ZACHARIAS DA COSTA GADELHA NETO

ELABORAÇÃO DE *CHECKLISTS* PARA VERIFICAÇÃO DA APLICAÇÃO DOS CONTROLES DA NORMA ABNT NBR ISO/IEC 27002:2005 EM IMPLANTAÇÃO DE REDES LOCAIS *WIRELESS*

Monografia apresentada ao Programa de Educação Continuada em Engenharia da Escola Politécnica da Universidade de São Paulo para obtenção do Título de MBA em Tecnologia da Informação.

Orientador: Prof. Stephan Kovach

São Paulo

2010

FICHA CATALOGRÁFICA

Gadelha Neto, Zacharias da Costa
Elaboração de checklists para verificação da aplicação dos controles da Norma ABNT ISO/IEC 27002:2005 em implantação de redes locais wireless / Z.C. Gadelha Neto -- São Paulo, 2010.
97 p.

Monografia (MBA em Tecnologia da Informação) – Escola Politécnica da Universidade de São Paulo. Programa de Educação Continuada em Engenharia.

1. Tecnologia da informação 2. Wireless (Implantação) 3. Gestão da segurança em sistemas computacionais I. Universidade de São Paulo. Escola Politécnica. Programa de Educação Continuada em Engenharia II. t.

AGRADECIMENTOS

Ao professor Stephan Kovach, por sua disposição e paciência para a orientação.

Ao professor Antonio Marcos de Aguirra Massola, pela oportunidade de participar deste curso.

Aos amigos, pelo estímulo constante, mesmo na minha longa ausência.

À família, sempre presente e que não deu chance para o esmorecimento.

E aos que, direta ou indiretamente, colaboraram para a execução deste trabalho.

OK

RESUMO

Este trabalho apresenta uma proposta de elaboração de um *checklist* focado em elementos componentes de redes locais *wireless* e destinado à verificação da aplicação do código de práticas de segurança da informação em projetos de implantação deste tipo de rede. A grande expansão do uso de tecnologias de redes *wireless* está tornando-as disponíveis em todos os lugares. Dentre estas tecnologias, as redes locais *wireless* (WLAN) vêm crescendo rapidamente nos últimos anos (e continuam a fazê-lo). Atualmente, as WLANs vêm se tornando muito populares tanto para uso doméstico quanto para uso corporativo. As redes locais *wireless* pessoais ou S.O.H.O (*Small Office Home Office*), com tecnologia de autenticação por chave pré-compartilhada, funcionam com um pequeno número de elementos e itens de configuração. Diferentemente, as redes locais *wireless* corporativas, baseadas na segurança 802.1x, utilizam maior quantidade e tipos de componentes. Além do aspecto operacional da implantação da tecnologia, onde os itens de configuração precisam seguir as regras impostas pelas normas técnicas pertinentes, existem demandas, também, para aplicar as diretrizes e recomendações das normas de segurança da informação focados em aspectos relacionados a processos e políticas de uso dos recursos. No Brasil, ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005 são as normas sobre segurança da informação. O *checklist,* um tipo de ajuda para tarefas informacionais ou mentais (numa forma simples "uma lista de coisas a lembrar" ou "a fazer"), pode ser útil para ajudar na verificação das atividades de aplicação dos objetivos de controle de segurança da informação sobre os ativos da empresa, em particular, sobre os elementos componentes de redes locais *wireless* de novas implementações, que necessitam estar alinhados e em conformidade com os padrões de segurança da informação. A adoção de *checklist* pode ser produtiva e interessante quando envolver grandes quantidades de registros e itens de controle a serem verificados.

ABSTRACT

This work presents a proposal for a checklist development focused in wireless LAN elements and oriented to follow the application of the information security code of practices in WLAN implementation projects. The wide spread use of wireless networks technologies is making them available everywhere. Among these technologies, the wireless local area networks (WLAN) have been growing rapidly (and continues doing it). Nowadays, the WLANs have become very popular for home use as well as for corporate use. The personal or S.O.H.O (*Small Office Home Office*) wireless local area networks with pre-shared key authentication technology work with few elements and configuration items. On the other hand, the enterprise wireless local area networks, 802.1x security based, use more amount and component types. Besides the technology implementation operational aspects, where the configuration items need to follow the pertinent technical standard rules, there are also demands to apply the information security guidelines and recommendations focused in process and policies for the use of resources. In Brazil, ABNT NBR ISO/IEC 27001:2006 and ABNT NBR ISO/IEC 27002:2005 are the standards about information security. The checklist, a type of aid to informational or mental job (in a simple way "a list of things to remember" or "to do") could be useful to help the verification of the application activities of information security control objectives over the enterprise assets, in particular, over the wireless LAN components of new implementations which need to be aligned and in compliance with the information security patterns. The checklist adoption could be useful and interesting when involving great amounts of records and control items to be verified.

LISTA DE ILUSTRAÇÕES

LISTA DE QUADROS

LISTA DE ABREVIATURAS E SIGLAS

3GPP	3rd Generation Partnership Project
ABNT	Associação Brasileira de Normas Técnicas
AES	Advanced Encryption Standard
AP	*Access Point*
BSS	Basic Service Set
CA	*Certificate Authority*
CDV	*Challenge-Do-Verify*
CIA	Confidenciality, Integrity, Availability
DHCP	Dynamic Host Configuration Protocol
DNS	Dynamic Name System
DV	*Do-Verify*
ETSI	European Telecommunications Standards Institute
GSM	Global System for Mobile Communication
GPRS	General Packet Radio Service
IEC	International Electrotechnical Commission
IEEE	Institute of Electrical and Electronics Engineers
IrDA	Infrared Data Association
ISO	International Organization of Standardization
ISOC	Internet Society
LAN	*Local Area Network*
MBWA	Mobile Broadband Wireless Access
NAS	Network Access Server
NBR	Denominação de norma da Associação Brasileira de Normas Técnicas

OECD	Organisation for Economic Co-operation and Development
PDCA	Plain-Do-Check-Act
PMBOK	Project Management Body of Knowledge
RADIUS	Remote Authentication Dial In User Service
RFC	Request for Comments
S.O.H.O.	Small Office Home Office
STA	Station
TKIP	Temporal Key Integrity Protocol
UMTS	Universal Mobile Telecommunication System
WAN	Wide Area Network
WECA	Wireless Ethernet Compatibility Alliance
WEP	Wired Equivalent Privacy
WISP	Wireless Internet Service Provider
WLAN	Wireless Local Area Network
WMAN	Wireless Metropolitan Area Network
WPA	Wireless Protect Access
WPA-EAP	WPA-Extensible Authentication Protocol
WPA2	Wireless Protect Access 2
WPA-PSK	WPA-Pre Shared Key
WPAN	Wireless Personal Area Network
WWAN	Wireless Wide Area Network

SUMÁRIO

1 INTRODUÇÃO

1.1 CONSIDERAÇÕES INICIAIS

Redes *wireless* são uma realidade cada vez mais freqüente. Nos dias atuais, em shoppings, aeroportos, livrarias, *coffee shops*, é comum encontrar pontos de acesso *wireless* - os chamados '*hotspots*' - e, em suas proximidades, muitos usuários com seus notebooks conectados à Internet. Alguns destes *hotspots* em locais públicos são "abertos", ou seja, qualquer um que esteja obtendo sinal em seu computador é livre para se conectar sem maiores restrições de acesso. A maioria, entretanto, exige algum tipo de comprometimento com regras de acesso e conduta e, em parte deles, exige-se um cadastramento inicial com fornecimento de uma senha obtida junto ao provedor do serviço de acesso.

Em universidades e instituições acadêmicas em geral, a proliferação dos pontos de acesso *wireless* segue em ritmo semelhante. No Brasil, apesar da falta de informações mais acuradas, sabe-se que as universidades também vêm partindo para a adoção deste tipo de tecnologia para uso de seu público específico. Poderíamos dizer que, aqui no país, de forma geral, este público que acessa os *hotspots* em áreas internas de campi acadêmicos, faz parte destas comunidades e se enquadra num dos três perfis tipicamente encontrados nestas instituições: alunos, professores ou funcionários. Neste ambiente, o mais comum é que os *hotspots* exijam algum tipo de cadastramento inicial para utilização do recurso e, uma vez que este esteja efetuado, é franqueado o acesso à Internet.

Empresas também empregam pontos de acesso *wireless*, só que, normalmente, em complemento à infra-estrutura cabeada (as ditas redes '*wired*'). Nestes ambientes, as redes *wireless* são adotadas, via de regra, como solução para comportar os usuários móveis, perfil típico apenas de parte dos seus quadros funcionais. Através do acesso *wireless*, os indivíduos pertencentes a este grupo têm direitos específicos que lhes permitem conectarem-se aos recursos de TI internos da instituição relacionados às suas atividades, não somente à Internet, como é o caso da maioria dos *hotspots* públicos.

Quando estamos tratando de *hotspots* providos por estabelecimentos comerciais, como os citados no início do presente texto, é comum as contas de usuários estarem cadastradas em sistemas simples, muitas vezes em bases de dados de aplicações '*embbeded*' (embutidas) no próprio dispositivo de acesso. Em outros casos, quando há provedores de acesso *wireless* especializados (WISP) prestando serviço a estes estabelecimentos comerciais, as contas podem estar previamente cadastradas em suas bases e apenas tickets com senhas são emitidos para uso dos clientes. Nestes ambientes não há uma maior preocupação em autenticar dados pessoais do cliente em uma base permanente. Já nas redes internas de empresas os "clientes" do acesso *wireless* são funcionários ou, eventualmente, convidados da organização. Nestes casos, seus registros estão armazenados em bases de dados centrais da entidade e a autenticação de seus acessos é feita dentro dos domínios de endereços utilizados pelas empresas.

Em empresas muito grandes ou, mais comumente, numa grande organização universitária, pode ocorrer de haver múltiplos domínios de endereços, cada qual com sua base de contas e servidores em locais diferentes e sob a administração de organismos operacionais de TI distintos. Nesta situação, a autenticação do usuário de um serviço de acesso *wireless* pode estar condicionada à disponibilidade de algum mecanismo que permita localizar a base adequada para validar esta operação. Esta necessidade aumenta a complexidade do sistema de acesso. Esta é apenas uma das dificuldades com a qual se tem de lidar neste contexto.

Como garantir que a segurança da organização, do ponto de vista de segurança da informação (proteção dos ativos informacionais contra ameaças pela exploração de vulnerabilidades), esteja sendo devidamente considerada - como um todo - quando da definição de um projeto e/ou implementação de rede *wireless*?

Como toda tecnologia de informação, a implementação de redes *wireless* implica na atenção a uma série de cuidados e decisões relacionadas à segurança da informação. Não se deve perder de vista que as iniciativas de estabelecer regras para preservação e proteção da informação devem sempre repousar sobre os três pilares da segurança da informação, ou seja, devem atender os requisitos básicos para a sua existência: confidencialidade, integridade e disponibilidade. Para isso, diversos aspectos como gestão dos ativos, segurança física e do ambiente, controle de acessos, gestão de incidentes, conformidade, dentre outros, têm de ser tratados

convenientemente. Uma das formas de se chegar a este resultado é procurar alinhar os procedimentos de aplicação de soluções baseados na tecnologia *wireless* com o atendimento dos objetivos de controle estabelecidos nas normas em vigor que cuidam de técnicas de segurança em tecnologia da informação, no caso brasileiro, as normas ABNT NBR ISO/IEC 27002:2005 - Tecnologia da informação - Técnicas de segurança - Código de pratica para a gestão de segurança da informação [1] e ABNT NBR ISO/IEC 27001:2006 - Tecnologia da informação - Técnicas de segurança - Sistemas de gestão de segurança da informação – Requisitos [2].

