anel.

O efeito dessas tendências tem sido a de aumentar o volume de dados geridos pelas LAN e, porque os aplicativos são mais interativos, reduzir o atraso aceitável na transferência de dados. A anterior geração de *Ethernet* a 10 Mbps[34] e *Token Ring* de 16 Mbps simplesmente não estava apta para o trabalho de suportar estes requisitos. Assim foram surgindo soluções tecnológicas que permitem o aumento destas velocidades de transferência de dados.

3.2.3 Rede local

Como nas WAN, uma LAN é uma rede de comunicações que interliga uma variedade de dispositivos e fornece um meio para troca de informações entre os dispositivos. Há várias distinções chaves entre LAN e WAN (Stallings, 2013):

1. O âmbito da LAN é pequeno, geralmente um único edifício ou um conjunto de edifícios. Esta diferença no âmbito geográfico leva a soluções técnicas diferentes;
2. Normalmente o caso é, que a LAN é propriedade da mesma organização que possui os dispositivos ligados. Para as WAN é o caso menos frequentemente, ou pelo menos uma fração significativa dos ativos de rede não são propriedade privada. Isto tem duas implicações:
   - Primeiro, devemos ter cuidado na escolha da LAN, porque pode haver um substancial investimento de capital para a compra e posterior manutenção;
   - Segundo, a responsabilidade de gestão de rede para uma LAN recai unicamente sobre a organização;
3. As taxas de transferência interna de dados das LAN são tipicamente muito maiores do que aquelas das WAN. As LAN podem ter um número de diferentes configurações. Os mais comuns são LAN comutadas e WLAN. A LAN comutada mais comum é uma LAN de *Ethernet* comutada, que pode consistir em um único *switch* com um número de dispositivos ligados, ou um número de *switches* interligados. As WLAN usam uma variedade de tecnologias de transmissão *wireless*, estruturas e funcionalidades diferenciadas.

3.2.4 Redes sem fios

Como já referido, as WLAN são comuns e cada vez mais amplamente utilizadas em ambientes organizacionais e como tal a tecnologia *wireless* também é comum para as redes de voz e dados nestas. As redes *wireless* fornecem vantagens nas áreas de mobilidade e facilidade de instalação e configuração.

Uma WLAN deve atender ao mesmo tipo de exigências típicas de qualquer LAN, incluindo a capacidade elevada, habilidade de cobrir distâncias curtas, conetividade total entre estações anexadas e capacidade de transmissão.

[34] *Megabit* por segundo - Unidade de transmissão de dados equivalente a 1.000 *kilobits* por segundo ou 1.000.000 *bits* por segundo.

Na figura 7 referem-se algumas das designações mais em uso no universo próprio das WLAN, procedendo-se à sua descrição em conformidade com os glossários dos *standards* de referência 802.11 permitindo numa forma agrupada percecionar os mesmos:

Designação	**Descrição**
Access Point (AP)	Qualquer entidade que tenha funcionalidades de AP e providencie acesso ao sistema de distribuição através do meio *wireless* para STA associadas
Basic Servisse Set (BSS)	Um conjunto de STA controlado por uma função simples de coordenação.
Coordination Function	Função lógica que determina quando a uma STA que opere um BSS é permitido transmitir e poderá receber PDUs
Distribution system (DS)	Sistema utilizado para interligar um conjunto de BSS e uma WLAN integrada, de forma a criar um ESS
Extended Servisse Set (ESS)	Um conjunto de BSS interligados e respetiva WLAN, de forma a parecerem um único BSS para o *Logical Link Control (LLC) layer* de qualquer STA com estes BSS
MAC	*Media Access Control*
MAC Protocol Data Unit (MPDU)	A unidade de dados trocada entre dois pares de entidades MAC que usam o serviço do *PHY*
MAC Service Data Unit (MSDU)	Informação que é entregue como uma unidade entre utilizadores MAC
PHY	*Physical Layer*
Station (STA)	Qualquer dispositivo que contenha MAC e *PHY* conforme o IEEE 802.11

Figura 7 – Termos mais utilizados em WLAN

Além disso, há uma série de requisitos específicos para o ambiente WLAN sendo os mais importantes os que se descrevem de seguida:

- ***Throughput*:** O protocolo MAC deve fazer uso o mais eficiente possível do meio *wireless* para maximizar a sua capacidade;
- ***Number of nodes*:** As WLAN podem necessitar de dar suporte a centenas de nós através de múltiplas células;
- **Ligação ao *backbone* da LAN**: Na maioria dos casos, interligação com estações em um *backbone* da LAN é necessário. Para infraestruturas das WLAN, isso é facilmente conseguido através da utilização de módulos de controlo que se ligam a ambos os tipos de LAN. Podem também precisar de ser alojamento para utilizadores móveis e WLAN *ad-hoc*.

Atendendo ao que determinados autores assumem considera-se que, por serem importantes numa perspetiva de implementação, se deve referir algumas exigências desses requisitos que permitem estabelecer redes viáveis e robustas:

- Cobertura de sinal dos AP;

- Capacidade média em conformidade com o número de utilizadores;
- Níveis de segurança, respeitantes à confidencialidade dos dados, autenticação e autorização dos utilizadores;
- Controlo de acesso granular: segmentação de rede, recursos, grupos e utilizadores;
- Suporte de autenticação por meio de certificados digitais;
- Autenticação integrada com o domínio corporativo;
- Gestão centralizada;
- Alta disponibilidade ao nível dos controladores que assegurem a continuidade do serviço;
- Túnel de dados para assegurar segurança da informação*;*
- Funcionalidade de *Adaptive Radio Management (ARM)*;
- Funcionalidade de *Band-Steering*[35].

Na mesma ordem de ideias podemos ainda considerar um conjunto de aspetos essenciais mais abrangentes e diretamente relacionados com as organizações como:

- Instalação da infraestrutura de rede cablada de suporte;
- Arquitetura física e lógica, tanto da solução como da respetiva rede de suporte;
- Serviços prestados pela infraestrutura *wireless*;
- Aspetos relacionados com a alta-disponibilidade da solução;
- Integração com os serviços da organização (Ex. domínio, autenticação, *proxy*);
- Aspetos de segurança do serviço *wireless*;
- Eficiência do espectro rádio utilizado.

3.3 Segurança da informação

Uma forte cultura de proteção da informação é necessária em organizações onde a confidencialidade, sensibilidade e privacidade da informação é entendida e tratada em conformidade. Isso é necessário para reduzir o risco do comportamento humano na proteção da informação, bem como para cumprir requisitos de privacidade do ponto de vista legal e regulamentar (Da Veiga e Martins, 2015).

De acordo com Bowen, Hash, Wilson, Bartol e Jamaldinian (2006, citado por Ahmad, Maynard e Park, (2014)) as organizações estão cada vez mais conscientes do papel que a informação e tecnologias associadas desempenham em quase todas as funções organizacionais, especialmente em promover a inovação e gerando vantagem competitiva.

Referem os mesmos autores, no ambiente moderno de informação, informação organizacional e serviços de tecnologia estão expostos a uma variedade de riscos de segurança, incluindo acesso a informações confidenciais e interrupção prolongada de acesso a *e-mail* e *internet*, resultando num impacto significativo à continuidade de negócio.

[35] Tecnologia que deteta se o cliente *wireless* tem funcionalidade de *dual-band*, e se tiver, força o cliente a ligar-se na frequência de 5 GHz menos congestionada.

Para lidar com esses riscos de segurança, uma organização deve implementar uma estratégia de segurança de informação através da criação de um quadro abrangente que permita o desenvolvimento, a institucionalização, avaliação e melhoria de um programa de segurança de informação. Em particular, a estratégia de segurança da informação deve apoiar planos globais estratégicos da organização, com seu conteúdo claramente rastreável a estas fontes de nível superior.

Referem também que o desenvolvimento rápido das TI e as mudanças na envolvente dos negócios apresentam uma gama de desafios para as organizações que dependem de tais tecnologias para operações diárias. Os sectores de infraestruturas críticas estão em risco especial, de interrupção das operações das TI, e isso pode levar a grandes perturbações económicas e sociais. Como resultado, é vital para os proprietários e operadores de tais infraestruturas críticas desenvolver estratégias adequadas para mapeamento e compreensão das camadas de informação mantidas nas redes de IT que precisam ser protegidos.

Segurança da informação é a proteção da informação e SI. Ela engloba toda a infraestrutura que facilita seu uso — processos, sistemas, serviços e tecnologias. A disciplina de segurança da informação em si tem sido sujeita a forças de convergência (Australian National Audit Office, 2005).

Segundo o mesmo documento do Australian National Audit Office (2005), segurança de TI é a disciplina que fornece controlos técnicos em torno das TI, que protege contra acessos não autorizado, uso, divulgação, destruição, alteração ou interrupção do acesso aos dados, sendo portanto, um subconjunto da segurança da informação que ajuda este processo, garantindo a proteção das informações, através do proteção dos sistemas de TI. Para a segurança de TI ser eficaz em proteger o interesse da organização, deve estar alinhada com as práticas de segurança física e pessoal da organização. Esta abordagem unificada é a prática de segurança da informação no seu cerne.

Com a crescente importância das TI, há uma necessidade urgente de medidas adequadas de segurança da informação, pelo que, a gestão sistemática de segurança de informação é uma das mais importantes iniciativas para gestão de TI. Pelo menos desde que relatórios e informações, sobre quebras de segurança e privacidade, práticas fraudulentas de contabilidade e ataques a sistemas de TI, apareceram em público, as organizações reconheceram as suas responsabilidades em proteger os seus ativos físicos e de informação (Disterer, 2013).

Segundo o mesmo autor os *standards* de segurança podem ser usadas como diretriz ou estrutura para desenvolver e manter um *Information Security Management System* (ISMS) adequado. Os *standards* ISO/IEC 27000, 27001 e 27002 são *standards* internacionais que vão recebendo reconhecimento e adoção crescente, sendo referidos como "língua comum das organizações ao redor do mundo", para segurança da informação. Com o *standard* ISO/IEC 27001, as organizações podem ter os seus ISMS certificados por uma organização terceira e assim mostrar provas das suas medidas de segurança aos seus clientes, fornecedores e funcionários.

Refere ainda que os *standards* surgem através do desenvolvimento de descrições detalhadas de características específicas de um produto ou serviço por especialistas de empresas e instituições científicas. Eles representam um consenso sobre características como qualidade, segurança e confiabilidade que deve permanecer aplicável por um período prolongado de tempo e, portanto, está documentada e publicada, sendo que o seu objetivo do desenvolvimento é apoiar tanto os indivíduos como as empresas quando da aquisição de produtos e serviços. Assim, os fornecedores de produtos e serviços podem aumentar sua reputação e imagem ao verem certificada a sua conformidade com estes *standards*.

A ISO é uma organização fundada em 1946 e apoiada por 159 países, sendo o principal organismo emissor de *standards* internacionais. Os *standards* ISO 27000 a ISO 27002 foram desenvolvidos em cooperação com o *International Electrotechnical Commission* (IEC), também ele um dos organismos responsáveis pela emissão de *standards* internacionais, mas na eletrónica e no setor de tecnologias relacionadas com a eletrónica e estabelecem referências na área de segurança de informação.

Os documentos indicados de seguida são indispensáveis na temática da segurança da informação sendo posteriormente analisados:

- ISO/IEC 27000:2014, *Information technology — Security techniques — Information security management systems — Overview and vocabulary;*
- ISO/IEC 27001:2013, *Information technology — Security techniques — Information security management systems — Requirements;*
- ISO/IEC 27002:2013, *Information technology — Security techniques — Code of practice for information security controls;*

Complementarmente referencia-se ainda o ISO/IEC 27033, *standard* multiparte derivado do *standard* anterior, de segurança de rede em cinco partes, ISO/IEC 18028, que fez a sua revisão substancialmente, para enquadramento nesta suíte ISO27k e que perante a temática do trabalho se evidência na sequência, de uma forma genérica mas que permitirá posteriormente o enquadramento com os standards IEE 802.11 das WLAN. De referir que a parte 6, ainda em *draft*, é exclusivamente dedicada a segurança de acessos a redes *wireless* IP. A ISO 27033 é relevante para todos os interessados em possuir, operar ou usar uma rede, incluindo aqueles envolvidos no planeamento, conceção e implementação dos aspetos arquitetónicos da segurança de rede (ISO/IEC 27033-1, 2015).

3.3.1 ISO/IEC 27000

O *standard* ISO/IEC 27000:2014 *Information technology — Security techniques — Information security management systems - Overview and vocabulary (third edition)* "fornece uma visão geral dos ISMS e define os termos relacionados.".

O vocabulário ou glossário de definições formais, cuidadosamente formuladas, abrange a maioria dos termos da informação especializada, relacionados com a segurança, utilizados nos *standards* ISO27k, na edição atual oitenta e nove. Segurança da informação, como a maioria de assuntos mais técnicos, usa

uma complexa teia de terminologia que vai evoluindo. Diversos termos nucleares em segurança da informação (tais como "*risk*") tem diferentes significados ou interpretações de acordo com o contexto, a intenção do autor e preconceitos do leitor. Poucos autores se dão ao trabalho de definir precisamente o que eles querem dizer, mas essa ambiguidade é distintamente inútil na arena dos *standards*, pois leva a confusão. Além do mais, seria estranho para avaliar e certificar a conformidade com o *standard* ISO/IEC 27001 se os termos técnicos significassem coisas diferentes para os avaliadores e os avaliados!

O *standard* ISO/IEC 27000 substitui as ISO/IEC *Guide 2:1996 "Standardization and related activities – General vocabulary", ISO Guide 73:2009 "Risk management – Vocabulary – Guidelines for use in standards"*, e ISO/IEC *2382-8: "Information technology - Vocabulary Part 8: Security*". Também inclui definições retiradas de alguns *standards* não ISO 27k. Termos que são reproduzidos sem alterações de outros *standards* ISO, como o ISO 9000, nem sempre são inteiramente apropriados no contexto de segurança da informação.

A visão geral de ISMS introduz a segurança da informação, gestão de riscos, segurança e sistemas de gestão. É uma descrição razoavelmente clara e prolongada da abordagem e *standards* ISO27k, a partir da perspetiva do comitê que os escreveu.

A primeira edição deste *standard* foi publicada em 2009 e a segunda em 2012. A terceira edição, publicada em 2014, incorpora termos usados em atualizações de 2013 para a ISO/IEC 27001 e 27002 e descarta ou altera alguns termos desde a edição anterior.

3.3.2 ISO/IEC 27001

O *standard* ISO/IEC 27001:2013 *Information technology — Security techniques — Information security management systems — Requirements (second edition)* especifica formalmente um ISMS e um conjunto de atividades relativas à gestão de riscos de segurança da informação.

O ISMS é um quadro global de gestão através do qual a organização identifica, analisa e soluciona seus riscos de segurança de informações. Assegura que as medidas de segurança são afinadas para manter o ritmo com as alterações das ameaças de segurança, vulnerabilidades e impactos nos negócios - um aspeto importante em um campo tão dinâmico e a principal vantagem da abordagem flexível orientada a risco do ISO27k em comparação com, digamos, o *Payment Card Industry - Data Security Standard* PCI-DSS[36]. O *standard* abrange todos os tipos de organizações (por exemplo, organizações comerciais, sem fins lucrativos, agências governamentais), todos os tamanhos (desde microempresas a enormes multinacionais) e todas as indústrias ou mercados (por exemplo, retalho, finanças, defesa, saúde, educação e governo).

[36] *Standards* do PCI *Security Standards Council* - fórum global aberto para o contínuo desenvolvimento, melhoramento, armazenamento, disseminação e aplicação de normas de segurança para a proteção de dados contabilísticos e de pagamento.

O ISO/IEC 27001 formalmente não obriga a controlos de segurança da informação específicos, uma vez que os controlos que são necessários variam consideravelmente em toda a vasta gama de organizações, que o adotam. Os controlos de segurança da informação da ISO/IEC 27002 constam no anexo A da ISO/IEC 27001, um pouco como um menu.

As organizações, que adotam este *standard* são livres para escolher quaisquer controlos de segurança da informação específicos que são aplicáveis às suas situações particulares, valendo-se daqueles registados no menu e, potencialmente, complementando-os com outras opções à *la carte* (às vezes conhecido como conjuntos de controlos estendido). Como com a ISO/IEC 27002, a chave para selecionar controlos aplicáveis é proceder a uma avaliação global dos riscos de segurança da informação da organização, pelo que é uma parte vital dos ISMS.