Checklists (ou listas de verificação) são recursos usados em diversas áreas de atividade e com diferentes aplicações, desde uma trivial lista do supermercado, até como parte indispensável dos procedimentos de preparação para decolagem de aeronaves. Em tecnologia de informação, são usadas tanto para apoio à ativação inicial de sistemas e equipamentos (*startup)*, como também como ferramentas para verificação de conformidade em auditorias da área de análise de risco. Para atividades onde é necessária a observação do *status* de muitos itens de configuração a utilização de *checklists* pode ser um recurso de grande valor.

A elaboração de um *checklist* para acompanhamento de aplicação de controles do código de práticas de segurança da informação da Norma ABNT NBR ISO/IEC 27002:2005 em projetos de implantação de redes locais *wireless* em ambiente corporativo pretende fornecer um subsídio para o acompanhamento de projetos de redes deste tipo em ambientes complexos, em que a quantidade de componentes envolvidos (pontos de acesso, roteadores, servidores de autenticação, de banco de dados, de nomes, de endereços, de logs, dentre outros elementos utilizados) seja tal que dificulte a memorização de detalhes e detecção de pendências não resolvidas.

1.2 OBJETIVOS DO TRABALHO/ PROPOSTA DO TRABALHO

Este trabalho apresenta uma proposta de elaboração de um *checklist* para uso na atividade de verificação da aplicação dos controles da norma ABNT NBR ISO/IEC 27002:2005 na implantação de projetos de rede local *wireless* em ambiente corporativo.

1.3 ESTRUTURA DO TRABALHO

O presente trabalho está composto em quatro partes. Na primeira, capítulo 1, do qual fazem parte as considerações gerais iniciais, os objetivos do trabalho e o presente resumo, estão inseridas informações para situar o leitor no contexto onde atuam as redes locais *wireless* e onde ocorrem os problemas relacionados à implantação de processos e controles na área de segurança da informação. A segunda parte, representada pelo capítulo 2, apresenta uma revisão de literatura cobrindo os aspectos relacionados à tecnologia de redes locais *wireless*, normas para gestão da segurança da informação e utilização de *checklist* como instrumento de apoio aos sistemas de gestão da segurança da informação. Em seguida, no capítulo 3, descreve-se a elaboração de um *checklist* específico para uso em acompanhamento de aplicação de controles do código de prática para a gestão de sistemas de informação em projetos de implementação de redes locais *wireless*. No final do capítulo, é apresentado um preenchimento parcial de um *checklist* com dados extraídos de um ambiente fictício. Por fim, o capítulo 4 contém as conclusões do trabalho e as considerações finais.

2 CONCEITOS

Neste capítulo, é feita uma apresentação de alguns conceitos importantes relacionados aos três temas centrais envolvidos no trabalho: redes locais *wireless*, normas de segurança da informação e *checklists*.

2.1 REDES LOCAIS *WIRELESS*

Na tradução literal, *wireless* significa "sem fio". Uma rede *wireless*, portanto, é uma rede que não utiliza fios ou cabos para estabelecer a comunicação entre seus elementos. Neste tipo de rede a tecnologia de comunicação é baseada na transmissão e recepção dos sinais através de ondas eletromagnéticas. IrDA, Bluetooth e Wi-Fi são tecnologias que enquadram-se nesta categoria de redes.

IrDA, um acrônimo de *Infrared Data Association*, é uma definição de padrão de comunicação sem fio que usa radiação infravermelha para transmissão de dados entre dispositivos. É usada para transferência de dados serialmente e em *half duplex* (não permite envio e recepção simultâneos), entre dispositivos a curta distância (até aproximadamente 4,5m) e independente de plataforma [3].

Bluetooth, tecnologia baseada em ondas de rádio, para transmissão de informações no chamado "espaço pessoal" (até distâncias de, aproximadamente, 10 metros). Os dispositivos são separados em três classes (1, 2 e 3) baseadas na potência de transmissão, com alcances aproximados de 1 metro, 10 metros e 100 metros, respectivamente. Originalmente concebida para ser uma substituta sem fio para cabos de interligação entre aparelhos domésticos (celulares e headphones, computadores e teclados/mouses, aparelhos de som e fones. Atualmente permite conexões antes impraticáveis, como interligar a câmera de um celular direto à impressora ou o celular ao aparelho de som do carro [4].

Wi-Fi, apesar de ser um termo muito empregado para designar, de forma generalizada, redes locais *wireless*, é um nome comercial e licenciado, criado por uma organização formada por empresas da área de tecnologia para certificação de produtos desenvolvidos dentro das especificações IEEE 802.11. Esta organização, originalmente denominada Wireless Ethernet Compatibility Aliance (WECA), em 1999 ratificou com o selo Wi-Fi o padrão IEEE 802.11b e continua certificando produtos com sua marca registrada. Atualmente, as redes do padrão 802.11a, b, g e n são certificadas pela organização, que desde 2002, passou a denominar-se Wi-Fi Alliance [5].

Apesar da popularidade do termo Wi-Fi, para os propósitos do presente trabalho, considerou-se mais adequada a adoção da denominação WLAN (*wireless local area network*), para a designação no sentido específico de 'redes locais sem fio' ou 'redes locais *wireless*'.

Uma das formas de se classificar as redes *wireless* é através de sua capacidade de abrangência (área de cobertura aproximada). Desta forma, obtêm-se referências aos seguintes agrupamentos:

Denominação original	Descrição	Aplicações	Abrangência (ordem de grandeza)	Padrão IEEE	Outros Padrões
WPAN (Wireless Personal Area Network)	Redes Pessoais Sem Fio	IrDA, Bluetooth, UWB, ZigBee (Piconet)	~10m	802.15 (Bluetooth)	ETSI Hiperpan
WLAN (Wireless Local Area Network)	Redes Locais Sem Fio	Wi-Fi, HiperLAN2	~100m	802.11	ETSI Hiperlan
WMAN (Wireless Metropolitan Area Network)	Redes Metropolitanas Sem Fio	WiMAX	~10Km	802.16	ETSI Hiperman e Hiperaccess
WWAN (Wireless Wide Area Network)	Redes locais de longa distância sem fio	Mobile wireless (GSM, GPRS, UMTS)	>10Km	802.20 (MBWA)	3GPP (GSM)

Quadro 1 – Classificação das redes *wireless* pela abrangência
Fontes: Redes sem fio - Wireless Networks [6], Bandwidth Efficiency of Wireless Networks of WPAN, WLAN, WMAN and WWAN [7]

2.1.1 Padrões de WLAN

O IEEE, *Institute of Electrical and Electronic Engineers*, desenvolveu o padrão 802.11 [8], publicado originalmente em 1999, com a finalidade de estabelecer especificações para conectividade sem fio para estações móveis, portáteis ou fixas dentro de uma rede local. O padrão também oferece um corpo regulatório para bandas de freqüência para uso em comunicações neste tipo de ambiente.

Como característica do próprio sistema de classificação dos padrões empregado pela organização, o agrupamento numérico inteiro, no caso, 802, designa a família da norma (a 802 tem como objetivo definir uma padronização para redes locais e metropolitanas). Os detalhamentos são representados por denominações decimais derivadas desta designação original. No caso, 802.11 (ou parte 11 da norma 802), refere-se a *Wireless LAN*. O aperfeiçoamento da norma é feito através do trabalho de comitês (os *task groups*), identificados por letras (ou conjuntos de letras) seqüenciais. Atualmente, há 27 *tasks groups* associados ao 802.11, em diferentes estágios de desenvolvimento dos trabalhos. Dentre os mais conhecidos, pode-se citar o ***a***, ***b***, ***g*** e ***n***, apresentados no Quadro 2 e, também, o ***i*** e o ***s***, que serão comentados ao longo deste capítulo.[1]

Padrão	Frequência	Taxa de transmissão (Max)	Alcance máximo nominal (indoor/outdoor)
802.11a	5 GHz	54 Mbps	30m/100m
802.11b	2.4Ghz	11 Mbps	35m/110m
802.11g	2.4 GHz	54 Mbps	35m/110m
802.11n	2.4 GHz ou 5 GHz	450 Mbps	70m/160m

Quadro 2 – Principais padrões da família IEEE 802.11 para redes locais *wireless*
Fontes: Wi-Fi Alliance. Discover and Learn [5], Bandwidth Efficiency of Wireless Networks of WPAN, WLAN, WMAN and WWAN [7]

[1] O link <http://www.ieee802.org/11/QuickGuide_IEEE_802_WG_and_Activities.htm> apresenta uma tabela sempre atualizada com a situação corrente de todos os *task groups* relacionados ao 802.11.

2.1.2 Componentes da arquitetura de uma WLAN

A norma IEEE 802.11 organiza os componentes da arquitetura de redes locais *wireless* em uma concepção celular. As células, consideradas o bloco construtivo fundamental do padrão, são denominadas *Basic Service Sets*, ou BSS. Há três modelos de conjuntos de componentes: IBSS, BSS e ESS.

Na configuração *Independent Basic Service Set* (IBSS), também chamada de '*modo Ad-hoc*', a comunicação entre as estações de trabalho é estabelecida diretamente, sem a necessidade de um AP e de uma rede física para conectar as estações.

A Figura 1 ilustra uma IBSS, com quatro estações de trabalho (STAs). O círculo simboliza a área de abrangência da célula. Se uma estação se move e sai da área de abrangência, perde o sinal de comunicação com as demais estações.

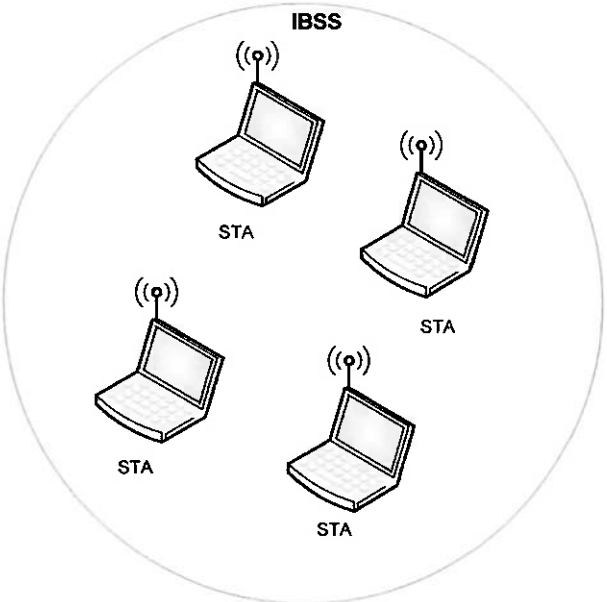


Figura 1 - Rede local *wireless* – modo *ad hoc*
Fontes: IEEE 802.11 [8], A Technical Tutorial on the IEEE 802.11Protocol [9]

Na configuração *Basic Service Set* (BSS), também denominada '*modo infra-estrutura*', os computadores são ligados entre si por meio de um equipamento central, o ponto de acesso (*Access Point*, ou AP). Este AP é um elemento fixo que coordena a comunicação entre as estações de trabalho (STAs) dentro da BSS e

funciona como uma ponte de comunicação entre a rede sem fio e a rede externa à BSS (de meio físico diverso do meio *wireless*).

O meio físico entre o AP e a rede externa à célula não é objeto de especificação da IEEE 802.11. Em função disso, ela apenas o considera como "distinto" do meio interno à BSS, não entrando em maiores detalhes. Porém, independente do suporte físico, esta interligação com a área externa à BSS é um elemento da arquitetura. Este elemento é denominado *Distribution System* (DS) e é o responsável pela conexão da BSS a outras BSS quando esta faz parte de uma rede maior, composta por múltiplas BSS. Quando numa rede com múltiplos BSS, o DS deve prover o necessário suporte para o direcionamento de endereços para os mapas de destino, sem solução de continuidade. O DS é um tipo de '*backbone*', normalmente Ethernet, mas também pode estar baseado em *wireless* [9].