Além disso, a gestão pode optar por evitar, transferir ou aceitar os riscos de segurança da informação ao invés de atenuá-los por meio de controlos - uma decisão de gestão de risco.

A ISO/IEC 27001 é derivado de BS 7799 parte 2, publicado em 1999. A BS 7799 parte 2 foi revisto pela BSI em 2002, incorporando explicitamente o conceito de processo cíclico de *Deming Plan-Do-Check-Act* e foi adotado pela ISO/IEC como ISO/IEC 27001, em 2005 sendo revista extensivamente em 2013, trazendo-a para a linha de outras *standards* ISO certificadas de sistemas de gestão e largando o conceito PDCA.

Foi muito mais do que apenas o aperfeiçoamento do conteúdo da edição de 2005, uma vez que a ISO/IEC *Joint Technical Committee* - JTC1 insistiu em alterações substanciais para alinhar este *standard* com outros *standards* de sistemas de gestão abrangendo também por exemplo, garantia de qualidade e proteção ambiental.

A ideia é que os gestores que estão familiarizados com qualquer um dos sistemas de gestão ISO vão entender os princípios básicos que sustentam um ISMS. Conceitos como certificação, política, não-conformidades, controlo de documentos, auditorias internas e revisões de gestão são comuns a todas as *standards* de sistemas de gestão e de facto os processos podem, em grande medida, ser normalizados dentro da organização.

A ISO/IEC 27002 por sua vez foi extensivamente revisto e republicado ao mesmo tempo, portanto, o anexo A da ISO/IEC 27001 foi completamente atualizada também.

De referir que o relatório técnico ISO/IEC TR 27023 efetua a comparação entre as edições de 2005 e 2013 trazendo algum esclarecimento destas alterações.

Uma corrigenda técnica para ISO/IEC 27001:2013 esclarecendo que informação é de facto uma mais-valia foi publicada em outubro de 2014.

3.3.3 ISO/IEC 27002

A ISO/IEC 27002:2013 *Information technology — Security techniques — Code of practice for information security controls (second edition)* tem como objetivo definir o estabelecimento de linhas de orientação e princípios gerais para iniciação, implementação, manutenção e melhorias da gestão da segurança da informação numa organização, objetivos estes que proporcionam orientações gerais nas metas comummente aceites em gestão da segurança da informação.

É um *standard* popular, reconhecido internacionalmente, de boas práticas para a segurança da informação traçando sua história até 30 anos atrás para os precursores da BS 7799.

Como a governança e gestão de riscos, gestão de segurança da informação é um tema amplo com ramificações ao longo de todas as organizações. Segurança da informação, e, portanto, ISO/IEC 27002, é relevante para todos os tipos de organização, incluindo empresas comerciais de todos os tamanhos (de *one-man-band* até gigantes multinacionais), não lucrativas, de caridade, departamentos governamentais e organismos quase autónomos - aliás qualquer organização que manipula e depende da informação. Os requisitos de controlo e risco de segurança da informação específicos podem diferir em detalhes, mas há muita coisa em comum, por exemplo a maioria das organizações precisa lidar com os riscos de segurança de informações relativas aos seus empregados além de empreiteiros, consultores e fornecedores externos de serviços de informação.

O *standard* explicitamente está preocupado com a segurança da informação, ou seja, a segurança de todas as formas de informação (por exemplo, dados de computador, documentação, conhecimento e propriedade intelectual) e não só isso, mas também com segurança de sistemas.

Enquanto a ISO/IEC 27001 formalmente define os requisitos obrigatórios para um ISMS, usa o ISO/IEC 27002 para indicar controlos de segurança da informação adequado dentro dos ISMS, mas como o ISO/IEC 27002 é meramente um código de boas práticas/orientação ao invés de um *standard* de certificação, as organizações são livres para selecionar e implementar outros controlos, ou efetivamente adotam suites completas alternativas de controlos de segurança da informação como entenderem. A ISO/IEC 27001 incorpora um resumo (pouco mais que os títulos de seção na verdade) dos controles da ISO/IEC 27002 no anexo A, pelo que na prática, a maioria das organizações que adotam a ISO/IEC 27001 também adotam a ISO/IEC 27002.

A ISO/IEC 27002 é um código de boas práticas - um documento consultivo, genérico, não uma especificação formal, tal como a ISO/IEC 27001. Ele recomenda controlos de segurança da informação abordando objetivos de controlo de segurança de informação provenientes de riscos para a confidencialidade, integridade e disponibilidade da informação. As organizações que adotam a ISO/IEC 27002 devem avaliar seus próprios riscos de segurança de informação, esclarecer seus objetivos de controlo e aplicar controlos adequados (ou mesmo outras formas de tratamento dos riscos) usando o *standard* de orientação.

O *standard* é estruturado logicamente em torno de grupos de controlos de segurança relacionados. Muitos controlos poderiam ter sido colocados em várias seções, mas, para evitar duplicações e conflito, foram arbitrariamente atribuídos a um e, em alguns casos, com referências cruzados de outros lugares. Por exemplo, um sistema de controlo de acesso-cartão para, digamos, uma sala de computadores ou arquivo/cofre é tanto um controlo de acesso como um controlo físico que envolve tecnologia, mais a política e procedimentos associados de gestão/administração e uso.

Das 20 seções ou capítulos do *standard*, 14 especificam objetivos do controlo e controlos. Estes 14 são as cláusulas do controlo de segurança.

Há uma estrutura padrão dentro de cada cláusula de controlo: uma ou mais subseções de primeiro nível, cada um afirmando um objetivo do controlo e cada objetivo do controlo sendo apoiado por sua vez, por um ou mais controlos declarados, cada controlo seguido pela orientação de implementação associada e, em alguns casos, notas explicativas adicionais. A quantidade de detalhes é responsável por o *standard* ter quase 90 páginas.

A ISO/IEC 27002 especifica os objetivos dos 35 controlos (um por 'categoria do controlo de segurança') para proteger a confidencialidade, integridade e disponibilidade da informação.

Os objetivos do controlo estão em um nível bastante elevado e, com efeito, compõem uma especificação de requisitos funcionais genéricos para arquitetura de gestão de segurança da informação da organização.

Cada um dos objetivos do controlo é suportado pelo menos por um controlo, dando um total de 114 agrupados em catorze diretrizes, que por sua vez são subdivididas em componentes, optando-se aqui por as indicar em inglês pela sua expressividade técnica, conforme constam no *standard*:

1. *Information security policies*
2. *Organization of information security*
3. *Human resource security*
4. *Asset management*
5. *Access control*
6. *Cryptography*
7. *Physical and environmental security*
8. *Operations management*
9. *Communications security*
10. *System acquisition, development and maintenance*
11. *Supplier relationships*
12. *Information security incident management*
13. *Information security aspects of business continuity management*
14. *Compliance*

3.3.4 ISO/IEC 27033

A ISO/IEC 27033 é um *standard* multiparte que estabelece as regras de segurança nas redes e foi revista para se enquadrar na suite ISO 27k, consiste em 6 partes, sob o título geral de *Information technology - Security techniques - Network security* (as partes 1-5 já foram publicadas e a parte 6 encontra-se ainda em *draft*):

- Parte 1: *Overview and concepts*
- Parte 2: *Guidelines for the design and implementation of network security*
- Parte 3: *Reference networking scenarios — Threats, design techniques and control issues*
- Parte 4: *Securing communications between networks using security gateways*
- Parte 5: *Securing communications across networks using Virtual Private Networks (VPNs)*
- Parte 6: *Securing wireless IP network access*

O propósito da ISO/IEC 27033 é fornecer orientações detalhadas sobre os aspetos de segurança, gestão, operação e utilização de redes de SI e suas interligações. Os indivíduos dentro de uma organização que são responsáveis pela segurança da informação em geral e em particular, pela segurança da rede, devem ser capazes de adaptar o material deste *standard* para satisfazer suas necessidades específicas (ISO/IEC 27033-1, 2015).

A ISO/IEC 27033 fornece ainda orientação detalhada sobre como implementar os controlos de segurança de rede que são introduzidos na ISO/IEC 27002. Aplica-se para a segurança dos dispositivos em rede e gestão da sua segurança, aplicações, serviços de rede, utilizadores da rede, além de segurança da informação, sendo transferida através dos *links* de comunicação dessa rede. Destina-se a utilizadores, *designers*, gestores e arquitetos de segurança de rede.

Os objetivos principais discriminados por partes são:

- ISO/IEC 27033-1:2015 Information *technology - Security techniques - Network security - Part 1: Overview and concepts* define e descreve conceitos associados e fornece orientações de gestão sobre segurança de rede. Isto inclui o fornecimento de uma visão geral de segurança de rede, definições relacionadas e orientações sobre como identificar e analisar os riscos de segurança de rede e em seguida, definir os requisitos de segurança dessa rede. Também refere como conseguir boa qualidade técnica de arquiteturas de segurança e risco, *design*, aspetos de controlo associado a cenários típicos de rede e áreas tecnológicas de rede;
- ISO/IEC 27033-2:2012 *Guidelines for the design and implementation of network security* define como as organizações devem alcançar arquiteturas técnicas de segurança de rede de qualidade, projetos e implementações que garantam a segurança de rede apropriada para seus ambientes de negócios, usando uma abordagem consistente para o planeamento, projeto e implementação de segurança de rede, conforme o caso, auxiliado pelo uso de

modelos/*frameworks*[37] e é relevante para todo o pessoal que está envolvido no planeamento, projeto e implementação dos aspetos arquitetónicos da segurança de rede;

- ISO/IEC 27033-3:2010 *Reference networking scenarios - threats, design techniques and control issues* define riscos específicos, técnicas de design e controlo de problemas associados com cenários típicos da rede. É relevante para todo o pessoal que estão envolvido no planeamento, projeto e implementação dos aspetos arquitetónicos da segurança de rede;
- ISO/IEC 27033-4:2014: *Securing communications between networks using security gateways* define riscos específicos, técnicas de design e controlo de problemas para garantir os fluxos de informação entre redes usando *gateways* de segurança. É relevante para todo o pessoal que está envolvido em planeamento detalhado, projeto e implementação de *gateways* de segurança;
- ISO/IEC 27033-5:2013: *Securing communications across networks using Virtual Private Networks (VPNs)* define riscos específicos, técnicas de *design* e controlo de problemas para proteger ligações estabelecidas usando VPN. É relevante para todo o pessoal que está envolvido em planeamento detalhado, projeto e implementação de segurança VPN;
- ISO/IEC 27033-6: *Securing wireless IP network access (DRAFT)* define os riscos específicos, técnicas de design e controlo de problemas para proteger redes *wireless* IP. É relevante para todo o pessoal que está envolvido em planeamento detalhado, projeto e implementação de segurança para redes *wireless*.

Ressalta que este *standard* internacional fornece orientações de aplicação mais pormenorizada sobre os controlos de segurança de rede que são descritos em um nível *standardizado* básico na ISO/IEC 27002, não sendo uma referência ou documento normativo para requisitos legislativos e regulamentares de segurança, por estarem dependentes por exemplo, do país, do tipo de negócio ou outro.

A primeira parte faculta também um glossário de termos específico de segurança da informação para redes, orientação sobre um processo estruturado para identificar e analisar os riscos de segurança de rede e, portanto, definir requisitos de controlo de segurança de rede, incluindo aqueles mandatados pelas políticas de segurança de informação pertinentes.

Ainda providencia uma visão geral dos controlos de suporte de arquiteturas de segurança técnica da rede e controlos técnicos relacionados, bem como controlos não-técnicos, além de outros controlos técnicos que não estão relacionados exclusivamente à segurança da rede de apoio (estabelecendo ligação com a ISO/IEC 27001, ISO/IEC 27002 e ISO/IEC 27005 e outros *standards* ISO27k à medida que vão sendo publicados), explicando as boas práticas em relação às arquiteturas técnicas de segurança de rede e os aspetos de risco, projeto e controlo associados com cenários típicos de rede e áreas de tecnologia de rede distribuído através das partes constituintes do ISO/IEC 27033 no seu todo.

[37] Neste contexto, um modelo/*framework* é usado para descrever uma representação ou descrição mostrando a estrutura e o funcionamento de alto nível de um tipo de arquitetura/*design* técnico de segurança.

Aborda ainda os problemas associados com a implementação e operação de controlos de segurança de rede, e o contínuo acompanhamento e revisão de sua implementação, estendendo as orientações de gestão de segurança previstas na ISO/IEC TR 13335 e ISO/IEC 27002 e outras, detalhando os mecanismos necessários para implementar controlos de segurança de rede em uma ampla gama de ambientes de rede, fornecendo uma ponte entre as questões de gestão de segurança de informação geral e os detalhes da implementação de controlos técnicos de segurança de rede em grande escala (por exemplo, *firewalls*, IDS/IPS, MIC), mencionando requisitos como não-repúdio e confiabilidade além da tríade clássica da CIA (confidencialidade, integridade e disponibilidade).

Este *standard* de alguma forma consegue fornecer uma visão razoavelmente técnica de segurança de rede com quase nenhuma referência para a pilha de rede OSI, o *Open Systems Interconnection Model* (*OSI Model*)[38].

3.4 Segurança em redes sem fios

Segundo Vilela (2012), citado por Alves, Ferreira, e Shinoda, (2013), as falhas existentes nos menus de segurança do *standard* IEEE 802.11 são evidentes. Isso mostra a necessidade em agregar outro mecanismo de segurança nas WLAN para minimizar as ameaças que exploram estas vulnerabilidades.

A utilização de WLAN implica sérios riscos de segurança, que podem ser explorados e causar indisponibilidade de serviços. Obviamente as necessidades de segurança variam e atingem graus de criticidade diferentes em conformidade com a utilização e confidencialidade dos dados que lá passam.

Portanto, para as WLAN, a segurança é um elemento necessário e obrigatório da tecnologia, da sua preparação e implementação numa perspetiva organizacional.

O *standard* IEEE 802.11 inicial (1999) define autenticação, encriptação e integridade de dados para o tráfego *wireless*. Mas neste *standard* a integridade de dados, encriptação e autenticação provou ser relativamente fraco e complicado para implementação pública e privada generalizada, pelo que a solução para essas deficiências foram resolvidas pelo IEEE 802.11i, posteriormente integrado na revisão de 2007 do IEEE 802.11, que referencia exclusivamente questões de segurança e protocolos a utilizar sobre as WLAN, aumentando consideravelmente a segurança, definindo melhores procedimentos para autenticação, autorização e criptografia.

De referir ainda que outros organismos têm intervindo no desenvolvimento de regras e *standards* proprietários como a *Wi-Fi Alliance*, criada e constituída por um conjunto de vendedores de soluções, para fazer face ao ritmo lento de resposta do IEEE para resolução dos problemas de segurança dos *standards wireless*, de onde surgem soluções como o *standard* de indústria *Wi-fi Protected Acess* – mais conhecido como WPA, compatível posteriormente com o standard 802.11i do qual derivou (do seu *draft*[39]).

[38] Define uma estrutura de rede para implementar protocolos em sete camadas.

[39] Proposta de projeto de *standard*, ainda em fase de aprovação, divulgado pelo IEEE antes de ser publicado para ajudar a facilitar o cumprimento antecipado e implementação.

Normalmente, um sistema de segurança de rede baseia-se em camadas de proteção e consiste em múltiplos componentes, incluindo *software* de monitoração e segurança de rede, além de *hardware* e *appliances* (ferramentas) especificas para garantir a segurança. Todos os componentes trabalham juntos para aumentar a segurança geral da rede informática.

As WLAN efetuam a difusão dos seus dados usando sinais de rádio. Ao contrário das tecnologias de LAN como a *Ethernet*, é difícil controlar o acesso a uma rede *wireless*. Por exemplo, com redes cabladas, precisamos de ter acesso físico a uma porta de rede. Nas redes *wireless*, não necessitamos sequer de estar no edifício, pode-se aceder do outro lado da rua. A diferença entre LAN e WLAN é ilustrada na seguinte comparação:

- Nas LAN, o meio é privado, não precisamos de nos preocuparmos sobre quem está a ligar, porque o pressuposto é que utilizadores não autorizados não conseguem ter acesso a uma porta de rede. Também não tem que se garantir que o tráfego é confidencial, porque o tráfego é enviado por um sistema de cablagem privada que não é acessível a utilizadores não autorizados.
- Nas WLAN, o meio é público. Qualquer pessoa com o equipamento *wireless* apropriado dentro do alcance rádio pode tentar ligar-se. O tráfego de rede deve ser igualmente confidencial porque, utilizadores não autorizados podem receber pacotes de dados sem estarem presentes em áreas fisicamente seguras e/ou protegidas.
- A utilização de redes *wireless* implica sérios riscos de segurança, que podem ser explorados e causar indisponibilidade de serviços.