A Figura 2 ilustra uma BSS, com quatro estações de trabalho (STAs) e um ponto de acesso (AP), que se interliga, via *Distribution System* (DS), a uma rede externa.

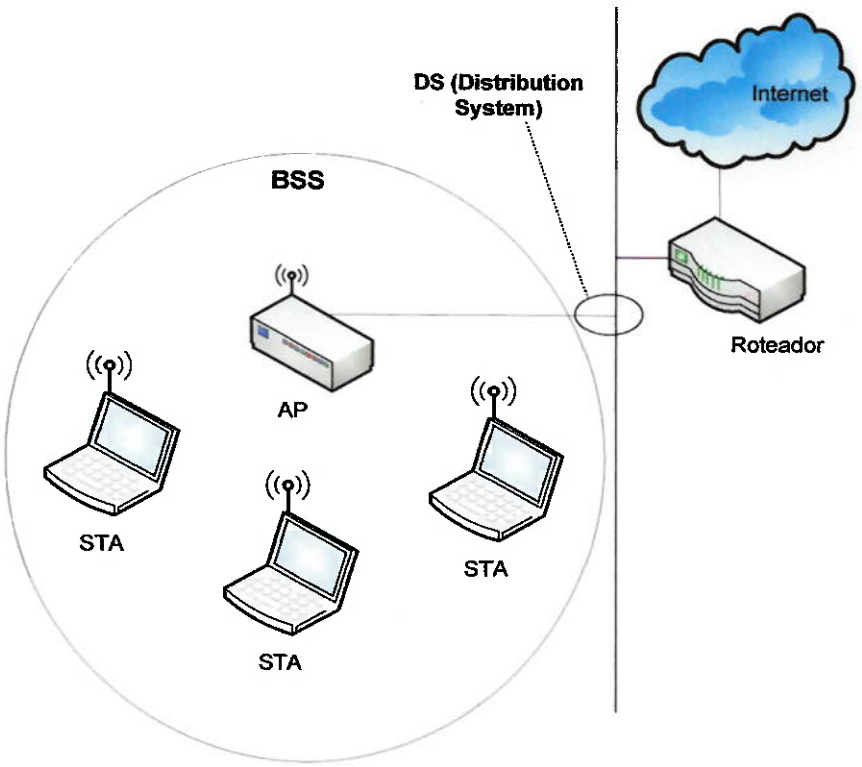


Figura 2 - Rede local *wireless* – modo infra-estrutura
Fontes: IEEE 802.11 [8], A Technical Tutorial on the IEEE 802.11 Protocol [9]

O terceiro modelo de conjunto de componentes, o *Extended Service Set* (ESS), representa redes de maior cobertura, onde diversos BSS são unidos através de um DS. As estações de trabalho (STAs) dentro de diferentes BSS de um mesmo ESS comunicam-se entre si e podem, também, mover-se livremente entre os BSS (*roaming*). O DS que une os BSS não faz parte do ESS.

A Figura 3 apresenta um ESS (ESS-1), composto por dois BSS (BSS-1 e BSS-2) unidos por um '*backbone*' comum, um único DS. O DS é externo ao ESS. No exemplo, as células se sobrepõem, porém, de acordo com a norma 802.11, isto não precisa ocorrer e, também, não há limite de distância entre os BSS.

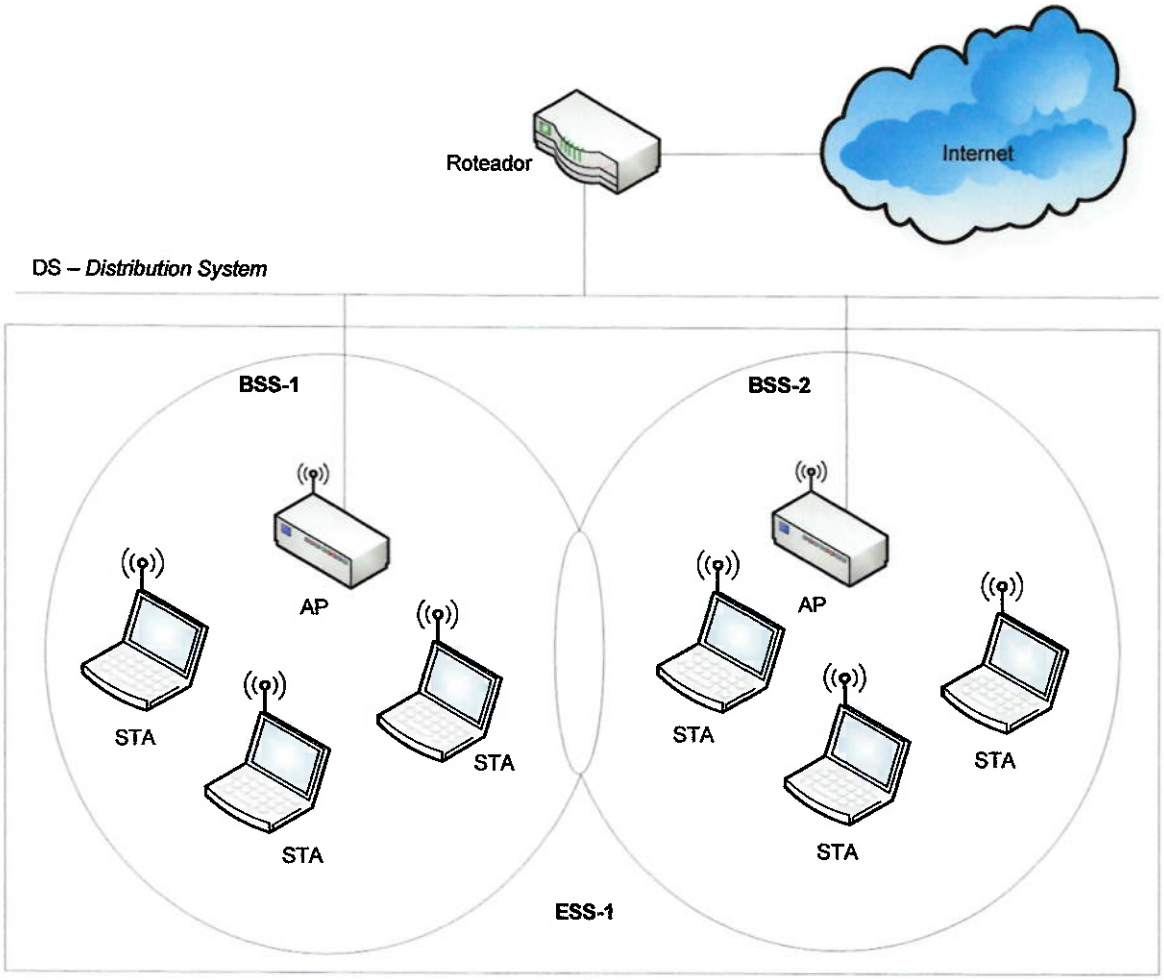


Figura 3 - Rede local *wireless* – modo infra-estrutura estendido
Fontes: IEEE 802.11 [8], A Technical Tutorial on the IEEE 802.11 Protocol [9]

2.1.3 Segurança em WLAN

Para reduzir a vulnerabilidade da comunicação nas redes locais *wireless*, o padrão IEEE 802.11 especifica a utilização de um sistema de autenticação e um de criptografia. O sistema de autenticação objetiva que a rede disponha de mecanismo para autenticar o usuário que está se conectando nela e, simultaneamente, que permita que o usuário também autentique a rede onde está se conectando (autenticação mútua). Este processo é efetuado pela interação entre o *access point* (AP) e a estação de trabalho (STA). Já a utilização de um sistema de criptografia visa garantir a autenticação, a confidencialidade e a integridade da comunicação [8][10][11].

Os mecanismos de segurança adotados pelo padrão IEEE 802.11 foram sendo aperfeiçoados e/ou substituídos ao longo do tempo em função do aumento das vulnerabilidades e demandas crescentes por segurança. Um quadro resumido das características dos três mecanismos utilizados nas diversas versões da norma é apresentado no Quadro 3.

Protocolo de segurança	WEP – Wired Equivalent Privacy	WPA- Wi-Fi Protected Access	WPA2- Wi-Fi Protected Access 2
Características principais	Estabelecido na primeira versão da IEEE 802.11. Proporciona controle de acesso e privacidade de dados	Hierarquia de chaves, sistemas personal e enteprise, permite atualização dos equipamentos com WEP (firmware), WPA é um *draft* do WPA2	Hierarquia de chaves, sistemas personal e enteprise, não permite atualização dos equipamentos com WEP (firmware), melhorias na autenticação em roaming
Autenticação	Aberta ou Chave partilhada (40 bits)	Distribuição e derivação de chaves automática, WPA-PSK (WPA personal – autenticação no AP), WPA-EAP (WPA enterprise – autenticação em um servidor de autenticação)	Distribuição e derivação de chaves automática, WPA-PSK (WPA personal – autenticação no AP), WPA-EAP (WPA enterprise – autenticação em um servidor de autenticação)
Criptografia	Algoritmo RC4 (mesma chave e algoritmo são usados para cifrar e decifrar os dados)	AES, TKIP (chave temporal)	AES, TKIP (chave temporal)
Vulnerabilidades	Tamanho de chave Reuso de chave Protocolo de autenticação ineficiente (permite ataque de escuta ao tráfego de dados)	PSK susceptível a ataques de dicionário	PSK susceptível a ataques de dicionário, Por ser novo, ainda pouco explorado.

Quadro 3 – Padrões de segurança para redes locais *wireless*
Fontes: The evolution of wireless security in 802.11 [10], Wireless Networking Security [11]

2.1.4 Outros padrões IEEE

A parte 11 da norma 802 do IEEE possui uma grande quantidade de grupos de trabalho atuando sobre especificações e melhoramentos no padrão sobre redes locais *wireless*. Algumas destas normas são particularmente importantes, notadamente do ponto de vista das redes com infra-estrutura e demandas mais complexas. A norma IEEE 802.1x não pertence à família 802.11, mas é essencial no contexto de segurança de redes *wireless* corporativas. Em seqüência, são feitos breves comentários sobre a IEEE 802.11i (segurança) e a IEEE 802.11s (redes *mesh*).

Padrão IEEE 802.1x

Os padrões IEEE 802.1x e IEEE 802.11i estão relacionados à segurança de redes. O padrão 802.1x, que não deve ser confundido com 802.11x, um indicador genérico da família de padrões *wireless* 802.11, é um padrão de autenticação baseado no EAP (*Extensible Authorization Protocol*) e no uso de servidor de autenticação AAA (*authentication, authorization, accounting*). O 802.1x compõe uma parte importante das propostas do IEEE 802.11i para aperfeiçoamento da segurança e pode ser aplicado a redes locais *wireless* baseadas em 802.11*a*, *b*, *g* ou *n*.

Com o EAP, é possível a utilização de diversos métodos de autenticação, como *token cards*, *passwords* do tipo *OTP* (*one time passwords*), certificados digitais etc. O problema na escolha do método é garantir a autenticação mútua. Se a autenticação é unidirecional, feita somente pelo servidor de autenticação, permite-se ataques do tipo "homem no meio", entre a estação de trabalho e o AP (interceptando a informação de autenticação enviada e usando-a para acesso à rede sem fio) [11][12].

O 802.1x [13] é um padrão que gerencia o acesso a rede através de controle de porta. É necessária uma autenticação do usuário para que o acesso à rede seja franqueado. Os elementos que compõem uma instalação com o padrão 802.1x são

o suplicante (cliente que deseja ser autorizado a obter acesso à porta controlada), o autenticador (normalmente o próprio Access Point que interliga a rede sem fio à rede cabeada) e o servidor de autenticação (tipicamente, um servidor RADIUS).

A Figura 4 apresenta o processo de autenticação numa rede com padrão 802.1x. Uma troca de mensagem de autenticação pode ser iniciada tanto pelo autenticador (AP), como pelo suplicante (estação do cliente). No processo, os passos iniciais (1 a 3) estão relacionados ao estabelecimento e reconhecimento da identidade do suplicante, em seguida (4 a 6), à autenticação. O passo 7 (acesso liberado) só ocorre se a autenticação foi bem sucedida. As comunicações entre o suplicante e o autenticador são feitas em frames EAPOL (EAP over LAN) e as efetuadas entre o autenticador e o servidor de autenticação em frames EAP.

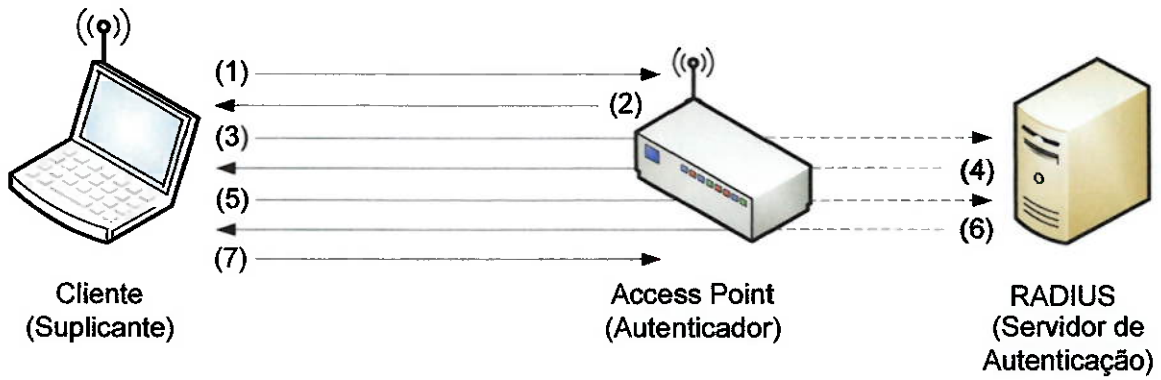


Figura 4 – Processo de autenticação numa rede com 802.1x
Fontes: Padrão IEEE 802.1x [13], 802.1x White Paper [14]

Numa rede local *wireless*, utilizando-se a autenticação padrão 802.1x, a tentativa de acesso de um cliente seguirá a seguinte seqüência:

Estado inicial da porta (localizada no AP) - fechada

(1) O cliente envia pedido de autenticação ao AP

(2) O AP responde pedindo a identidade do cliente

(3) O cliente envia sua identificação que é redirecionada pelo AP ao servidor de autenticação

(4) O servidor de autenticação verifica a identidade do cliente e envia uma mensagem de requisição de *password* (desafio)

(5) O cliente envia ao servidor de autenticação suas credenciais de autenticação como resposta ao desafio

(6) O servidor de autenticação envia uma resposta (sucesso ou fracasso) ao cliente, através do autenticador. Se sucesso, o AP abre a porta, se fracasso, ela é mantida fechada.

(7) Se a autenticação foi aceita o cliente utiliza o acesso através da porta controlada. O cliente encerra a sessão através de uma mensagem de *logoff*. Esta é enviada ao AP que, imediatamente, fecha a porta novamente.

O servidor de autenticação RADIUS (*Remote Authentication Dial In User Service*), ilustrado na Figura 7, é um protocolo cliente/servidor, originalmente desenvolvido como produto comercial pela empresa Livingston Enterprises. Posteriormente, foi publicado como RFCs da ISOC (RFC 2138 – Especificação do RADIUS e RFC 2866 – Padrão de auditoria do RADIUS) [15]. Este protocolo, do tipo AAA (*authentication, authorization, accounting*)[2], é composto por dois módulos distintos e complementares: servidor de acesso à rede (NAS) e servidor RADIUS e é usado para autenticação de usuários através da verificação de identidade e senha fornecidas por estes.

Padrão IEEE 802.11i

O padrão IEEE 802.11i, finalizado e publicado em 2004, é um padrão desenvolvido com o intuito de aperfeiçoar a segurança do padrão 802.11 e recuperar a imagem comprometida pelas fraquezas do WEP, particularmente as vulnerabilidades da criptografia utilizada pelo protocolo. Para isso, ele implementa o protocolo WPA2 (uma versão completa do WPA, que era seu draft) e utiliza

[2] Servidor **AAA** (***A**uthentication **A**uthorization **A**ccounting*). Servidor de rede usado para controle de acesso. *Authentication*- identifica o usuário.*Authorization*- implementa políticas que determinam quais recursos e serviços um usuário válido pode acessar. *Accounting* - mantém registro de tempo e recursos de dados usados para análise e faturamento. Fonte: PC Magazine Encyclopedia. Disponível em: <http://www.pcmag.com/encyclopedia_term/0,2542,t=AAA+server&i=37311,00.asp>

criptografia com AES (*Advanced Encryption Standard*). Oferece suporte a *roaming* e utiliza o sistema de autenticação do padrão 802.1x [16].

Padrão IEEE 802.11s

O padrão IEEE 802.11s, em desenvolvimento, prevê a criação de especificações para redes locais *wireless* '*mesh*', ou "em malha". Este tipo de rede se propõe a oferecer uma alternativa para o aumento da complexidade causado pelo grande crescimento da demanda por cobertura WLAN e conseqüentemente da quantidade necessária de APs para suportá-la. No contexto das redes locais sem fio, as redes locais em malha são uma derivação das redes *ad-hoc* e, assim como estas, tem seus elementos interconectados entre si via *wireless,* de forma independente de infra-estrutura. Não contando com uma infra-estrutura centralizada, os próprios nós da rede (MPs, ou *Mesh Points*), sejam eles APs (MAPs, ou *Mesh* APs), ou estações (MSTAs, ou *Mesh* STAs), assumem a função de roteadores dos pacotes de informação para os outros elementos da rede. O *mesh portal* é um MP que faz a conexão entre a rede *mesh* e a Internet, através de uma infraestrutura cabeada, enquanto que o *gateway* MP é o responsável pela interligação *wireless* de duas diferentes redes *mesh* [17].

2.1.5 Redes locais *wireless* no ambiente corporativo

Como visto anteriormente, as redes locais *wireless* compõem-se de alguns elementos mínimos típicos. Numa rede no modo infra-estrutura, uma BSS deve conter, no mínimo, uma estação (STA), um ponto de acesso (AP) e uma conexão deste à infra-estrutura externa à célula (esta normalmente suportada por um roteador).

No ambiente doméstico, um único equipamento integrado normalmente supre todas as necessidades de acesso, oferecendo tanto a conexão *wireless* (WLAN), como a parte WAN (Internet) e, muitas vezes, também um circuito LAN. No ambiente corporativo parte das funções envolvidas são distribuídas por diferentes servidores,

muitas vezes não dedicados exclusivamente ao atendimento da infra-estrutura de rede *wireless*.

Na Figura 5, estão representados os componentes físicos responsáveis pelo suporte a uma rede *wireless* protegida, num ambiente corporativo.

O esquema, adaptado de *Securing Wireless LANs with Certificate Services* [18], apresenta os componentes físicos de uma rede *wireless* simples, padrão 802.1x, cujo conjunto será definido como o contexto para o desenvolvimento do presente trabalho. Neste desenho, as linhas sólidas entre componentes apenas indicam que há relacionamentos entre eles.

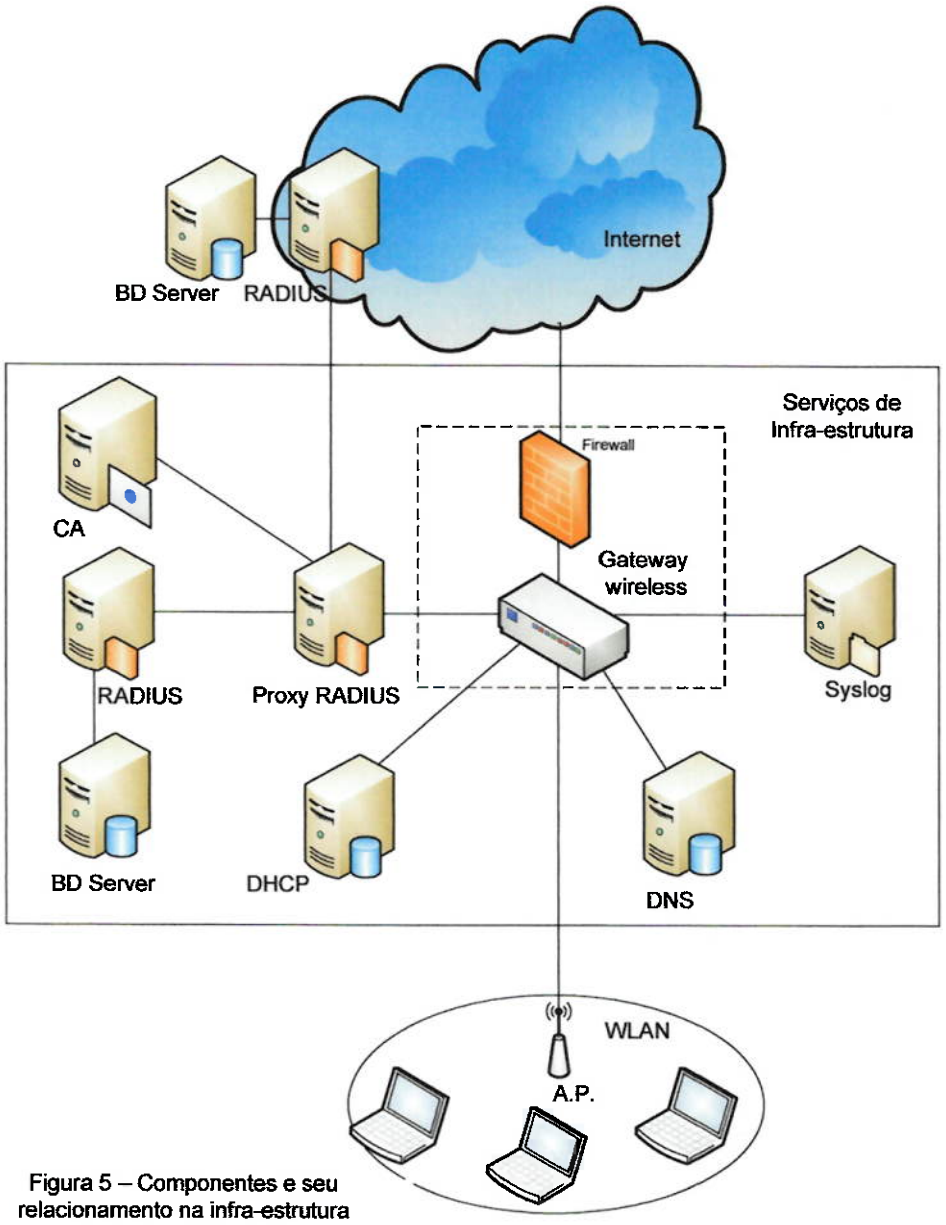


Figura 5 – Componentes e seu relacionamento na infra-estrutura

Pode-se observar a representação de três áreas bem delineadas:

- "Internet", representada pela nuvem;

- O bloco denominado "Serviços de infra-estrutura", representado pelo retângulo maior, contendo dois conjuntos de elementos: os componentes que já fazem parte da infra-estrutura central da organização (serviços de rede e diretório existentes e que atendem, também, outros sistemas) e uma área central, hachuriada, onde está representado o *gateway wireless*.[3]

- O terceiro bloco, denominado "WLAN", contém os *Access Points (APs)* e os clientes sem fio, componentes que ficam situados em localidade física remota.