As propriedades de comunicações por redes *wireless* protegidas consistem de:

- **Autenticação** - antes de ser autorizado a troca de tráfego de dados com a rede *wireless*, o nó de rede *wireless* deve ser identificado e, dependendo do método de autenticação, deve apresentar credenciais que possam ser validadas;
- **Encriptação** - antes de enviar um pacote de dados *wireless*, o nó de rede *wireless* deve encriptar os dados para garantir a confidencialidade destes;
- **Integridade dos dados** - antes de enviar um pacote de dados *wireless*, o nó de rede *wireless* deve incluir informações no pacote para que o recetor possa determinar que os conteúdos do pacote não foram modificados em trânsito.

Devido à natureza da transmissão de redes WLAN, a espionagem e o *sniffing*[40] remoto de pacotes nas WLAN é muito fácil, pelo que para evitar isto o *standard* IEEE 802.11 define o protocolo WEP para fornecer um nível de confidencialidade e integridade de dados, equivalente a uma rede cablada.

[40] Ferramenta que permite a indivíduos capturar dados que são transmitidos através de uma rede.

O principal problema com o WEP é que a determinação e a distribuição de chaves de criptografia WEP não estão definidos. As chaves WEP devem ser distribuídas por meio de um canal seguro fora do protocolo 802.11. Na prática, as chaves WEP são sequências de texto que devem ser configuradas manualmente usando um teclado para o AP e clientes *wireless*. Obviamente, este sistema de distribuição de chaves não se adapta bem a uma organização e não é seguro (Gandhi, 2014).

Além disso, segundo o mesmo autor, não há nenhum mecanismo definido para alterar as chaves de criptografia WEP, quer por autenticação ou periodicamente, para uma ligação autenticada. Todos os AP e clientes usam a mesma chave WEP configurada manualmente para múltiplas sessões. Com vários clientes *wireless*, enviando uma grande quantidade de dados, um atacante pode capturar remotamente grandes quantidades de texto cifrado WEP e usar métodos de criptoanálise para determinar a chave WEP.

Refere também que a falta de um protocolo de gestão de chaves WEP é uma limitação primordial para proporcionar segurança no 802.11, especialmente no *infraestruture mode*, com um grande número de STA. Alguns exemplos deste tipo de rede incluem campus corporativos, educacionais e lugares públicos, como aeroportos e *shoppings*. A falta de autenticação automatizada e determinação de serviços chave também afeta a operação em modo *ad-hoc*, em que os utilizadores podem querer ligar-se em comunicação *peer-to-peer* colaborativa em áreas como salas de conferências.

Além de encriptação WEP, as seguintes técnicas são por vezes utilizadas para proteger redes *wireless* 802.11 (Dhanalakshmi e Sathiya, 2015):

- Não difusão nas redes *wireless*;
- Filtragem de endereço MAC.

As questões de segurança que existiam com o padrão 802.11 original eram as seguintes (Holt e Huang, 2010):

- Nenhuma deteção de AP falsos;
- Nenhuma identificação do utilizador e autenticação;
- Nenhum mecanismo para autenticação central, autorização e avaliação;
- Algumas implementações derivam senhas, resultando em palavras-chave WEP fracas;
- Não há suporte para métodos de autenticação estendida. Por exemplo, cartões de *token*, certificados/cartões inteligentes, senhas únicas, biometria e outros;
- Não há suporte para gestão de palavras-chave. Por exemplo, renovação de palavras-chave, chaves globais e gestão dinâmica de palavras-chave por STA ou por sessão.

Devem assim ser aplicadas normas adicionais que forneçam métodos de autenticação mais fortes e discutam melhorias para a encriptação originalmente definida assim como, métodos para garantir a integridade de dados.

A solução para estas deficiências, do definido originalmente pelo *standard* IEEE 802.11, é o IEEE 802.1X que fornece mecanismos de autenticação, autorização e acordo da chave de criptografia

compatíveis para apoio à comunicação segura entre dispositivos conectados em conformidade com o IEEE 802 já anteriormente referido.

Existem duas características de uma LAN que não são inerentes a uma WLAN:

- A fim de transmitir em uma LAN, uma STA deve ser fisicamente ligada à LAN enquanto numa WLAN, qualquer estação dentro do alcance de rádio dos outros dispositivos na rede local pode transmitir. Em certo sentido, há uma forma de autenticação com uma LAN, que requer alguma ação positiva e presumivelmente observável para conectar uma STA a uma LAN;
- Da mesma forma, a fim de receber uma transmissão de uma STA que faz parte de uma LAN, a STA recetora também deve ser ligada à LAN mas numa WLAN, qualquer STA dentro do alcance do rádio pode receber. Assim, uma LAN fornece um grau de privacidade, limitando a receção de dados de STA conectadas à rede local.

3.4.1 Acesso e serviços de privacidade

O IEEE 802.11 define três serviços que fornecem uma WLAN com os recursos, de autenticação de acesso e a privacidade (Holt e Huang, 2010):

1. **Autenticação**: Estabelece a identidade das STA para cada um dos outros considerando-se que:
   - Em uma LAN, geralmente presume-se que o acesso a uma conexão física transmite autoridade para se ligar a essa LAN não sendo uma suposição válida para uma WLAN, em que conetividade é alcançada simplesmente por ter uma antena ligada e ajustada corretamente;
   - O serviço de autenticação é usado pelas STA para estabelecer a sua identidade com as STA com que se desejam comunicar;
   - O IEEE 802.11 suporta vários esquemas de autenticação e permite a expansão da funcionalidade desses esquemas. O *standard* não obriga a qualquer esquema de autenticação específico, podendo variar do *handshaking*, relativamente não seguro, para esquemas de criptografia de chave pública;
   - No entanto o IEEE 802.11 requer, por aceitação mútua, autenticação bem-sucedida antes de uma STA, poder estabelecer uma associação com um AP;
2. **Deautenticação:** Este serviço é chamado sempre que uma autenticação existente está a ser finalizada;
3. **Privacidade**: Impede que o conteúdo das mensagens seja lido por outro que não o destinatário pretendido. O *standard* prevê o uso opcional de criptografia para assegurar essa privacidade.

3.4.2 *Standards* de segurança das redes locais sem fios

O *Standard* 802.11 inicial incluía um conjunto de recursos de segurança para autenticação e privacidade bastante fracos. Para a privacidade, o 802.11 definiu o algoritmo WEP que continha muitos pontos fracos. Na sequência do desenvolvimento do WEP, o grupo tarefa do 802.11i desenvolveu um

conjunto de recursos para abordar as questões de segurança das WLAN. A fim de acelerar a introdução de segurança forte em WLAN, o *Wi-Fi Alliance* promulgou o *Wi-Fi Protected Access* (WPA) como um *standard* de *Wi-Fi*. O WPA é um conjunto de mecanismos de segurança que elimina a maioria dos problemas de segurança 802.11 e baseou-se na correção do *standard* 802.11i ao 802.11 e com este irá evoluir para manter a compatibilidade.

Segundo (Angela, 2014) o IEEE 802.11i abordava três áreas principais de segurança: autenticação, gestão de chaves e privacidade de transferência de dados. Para melhorar a autenticação, o 802.11i requeria o uso de um *Authentication Server* (AS) - e define um protocolo de autenticação mais robusto normalmente designado como *Extensible Authentication Protocol* (EAP)[41] que realiza a comunicação entre o cliente e o AP, mas existem mais.

O AS também desempenha um papel na distribuição de chaves. Para a privacidade, o 802.11i fornece três esquemas diferentes de criptografia, o WEP de 64 e 128 bits, o WPA e o *Advanced Encryption Standard* (AES). O esquema que fornece uma solução a longo prazo faz uso do AES com chaves de 128 bits. No entanto, porque o uso de AES exigiria *upgrades* caros dos equipamentos existentes, esquemas alternativos com base no RC4[42] 104-*bit*[43] também são definidos.

3.4.2.1 Visão geral da forma de operacionalização do 802.11i

Pela importância de que se reveste em termos de segurança para as WLAN descreve-se de seguida uma perspetiva global, da forma de operacionalização do *standard* 802.11i, para perceção das sugestões posteriores em matéria de segurança para implementação das WLAN utilizando-se nesta visão o descrito por Angela, (2014), Dhanalakshmi e Sathiya (2015) e o próprio *standard* IEE 802.11i entretanto incorporado na revisão do standard IEE 802.11 de 2007 e como tal também já refletido na versão de 2012 como referido anteriormente.

Após a identificação da rede pela transmissão do BSS, é efetuada uma troca entre uma STA e um AP, que permite aos dois chegar a acordo sobre o conjunto de recursos de segurança a ser usado. Então, uma troca envolvendo o AS e a STA fornece uma autenticação segura. A AS é responsável pela distribuição de chaves para a AP, que por sua vez, gere e distribui as chaves para as STA. Finalmente, criptografia forte é usada para proteger a transferência de dados entre a STA e o AP.

A arquitetura 802.11i é composta por três principais ingredientes:

[41] Estrutura de autenticação, que fornece o transporte e o uso de material protegido e os parâmetros gerados por métodos EAP

[42] Algoritmo simétrico de criptografia de fluxo – a encriptação WEP usa uma técnica chamada *Rivest Ciper*-4 (RC4) com uma chave de 40 ou 104 *bit*.

[43] A chave WEP é tipicamente identificada como de 64 ou 124 *bit*, mas a chave inclui um vetor de inicialização de 24 *bit*, assim a chave atual é de 40 ou 104 *bits*.

- **Autenticação**: Um protocolo é usado para definir uma troca entre um utilizador e um AS que fornece autenticação mútua e cria chaves temporárias para serem usadas entre o cliente e o AP sobre a ligação *wireless*;
- **Controle de acesso**: Esta função impõe o uso da função de autenticação, roteia as mensagens corretamente e facilita a troca de chaves. Pode trabalhar com uma variedade de protocolos de autenticação;
- **Privacidade com integridade de mensagem**: Ao nível de dados de MAC, por exemplo, uma *Protocol Data Unit Logical Link Control* (PDU LLC), são criptografados, juntamente com um código de integridade de mensagem que garante que os dados não foram alterados.

3.4.2.2 Autenticação

A autenticação opera a um nível acima dos protocolos LLC e MAC e é considerada fora do âmbito do 802.11. Há um número de protocolos de autenticação populares em uso, incluindo o EAP e o *Remote Authentication Dial-In User Service* (RADIUS)[44].

3.4.2.3 Controle de acesso

Referem os mesmos autores que o IEEE 802.11i faz uso de um outro *standard* que foi projetado para fornecer funções de controlo de acesso para redes locais. O *standard* é o IEEE 802.1X, atualizado em 2012,que estabelece regras de *Port-Based Network Access Control (PNAC*). O IEEE 802.1X usa os termos *supplicant, authenticator* e *AS*. No contexto de uma WLAN 802.11, os dois primeiros termos correspondem às STA e ao AP. O AS é normalmente um dispositivo separado no lado da LAN (ou seja, acessível sobre *Domain Services* (DS)), mas que também pode residir diretamente sobre o *authenticator*.

Antes de um *supplicant* ser autenticado pelo AS, usando um protocolo de autenticação, o *authenticator* só passa mensagens de controlo ou autenticação entre o *supplicant* e o AS; o canal de controlo 802.1X está desbloqueado, mas o canal de dados 802.11 está bloqueado. Uma vez que o *supplicant* é autenticado e as chaves são fornecidas, o *authenticator* pode encaminhar dados do *supplicant*, sujeitos a limitações predefinidas do controle de acesso do *supplicant* para a rede. Nestas circunstâncias, o canal de dados está desbloqueado.

O 802.1X usa os conceitos de portas controladas e não controladas. Portas são entidades lógicas definidas dentro do *authenticator* e referem-se a ligações de rede física. Para uma WLAN, o *authenticator* (AP) pode ter apenas duas portas físicas, uma ligando-se ao DS e outra para a comunicação *wireless* dentro de sua BSS. Cada porta lógica é mapeada para uma dessas duas portas físicas. Uma porta não controlada permite a troca de PDUs entre o *supplicant* e o AS independentemente do estado de autenticação do outro

[44] Protocolo de rede que fornece de forma centralizada autenticação, autorização e contabilização, no processo de gestão de computadores que se ligarão e utilizarão um determinado serviço de rede.

supplicant. Uma porta controlada permite a troca de PDUs entre um *supplicant* e outros sistemas na LAN, somente se o estado atual do *supplicant* autoriza tal troca.

A *framework* 802.1X, com um protocolo de camada superior de autenticação, encaixa-se muito bem com uma arquitetura BSS que inclua um número qualquer de STAs e um AP. No entanto, para um *Independent Basic Service Set* (IBSS**)**, não há nenhum AP. Para um IBSS, o 802.11i fornece uma solução mais complexa que, em essência, envolve autenticação emparelhada entre STA no IBSS.

3.4.2.4 Privacidade com integridade de mensagem

O IEEE 802.11i define dois métodos para proteger os dados transmitidos em 802.11 MAC PDUs (IEEE 802.11, 2012) que se descrevem de seguida:

O primeiro método conhecido como TKIP, normalmente designado por WPA-1. O TKIP é projetado para exigir apenas alterações de *software* para dispositivos que são implementados com uma abordagem de segurança anterior da WLAN chamada WEP; usa o mesmo algoritmo de criptografia de fluxo RC4 que a WEP.

O segundo método conhecido como CCMP, normalmente designado por WPA-2. O CCMP faz uso do protocolo de encriptação AES. Ambos, TKIP e WPA-2, acrescentam um *Message Integrity Code* (MIC) à estrutura 802.11 MAC após o campo de dados. O MIC é gerado por um algoritmo, chamado *Michael*[45], que determina um valor de 64-*bit* calculado a partir da fonte, dos valores do endereço MAC de destino e do campo de dados. Em seguida, esse valor é codificado (encriptado) usando uma chave separada da utilizada para codificar (encriptar) os campos de dados. Assim, ambos os campos, MIC e dados são encriptados. O uso de um algoritmo mais complexo, uma chave criptográfica separada, com um comprimento de 64 *bits*, fazem do MIC, substancialmente, um recurso de autenticação de mensagem mais forte do que o *Integrity Check Vector* (ICV). O MIC serve o propósito de autenticação de mensagem.

3.5 Evolução das redes locais sem fios na organização

A emergente *Wi-Fi* de alta velocidade, com base no protocolo em 802.11ac, perspetiva-se que terá um enorme impacto sobre as arquiteturas de rede. Ao mesmo tempo, muitas organizações e departamentos de TI estão tentando adaptar-se a outra tendência igualmente significativa — personalizar a experiência móvel. Compreendendo cada uma e a relação entre elas, poderão pensar melhor a sua estratégia para incorporar as tecnologias de alta velocidade atuais na sua arquitetura de rede e permitir que tendências futuras também possam utilizar essa mesma arquitetura.

Por outro lado o IEEE 802.11ad, alteração para o *standard* 802.11 que permite comunicações wireless *multi-gigabit* na banda de 60 GHz, complementa o 802.11ac.

[45] Função *hashing* que permite calcular o MIC.

Esta especificação *WiGig*[46] contribuiu para o processo de normalização IEEE 802.11ad e foi confirmada em maio de 2010 como base para o projeto de *standard* 802.11ad, ratificada finalmente em 2012, sendo projetada para conduzir a um ecossistema global de produtos interoperáveis.

A especificação define uma nova arquitetura de rede que permite que dois dispositivos se comuniquem diretamente uns com os outros, permitindo que novos usos tais como, sincronizar rapidamente dois dispositivos, e por exemplo, permitir transmissão direta de dados audiovisuais para um projetor ou TV. Além disso e mais importante, a especificação também suporta arquiteturas de rede 802.11 existentes, incluindo o uso de um AP compartilhado, como nas redes *Wi-Fi* de hoje.

A especificação *WiGig* utiliza segurança avançada que se baseia nos mecanismos de segurança forte usados no IEEE 802.11. O *WiGig* usa *Galois* / *Counter Mode* (GCM)[47], um modo altamente eficiente de funcionamento que é projetado para suportar velocidades de comunicação de mais de 10 *Gbps*, fornece criptografia forte baseada sobre o AES, é recomendado pelo NIST e governo dos Estados Unidos e pode ser implementado em *hardware* para elevar o desempenho e eficiência.