Um detalhe refere-se aos componentes representados dentro da área hachuriada. O componente "*gateway wireless*", neste contexto, pode ser um elemento integrado com um *firewall*[4] numa mesma caixa (*in-a-box*)[5], ou, dependendo da solução adotada, o *firewall* pode ser um componente externo. Este *firewall* não é o da infra-estrutura central da organização. Ele opera dedicado ao *gateway* e possui uma gama limitada de recursos. A configuração apresentada na Figura 5, refere-se a uma instalação mínima, adotada apenas para facilitar o entendimento nesta apresentação. O bloco "WLAN", na prática, costuma conter vários APs e, além disso, é comum existirem vários blocos como este numa única planta de infra-estrutura. Numa configuração real, costuma-se considerar, no mínimo, um bloco "WLAN" para cada edificação. O mesmo se aplica aos componentes da estrutura central, o bloco "Serviços de infra-estrutura". Apesar de ser uma área central única, o número de componentes varia em função do porte da instalação a ser atendida. Em particular, para cada bloco "WLAN", há um *gateway wireless* previsto.

---

[3] Dispositivo de rede que roteia pacotes de uma rede WLAN para outra rede, tipicamente, uma rede WAN cabeada. Vide: <http://en.wikipedia.org/wiki/Wireless_gateway>.

[4] No ponto da rede em que está instalado, este elemento implementa uma política de segurança e, através desta e por intermédio de filtros de pacotes, controla o tráfego de dados entre ambos segmentos ou redes distintas, impedindo a passagem de acessos não autorizados. Vide Wikipedia em: <http://en.wikipedia.org/wiki/Firewall>.

[5] Sobre esta característica é oportuno lembrar que, atualmente, significativa parte dos equipamentos *wireless* para aplicação doméstica contém, numa mesma caixa física, o AP, o *gateway* (roteador) e, freqüentemente, também, um *firewall* com alguns recursos para filtragem.
Já *gateways* corporativos são equipamentos de maior porte, adequados para acomodar uma grande quantidade de conexões de APs externos e que podem oferecer acesso direto a servidores de autenticação, entre outros serviços incorporados.

Os componentes considerados, representados na Figura 5 por ícones de servidores, na prática podem ser executados como servidores dedicados ou como serviços, compartilhando servidores físicos com outras aplicações. Conforme já comentado, há várias soluções disponíveis no mercado para a função de *gateway wireless*. Num ambiente corporativo pode se encontrar servidores genéricos com softwares aplicativos específicos para dotá-los desta capacidade ou, então, '*appliances*'[6] dedicados para esta função.

Descrição sumária dos componentes:

Access Points: dispositivos que interfaceiam a rede cabeada com uma rede sem fio.

Gateway wireless: dispositivo que providencia a autorização para que uma solicitação do AP seja convertida numa sessão na Internet.

RADIUS: servidor que providencia a autenticação do usuário junto a um servidor de banco de dados que contém o cadastro do usuário.

Proxy RADIUS: um servidor ou um serviço de um servidor RADIUS, que providencia contato com outros servidores RADIUS (normalmente existentes em localidades remotas) em busca de autenticação de usuários.

BD: banco de dados de registros de usuários.

DHCP: Protocolo para configuração dinâmica de hosts, fornece endereços IP e outros parâmetros de configuração para clientes de rede.[7]

DNS: Sistema de gerenciamento de nomes hierárquico e distribuído que tem por função resolver nomes de domínios em endereços de rede (IPs). Um servidor DNS é responsável pela tradução de nomes no formato FQDN ('*Fully Qualified Domain Name*', ou nome completo do host no domínio), em endereços IP e vice-versa, com a finalidade de possibilitar identificar a rede ou o domínio do host, respectivamente.[8]

---

[6] *Appliance* é um equipamento desenvolvido e configurado para executar uma função específica dentro de um sistema. Este equipamento é usualmente baseado em um produto de software de uso genérico, porém otimizado para integrar somente os componentes necessários à sua aplicação-alvo. É a integração harmoniosa entre software e hardware. Fonte:<http://pt.wikipedia.org/wiki/Appliance>.

[7] Vide Wikipedia em: <http://pt.wikipedia.org/wiki/dhcp>.

[8] Vide Wikipedia em: <http://pt.wikipedia.org/wiki/dns>.

SysLog: servidor de *logs*. Armazena trilhas de auditoria e *logs* de eventos gerados por outros servidores.

CA: Certificate Authority, servidor responsável pela emissão de certificados digitais, no caso, uma autoridade de certificação interna (somente no âmbito da organização).

A Figura 6, também representa o modelo físico deste ambiente. Entretanto, além dos componentes vistos no diagrama da Figura 5, foram acrescentados os segmentos de rede envolvidos, permitindo a sua visualização.

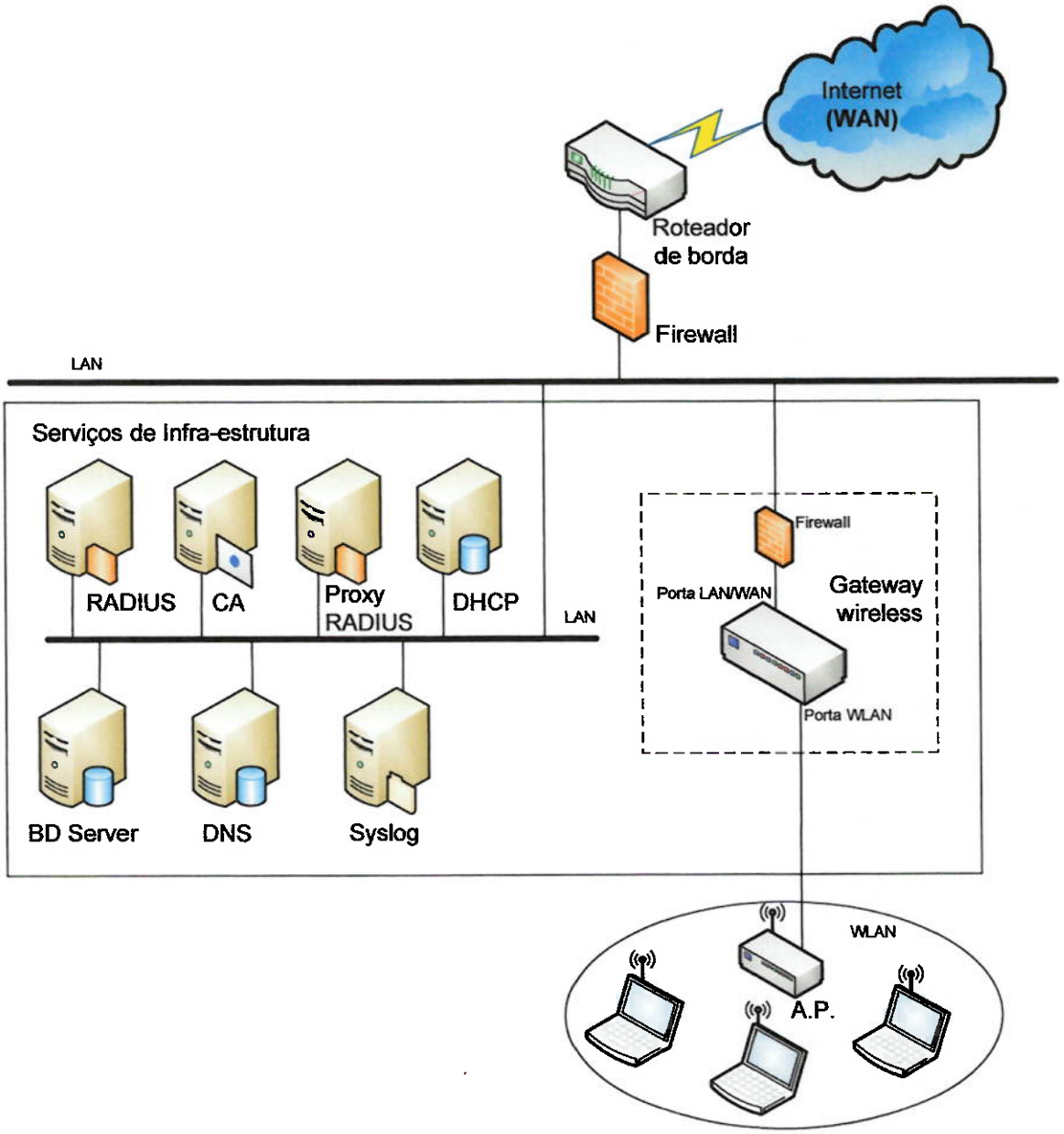


Figura 6 - Exemplo de rede local *wireless* corporativa baseada em 802.1X

Aqui, já fica nítida a existência de três segmentos distintos de rede (WAN, LAN e WLAN), os quais são devidamente segregados, por medidas de segurança, quando num ambiente de produção.

Este lay-out pode variar um pouco, mas é importante notar que o segmento WLAN tem um único ponto de contato com as demais redes e equipamentos da infra-estrutura e este contato é feito por intermédio do *gateway wireless*.

Um novo componente, o roteador, aparece representado na fronteira entre a rede interna da organização e a Internet. Os roteadores são equipamentos que trabalham na camada de rede, interconectando duas ou mais sub-redes (diferentes prefixos de endereços IP).[9] No contexto de empresa, o roteador, da mesma forma que o *gateway wireless* descrito na página 27, pode ser implementado sobre um servidor genérico com software aplicativo, ou ser um equipamento (*appliance*) especificamente construído para esta finalidade. Outro componente que agora aparece mais de uma vez na ilustração é o *firewall*. Este também pode ser executado sobre um servidor genérico através de software específico ou ser um hardware dedicado e altamente customizado.

[9] Vide Wikipedia em: <http://pt.wikipedia.org/wiki/Roteador>.

2.2 SEGURANÇA DA INFORMAÇÃO E AS NORMAS CONCERNENTES

De acordo com a norma ABNT NBR ISO/IEC 27002:2005 [1], segurança da informação é a proteção da informação contra ameaças que possam comprometer a continuidade do negócio. Através da implantação e gestão de controles adequados deve-se procurar minimizar os riscos e maximizar os resultados que este ativo pode produzir para a organização.

Os atributos básicos da segurança da informação, conhecidos pelo acrônimo 'CIA', referem-se às características essenciais que precisam ser consideradas e preservadas no ambiente informacional: confidencialidade, integridade e disponibilidade (na versão original, o "A", de *availability*).

Pelo vocabulário padronizado da norma ISO/IEC 27000 [19] confidencialidade significa que a informação não estará disponível a indivíduos, entidades ou processos que não estejam devidamente autorizados a acessá-la; integridade é a propriedade de preservar a precisão e inteireza do ativo informacional e disponibilidade, a propriedade deste ativo estar disponível sempre que demandado pelo usuário autorizado.

A norma ISO 27002 é, hoje, amplamente aceita como um padrão para a gestão da segurança da informação e adotada por organizações de todo o mundo [20][21].

Nos dias atuais, esta norma faz parte da série ISO 27000 ('ISO27K'), normas internacionais ISO que estão sendo compostas como uma família de padrões orientados à gestão da segurança da informação. No Anexo 1, página 78, é apresentado um quadro com uma relação atualizada desta família de normas e respectivos status.

Historicamente, todas estas normas têm como ancestral comum a norma britânica BS-7799. Nos Quadros 4 e 5, procurou-se sintetizar a evolução das normas internacionais de segurança da informação, das iniciativas precursoras que levaram à BS-7799 até sua transformação nas atuais versões da ISO/IEC 27002:2005 e ISO/IEC 27001:2005.

Título	Conteúdo	Responsável	Informações pertinentes	Publicado
Information Security Policy Manual	Enfoque em conceitos de segurança para mainframes	Royal Dutch/Shell Group	Documento interno da Shell doado para comunidade	Meados de 1980
DTI CCSC User's Code of Practice	Guia de segurança da informação para os membros da DTI CCSC	UK Department of Trade and Industry's Commercial Security Centre (DTI CCSC)	Desenvolvido tendo por base o documento da Shell	1989
BSI-DISC PD003:1993 - DTI Code of Practice for Information Security Management	Código de práticas para a gestão da segurança da informação	UK Department of Trade and Industry's Commercial Security Centre (DTI CCSC)	Pre-release da primeira norma oficial de segurança da informação britânica . Foi distribuído como BSI-DISC PD003 (British Standards Institution - Delivering Information Solutions to Customers - Public Document 003)	1993
BS 7799:1995	Código de práticas para a gestão da segurança da informação	BSI (British Standards Institute)	Versão inicial como norma oficial britânica	1995
BS 7799 Part 1:1998	Código de práticas para a gestão da segurança da informação	BSI (British Standards Institute)	Renomeada como "Parte 1" quando do lançamento da 2ª. Parte, referente a sistema de gestão e padrão de certificação	Fev/1998
BS 7799 Part 1:1999	Código de práticas para a gestão da segurança da informação	BSI (British Standards Institute)	Versão revista e reimpressa	Abr/1999
ISO/IEC 17799:2000	Código de práticas para a gestão da segurança da informação	ISO/IEC JTC1/SC27	Primeira versão ISO/IEC da BS7799 Parte1:1999. Considerada "ponto de partida" pela comunidade ISO/IEC (não suportada completamente nesta versão)	Dez/2000
ISO/IEC 17799:2005	Código de práticas para a gestão da segurança da informação	ISO/IEC JTC1/SC27	Revisão da versão ISO/IEC 17799:2000 com alterações significativas e alteração de formato	Jun/2005
ISO/IEC 27002:2005	Código de práticas para a gestão da segurança da informação	ISO/IEC JTC1/SC27	Versão atual da norma. Texto idêntico ao da ISO/IEC 17799:2005 Renomeado para compor a família 27000 de padrões da ISO/IEC	Jul/2007

Quadro 4 – Resumo histórico dos documentos que antecederam a Norma ISO/IEC 27002:2005
Fontes:[21] [22] [23] [24]

Título do documento	Conteúdo	Responsável pela sua produção	Informações pertinentes	Publicado
BS 7799 Part 2:1999	Especificação para sistemas de gestão de segurança da informação	BSI (British Standards Institute)	Padrão que especifica os requisitos do modelo de gerenciamento, objetivos e controles de um sistema de gerenciamento de segurança da informação. Adota um esquema de certificação que opera de forma semelhante a ISO 9000	Fev/1998
BS 7799 Part 2:2002	Especificação para sistemas de gestão de segurança da informação	BSI (British Standards Institute)	Revisão da versão de 1999, incorporando, principalmente, o ciclo de Deming (PDCA)	Set/2002
ISO/IEC 27001:2005	Requisitos para sistemas de gestão de segurança da informação	ISO/IEC JTC1/SC27	Versão BS 7799 Part2:2002 adotada pela ISO/IEC em 2005. Versão atual da norma.	Out/2005

Quadro 5 – Resumo histórico dos documentos que antecederam a Norma ISO/IEC 27001:2005
Fontes:[21][22][23][24]

O desenvolvimento de padrões dentro da ISO é conduzido por comissões técnicas mistas. No caso de tecnologia da informação, que abrange segurança da informação, este trabalho é efetuado pela ISO/IEC JTC 1 (Comissão Técnica Mista 1). Em 1988, foi constituída a SC267, uma subcomissão para cuidar especificamente de técnicas de segurança [25].

No Brasil, a Associação Brasileira de Normas Técnicas (ABNT) é o Fórum Nacional de Normalização (órgão responsável pela normalização técnica no país) e representante exclusiva da ISO (International Organization for Standardization). As normas correntes, ABNT NBR ISO/IEC 27001:2006 e ABNT NBR ISO/IEC 27002:2005, foram elaboradas no Comitê Brasileiro de Computadores e Processamento de Dados (ABNT/CB-21), pela comissão de Estudos de Segurança Física em Instalações de Informática (CE-21:204.01) [26].

Um breve histórico das versões brasileiras das normas de segurança da informação está sumarizado no Quadro 6.

Título do documento	Conteúdo	Informações pertinentes	Publicado
NBR ISO/IEC 17799:2000	Código de práticas para a gestão da segurança da informação	Primeira versão brasileira da norma ISO, disponibilizada para consulta pública em abril de 2001. Homologada em setembro do mesmo ano	Set/2001
ABNT NBR ISO/IEC 17799:2005	Código de práticas para a gestão de segurança da informação	Segunda edição atualizada da norma brasileira. Entrou em vigor em 30 de setembro de 2005. Totalmente equivalente à ISO/IEC 17799:2005	Ago/2005
ABNT NBR ISO/IEC 27001:2005	Requisitos para sistemas de gestão da segurança da informação	Publicada em 31.03.2006 e válida a partir de 30.04.2006. É uma tradução idêntica da ISO/IEC 27001:2005.	Mar/2006
ABNT NBR ISO/IEC 27001:2006	Requisitos para sistemas de gestão da segurança da informação	Publicada em 28.08.2006. É uma versão corrigida da ABNT NBR ISO/IEC 27001:2005. Versão atual da norma.	Ago/2006
ABNT NBR ISO/IEC 27002:2005	Código de práticas para a gestão de segurança da informação	Totalmente equivalente à versão corrigida de 02.07.2007 da ABNT NBR ISO/IEC 17799:2005. Versão atual da norma.	Jul/2007

Quadro 6 – Resumo da evolução das versões brasileiras das normas de segurança da informação
Fontes: [2][26][27][28]

Em síntese, as diretrizes e informações explicativas para gestão da segurança da informação da antiga BS7799-Parte1 são suportadas, hoje, pela ISO 27002 – Código de Prática para a Gestão de Sistemas de Informação e o modelo para organizações elaborarem e executarem um sistema de gestão da segurança da informação, conteúdo da antiga BS7799-Parte2, é o escopo da atual ISO 27001-*Information Security Management System* (ISMS) – Requisitos [29]. No Brasil, a ABNT NBR ISO/IEC 27002:2005 faz correspondência exata com a ISO 27002 e a ABNT NBR ISO/IEC 27001:2006, com a ISO 27001. Em função desta equivalência, para os propósitos do presente trabalho, foi adotada a denominação brasileira destas normas.

2.2.1 Norma ABNT NBR ISO/IEC 27001:2006

O objetivo básico da norma ISO/IEC 27001 é o estabelecimento dos requisitos para a construção, implementação e operação de um sistema de gestão de segurança da informação, SGSI, com enfoque na gestão de riscos para o negócio e organização.

Conforme indicado no resumo apresentado no Quadro 5, derivou-se da norma britânica BS-7799, Parte2, posteriormente transformada em norma internacional ISO. Criada, originalmente, como um complemento ao código de práticas da BS-7799, que carecia de um arcabouço sobre o qual se pudesse implementar um processo de certificação, para este fim, incorporou uma metodologia semelhante ao da ISO 9000.

De acordo com Gamma [24] a BS 7799-Parte 2, criada em meados de 1988, visava detalhar o que um auditor precisa fazer para garantir certificar com sucesso a segurança da informação de uma organização. O que ocorreu, paralelamente, foi que, com este documento, o conceito de um ISMS tornou-se mais amplo que o contexto original de implementação do código de práticas (BS-7799-Parte 1), passando, mesmo, a ser até mais importante que este. Ao incluir mecanismos de *feedback* permitiu aos gestores monitorarem e controlarem determinados eventos e comportamentos de forma a minimizar riscos e garantir a manutenção dos requisitos de segurança. A partir da versão 2002 da BS7799-Parte 2, com a inclusão do ciclo PDCA, melhorou-se a eficiência dos procedimentos que permitem aperfeiçoar a organização do sistema de informação, em particular na avaliação de riscos e no projeto, implementação e gestão de segurança. Não à toa, esta versão foi publicada praticamente na mesma data que as diretrizes da OECD - ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, uma vez que se alinha com seus princípios [30].

As Diretrizes da OECD para a segurança de sistemas de informação e redes, publicado em julho de 2002, cujo subtítulo é "Em direção a uma cultura de segurança", compõem-se de uma série de princípios cujo objetivo é nortear as implementações da área de TI: conscientização, responsabilidade, resposta, ética,

democracia, avaliação de riscos, arquitetura e implementação de segurança, gestão de segurança e reavaliação.

A relação entre a ISO/IEC 27001 e os princípios da OECD é tão estreita que uma tabela com correspondências entre princípios da OECD, a fase correspondente no processo PDCA e o requisito equivalente no SGSI da ISO/IEC 27001 foi incluída no documento desta norma (Anexo B da ISO/IEC 27001).

2.2.2 Norma ABNT NBR ISO/IEC 27002:2005

A principal finalidade desta norma é nortear a gestão da segurança da informação no ambiente das organizações.

Para isso apresenta um conjunto de controles que considera "como princípios básicos para a gestão da segurança da informação", aplicáveis na maioria dos ambientes e organizações.

No documento, estes controles são distinguidos em dois grupos:

- Controles considerados essenciais, do ponto de vista legal, relacionam-se diretamente à propriedade e privacidade: "proteção de dados e privacidade de informações pessoais", "proteção de registros organizacionais" e "direitos de propriedade intelectual".

- Controles relacionados às práticas para segurança da informação: "documento de política de segurança de informação", "atribuição de responsabilidades para a segurança da informação", "conscientização, educação e treinamento em segurança da informação", "processamento correto nas aplicações", "gestão de vulnerabilidades técnicas", "gestão da continuidade do negócio", "gestão de incidentes de segurança da informação e melhorias".

2.3 *CHECKLIST*

Checklist, ou "lista de verificação", como é denominada literalmente em português, conforme a definição de dicionários online consiste "numa lista de coisas a serem verificadas ou feitas".[10]

Para os efeitos deste trabalho, vamos utilizar indistintamente os termos "lista de verificação" e "*checklist*" para designar o mesmo recurso, de forma a respeitar a forma original usada na literatura citada. Um *checklist* é composto de uma lista de itens chamados "*checkpoints*", em português, "pontos de verificação".

O PMBOK, como documento orientado à gestão de projetos, define listas de verificação como "Itens listados juntos para facilitar a comparação ou para garantir que ações associadas a eles sejam gerenciadas adequadamente e não sejam esquecidas" [31]. Os *checklists* são muito utilizados em programas de qualidade, notadamente no processo de controle da qualidade.