[46] Também conhecido como 802.11ad, é conhecido como "micro-ondas *Wi-Fi*", uma vez que opera numa banda de frequência diferente, muito mais elevada, a de 60GHz.

[47] NIST SP 800-38D - Recommendation for *Block Cipher Modes of Operation: Galois/Counter Mode (GCM) and GMAC.*

4 Implementação de redes locais sem fios

Neste capítulo, na sequência da caraterização do problema no anterior e referenciação dos elementos essenciais à criação, desenho e implementação com sucesso de uma WLAN segura, utilizando os *standards* que servem de base à questão da segurança da informação e da tecnologia, enquadrando-se com:

- Possibilidade de integração ou não com as infraestruturas existentes;
- Questões de segurança que se colocam e a forma de as resolver;
- Perspetivas de evolução;
- Diversas soluções encontradas para garantir que a WLAN corresponde ao exigido pela organização,

pretende-se estabelecer um referencial das opções e requisitos a ter em atenção na implementação de WLAN por qualquer organização, nomeadamente o que será necessário observar para garantir que seja bem-sucedida, tentando-se fornecer orientação para a definição dos princípios básicos a considerar.

As etapas de desenho, instalação, configuração e teste devem considerar na organização todas as áreas funcionais, entre elas, o apoio às redes, aplicações e serviços, segurança e manutenção do edifício, considerando que a WLAN deve encontrar-se preparada e dimensionada para uma eventual expansão futura a outras localizações e conteúdos diferentes.

Com base no estabelecido nos *standards* de referência e recomendações dos diversos organismos internacionais considera-se que serão de considerar e abordar aspetos, tais como:

- Princípios orientadores para essa implementação;
- Infraestrutura existente ou necessária;
- Arquitetura física e lógica, tanto da solução como da respetiva rede de suporte, considerando a eficiência do espectro rádio utilizado, os vários serviços prestados pela infraestrutura *wireless* e aspetos relacionados com a alta disponibilidade ou não da solução;
- Infraestrutura da WLAN, considerando o tipo de funções que deverão ser asseguradas pelos equipamentos de base;
- Aspetos de segurança do serviço *wireless*, perspetivando-se a questão da integração com os serviços corporativos da organização (domínio, autenticação, *proxy*[48] por exemplo)

4.1 Princípios orientadores

Como em todas as decisões criticas e importantes, também na questão da adoção das WLAN, é necessário um planeamento, de forma a garantir que as opções, na arquitetura a definir, nas políticas, considerando que com a utilização de dispositivos próprios, um novo nível de requisitos de gestão e

[48]Servidor (computador ou aplicação) que age como intermediário para pedidos de clientes solicitando recursos de outros servidores.

decisões deverão ser tomadas e consideradas, pois podem afetar investimentos em outras áreas de tecnologia como *hardware*, *software* e segurança (Education, 2011).

Pretende-se fornecer princípios e um referencial, do processo de decisão, desenho, implementação e gestão, a considerar numa solução *wireless*, permitindo identificar áreas críticas que devam ser consideradas.

Assim e considerando que o NIST (NIST SP 800-36, 2003) referencia cinco fases, no modelo de ajuda para implementações de WLAN, permitindo às organizações determinarem em que momento, nas suas implementações, uma prática recomendada pode ser relevante, são aqui descritas essas fases que deverão apoiar o processo de decisão da adoção das WLAN e forma de o fazer:

1º. **Iniciação** - inclui as tarefas que uma organização deve executar antes de começar a projetar a sua solução WLAN. Isto incluí fornecer uma visão geral em como o WLAN deverá apoiar a missão da organização, criando uma estratégia de alto nível para a sua implementação, desenvolvendo uma política de utilização, especificando requisitos funcionais e de negócio para a mesma;

2º. **Aquisição e desenvolvimento** - Divide-se em duas para efeitos da construção do modelo que se quer sugerir e pela sua diferenciação específica:

   a. Planeamento e Design - Nesta primeira parte da fase, os WLAN *network architects*[49] especificam as caraterísticas técnicas da solução WLAN e componentes de rede relacionados. Estas características incluem:

      i. Método EAP ou métodos usados para oferecer suporte à autenticação;
      ii. Os protocolos usados para apoiar a comunicação entre o AP e o AS;
      iii. *Access Control Lists* (ACL) e regras de *firewall* para segregar o tráfego da WLAN;
      iv. Natureza da *Public Key Infrastructure* (PKI) de suporte;
      v. Os tipos de clientes a serem implementados, também, devem ser considerados, uma vez que eles podem afetar as políticas de segurança desejadas. Há uma grande variedade de *supplicants* que podem ou não suportar os métodos desejados; deve-se ter cuidado para garantir que a política de segurança pode ser utilizada e aplicada por todos os componentes (clientes, AP e AS);
      vi. Um *site survey*[50] é conduzido normalmente para ajudar a determinar o número e a colocação de AP, bem como a forma como vão integrar a rede existente.

   b. Aquisição - Esta segunda parte da fase envolve a especificação do número e tipo de componentes WLAN que devem ser adquiridos, conjuntos de recursos que devem suportar, assim como quaisquer certificações que devem assegurar.

[49] Desenham e implementam, realizam modelagem de rede, análise e planeamento. Também podem criar medidas de rede e segurança.

[50] Processo de planeamento e projeto de uma WLAN, para fornecer uma solução *wireless* que entregue a cobertura *wireless* necessário, taxas de dados, capacidade da rede, de *roaming* e QoS.

3º. **Implementação** - Nesta fase, os equipamentos adquiridos são os primeiros a ser configurados para satisfazer os requisitos operacionais e de segurança, sendo posteriormente instalados e ativados numa rede de produção. A implementação inclui alterar a configuração de outros controlos de segurança e tecnologias, tais como *logs*[51] de eventos de segurança, gestão de rede, integração do servidor de *Authentication, Authorisation and Accounting* (AAA) e PKI.

4º. **Operações/manutenção** - Essa fase inclui tarefas relacionadas com segurança, que uma organização deve executar em uma base contínua, uma vez que a WLAN está operacional, incluindo revisão de *log* e deteção de *rogue* AP.

5º. **Remoção/eliminação** - Esta fase engloba tarefas que ocorrem após um sistema ou seus componentes terem sido retirados, incluindo preservação de informações para atender requisitos legais, limpeza de mídias e eliminação de equipamentos em conformidade com a legislação em vigor.

As organizações são fortemente encorajadas a adotar as recomendações de "melhores práticas". Falhas dos procedimentos para implementá-las aumentam significativamente o risco de uma falha de segurança na WLAN. As organizações também devem examinar cada uma das "deve-se considerar" recomendações, da SP 800-36 da NIST, para determinar sua aplicabilidade para o ambiente de destino.

De referir ainda que para o conjunto de sugestões modulares que se indicam, foram analisados os *case study* (NIST SP 800-97, 2007) e identificados os passos a efetuar, pelo que se considera que numa fase inicial deverá ser efetuado um levantamento que permita identificar quais os principais requisitos necessários à futura solução.

Apresenta-se de seguida um resumo destes mesmos requisitos:

- Cobertura de sinal das áreas onde se quer implementar a solução;
- Qual a média de utilizadores (capacidade a instalar);
- Níveis de segurança, no que respeita à confidencialidade dos dados, autenticação e autorização dos utilizadores:
  - Controlo de Acesso granular: por segmento de rede, recursos, grupos e utilizadores;
  - Suporte de autenticação por meio de certificados digitais;
  - Autenticação integrada com o domínio corporativo.
- Gestão centralizada;
- Alta disponibilidade ao nível dos controladores que assegurem a continuidade do serviço (identificar quais as áreas mais importantes para a cobertura do serviço, o que permite determinar, não só a localização "exata" para a instalação dos AP, bem como a quantidade necessária a uma cobertura aceitável em cada uma das áreas);

[51] Processo de registo de eventos relevantes.

- Análise dos níveis de ruído e interferências externas que possam condicionar as decisões do projeto - *site-survey*.

4.2 Infraestrutura

A infraestrutura depende em última análise da arquitetura da solução *wireless* a implementar, pelo que a plataforma deverá ser definida em conformidade, atendendo ao que determinados autores, anteriormente referidos, assumem considera-se um conjunto de funções principais:

- Gestão, aprovisionamento e monitorização de toda a infraestrutura *wireless*;
- Gestão automatizada do espectro rádio utilizado pela infraestrutura *wireless;*
- Ponto único e centralizado no controlo de acesso dos clientes *wireless* à rede corporativa - *Role-Based Access Control* (RBAC)[52];
- Aplicação de medidas de segurança, tais como, autenticação, autorização e controlo/filtragem de tráfego;
- Deteção e prevenção de intrusões provenientes da rede *wireless*;
- Deteção e contenção de dispositivos/serviços *wireless* não autorizados (*rogue*) dentro do perímetro das instalações.

Deverá ser considerada a forma como o acesso à rede é assegurado existindo um conjunto de arquiteturas possíveis.

Uma arquitetura base essencial que permita assegurar minimamente uma rede organizacional (Acker, 2010; Cisco Systems, 2011) deverá ser constituída por AP, dedicando-se exclusivamente às funcionalidades de acesso ao meio, controladores que ficam encarregues das operações mais complexas, tais como, segurança, gestão, *roaming*[53], entre outras.

Numa arquitetura de *infrastructure mode*, como representado esquematicamente na figura 8, os AP devem encontrar-se intrinsecamente associados e dependentes de um controlador, que atua como um *switch*, papéis representados (controlador e *switch*) autonomamente na figura para melhor perceção, que comuta os dados entre os clientes *wireless* e as restantes redes, descrita genericamente como LAN.

O tráfego entre os AP e o controlador será encapsulado através de um túnel de dados, com recurso a um protocolo que permita este encapsulamento, como por exemplo, o *Generic Router Encapsulation* (GRE)[54], estabelecido no momento em que o AP é ligado e aprovisionado na rede. Os dados dos clientes são enviados para o controlador através deste túnel, não existindo, em qualquer momento, dados que

[52] Abordagem de restrição de acesso ao sistema para utilizadores autorizados, habitualmente baseado nas funções ou papéis desempenhados e mais usado por organizações com mais de 500 funcionários.

[53] O *Wi-Fi* do dispositivo movimenta-se automaticamente a partir de um ponto de acesso para outro conforme necessita para fornecer conectividade sem interrupção na ligação.

[54] Protocolo de encapsulamento desenvolvido pela Cisco *Systems* que encapsula uma ampla variedade de protocolos de camada de rede no interior de *links* virtuais ponto-a-ponto sobre *Internet Protocol internetwork*.

possam ser transmitidos diretamente do AP para a rede (salvo em caso de configuração explícita do modo *split-tunnel*[55]).

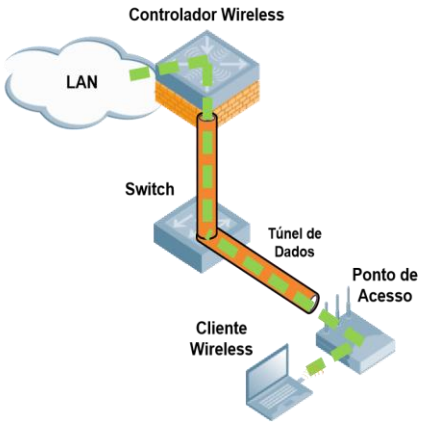

Figura 8 - Arquitetura simplificada
(Adaptado de Acker, (2010);Cisco Systems, (2011))

Para cada implementação dever-se-á perspetivar os cenários que se querem aplicar, sendo o mais comum o que considera pelo menos um conjunto de três redes *wireless* (diferentes **SSID**), a fim de corresponder a utilizadores com diferentes perfis de acesso e utilização, e que normalmente correspondem a funcionários e colaboradores, visitantes, e quarentena**.**

Assim, em termos de segurança, podem-se aplicar, de forma diferenciada, diferentes politicas, e o tráfego proveniente dos diferentes utilizadores é encapsulado até aos controladores *wireless* que, por sua vez, o encaminham para as redes corretas, de acordo com o perfil associado a cada um desses utilizadores, por exemplo um utilizador interno terá um perfil de utilização que lhe permitirá aceder a todos os recurso da organização e um externo não.

Descreve-se de seguida a arquitetura da infraestrutura de rede passiva/ativa, com os requisitos mínimos necessários, pois como anteriormente referido cada implementação deverá ser corretamente enquadrada com a organização e respetiva estratégia, para garantir uma implementação que garanta integração e segurança da rede, que pode passar ou não por contemplar a necessidade de instalação de nova cablagem e equipamentos ativos (*switchs*) de suporte à distribuição de rede entre os controladores, e os vários AP a instalar nas diversas áreas.

Distinguimos assim dois tipos de infraestrutura possível:

- Distribuição de Rede Vertical que permite interligar o *core* da rede com as várias áreas a considerar;
- Distribuição de Rede Horizontal que permite interligar os AP, instalados nas áreas, com seus respetivos *switches*.

[55] O processo de permitir que um utilizador remoto VPN aceda a uma rede pública, mais comumente a *Internet*, ao mesmo tempo que tem autorização para aceder a recursos em VPN.

Para determinação da localização da instalação de cada um dos AP, assim como a quantidade necessária para a cobertura da área, deverá ser utilizada a informação do *site-survey* espacial já referido, a efetuar inicialmente, devendo ser identificadas as áreas de maior densidade de utilizadores, colocando um AP no seu centro. Este critério permite concentrar a cobertura do sinal nas áreas de maior importância.

Quanto aos Controladores *Wireless* deverão ser instalados em sitio reservado e de acesso limitado e seguro, ligados diretamente ao *core* da rede, a *switchs* e a fontes de alimentação distintas, assegurando assim a redundância do equipamento.

4.3 Arquitetura lógica

Segundo Gandhi (2014) a adoção de WLAN na organização poderá obrigar à criação de novas infraestruturas de rede a integrar nas existentes em conformidade com as opções tomadas, de forma a suportar a gestão e operação da plataforma *wireless*, os diversos perfis de utilizador e ainda os critérios de segurança pré-definidos.

Assim sendo, não deverá ser esquecido que cada uma destas redes necessitará de segmentação e endereçamento específico de forma a garantir os níveis de segurança conforme estabelecido nos *standards* ISO (ISO/IEC 27002, 2013). Logicamente, segundo o estabelecido nos mesmos, deverão ser consideradas pelo menos as seguintes redes:

- **Rede de Gestão** - rede da infraestrutura *wireless*. É através desta rede que o controlador efetua as operações de manutenção, gestão e aprovisionamento dos AP. Todos os AP devem estar única e exclusivamente nesta rede e o tráfego cliente é encapsulado até ao controlador através dela;
- **Rede de Convidados** - rede para os utilizadores convidados. Um utilizador convidado é aquele que não pertence à organização e apenas necessita de acesso temporário à rede pública (*Internet*);
- **Rede Corporativa - Internos** - rede para os utilizadores corporativos internos. Um utilizador corporativo interno é aquele que pertence à organização e tem acesso aos seus recursos internos;
- **Rede Corporativa - Externos** - rede para os utilizadores corporativos externos. Um utilizador corporativo externo é aquele que não pertence à organização (colaborador) e tem acesso limitado aos recursos internos;
- **Rede de Quarentena** - qualquer utilizador corporativo (externo ou interno) tem de aceder antecipadamente a esta rede para que lhe seja aprovisionado o acesso à rede corporativa.

Todas estas redes devem estar concentradas no controlador *wireless*, que por sua vez, faz a multiplexagem do tráfego cliente de acordo com as políticas de perfil de utilizador que lhe foram aplicadas. Desta forma, ir-se-á conseguir evitar a propagação das novas configurações de rede por toda a infraestrutura, reduzindo as alterações apenas ao *core* da mesma. A configuração de futuras novas redes fica ela também muito mais facilitada, não implicando alterações de impacto relevante.

Como requisito de segurança, a rede de gestão da infraestrutura *wireless* deverá ser propagada até aos pontos de acesso num segmento de rede separado, embora este procedimento possa ser desnecessário devido ao facto do tráfego cliente poder ser encapsulado num túnel de dados até ao controlador.

Com a estrutura certa, cada cliente poderá ser colocado na rede correta, recorrendo a uma *bridge*[56] *Ethernet*, de acordo com o perfil de utilizador que lhe é aplicado.