O exemplo típico de "*checklist*", contudo, é o utilizado pelos pilotos de aviões nos procedimentos de vôo. De acordo com um documento da Federal Aviation Administration [32] os *checklists* têm sido a base da padronização e segurança da cabine para os pilotos. Em seu capítulo 10, dedicado aos métodos de projeto destes recursos, é feita uma distinção entre dois métodos específicos de *checklist* utilizados neste ambiente: o método "*challenge-do-verify*" (CDV), usado em tripulações com mais de um indivíduo (também conhecido como método 'desafio-resposta') e o método "*do-verify*" (DV). No método 'desafio-resposta', que deve ser aplicado metodicamente e sem variação de seqüência, um dos tripulantes faz o desafio (lê, em voz alta, um item da seqüência da lista de verificação) antes que a ação seja iniciada, em seguida, um segundo tripulante aciona a ação, observando visualmente e informando verbalmente seu efeito (que é anotado pelo primeiro tripulante). E, assim, sucessivamente até o final da lista de verificação. Este método,

---

[10] Free Online Dictionary (http://www.thefreedictionary.com/checklist):
check·list (chklst) n. A list of items to be noted, checked, or remembered.
Babylon's free dictionary (http://dictionary.babylon.com/checklist):
checklist n. list of things or tasks to be done or checked; list of names to be checked or consulted.
Merriam-Webster Online Dictionary (http://www.merriam-webster.com/dictionary/CHECKLIST):
check·list. n (1853): a list of things to be checked or done <a pilot's checklist before takeoff>; also : a comprehensive list.

deliberadamente sistemático, provê confirmação passo a passo da verificação. O segundo método, o "*do-verify*" (DV), não utiliza o desafio e permite que as verificações sejam efetuadas seguindo fluxos-padrão de memória, de forma a certificar séries de ações rapidamente. Após todos os itens da seqüência terem sido executados, a lista de verificação é lida novamente enquanto cada item é verificado. Segundo o documento citado, este método, possui um alto risco de falha de itens e não é recomendado para substituir o método CDV onde este é aplicável. Tradicionalmente, nos *checklists* de condições normais ambos são comumente utilizados.

Esta distinção entre os dois métodos evidencia uma característica importante, relacionada com a forma como a lista de verificação vai ser executada. Quando o usuário vai lendo a lista de itens e executando as ações uma a uma, ele está utilizando-a como uma "*do list*" (atividades a fazer). Quando ele executa todas as atividades de um grupo e, então, vai verificar a lista e rever todas as ações para se certificar de não ter esquecido nada, ele está utilizando-a como um "*checklist*". O *checklist*, portanto, é uma lista de itens composta por tarefas que são verificadas, uma a uma, para se obter a certeza de que estão completas ou foram executadas [33].

A finalidade básica do *checklist* é manter o usuário no foco/objetivo [34]. É possível concentrar o foco nas atividades prioritárias, sem perda de controle sobre o que está pendente [33]. O objetivo principal não é detalhar cada processo/ atividade, mas servir de guia para o profissional que o está utilizando [35]. Para Scriven [36] os *checklists* são dispositivos mnemônicos. Por isso, eles reduzem as chances da ocorrência de esquecimento de algo importante, reduzindo, então, os erros de omissão se alguém inclui decisões baseadas nos seus resultados. Servem, portanto, como auxílio à memória para garantir que os itens/eventos importantes tenham sido considerados [37]. Muitos processos não requerem um *checklist*, entretanto, ele é muito útil nas situações em que se tenham operações complexas, com muitos itens, em que partes podem ser esquecidas [33].

Um dos benefícios possíveis da adoção do *checklist* é a possibilidade de padronização e a simplicidade. Permite a inclusão de novos atributos, atividades e itens que podem ser adicionados a qualquer tempo, sem prejuízo do andamento.

Além disso, auxilia no aprendizado de novas pessoas (a assimilação das relações entre grupos e itens é facilmente absorvida) [33].

Em termos de implementação, os *checklists* costumam ser programados para receber apenas um "tique" (executado/concluído) como resposta a cada item (*checkpoint*). Esta é a forma clássica, os itens representam características que podem estar ou não presentes ("ticado"/não "ticado"). Outras aplicações, entretanto, utilizam respostas "Sim/Não", "C/I" (Completo/Incompleto), ou mesmo valores de uma escala pré-determinada (escalas de Likert, quando em aplicações na área de controle de qualidade) [37][38].

Para o desenvolvimento de um novo *checklist*, Stufflebeam [39], recomenda que se faça uma atividade exploratória, criando uma lista de *checkpoints* candidatos. Os itens (*checkpoints*) têm de ser criados de forma a serem coerentes com o propósito do *checklist* e, seu conjunto, deve compor um conjunto consistente.

De acordo com Paiva [35], a descrição de cada item deve ser suficientemente curta para que o *checklist* seja compacto, mas deve ser suficientemente detalhada para que o profissional que vai aplicá-lo saiba exatamente do que se trata. Numa eventual etapa seguinte de avaliação, um profissional bem treinado deve saber executar o processo com base na descrição do *checkpoint*.

Estes itens podem ser questões ou ações a realizar [37] e, para a ferramenta ser eficaz, eles tem de estar voltados para resultados [34]. Na sua criação, deve-se procurar utilizar definições completas, mas tão curtas quanto possível [34]. Eles têm de ser tão detalhados quanto for relevante para o controle que vai ser efetuado e devem estar classificados dentro de alguma ordem lógica para quem vai executá-los. Os itens devem ser claros para quem for utilizá-los e não deixarem margem à dúvida ou má interpretação de seu conteúdo [37].

Quando de sua elaboração, é possível que o *checklist* cresça por um tempo (em número de itens) até que se estabilize. É preciso cuidado na definição destes, para que os resultados sejam utilizáveis e confiáveis. Deve-se lembrar que este instrumento tem de ser usado e testado para que possa se tornar efetivo [33][37].

O site *Evaluation Checklist Project* do *The Evaluation Center* da *Western Michigan University*[11] contém informações e artigos relacionados a construção e avaliação de *checklists*. Num destes trabalhos, Bichelmeyer [40] apresenta um *checklist* para formatação de *checklists*, onde categoriza em cinco grupos os itens que devem ser considerados quando do projeto de novas listas: contexto, conteúdo, estrutura, imagem (se necessário) e usabilidade.

2.3.1 *Checklists* e normas de segurança da informação

O uso do *checklist* em aplicações de normas de segurança da informação não é inédito. Considerando apenas as versões mais recentes destas normas, ou seja a ISO 27002 (denominação corrente) e a 17799 (denominação imediatamente anterior) e recorrendo a uma pesquisa no Google, utilizando como chave de busca as combinações "*checklist*"+"ISO 27002" e "*checklist*"+"ISO 17799", foi possível obter registros de diversas aplicações deste recurso associadas a práticas de implantação de normas de segurança da informação[12], em sua maioria, em aplicações de auditoria, para fins de verificação de conformidade ou '*gap analysis*'.[13]

Algumas das aplicações pesquisadas e suas características principais:

- O SANS Institute possui um *checklist* publicado com o título "Audit Check List for ISO 17999:2005" [41]. A cada um dos controles da norma 17799:2005 (os mesmos controles da norma 27002:2005, conforme visto anteriormente) aplica-se uma "Audit question" com dois possíveis campos para resposta: "Findings" e "Compliance" .

- O "Router Technical Audit Checklist" é um *checklist* baseado nos controles da ISO/IEC 27001, para auditoria de roteadores Cisco [42]. Nesta aplicação, a cada

---

[11] Disponível em: (http://www.wmich.edu/evalctr/checklists/)

[12] Nesta pesquisa foram examinados os 120 documentos iniciais de um total de 40.000 registros recuperados (aproximadamente 10.000 p/ISO-27002 e 32.000 p/ISO-17799).

[13] *Gap* – intervalo, lacuna, espaço vazio. Em tecnologia da informação, um *gap analysis* é uma ferramenta de avaliação que pode ser usada para apontar quais requisitos estão sendo atendidos e quais não, ou, a diferença entre requerimentos estabelecidos e a condição da infra-estrutura existente. Fonte: http://searchcio-midmarket.techtarget.com/sDefinition/0,,sid183_gci831294,00.html

linha do documento uma característica técnica de configuração do equipamento está associada a um ou mais controles da norma relacionados a questões pertinentes de segurança. Um campo de respostas ("Findings") admite duas respostas possíveis (Yes/No), selecionáveis com um 'clique'. Como complemento, a cada registro, há um campo contendo a descrição do padrão e da melhor prática para aquela situação.

O site DesktopAuditing [43] é um repositório que contém cópias de dezenas de *checklists* baseados em normas, entre outras, na ISO 27001 e 27002. Estes recursos são orientados à avaliação de itens específicos. Exemplos: *ISO 27001 Checklist: Router Audit Program; Network Management Security Recommendation from ISO27002/27001; IT Security Incident Monitoring Templates; ISO 27001 Certification Documentation Checklist; ISO 27001 Security Compliances Checklist.*

O site ControlSCADA [44] também é um repositório que disponibiliza *checklists*, entre outros, *checklists* baseados nas normas 27001 e 27002 para a comunidade da Internet. Alguns exemplos: 'Data Center Security Audit Checklist'; 'Risk Assessment Audit Program Checklist'; 'Wireless Administrator Checklist'; 'ISO 27001/ISO17799 Wireless LAN Security Summary'.

Este último chamou a atenção pelo fato de tratar-se de um *checklist* específico para aplicação em controles de implantação de rede *wireless* e, portanto, de interesse para o presente trabalho. Buscas complementares permitiram identificar a fonte original ('*Wireless LAN Security Summary*'), como parte do documento 'Wireless Network Security. 802.11, Bluetooth and Handheld Devices.', publicado pelo NIST, National Institute of Standards and Technology, órgão do Departamento de Comércio do governo norte-americano, como '*Special Publication 800 48*', em novembro de 2002 [45]. Neste, '*Wireless LAN Security Summary*' é uma tabela com uma relação de 57 objetivos de controle (que o documento referencia como 'recomendações de segurança') e respectivas diretrizes, onde constam orientações focadas em segurança da informação para a implementação e configuração de redes locais wireless e seus elementos. O Anexo 4, na página 93, contém uma cópia completa da tabela. As recomendações abrangem tanto aspectos de configuração de APs e estações numa rede *wireless* quanto aspectos relacionados a política de uso destes recursos.

Em junho de 2008, como revisão do '*Special Publication 800 48*', o NIST publicou o '*Special Publication 800 48 rev. 1*', com o título 'Guide to Securing Legacy IEEE 802.11 Wireless Networks. Recommendations of the National Institute of Standards and Technology' [46]. Neste novo documento, são reforçadas as recomendações para tratamento das fragilidades do WLAN em redes legadas baseadas exclusivamente no 802.11, enquanto sugere a avaliação de produtos baseados no 802.11i como padrão de segurança para a migração destas ou para novas redes sem fio a serem implementadas.[14] Nesta revisão as recomendações integrantes da versão anterior estão atualizadas e complementadas, porém, na forma de texto dissertativo e não mais como uma lista de controles nos moldes de um *checklist*.

[14] Para as novas WLANs, sugere, também, seguir as recomendações do NIST *Special Publication 800-97* "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i", disponível em: http://csrc.nist.gov/publications/nistpubs/800-97/SP800-97.pdf

3 PROPOSTA DE *CHECKLIST* PARA VERIFICAÇÃO DA APLICAÇÃO DE CONTROLES DA NORMA ABNT NBR ISO/IEC 27002:2005 EM PROJETOS DE IMPLANTAÇÃO DE REDES LOCAIS *WIRELESS*

Do ponto de vista da tecnologia, após as atividades relacionadas à definição e especificação de todos os elementos físicos componentes de uma nova rede local *wireless* e a aprovação do projeto, pode-se passar para a fase de sua implementação. Contudo, esta rede não pode ser tratada apenas com esta visão. Ela tem de ser considerada, também, no contexto da segurança da informação. Para tal, os componentes desta rede terão de ser submetidos ao conjunto de regras e procedimentos que permitem proporcionar o alinhamento à política de segurança da informação adotada pela entidade e às normas nas quais esta se baseia.