O segmento de rede de gestão poderá ser configurado numa infraestrutura de rede periférica, com o objetivo de isolar o canal de gestão entre os controladores e os AP. Os restantes segmentos poderão ser configurados entre o controlador e a infraestrutura de *switching* de *core*.

4.4 Infraestrutura das redes sem fios

Considerando o que determinados autores assumem e as publicações NIST SP 800-48r1, (2008), NIST SP 800-153, (2012) e NSA, (2014) referenciando os *standards* IEE 802.11, no que diz respeito ao serviço *wireless*, em qualquer arquitetura, devem ser consideradas pelo menos três redes (com SSID diferenciados) de forma a garantir a segurança na mesma (segmentação de rede) e a interligação com as políticas da organização, que deverão ser implementadas para os utilizadores, a aplicar para cada uma delas de forma diferenciada e em conformidade com o perfil de utilizador como exemplificado:

- **Rede de Convidados/Hóspedes** - Utilizadores convidados. Um utilizador convidado é aquele que não pertence à organização e apenas necessita de acesso temporário à rede pública (*Internet*) e aos serviços básicos de rede (*Domain Name System* (DNS), *Dynamic Host Configuration Protocol* (DHCP), por exemplo);
- **Rede Corporativa** - Utilizadores corporativos internos e externos. Os utilizadores corporativos são aqueles que necessitam de aceder aos recursos locais da organização. Em função do perfil do utilizador, é-lhe atribuído o perfil de acesso à rede mais adequado;
- **Rede de Quarentena** - Utilizadores de quarentena. Um utilizador corporativo (externo ou interno) deve aceder antecipadamente a esta rede para que lhe seja aprovisionado o acesso à rede corporativa (através da emissão de certificados ou outros).

Qualquer uma das redes poderá e deverá ser anunciada por toda a infraestrutura, de forma a garantir a disponibilidade de todas ao longo de toda a área de cobertura da WLAN.

A figura 9 esquematiza os tipos de clientes *wireless* que se podem diferenciar, associando-os às respetivas redes e a forma como serão encaminhados em conformidade com as políticas para as redes a que poderão aceder. Como é abrangente surge um *switch*, que se identifica "de piso" mas representa qualquer segmentação que se queira implementar na rede por necessidades de distribuição espacial na zona de implementação (NSA,2014)

[56] Dispositivo que liga duas ou mais redes informáticas que usam protocolos distintos ou iguais, ou dois segmentos da mesma rede que usam o mesmo protocolo.

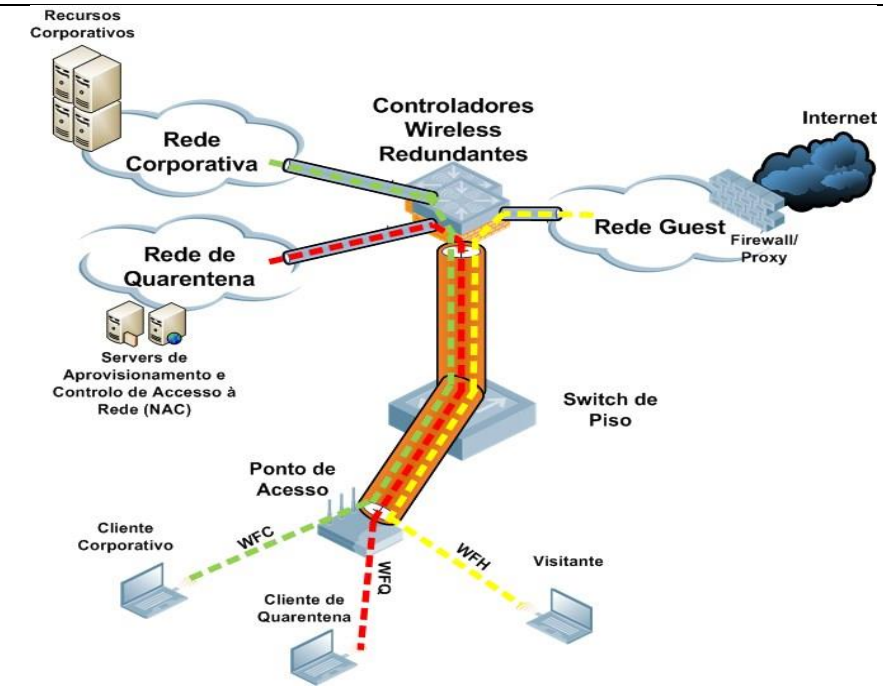

Figura 9 - Exemplo estrutura de segmentação de redes aconselhável (Adaptado de NSA, (2014))

Segundo a mesma bibliografia e considerando a questão da segurança de acesso relativamente ao meio físico, deverá ser, desde logo, ponderado o modo de configuração dos AP, pois existem vários modos de funcionamento, entre eles, o modo de *AP* e o modo *Air Monitor* (AM) explicados de seguida:

- O modo *AP* é, como o próprio nome diz, um modo de funcionamento em ponto de acesso *wireless* à rede, permitindo o acesso dos utilizadores à rede local da organização. Este modo lida única e exclusivamente com as tarefas associadas à prestação do serviço *wireless*.
- O modo *AM* é um modo de funcionamento que permite colocar o AP exclusivamente dedicado às tarefas de monitorização do espectro RF e de deteção de intrusões. Este modo garante uma maior eficácia nestas tarefas sem se traduzir em degradação do serviço prestado (pelo facto de estas serem desempenhadas por AP distintos). Os dados recolhidos por um *AM* são ainda enviados para o controlador que, por sua vez, os utiliza para melhorar o desempenho geral da infraestrutura *wireless*.

A configuração de AP em modo *AM* deve ser efetuada em áreas e locais considerados críticos, do ponto de vista da segurança. Estes têm como principal função detetar/prevenir ataques ao serviço e clientes, bem como, detetar dispositivos não autorizados, os conhecidos *Rogue Devices*[57].

[57] Qualquer ponto de acesso *Wi-Fi* que está instalado em uma rede, mas não está autorizado para a operação da rede e não está sob a gestão do administrador de rede.

Outro aspeto a ter em consideração na distribuição dos AP é a sua localização (para assegurar a melhor cobertura possível do serviço), que deverá considerar quais as zonas de maior densidade de utilizadores, com o objetivo de maximizar a utilização do espectro RF, ou seja, de oferecer melhor débito.

Para efeitos de enquadramento futuro e possíveis evoluções da rede, atendendo ainda às condições de interferência encontradas durante a fase de *site-survey*, deverão ser explicitados o(s) *standard(s)* utilizados para a difusão do serviço *wireless* de forma a garantir taxas de transferência ótima e compatibilidade com sistemas anteriores implementados.

Poder-se-á ainda, numa perspetiva de obtenção da melhor qualidade possível para os utilizadores internos/externos, restringir a utilização de determinados *standards* às redes prioritárias do negócio.

Nos casos de redes maiores e mais complexas deve-se assegurar alta disponibilidade da solução com recurso a equipamentos redundantes (controladores ou AP).

Existem ainda mais três funcionalidades, a considerar no desenho da arquitetura, que nos permitirão garantir elevadas taxas de operacionalidade da rede que são:

- Funcionalidade de ARM (Tech Brief, 2013) que permite ao controlador, com base nas várias estatísticas/leituras recolhidas pelos diversos AP da infraestrutura, determinar qual a configuração de potência de sinal de cada AP que maximiza a utilização do espectro *wireless*. Esta configuração de potência deve ser realizada de forma contínua e automática, permitindo à infraestrutura *wireless* combater em tempo real interferências rádio, níveis de ruído elevados, falhas na cobertura do serviço ou mesmo até colmatar falhas de AP que possam surgir;
- Funcionalidade de *Roaming* - permite que um cliente em movimento se possa associar a vários pontos de acesso mantendo sempre o estado da sua ligação (desde que assegurada a cobertura de sinal);
- Funcionalidade de *Band-Steering* - permite "conduzir" os clientes com capacidade de *standards* diferentes para o respetivo serviço, assegurando que o cliente se associa sempre com a melhor qualidade de sinal possível. A implementação de *band-steering* deve ser compatível com os *standards* 802.11 e funcionar de forma transparente, tanto para o utilizador como para o *firmware* das placas *wireless* dos equipamentos.

4.5 Segurança nas redes sem fios

As WLAN trazem, ao mesmo tempo evolução, facilidade de uso e mobilidade mas também novos riscos associados ao meio físico e aos novos protocolos. De facto, protocolos como o WEP e especificações como o IEEE 802.11i e IEEE 802.1X foram desenvolvidos para que os riscos inerentes a uma comunicação *wireless* fossem minimizados. Porém, foi visto que muitos problemas ainda persistem, de modo que somente o uso da tecnologia não é suficiente para uma proteção adequada.

As WLAN, como nas outras redes, ilustram bem a necessidade de uma estratégia de segurança bem definida, na qual devem ser considerados os aspetos humanos e processuais do ambiente, além dos aspetos

tecnológicos. Isso faz com que não só os protocolos e *standards* de segurança sejam usados corretamente, mas também os utilizadores, administradores e executivos saibam dos riscos existentes, e tentem com isso minimizar as perdas potenciais. Atendendo ao estabelecido nos *standards* ISO/IEC 27000, (2014) e IEEE 802.11, (2012) o primeiro passo para o uso de WLAN nas organizações deve ser o estabelecimento de uma política de utilização, atendendo a que sem essa política, a instalação e o uso indiscriminado de AP dentro da organização representam um grande e inadmissível risco, que pode tornar a existência de outros sistemas de segurança, como *firewalls* e *Wireless Intrusion Prevention Systems* (WIPS)[58], totalmente inúteis.

De facto, uma nova porta de entrada se abre com a expansão do perímetro da rede, que pode ser usada para acessos indevidos.

4.5.1 Confidencialidade e autenticação

Nesta perspetiva da confidencialidade e autenticação, as configurações das WLAN devem incluir sempre que possível forma de oferecer acesso confidencial e autorizado, recorrendo a mecanismos de cifra e autenticação forte[59]. Paralelamente devem ser utilizados mecanismos de controlo de acesso, tais como, a aplicação de políticas baseadas em perfis (*role-based policies*) e filtragem de tráfego (*firewall*) orientado à sessão.

Novamente com recurso ao que é assumido por diversos autores em conformidade com os *standards* de referência nesta área, NIST SP 800-48r1, (2008), NIST SP 800-153, (2012), NSA, (2014) e *standards* IEE 802.11 podemos diferenciar dois tipos de autenticação, conforme o tipo de utilizador.

A primeira deve ser integrada com o domínio corporativo, no caso de existir, suportando nativamente os utilizadores/grupos existentes e para cada uma das redes a criar, que devem apresentar os mesmos requisitos de confidencialidade, devem ser definidos requisitos de autenticação distintos, definidos explicitamente através de uma política de segurança para as redes, exemplificando-se de seguida com os três tipos de redes, que deverão existir e já anteriormente mencionados, com opções que poderão ser tomadas em termos dessa mesma autenticação que se exemplifica de uma forma muito simples:

- Rede Corporativa
  - Apenas os utilizadores corporativos internos e externos poderão autenticar o serviço;
  - A autenticação do utilizador deverá ser efetuada por meio de certificados digitais temporários;
  - A autenticação do utilizador deverá estar integrada com o domínio corporativo, quando exista;
  - A confidencialidade deve ser assegurada com mecanismos de cifra forte.

[58] Dispositivo de rede que monitoriza o espectro de radiofrequências para deteção da presença de pontos de acesso não autorizado (deteção de intrusão), e pode assumir automaticamente contramedidas (prevenção de intrusão).

[59] Mecanismos que permitem garantir que a informação que circula na rede é entregue de um modo seguro e com garantia de integridade e não repudiação para ambas as partes.

- Rede de Quarentena
  - Apenas os utilizadores corporativos internos e externos deverão autenticar o serviço;
  - A autenticação do utilizador deverá ser efetuada por meio de credenciais;
  - A autenticação do utilizador deverá estar integrada com o domínio corporativo, quando exista;
  - A confidencialidade deve ser assegurada com mecanismos de cifra forte.
- Rede de Convidados/Hóspedes
  - Apenas os utilizadores convidados temporários poderão autenticar o serviço;
  - A autenticação do utilizador deverá ser efetuada por meio de credenciais temporárias;
  - A autenticação do utilizador deverá estar separada do domínio corporativo, quando exista;
  - A confidencialidade deve ser assegurada com mecanismos de cifra forte.

Quando exista domínio corporativo o método de autenticação do utilizador poderá ser através do RADIUS do domínio inserindo os utilizadores do domínio diretamente na autenticação da WLAN permitindo centralizar a gestão e aprovisionamento dos utilizadores do serviço *wireless*, e considerar aspetos integrados, tais como, autenticação, políticas de acesso, *Certification Authority* (CA)[60], entre outros.

A segunda relacionada com a gestão de credenciais de convidado (*guest*) onde se poderá utilizar o controlador referido acima, com um portal interno para a gestão da base de dados de credenciais temporárias (*guest*). Para aceder a este portal basta criar uma conta com perfil de gestão do portal e automaticamente, após autenticação de acesso no controlador, terá unicamente acesso às funções de gestão e aprovisionamento de novas credenciais temporárias permitindo-lhe fazer uma gestão global dos utilizadores com este tipo de credenciais.

Em termos de segurança é importante referir que na criação de credenciais deverá ser possível descriminar parâmetros, tais como: dados do utilizador, departamento ou área que requisita a criação da conta, tempo de validade. O perfil aplicado ao utilizador criado, deve ser sempre "*guest*" e encontrar-se configurado para ter acesso unicamente à rede de convidados. Após a validade de uma credencial ter expirado, esta é automaticamente eliminada da base de dados.

O controlo de acesso e autorização dos utilizadores deve-se encontrar assegurado pela *firewall* interna do controlador. Esta permite realizar a filtragem do tráfego dos utilizadores da rede sem fios. As regras de filtragem de tráfego são *session-based* e mantêm o seu estado durante o período da sessão (*stateful*[61]).

[60] Entidade administrativa central fidedigna que pode emitir certificados digitais para utilizadores e servidores.

[61] Um serviço de *stateful* é aquele em que as solicitações subsequentes para o serviço dependerão dos resultados do primeiro pedido.

4.5.2 Políticas de segurança de utilizador

Atendendo ao que alguns autores assumem recomenda-se a definição de diferentes políticas de controlo de acesso para os diversos perfis de utilizador que possam ser criados, basicamente, pelo menos quatro, o de convidados, quarentena, interno da rede corporativa e externo da rede corporativa mas, tantos quanto se necessitem em termos de gestão e diferenciação, cada um com políticas explícitas, claras e diferenciadas, de modo a garantir o enquadramento correto em termos de segurança.

Seguidamente exemplificam-se políticas para cada um dos perfis de utilizador que de uma forma simples e clara poderão impor o tipo de acesso na sequência do referenciado:

- **Política para Utilizador de Rede de Convidados**: Nesta rede apenas se permite o acesso aos serviços básicos de rede e à internet através do *proxy* local;
- **Política para Utilizador da Rede de Quarentena**: Nesta rede apenas se permite o acesso aos serviços básicos de rede e à CA local, para o aprovisionamento de acesso à rede corporativa;
- **Política para Utilizador Interno da Rede de Corporativa**: Nesta rede permite-se o acesso a todos os serviços locais;
- **Política para Utilizador Externo da Rede de Corporativa**: Nesta rede permite-se o acesso a todos os serviços locais.

Embora esta não seja uma funcionalidade de segurança, deve-se desabilitar a funcionalidade de SSID *broadcast* das várias redes *wireless* a instalar, garantindo que um utilizador que pretenda associar-se à WLAN terá de saber/configurar, em antemão os respetivos SSID. Para um utilizador que não pertença à organização, esta medida oferece um nível de "obscuridade" complementar pois não vai perceber a existência dessa rede.

4.5.3 Sistema de deteção de intrusão sem fios

Os dispositivos de rede (AP, controladores e outros) deverão incorporar funcionalidades de deteção e prevenção contra ataques, o *Wireless Intrusion Detection System* (WIDS) que permita, entre outros (NIST SP 800-94, (2007); NSA, (2012); Shourbaji e Amer, (2013)):

- Mitigar ataques conhecidos ao protocolo 802.11;
- Ataques de *DoS*;
- Detetar/bloquear dispositivos não autorizados.

Numa primeira fase, a configuração poderá ser pouco intrusiva, do ponto de vista das medidas de resposta levadas a cabo pelo controlador, considerando simplesmente a deteção e mitigação de ataques à infraestrutura e a deteção de *rogues*, inibindo a utilização de medidas ativas (mais eficientes) que interfiram com o normal funcionamento das redes e dispositivos de organizações na vizinhança.

Algumas das funcionalidades primárias que poderão ser consideradas em tais sistemas:

- Deteção e mitigação de ataques à infraestrutura - Permitirá detetar ataques conhecidos às redes 802.11, tais como, *impersonating attacks*[62], *deauthentication attacks*[63] e *DoS attacks*[64], tomando medidas de forma a minimizar o seu impacto/sucesso;
- *Blacklisting* - Permitirá detetar *brute-force attacks*[65], colocando o atacante numa lista negra durante um determinado período de tempo. Este tipo de medida reduz eficazmente o sucesso deste tipo de ataques;
- Deteção de dispositivos não autorizados - Esta funcionalidade permite detetar na rede dispositivos *wireless* não autorizados. Entre estes encontram-se *rogue* AP, *bridges* e *routers wireless*. Esta funcionalidade poderá ser configurada para atuar exclusivamente ao nível de deteção e não da mitigação destes dispositivos.

[62] Simulação de outro personagem ou *web site*.

[63] Envia pacotes para desassociar a comunicação de um ou mais clientes, que estão associadas a um ponto de acesso específico, para perderem a ligação.

[64] Projetado para deitar a rede abaixo, inundando-o com tráfego inútil.

[65] Ataques de autenticação constantes.

5 Referenciais a considerar

Este capítulo, na sequência do referido no anterior, procede de forma sistematizada ao enquadramento dos aspetos principais que servirão de referencial para a implementação de WLAN nas organizações, estabelecendo linhas orientadoras para este referencial.

É através das estratégias competitivas que as organizações procuram obter ou manter uma posição favorável na indústria, perante a concorrência. No contexto tecnológico, a estratégia é um caminho a ser trilhado em consonância com os produtos, sensibilidade dos gestores de topo e sua apetência tecnológica. Da interação de tais elementos, assim como das impostas pelos clientes, funcionários e tendências, surge muitas vezes a necessidade de adoção de estratégias de implementação de tecnologias não previstas.

Este trabalho fez uma revisão da literatura (Coutinho, 2014) e levantamento de informações utilizadas para análise, projeção, implementação e segurança de redes organizacionais, muito especificamente as baseadas nos *standards wireless* 802.11 do IEEE, fazendo uma análise dos modelos adotados pelas TI, a nível da organização incluindo o contexto do ambiente (Cummings e Worley, 2014).

No referido contexto, a utilização dos *standards* 802, 802.11 do IEE e suas alterações, dos ISO/IEC 27000 a 27002 e 27033, das *Special Publications* da NIST, publicações e recomendações dos diversos autores mencionados, contribuíram para assegurar o estabelecimento de um modelo básico de referência para a implementação com sucesso da WLAN organizacional conforme descrito neste capitulo.

As LAN tradicionais são constituídas por um conjunto comum de componentes, como *switches*, *routers* e *gateways*. Todos estes componentes são fáceis de reunir e agregar de acordo com as funcionalidades pretendidas em cada caso concreto, implementando uma solução de LAN com uma razoável certeza de que os objetivos de segurança são alcançados.

As WLAN seguem uma filosofia semelhante às das LAN, mas com um grau diferente de complexidade e variedade, relacionado com a localização de algumas das funcionalidades e forma como o tráfego se movimenta através da rede *wireless*. Com esta variedade de arquiteturas, é útil, para estabelecer a arquitetura correta para cada organização, pensar que o futuro das WLAN assenta em dados distribuídos, gestão centralizada e controlo distribuído e centralizado. Mas o grau de variação da arquitetura irá aumentar antes que a convergência seja um dado adquirido; ainda é demasiado cedo na história destas tecnologias.

No entanto, para qualquer tecnologia *wireless* os riscos são inerentes. Alguns desses riscos são semelhantes aos das LAN; alguns são exacerbados pela conectividade *wireless*; alguns são novos. Talvez a mais significativa fonte de riscos nas WLAN é que o meio de comunicação subjacente à tecnologia, a transmissão pelo ar, está aberto aos intrusos, tornando-se o equivalente lógico de não ter nenhuma proteção física de proteção de acessos. A perda de confidencialidade e integridade e a ameaça de ataques de DoS são riscos normalmente associados às WLAN.

Em virtude disto utilizadores não autorizados podem obter acesso a informações e sistemas organizacionais, corromper dados, consumir largura de banda de rede, degradar o desempenho da rede, lançar ataques que impeçam utilizadores autorizados de acederem à rede, ou usar recursos de organização para lançar ataques a outras redes (Gandhi, 2014).

Neste contexto a mobilidade tornou-se um sistema, ou um sistema de sistemas que tem que ser olhado e tratado como um todo. Como as WLAN estão ganhando cada vez mais atenção na organização pelas vantagens que fornecem relativamente às LAN como mobilidade, alcance da cobertura, facilidade de uso, escalabilidade, baixo custo e assim por diante, verifica-se que nos últimos anos, mais e mais organizações criam ambientes WLAN no seu SI. No entanto, a introdução das WLAN expõe um ponto adicional de vulnerabilidade. Os atacantes potenciais podem invadir o SI através da vulnerabilidade das WLAN. Avaliação de risco é um método muito eficiente para reduzir o risco do SI a um nível aceitável e deverá ser considerado pelas organizações quando da aplicação da sua estratégia de implementação (Liang, et al., 2014).

Ao implementar uma WLAN na organização, para estabelecer uma rede segura, deve-se tomar em consideração alguns aspetos e requisitos importantes, referidos anteriormente, que poderão servir de base a um referencial, descrito de seguida, indicando-se as diferentes hipóteses de configurações e técnicas para garantir isto, o estabelecimento de uma rede segura, pois não podemos esquecer os riscos envolvidos por esta tomada de decisão de adoção de WLAN. As técnicas de projetar e desenhar uma WLAN segura podem ser usadas para combater os riscos de segurança.

Pode assim concluir-se que, quando da opção por adoção de WLAN nas organizações, se deverá ter me atenção um conjunto de questões, como os possíveis cenários de implementação, projeção e planeamento correto da sua implementação e dos requisitos necessários, desenho, níveis de segurança que se desejam atingir, mecanismos de controlo e *auditing* das mesmas assegurando assim a satisfação dos utilizadores, os objetivos das organizações e a continuidade do negócio.

Neste contexto é importante não esquecer que a segurança não é só uma questão das WLAN mas sim um problema das redes e que deve ser tratado de modo global, seguro e adequado. As WLAN podem ser extremamente seguras mas terão que ser corretamente planeadas e desenhadas, pois soluções de segurança estão disponíveis hoje e continuarão a evoluir mas, teremos que as considerar desde logo na implementação e na perspetiva futura de evolução.

Do trabalho desenvolvido, emergem dois aspetos principais, a implementação de WLAN e a segurança dessas redes, que nos conduz ao estabelecimento de linhas orientadoras que poderão ser consideradas quando da necessidade de adoção de tal tecnologia.

5.1 Aspetos a considerar na implementação de WLAN

No respeitante à implementação das WLAN, devem ser considerados os seguintes aspetos:

- Uma rede mal concebida, desenhada ou projetada resulta em:

- Custos acima do estabelecido à medida que as redes se tornam sobre dimensionadas, na tentativa de acomodar a alta taxa de transferência e o poder de processamento necessário;
- Complexidade alta, particularmente para as organizações com múltiplos locais remotos;
- Requisitos mais elevados de suporte, à medida que tecnologias mais novas, mais rápidas, são incorporadas na rede;

- A natureza intensiva do processo da mobilidade moderna é provável que torne rapidamente obsoletas as WLANs existentes pelo que no desenho da sua arquitetura deverá ser considerada a capacidade adaptativa e de evolução;
- As WLAN podem operar de duas maneiras básicas, em *infrastructure mode*, onde as STA se conectem a AP, que funcionam como pontes entre estas e o *backbone* da rede existente ou em *peer-to-peer (ad-hoc*) WLAN, em que vários utilizadores dentro de uma área limitada, como uma sala de conferências, podem formar uma rede temporária sem usar AP, se não necessitarem de acesso a recursos de rede;
- De referir que existe uma terceira possibilidade, surgida recentemente, aqui introduzida o *Mixed Network Mode* em que cada STA pode trabalhar nas duas modalidades acima referidas, simultaneamente, constituindo o chamado *Extended Basic Service Set* (EBSS) (Sridevi, 2013).

5.2 Aspetos respeitantes à segurança

Já no respeitante à segurança as principais conclusões são:

- A tecnologia WLAN tem problemas de segurança inerentes, em sua arquitetura;
- Existe uma ampla gama de ataques - de passivo para ativo - em WLAN e visam a confidencialidade e a integridade da informação e a disponibilidade de rede;
- As falhas detetadas nos *standards* IEEE 802.11 implicam que, uma combinação de medidas de segurança, é necessária, para aumentar ainda mais a segurança oferecida pelas tecnologias WLAN;
- Avaliação de riscos de segurança é necessária a fim de produzir uma lista de ameaças a que uma rede é propensa e a gravidade que cada tem na rede;
- A definição de uma boa política de segurança é necessária para defender a WLAN. Não é prático ou possível defender qualquer rede contra todos os possíveis ataques. O objetivo, no entanto, é reduzir o risco associado a um nível aceitável;
- Existe um número de contramedidas para reduzir numa rede, um risco específico. Algumas destas medidas são simples, alguns são complicadas. Uma combinação de medidas defensivas, no entanto, garante que uma rede é robusta e mais segura contra um ataque.
- É essencial que as organizações assumam medidas de proteção adequadas para a sua WLAN. Apesar dos *standards* IEEE 802.11 fornecerem segurança, não é infalível o suficiente para dar o nível de proteção necessária para a infraestrutura de rede das organizações pelo que a avaliação de vulnerabilidade é necessária para determinar a combinação de medidas que devem ser implementadas para mitigar os riscos associados ao uso de tecnologias wireless;

- Os *Capability Packages*, sugeridos no documento (NSA, 2014), são independentes de fornecedor e facultam orientação de alto nível de segurança e configuração para os clientes e/ou integradores de soluções, pelo que, esta opção deverá ser ponderada no momento de desenho e aquisição da WLAN;
- Duas ameaças emblemáticas são resultantes de duas dinâmicas humanas:
  - Uma é derivada do crescimento dos ataques;
  - A outra da contínua ignorância dos utilizadores e dos profissionais de TI acerca das ameaças *wireless*.

5.3 Linhas orientadoras

Assim em conformidade com o estabelecido anteriormente e documentação analisada, no processo de decisão, implementação e gestão de redes *wireless* nas organizações deverão ser observadas uma série de etapas, que servirão para o estabelecimento de um modelo de referência com linhas orientadoras genéricas.

Perante isto sugerem-se quatro fases, que apresentam características especificas próprias:

Fase preparatória – Perspetivar como a WLAN deverá apoiar a missão da organização, criando uma estratégia de alto nível para a sua implementação, desenvolvendo uma política de utilização, especificando o conjunto de requisitos funcionais e de negócio para a mesma, não esquecendo a segurança da informação e tecnológica:

i. Cobertura de sinal das áreas onde se quer implementar a solução;
ii. Qual a média de utilizadores (capacidade a instalar);
iii. Níveis de segurança, no que respeita à confidencialidade dos dados, autenticação e autorização dos utilizadores:
    b. Controlo de Acesso granular por segmento de rede, recursos, grupos e utilizadores;
    c. Suporte de autenticação por meio de certificados digitais;
    d. Autenticação integrada com o domínio corporativo.
iv. Gestão centralizada;
v. Alta disponibilidade ou não ao nível dos controladores que assegurem a continuidade do serviço;
vi. Análise dos níveis de ruído e interferências externas que possam condicionar as decisões do projeto - *site-survey*.

Fase anterior à implementação – Efetuar o planeamento e *design* do modelo que se quer construir especificando as caraterísticas técnicas da solução WLAN e componentes de rede relacionados. Estas características incluem:

i. Métodos usados para oferecer suporte à autenticação;
ii. Protocolos usados para apoiar a comunicação entre o AP e o AS;

iii. ACL e regras de *firewall* para segregar o tráfego da WLAN;
iv. Natureza da PKI de suporte;
v. Tipos de clientes a serem implementados, uma vez que eles podem afetar as políticas de segurança estabelecidas.
vi. Execução do *site survey* para ajudar a determinar o número e a colocação de AP, bem como a forma como vão integrar a rede existente.

Ainda nesta fase, na sequência do trabalho efetuado, especificação do número e tipo de componentes WLAN que devem ser adquiridos, conjuntos de recursos que devem suportar, assim como quaisquer certificações que devem assegurar.

Fase de implementação - Esta fase é constituída pela instalação e ativação dos equipamentos adquiridos, configurados para satisfazer os requisitos operacionais e de segurança. A implementação inclui alterar a configuração de outros controlos de segurança e tecnologias, tais como *logs* de eventos de segurança e gestão de rede.

Fase pós implementação - Essa fase inclui tarefas de operações/manutenção relacionadas com segurança e gestão da WLAN durante o seu tempo de vida útil, incluindo posteriormente a remoção/eliminação quando o sistema for descontinuado mas considerando a preservação de informações para atender requisitos legais, limpeza de mídias e eliminação de equipamentos em conformidade com a legislação em vigor.

Recomenda-se assim que as organizações, em conformidade com a estratégia definida para o que pretendam obter na implementação da sua WLAN façam uma análise, projeção, implementação e estabelecimento dos níveis de segurança que querem obter, utilizem o referencial quer a nível dos requisitos de implementação, segurança e fases de planeamento/implementação para o estabelecimento de uma WLAN com sucesso.

Além disso organizações com forte consciência e ou necessidades maiores na área da segurança deverão reforçar a sua estratégia para as WLAN com uma abordagem de segurança em camadas, que se aproxime das práticas de segurança aceites nas LAN. Esta abordagem de segurança em camadas deve endereçar todos os componentes de rede fechando o perímetro da WLAN, segurança das comunicações através da WLAN e monitorização do tráfego de rede.

Pretende-se assim que os requisitos constantes neste documento possam servir como uma orientação e apoio para o desenvolvimento, implementação e avaliação de WLAN organizacionais.

6 Conclusões

Este capítulo aborda os resultados e conclusões do trabalho desenvolvido procedendo-se a uma reflexão sobre o tema apresentado, em forma de conclusão, e na contribuição, para as organizações, de um modelo de referência na criação da sua WLAN, e integração desta com a sua infraestrutura e negócio.

São ainda identificadas linhas orientadoras para estudos futuros de forma a consolidar todo o trabalho desenvolvido.

O enquadramento inicial dos trabalhos beneficiou de uma ampla e aturada revisão de literatura, que versou sobre a temática genérica das comunicações *wireless*, essencial à contextualização do tema, *standards* do IEEE e diversos documentos de organizações reguladoras de produtos e equipamentos, cuja solidez influenciou a continuidade e consistência dos resultados além de contribuir para a sua compreensão.

Desta forma os nossos objetivos específicos concretizam-se, se se verificar que os benefícios da tecnologia *wireless* atraem as organizações para a implementarem nas suas redes, verificando-se que também nestes sistemas, as questões de segurança se tornaram, também elas, cada vez mais importantes, pelo que se tentou validar as soluções existentes e a adotar, em conformidade com os *standards* em vigor e as recomendações das organizações internacionais de referência como o IEEE, NIST e NSA.

6.1 Resultados

Inicialmente procurou-se estabelecer um enquadramento teórico considerado adequado ao trabalho a desenvolver, na perspetiva das diversas vertentes a analisar, organizações, informação e a necessidade de segurança, infraestruturas tecnológicas, as WLAN e os *standards* de referência. De um modo genérico, os resultados obtidos permitiram reforçar a perceção inicial da evolução que as WLAN tiveram em termos tecnológicos e do garante da segurança da informação que transita nela, assim como a possibilidade de integração com as infraestruturas existentes nas organizações, as vantagens que poderão daí advir, permitindo-nos caracterizar o problema na sua plenitude.

Neste sentido, o apoio e utilização dos diversos *standards*, recomendações e boas práticas dos mais diversos organismos internacionais e organizações, que de forma direta ou indireta foram e vão estabelecendo regras para o desenho, projeção e implementação das WLAN, consideram-se essenciais para a obtenção de uma visão mais alargada acerca das diversas vertentes de evolução e desenvolvimento da problemática da adoção de este tipo de redes nas organizações.

Assim ao longo do trabalho desenvolvido conseguiu-se obter uma perspetiva global da temática das WLAN e dos problemas de segurança que estas criam para as organizações, soluções que existem e vão sendo apontadas pelos diversos organismos internacionais e outros intervenientes no processo de desenvolvimento de equipamentos e conceitos.

Através disto conseguiu-se apontar para um conjunto de requisitos básicos específicos essências para a implementação, garantia de obtenção de níveis de segurança e linhas orientadoras a observar quando da adoção ou avaliação de WLAN conseguindo-se atingir os objetivos inicialmente estabelecidos para o sucesso deste trabalho.

Face a estas considerações, desconhece-se que exista, atualmente, uma única organização que possua uma arquitetura *Wi-Fi* que possa reivindicar como a melhor. Em parte porque é muito difícil (e com frequência demasiado caro) caracterizar o desempenho e realizar análises comparativas, em particular tendo em conta o impacto dos dispositivos utilizados por exemplo ao nível variado de tráfego e ciclos de funcionamento. No entanto, esta realidade irá melhorar lentamente com a implementação de novas ferramentas de análise do desempenho e iremos assistir, nos próximos anos, ao aparecimento de histórias de sucesso que virão a generalizar-se como a melhor abordagem para diferentes aplicações.

Como limitações para este estudo verifica-se que a maioria das organizações não divulgam informação sobre as suas opções estratégicas, também nesta matéria, pelo que existem muito poucos estudos sobre esta temática.

Outras limitações relacionadas com a metodologia aplicada podem ser referidas, desde logo, uma vez que a o horizonte temporal para o desenvolvimento do trabalho não foi o mais adequado, e impediu uma investigação e análise prévia mais profunda da vasta literatura existente em artigos e jornais científicos sobre as especificações e requisitos da tecnologia agora objeto de análise.

6.2 Contributos organizacionais

A mobilidade faz hoje parte da vida das pessoas, integrando a sua vida pessoal e profissional. A utilização crescente de *smart devices*, dentro e fora do local de trabalho, mudou totalmente a forma como as pessoas interagem e trabalham. Neste impasse, os colaboradores continuam a querer explorar todas as funcionalidades dos seus equipamentos e os departamentos de TI precisam de um sistema robusto, de simples e rápida instalação, que lhes permita garantir a segurança dos dispositivos e dos dados móveis. Para implementarem esta mudança, as organizações necessitam de definir como ultrapassar alguns obstáculos, tais como a configuração e a gestão dos dispositivos, a segurança e proteção da informação e a convivência de dados corporativos com dados pessoais no mesmo equipamento. Existem muitas abordagens tecnológicas disponíveis, com vista à integração dos dispositivos móveis no ambiente corporativo. Porém, a diversidade de opções dificulta a escolha por parte das organizações, preocupadas em proteger o seu investimento e definir soluções para o futuro.

As alterações organizacionais estão totalmente relacionadas com o controle do fluxo da propriedade intelectual da empresa – como aprovisionar e proteger os dados na rede e nos equipamentos – e todas as responsabilidades inerentes a esta realidade.

6.3 Tendências de Evolução e trabalhos futuros

De toda a revisão de literatura efetuada surgem desde logo, um conjunto de tendências que apontam genericamente a evolução percecionada pelos diversos intervenientes no processo de desenvolvimento tecnológico das WLAN e das quais se indicam alguns, no respetivo capítulo.

Mas ainda sem consolidação suficiente na tecnologia surgem desde já novos conceitos e aplicações tecnológicas como por exemplo os equipamentos com *Power-over-Ethernet* (PoE)[66] mas também noutros conceitos evolutivos que acompanham as necessidades móveis dos utilizadores.

6.3.1 Tendências de evolução

Os *standards* IEEE desenvolvidos ao longo de décadas foram originalmente concebidos para funcionar em WLAN com dispositivos estacionários. Mas, atualmente, muitas pessoas têm pelo menos um dispositivo móvel consigo e os identificadores são enviados às claras, sempre que um dispositivo se liga – ou tenta ligar-se – a uma rede *wireless*. Isso, relacionado com o facto dos *standards* 802.11 associados à tecnologia de comunicações *wireless* estabelecerem que cada dispositivo móvel tem o seu próprio MAC, permite que potenciais utilizadores, autorizados e não autorizados, monitorizem a utilização dos dispositivos.

Assim, um grupo de trabalho do IEEE recomenda, desde já, aos fabricantes a adoção de tecnologia capaz de suportar a utilização de endereços MAC aleatórios, numa antecipação da atualização do *standard* de *Wi-Fi*, que recomenda o uso de endereços MAC gerados aleatoriamente, para maior segurança e privacidade.

Também já numa perspetiva evolutiva, o IEEE 802 iniciou um grupo-tarefa para investigar e entregar a próxima geração de tecnologias WLAN para cenários de redes densas, com um grande número de STA e AP. A proposta é especificada como a alteração IEEE 802.11ax. Devido ao aumento significativo da capacidade de rede alcançado pelo 802.11ax, o termo *High-Efficiency* WLAN (HEW) também é usado como referência para esta nova alteração. Atividades de normalização para o IEEE 802.11ax já estão em andamento com alterações das características no desenho da PHY e MAC, em direção a uma nova era de WLANs, são também discutidos (Deng, Chen, e Cheng, 2014).

6.3.2 Trabalhos Futuros

A delimitação dos trabalhos futuros encontra-se na dificuldade de enquadramento dos mesmos, perante a infinidade de contextos estudados e a sua abrangência, que abrem um grande leque de opções, quer ao nível das tecnologias, equipamentos e suas capacidades, quer no âmbito da segurança das WLAN ou da informação.

[66] A tecnologia PoE vai sendo adotada de forma crescente por causa da melhoria da conveniência, eficiência e flexibilidade de fornecimento de energia sobre infraestrutura fixa de CAT5 ou superior como se fosse dados.

Como trabalhos futuros no mesmo âmbito do presente sugere-se o seu desenvolvimento numa perspetiva de continuidade garantindo a melhoria do referencial, acompanhando a evolução tecnológica inerente às WLAN, o aumento da necessidade de sua implementação como rede primária da organização e o papel que poderão ter na evolução destas e em ganho de vantagens competitivas no mercado global.

Sendo a monitorização um aspeto importante a considerar na gestão e manutenção de redes poderemos também perspetivar o desenvolvimento de trabalho futuro nesta área analisando ferramentas de monitorização e controlo específicas que permitam monitorizar e tratar os registos de todas as atividades de segurança, gestão e *auditing* para servidores de *syslog*[67] locais (com correlação de eventos).

Outra perspetiva de trabalho futuro inclui investigar o desempenho de segurança de novos *standards* IEEE 802.11 usando implementações de software e hardware de criptografia e porque não o alargamento das arquiteturas de segurança através de interfaces WLAN/4G.

6.4 Conclusões finais

Este trabalho, com a diversidade existente em termos da temática das WLAN e da sua segurança, tornou difícil a apreciação pormenorizada de cada uma delas, pelo que, para atingir os objetivos identificados tornou-se necessário focar a atenção nas implicações da implementação das WLAN nas organizações e o que provoca globalmente nestas.

Assim, para as organizações, as WLAN podem fornecer inúmeras oportunidades de aumentar a produtividade e reduzir custos, sendo necessário que estas adotem uma estratégia conducente a integrar esta implementação com a estratégia de negócio, mas também podem alterar o perfil de risco de segurança global dos SI na organização, pois esta opção de adoção de WLAN comporta em si riscos específicos, associados a este tipo de redes, que embora não seja possível eliminar completamente permite atingir um nível razoável de segurança global, com a adoção de uma abordagem sistemática para a avaliação e gestão de risco.

Não podemos esquecer afinal que ameaças e vulnerabilidades associadas à tecnologia de redes *wireless* se desenvolvem em três dimensões, os clientes, os AP e o meio de transmissão, sendo necessário um esforço combinado dos utilizadores, organizações e administradores de sistema para lutar contra estes perigos de segurança.

Deverá ainda existir um esforço conjunto na implementação de contramedidas adequadas em cada uma das componentes que ajudem a organização a minimizar o risco de penetração ilegal. Ferramentas atualizadas, monitoramento constante, uma gestão e mecanismos de defesa adequada são as armas finais para lutar contra ataques de segurança *wireless*.

[67] Padrão criado pela *Internet Engineering Task Force* (IETF) para transmissão de mensagens de log em redes IP.

Mas mais importante é o facto de as WLAN apresentarem os seus próprios desafios de análise, projeção, implementação e segurança, distintos de organização para organização, na definição da estratégia de implementação, mas muito especificas da tecnologia *wireless* e das formas de utilização que permite, pelo que será na fase inicial da decisão que as organizações deverão desde logo assegurar um conjunto de parâmetros conducentes ao que se pretende implementar. Mas não existe uma solução única e exclusiva devendo ser analisado caso a caso em conformidade com os fatores já mencionados, mas que não se esgota nestes.

7 Bibliografia

2rd Annual Trends in Enterprise Mobility. (2013). CompTIA.

3rd Annual Trends in Enterprise Mobility. (2014). CompTIA.

Acker, S. (2010). *Cisco Unified Wireless Network Overview.* Cisco Systems. Cisco Public.

Adaptive Radio Management - Tech Brief. (2013). *TB ARM 051413*. Sunnyvale: Aruba Networks, Inc. Retrieved from www.arubanetworks.com

Ahmad, A., Maynard, S. B., & Park, S. (2014, April). Information security strategies: Towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing*. doi:http://dx.doi.org/10.1007/s10845-012-0683-0

Ahmad, A., Maynard, S. B., & ParK, S. (2014). Information security strategies: towards an organizational multi-strategy perspective. *Journal of Intelligent Manufacturing, 25*(2), 357-370.

Alliance, W. F. . (jan 2012). *The State of Wi-Fi® Security.* Wi-Fi Alliance.

Alshaikh, M., Ahmad, A., Maynard, S. B., & Chang, S. (2014). Towards a Taxonomy of Information Security Management Practices in Organisations. *25th Australasian Conference on Information Systems, 8th - 10th December.* Auckland, New Zealand: ACIS.

Alves, G., Ferreira, E. T., & Shinoda, A. A. (2013). Uma Proposta De Avaliação De Dados De Redes De Sensores Utilizando Redes Em Malha Sem Fio. *Sistema de Publicações, 1*(1).

Amaral, L., Magalhães, R., Morais, C. C., Serrano, A., & Zorrinho, C. (2005). *Sistemas de informação organizacionais.* Edições Sílabo.

ANACOM, A. N. (2015). *Glossário de Comunicações electrónicas e serviços postais*. Retrieved 08 15, 2015, from http://www.anacom.pt/render.jsp?contentId=597525&pag=1

Angela, A. I. (2014, July). Evaluation of Enhanced Security Solutions in 802.11-Based Networks. *International Journal of Network Security & Its Applications (IJNSA), 6*(4), 29-42. doi:10.5121/ijnsa.2014.6403

Australian National Audit Office. (2005). *IT Security Management Audit Report.* Australian National Audit Office. Retrieved from www.anao.gov.au/uploads/documents/2005-06_Audit_Report_23.pdf

Balocco, R., Mogre, R., & Toletti, G. (2009). Mobile internet and SMEs: a focus on the adoption. *Industrial Management & Data Systems, 109(2),* pp. 245-261. doi:http://dx.doi.org/10.1108/02635570910930127

Bento, F., Martens, C., & Freitas, H. (2013). Proposição de elementos decorrentes da adoção de tecnologias móveis em equipes comerciais. *Anais do Encontro de Administração da Informação.* Bento Gonçalves, RS, Brasil, 4.

Cappellozza, A., Sanchez, O., & Albertin, A. (2011). Estudo da influência da infraestrutura de tecnologia de informação à mobilidade computacional dos usuários e utilização da computação em nuvem, aplicado em empresas do setor de serviços. *Anais do Encontro de Administração da Informação.* Porto Alegre, RS, Brasil, 3.

Cassarro, A. C. (2010). *Sistemas de informações para tomada de decisões.* São Paulo: Pioneira Thomson Learning.

Castells, M. (2011). *The rise of the network society: The information age: Economy, society, and culture (Vol. 1).* John Wiley & Sons.

Chen, L., & Nath, R. (2008). A socio-technical perspective of mobile work. *Information Knowledge Systems Management, 7 (1/2),* pp. 41-60.

Cisco Systems. (2011). *Cisco TrustSec™ 2.0: Design and Implementation Guide.* Cisco System. Cisco Public Information.

Cisco Systems. (2014). *802.11ac: The Fifth Generation of Wi-Fi.* Cisco Systems, Inc.

Corso, K., Freitas, H., & Behr, A. (2012). Os paradoxos de uso da tecnologia de informação móvel: a percepção de docentes usuários de smartphones. *Anais do Encontro Nacional da Associação Nacional de Pós-Graduação e Pesquisa em Administração.* Rio de Janeiro, RJ, Brasil, 36.

Costa, E., Saccol, A., & Vieira, L. (2011). Análise da utilização de tecnologias da informação móveis e sem fio (TIMS) na cadeia bovina: um estudo de caso no Estado de Goiás. *Anais do Encontro Nacional da Associação Nacional de Pós-Graduação e Pesquisa em Administração.* Rio de Janeiro, RJ, Brasil, 35.

Coutinho, C. P. (2014). *Metodologia de investigação em ciências sociais e humanas.* Leya.

Cragg, P., & King, M. (1993). Small-firm computing: motivators and inhibitors. *MIS Quarterly, 17*(1), 47-60. doi:10.2307/249509

Cummings, T., & Worley, C. (2014). *Organization development and change.* Cengage Learning.

Cunha, M. P., Rego, A., Cunha, R. C., & Cardoso, C. (2007). *Manual de comportamento organizacional e gestão.* Lisboa: Editora RH.

Da Veiga, A., & Martins, N. (2015). Information security culture and information protection culture: A validated assessment instrument. *Computer Law & Security Review,, 31*(12), 243-256.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*(3), pp. 319-340.

Deng, D. J., Chen, K. C., & Cheng, R. S. (2014, August). IEEE 802.11 ax: Next generation wireless local area networks. In Heterogeneous Networking for Quality, Reliability, Security and Robustness (QShine). *2014 10th International Conference on* (pp. 77-82). IEEE.

Dhanalakshmi, S., & Sathiya, M. (2015, January). An Overview of IEEE 802.11 Wireless LAN Technologies. *International Journal of Computer Science and Mobile Computing, 4*(1), 85 – 93.

Dictionary, O. E. (Ed.). (n.d.). *organization.* Retrieved 15 setembro, 2015, from Dictionary.com: http://dictionary.reference.com/browse/organization

Disterer, G. (2013). ISO/IEC 27000, 27001 and 27002 for Information Security Management. *Journal of Information Security, 4*(2), 92-100. doi:10.4236/jis.2013.42011.

Eco, U. (2007). *Como se faz uma Tese em Ciências Humanas* (13ª ed.). Lisboa: Presença.

Education, A. (Ed.). (2011). *Wireless local area network (WLAN) best practices guide.* Retrieved 08 10, 2015, from Alberta Education School Technology branch: http://education.alberta.ca/admin/technology/research.aspx

Falsarella, O. M., Beraquet, V. S., & Jannuzzi, C. A. (2003). Informação empresarial: dos sistemas Transacionais à Latência Zero. *Transinformação, Número especial*, pp. 141-156.

Gandhi, V. K. (2014, Sept). A Study On Wireless Lan Fundamentals, Architecture, Benefits And Its Security Risks. *Indian Streams Research Journal, 4*(8). Retrieved from http://ssrn.com/abstract=2503782

Garber, L. (2012). Wi-fi Races into a Faster Future. *Computer, 3.* doi:10.1109/MC.2012.104

Ghose, A., & Han, S. (2011). An empirical analysis of user content generation and usage behavior on the mobile Internet. *Management Science, 57(9),* pp. 1671-1691. doi:10.1287/mnsc.1110.1350

Giddens, A. (2000). *O Mundo na era da globalização.* Lisboa: Presença.

Gil, A. (2002). *Como elaborar Projetos de Pesquisa* (4ª ed.). São Paulo: Atlas.

Gil, A. C. (2009). *Estudo de caso.* São Paulo: Atlas.

Gonçalves, A., & Joia, L. (2011). Uma investigação acerca dos paradoxos presentes na relação entre executivos e smartphones. *Anais do Encontro Nacional da Associação Nacional de Pós-Graduação e Pesquisa em Administração.* Rio de Janeiro, RJ, Brasil, 35.

Grandon, E., & Pearson, J. (2004). Electronic commerce adoption: an empirical study of small and medium US businesses. *Information & management, 42*(1), 197-216. doi:10.1016/j.im.2003.12.010

Grant, R. (2003). Strategic planning in a turbulent environment: evidence from the oil majors. *Strategic Management Journal, 24*(6), 491-517. doi:10.1002/smj.314

Haraszczuk, R. (2005). Wireless LAN at home, in institutions and organizations. *Annales UMCS Informatica AI 3*, (pp. 305-313). Lublin.

Hirst, P., Thompson, G., & Bromley, S. (2015). *Globalization in question.* John Wiley & Sons.

Holt, A., & Huang, C. Y. (2010). *802.11 wireless networks: security and analysis.* Springer.

IEEE 802. (2014). *Standard for Local and Metropolitan Area Networks: Overview and Architecture*. Institute of Electrical and Electronics Engineers.

IEEE 802.11. (2012). *Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications*. New York: Institute of Electrical and Electronics Engineers.

IEEE 802.11aa. (2012). *Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications - Amendment 2: MAC Enhancements for Robust Audio Video Streaming*. Institute of Electrical and Electronics Engineers.

IEEE 802.11ac. (2013). *Telecommunications and information exchange between systems Local and metropolitan area networks - S R - Part 11: Wireless LAN (MAC) and (PHY) Specifications: Amendment 4: Enhancements for Very High Throughput for Operation in Bands below 6 GHz.* New York: Institute of Electrical and Electronics Engineers.

IEEE 802.11ad. (2012). *Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications -*

Amendment 3: Enhancements for Very High Throughput in the 60 GHz Band. Institute of Electrical and Electronics Engineers.

IEEE 802.11ae. (2012). *Local and metropolitan area networks - Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 1: Prioritization of Management Frames*. Institute of Electrical and Electronics Engineers.

IEEE 802.11af. (2013). *Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 5: Television White Spaces (TVWS) Operation*. Institute of Electrical and Electronics Engineers.

IEEE 802.1X. (2010). *Standard for Local and metropolitan area networks - Port-Based Network Access Control*. New York: Institute of Electrical and Electronics Engineers.

ISO/IEC 27000. (2014). *Information technology - Security techniques - Information security management systems - Overview and vocabulary*. International Standard Organization.

ISO/IEC 27001. (2013). *Information technology — Security techniques - Information security management systems — Requirements*. International Standard Organization.

ISO/IEC 27002. (2013). *Information technology - Security techniques - Code of practice for information security controls*. International Standard Organization.

ISO/IEC 27033-1. (2015). *Information technology -- Security techniques -- Network security -- Part 1: Overview and concepts*. International Standard Organization.

ISO/IEC 27033-2. (2012). *Information technology -- Security techniques -- Network security -- Part 2: Guidelines for the design and implementation of network security*. International Standards Organization.

ISO/IEC 27033-3. (2010). *Information technology -- Security techniques -- Network security -- Part 3: Reference networking scenarios -- Threats, design techniques and control issues*. International Standards Organization.

ISO/IEC 27033-4. (2014). *Securing communications between networks using security gateways*. International Standard Organization.

ISO/IEC 27033-5. (2013). *Information technology -- Security techniques -- Network security -- Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*. International Standards Organization.

ISO/IEC DIS 27033-6. (Draft). *Information technology -- Security techniques -- Network security -- Part 6: Securing wireless IP network access*. International Standards Organization.

ISO/IEC TR 27023:2015. (2015). *Information technology — Security techniques — Mapping the revised editions of ISO/IEC 27001 and ISO/IEC 27002*. International Standard Organization.

Jannuzi, C. A., Falsarella, O. M., & Sugahara, C. R. (2014, out/dez). Sistema de informação: um entendimento conceitual para a sua aplicação nas organizações empresariais. *Perspetivas em Ciência da Informação, 19*(4), pp. 97-117.

Jarvenpaa, S., & Lang, K. (2005). Managing the paradoxes of mobile technology. *Information Systems Management,, 22/4*, pp. 7-23. doi:10.1201/1078.10580530/45520.22.4.20050901

Kaur, A., & Singh, H. (2014, May). Security in WLAN - Review of Security and Throughput Tradeoff. *International Journal of Computer Science and Mobile Computing*, pp. 1243 – 1246.

Kim, H. W., Chan, H. C., & Gupta, S. (2007). Value-based adoption of mobile internet: an empirical investigation. *Decision Support Systems, 43*(1), pp. 111-126.

Klein, A., Karl, F., & Cunha, M. (2013, setembro). A capacidade organizacional para a mobilidade e seus componentes. *Anais do Encontro Nacional da Associação Nacional de Pós-Graduação e Pesquisa em Administração.* Rio de Janeiro, RJ, Brasil, 37.

Kraus, M. (2013). *Cisco Secure Mobility*. Cisco Systems. Cisco Public.

Kuan, K., & Chau, P. (2001). A perception-based model for EDI adoption in small businesses using a technology–organization–environment framework. *Information & Management, 38*(8), 507-521. doi:10.1016/S0378-7206(01)00073-8

Laudon, K., & Laudon, P. (2010). *Sistemas de informações gerenciais.* São Paulo: Pearson Prentice Hall.

Liang, L., Yang, G., Du, J., Liu, Z., He, Q., Bai, Y., & Yang, S. (2014). The practical risk assessment for enterprise Wireless Local Area Network. *Information Science Electronics and Electrical Engineering (ISEEE), 2014 International Conference. 3*, pp. 1936-1940. IEEE.

(n.d.). *LightRadio Wi-Fi WLAN Gateway.* ALCATEL-LUCENT Application Note.

Lin, H. (2011). An empirical investigation of mobile banking adoption: the effect of innovation attributes and knowledge-based trust. *International Journal of Information Management, 31*(3), 252-260. doi:10.1016/j.ijinfomgt.2010.07.006

Lunardi, G., Dolci, P., & Maçada, A. (2010). Adoção de tecnologia de informação e seu impacto no desempenho organizacional: um estudo realizado com micro e pequenas empresas. *Revista de Administração, 45*(1), 5-17.

Machado, C. B., & Freitas, H. (2007). Modelo para Planejamento de Iniciativas de Adoção de Tecnologias Móveis na Interação entre Organização e Indivíduo. *ENCONTRO DE ADMINISTRAÇÃO DA INFORMAÇÃO (ENADI). 1*. Florianópolis/SC: Anpad.

Mandal, S., & Saini, N. (2015, May). Review paper on 802.11 Wireless LAN Security. *International Journal of Research (IJR), 2*(3), pp. 33-37. Retrieved from http://internationaljournalofresearch.org/

Manica, A., & Saccol, A. (2009). Avaliação dos resultados de adoção de tecnologias da informação móveis e sem fio (TIMS): o caso do IBGE – censo 2007. *Anais do Encontro Nacional da Associação Nacional de Pós-Graduação e Pesquisa em Administração.* São Paulo, SP, Brasil, 33.

Mathews, M., & Hunt, R. (2007). Evolution of Wireless Lan Security Architecture to IEEE 802.11i (WPA2). *In Proceedings of the fourth IASTED Asian Conference on Communication Systems and Networks*.

Maximiano, A. C. (1992). *Introdução a administração* (3ª ed.). São Paulo: Editora Atlas.

Monteiro, E., & Boavida, F. (2011). *Engenharia de Redes Informáticas* (10ª ed.). Lisboa: FCA Editora.

NIST S P 800-64r2. (2008, October). *Security Considerations in the System Development Life Cycle*. National Institute of Standards and Technology (NIST).

NIST SP 800-124r1. (2013, June). *Guidelines for Managing the Security of Mobile Devices in the Enterprise*. National Institute of Standards and Technology (NIST).

NIST SP 800-153. (2012, February). *Guidelines for Securing Wireless Local Area Networks (WLANs)*. National Institute of Standards and Technology (NIST).

NIST SP 800-36. (2003, Octobre). *Guide to Selecting Information Technology Security Products*. National Institute of Standards and Technology (NIST).

NIST SP 800-48r1. (2008, July). *Guide to Securing Legacy IEEE 802.11 Wireless Networks*. National Institute of Standards and Technology (NIST).

NIST SP 800-94. (2007, February). *Guide to Intrusion Detection and Prevention Systems (IDPS)*. National Institute of Standards and Technology (NIST).

NIST SP 800-97. (2007, february). *Establishing wireless robust security networks: A guide to ieee 802.11i*. National Institute of Standards and Technology (NIST).

NSA. (2012). Guidelines for the Development and Evaluation of IEEE 802.11 Intrusion Detection Systems (IDS). National Security Agency (NSA).

NSA. (2014, March 04). Campus WLAN Capability Package. *Commercial Solutions for Classified (CSfC) Campus IEEE 802.11 Wireless Local Area Network (WLAN) Capability Package*. (N. S. (NSA), Ed.) Information Assurance Directorate (IAD). Retrieved Fevereiro 2015, from https://www.nsa.gov/ia/ia_at_nsa/index.shtml

O'Brien, J. A., & Marakas, G. M. (2013). *Administração de Sistemas de Informação* (15ª ed.). Porto Alegre: AMGH/McGraw-Hill/Bookman.

OECD. (2009). Measuring the Information Economy . *OECD Publications*.

Oliveira, T., Martins, M. F., & Lisboa, U. N. (2011). Literature Review of Information Technology Adoption Models at Firm Level. *The Electronic Journal of Information Systems Evaluation, 14*, 110-121.

Pacheco, J. A., Pestana, T., Figueiredo, J., & Martins, D. (2014). Globalização, currículo e aprendizagem para uma análise crítica das práticas curriculares em contextos diferenciados. *XXI Colóquio da Secção Portuguesa da AFIRSE: Educação, Economia e Território: o papel da educação no desenvolvimento*, (pp. 1190-1198).

Pardal, L., & Correia, E. (1995). *Métodos e Técnicas de Investigação Social*. Porto: Areal Editores.

Pavlou, P., & El Sawy, O. (2010). The “third hand”: IT-enabled competitive advantage in turbulence through improvisational capabilities. *Information Systems Research, 21*(3), 443-471. doi:10.1287/isre.1100.0280

Perahia, E., & Stacey, R. (2013). *Next Generation Wireless LANS: 802.11 n and 802.11 ac*. Cambridge university press.

Phifer, L. (2014). *Next-Gen WLAN: How 802.11ac Will Change Your Network Forever*. Searchnetworking.com.

Porter, M. E. (1980). *Competitive strategy.* New York: Free Press/Macmillan.

Porter, M. E. (1985). *Competitive advantage.* New York: Free Press/Macmillan.

Prates, G., & Ospina, M. (2004). Tecnologia da informação em pequenas empresas: fatores de êxito, restrições e benefícios. *Revista de Administração Contemporânea, 8*(2), 9-26. doi:10.1590/S1415-65552004000200002

Reisswitz, F. (2008). *Análise De Sistemas Vol 1.* Clube de Autores.

Rezende, D. A., & Abreu, A. F. (2013). *Tecnologia da informação aplicada a sistemas de informação empresariais* (9ª ed.). São Paulo: Atlas.

Robbins, S. P. (1990). *Organization theory.* Englewood Cliffs: Prentice-Hall.

Rodrigues, L. C., & Fernandez, M. J. (2012). Alinhamento estratégico da tecnologia de informação e inteligência competitiva. *Revista Inteligência Competitiva, 1*(3), pp. 328-344.

Saccol, A., & Reinhard, N. (2005). Processo de adoção e decorrências da utilização de tecnologias de informação móveis e sem fio no contexto organizacional. *Anais do Encontro Nacional da Associação Nacional de Pós-Graduação e Pesquisa em Administração.* Brasília, Brasil, 29.

San Martín, S., López-Catalán, B., & Ramón-Jerónimo, M. (2012). Factors determining firms' perceived performance of mobile commerce. *Industrial Management & Data Systems, 112(6)*, pp. 946-963. doi:10.1108/02635571211238536 Internet Móvel nas Organizações 703

Sanaei, Z., Abolfazli, S., Gani, A., & Buyya, R. (First Quarter 2014). Heterogeneity in Mobile Cloud Computing: Taxonomy and Open Challenges First Quarter 2014. In IEEE (Ed.), *Communications Surveys & Tutorials, 16*, pp. 369,392.

Santos, A. P., & Barbosa, R. R. (2011). Desafios da Mobilidade Corporativa para a Gestão da Informação e do Conhecimento. *Informação & Sociedade: Estudos, 21*(2), 49-62.

Santos, J. V. (2009). A Sociedade e as Organizações. UFT - Universidade Federal do Tocantins..

Shankar, V., Venkatesh, A., Hofacker, C., & Naik, P. (2010). Mobile marketing in the retailing environment: current insights and future research avenues. *Journal of Interactive Marketing, 24*(2), 111-1120. doi:10.1016/j.intmar.2010.02.006

Shourbaji, I. A., & Amer, R. A. (2013, February). Wireless Intrusion Detection Systems (WIDS). *Advances in Computer Science and its Applications (ACSA), 2*(3). doi:arXiv:1302.6274v2

Shuman, J. (1982). Strategic planning and information systems. *Bulletin of the American Society for Information Science and Technology, 8*, pp. 23-27.

Sridevi. (2013, September). Wireless Lan Vulnerabilities, Threats and Countermeasures. *Indian Journal of Applied Research, 3*(9), pp. 123-126.

Stallings, W. (2013). *Data and Computer Communications.* (10ª ed.). New Jersey: Pearson/Prentice Hall.

Stallings, W., & Beard, C. (2015). *Wireless Communication Networks and Systems.* Pearson.

Strechie, M. (2014). Latin Etymologies in Communication Terminology. *International Letters of Social and Humanistic Sciences, 07*, 56-61.

Tan, H., & Mathews , J. A. (february de 2010). Cyclical industrial dynamics: The case of the global semiconductor industry. *Technological Forecasting and Social Change, 77*(2), 344-353.

Tavares, E., Lucas, C., Dialo, M., Leo, P., Monnoyer, M., & Philippe, J. (2012). A influência do uso de tecnologias móveis na inovação em serviços. *Anais do Encontro Nacional da Associação Nacional de Pós-Graduação e Pesquisa em Administração.* Rio de Janeiro, RJ, Brasil, 36.

Turban, E., Leidner, D., McLean, E., & Wetherbe, J. (2010). *Tecnologia da informação para gestão.* Porto Alegre: Bookman.

Turban, E., Ranier JR, R. K., & Potter, R. E. (2007). *Introdução a sistemas de Informação uma abordagem gerencial.* (D. Vieira, Trans.) Rio de Janeiro: Elsevier.

Ungan, M. (2004). Factors affecting the adoption of manufacturing best practices. *Benchmarking: an International Journal, 11*(5), 504-520. doi:10.1108/14635770410557726

Vilela, D. W. (2014). Segurança em redes sem fio: estudo sobre o desenvolvimento de conjuntos de dados para comparação de IDS.

Vilela, D. W., Ferreira, E. T., & Shinoda, A. (2013). Construção De Uma Base De Dados Para Auxiliar A Avaliação De Sistemas De Detecção De Intrusos Com Criptografia Ieee 802.11 Ie Ieee 802.11 W Habilitada. *Sistema de Publicações, 1*(1).

Ward, J., Griffiths, P., & Whitmore, P. (1990). *Strategic Planning for Information Systems,, , .* Chichester: John Wiley & Sons.

Webster, F. (2014). *Theories of the information society.* Routledge.

Whitten, J., & Bentley, L. (2007). *Systems analysis e design methods* (7ª ed.). Nova York: McGraw-Hill/Irwin.

(2004). *Wi-Fi in the Enterprise.* Proxim Corporation.

Zamani, A. T., & Ahmad, J. (2014, February). IEEE 802.11 Wireless LAN: Security Risks. *International Journal of Research in Information Technology (IJRIT), 2*(2), 114- 122. Retrieved from www.ijrit.com

Zhang, L., Zhu, J., & Liu, Q. (2012). A meta-analysis of mobile commerce adoption and the moderating effect of culture. *Computers in Human Behavior, 28*(5), 1902-1911. doi:10.1016/j.chb.2012.05.008

Zimmerman, T., & Fabbi, M. (2012). *Magic Quadrant for the Wired and Wireless LAN Access Infrastructure*. Retrieved from http://www.gartner.com/technology/reprints.do?id=1-1AX5XXB&ct=120614&st=sb