A implantação de uma rede local *wireless* no ambiente de uma empresa que demanda uma grande área de cobertura ou que possui uma área com grande densidade de usuários, pode implicar na necessidade de um grande número de componentes, particularmente, APs e gateways. Outro requisito que pode somar complexidade a este cenário é a necessidade de provimento de acesso autenticado a várias diferentes comunidades de usuários (domínios de endereços distintos), o que pode demandar mais alguns componentes específicos (servidores RADIUS, *proxy* RADIUS, bancos de dados, servidores de certificado etc), além dos já considerados. Além destes, outros elementos complicadores, como por exemplo, as instalações a serem cobertas pela rede ocuparem várias edificações diferentes num campus, podem exigir o acréscimo de mais itens à lista de componentes. Assim, numa organização grande pode-se, facilmente, chegar a algumas dezenas de componentes num único projeto.

Numa situação como esta, onde muitos elementos compõem a infra-estrutura da nova rede, a aplicação de um *checklist* construído sobre um modelo tal como o '*Wireless LAN Security Summary*', conforme citado na página 41 ('ISO 27001/ISO17799 Wireless LAN Security Summary'), exige que se considere a rede toda como uma única unidade em observação. Assim, por exemplo, uma questão de *checklist* sobre o item 12 ("Os APs estão posicionados em áreas seguras para evitar

acesso físico não autorizado e manipulação por usuários?"), deve considerar todos os APs envolvidos no projeto. Desta mesma maneira, as respostas possíveis são: 'sim' (significando que 100% dos APs envolvidos atendem ao quesito), 'não' (se apenas um dos APs não atender ao quesito).

Neste capítulo é apresentada uma proposta de elaboração de um modelo de *checklist* que permite o acompanhamento e/ou verificação da aplicação dos controles e diretrizes do código de prática para a gestão de sistemas de informação em componentes individuais dos projetos de implementação de redes locais *wireless,* ao mesmo tempo em que permite manter todos os registros do mesmo item de controle visíveis ao usuário.

Para tal fim, descreve-se a proposição de desenvolvimento de dois elementos. O primeiro é um repositório de listas de itens de controle para componentes de redes *wireless*, conforme exemplo esquemático abaixo.

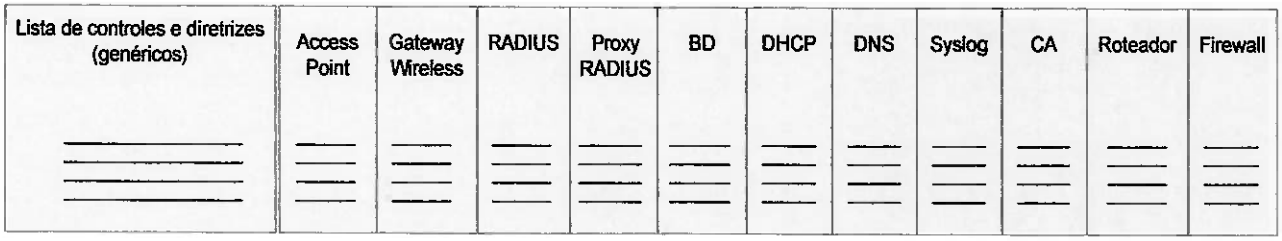


Figura 7 - Repositório de listas de itens de controle de componentes (em cada coluna, a estrutura de itens de controle de um componente)

O segundo é a produção de um modelo de *checklist* para ser populado posteriormente pelo usuário com colunas a serem extraídas do repositório acima, de acordo com os componentes necessários ao projeto a ser observado. A figura abaixo ilustra, de forma esquemática, este segundo produto.

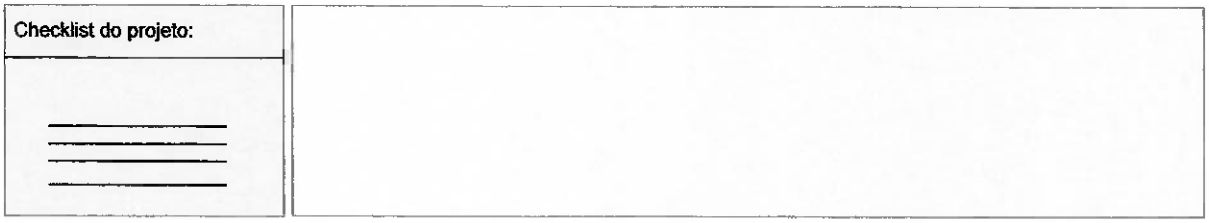


Figura 8 – Matriz para montagem de checklists pelo usuário

A Figura 9 exibe, num diagrama esquemático, o processo de criação do *checklist* utilizado para o desenvolvimento destes dois produtos.

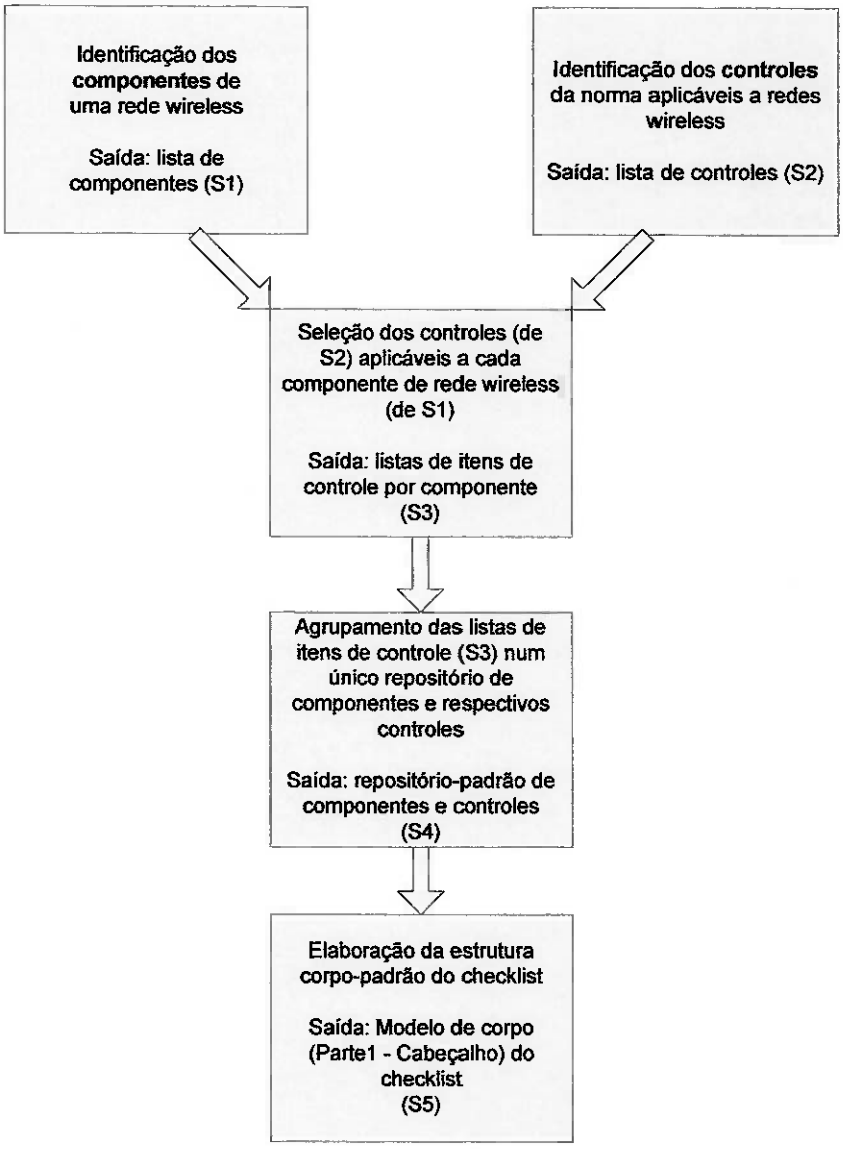


Figura 9 – Diagrama esquemático de criação do checklist

O diagrama acima sintetiza o que é tratado no capítulo 3 e que segue o seguinte roteiro: No item 3.1, é apresentado um contexto de rede local *wireless* corporativa típica, baseada no padrão 802.1x, a partir do qual é produzida uma lista de componentes (S1) para utilização como insumo das etapas seguintes. A seguir, no item 3.2, são identificados os controles de práticas de segurança da informação do corpo da norma ABNT NBR ISO/IEC 27002:2005 e gerada uma lista de controles (S2) para aplicação na seqüência do trabalho. No item seguinte, 3.3, os controles da

lista S2 são cotejados um a um frente a cada um dos componentes de S1, gerando como saída, um conjunto de listas de itens de controles, ou seja, uma lista de itens de controles para cada componente analisado (Listas S3). No item 3.4, é organizado um repositório-padrão de componentes e controles (S4), agregando as listas S3 produzidas na etapa anterior. No item 3.5, é produzida uma estrutura em duas partes do *checklist*-modelo (S5), que pode ser organizado posteriormente pelo usuário, de acordo com os elementos necessários para suas listas de verificação de implantação de projetos de redes locais *wireless*. Por fim, em 3.6, é apresentado um exemplo de preenchimento de um *checklist* com dados de um projeto de rede local sem fio hipotético.

3.1 SELEÇÃO DE COMPONENTES DE REDES LOCAIS *WIRELESS*

Como visto no item 2.1.5, as redes locais *wireless* implementadas em ambientes corporativos podem compor-se de vários elementos discretos distintos e não é incomum que estes elementos (ou parte deles) sejam suportados por servidores não dedicados exclusivamente ao suporte da infra-estrutura de rede local *wireless*. Baseado nos componentes físicos de uma rede local *wireless* corporativa apresentados no referido item, selecionou-se este conjunto de elementos no Quadro 7, como contexto para o desenvolvimento do presente trabalho.

Componentes selecionados
Access Point
Gateway wireless
RADIUS
ProxyRADIUS
BD
DHCP
DNS
SysLog
CA (Certificate Authority)
Roteador
Firewall

Quadro 7 - Componentes selecionados de uma rede *wireless* corporativa (S1)

3.2 DEFINIÇÃO DA LISTA DE CONTROLES DA NORMA ABNT NBR ISO/IEC 27002:2005 APLICÁVEIS A REDES LOCAIS *WIRELESS*

A segurança da informação é obtida, segundo proposto na própria norma ABNT NBR ISO/IEC 27002:2005, através da implementação de um conjunto de controles adequados. A norma não delimita o nível de detalhamento em que se deve analisar os recursos de processamento de informação (qualquer sistema de processamento de informação, serviço ou infra-estrutura, ou as instalações físicas que os abriguem), mas orienta o interessado a procurar o nível mais significativo para suas necessidades de forma a obter, como resultado, o controle efetivo da segurança da informação como um todo. Em seu capítulo introdutório são elencados alguns controles recomendados para nortear o início do trabalho de implementação da segurança da informação. Conforme visto no item 2.2, estes baseiam-se tanto em requisitos legais (em função da legislação aplicável), como em melhores práticas utilizadas de segurança da informação. O Quadro 8 apresenta uma relação parcial de seções, categorias e controles da norma ABNT NBR ISO/IEC 27002:2005 (para visualizar a lista completa, consulte a tabela apresentada no Anexo 2, na página 79, produzida com dados extraídos da norma).

Organização dos Controles da Norma ABNT NBR ISO/IEC 27002:2005 (continua)

No.	Seções, categorias e controles
5	**Política de segurança da informação**
5.1	**Política de segurança da informação**
5.1.1	Documento da política de segurança da informação
5.1.2	Análise crítica da política de segurança da informação
6	**Organizando a segurança da informação**
6.1	**Infra-estrutura da segurança da informação**
6.1.1	Comprometimento da direção com a segurança da informação
6.1.2	Coordenação da segurança da informação
6.1.3	Atribuição de responsabilidades para a segurança da informação
6.1.4	Processo de autorização para os recursos de processamento da informação
6.1.5	Acordos de confidencialidade
6.1.6	Contato com autoridades
6.1.7	Contato com grupos especiais
6.1.8	Análise crítica independente de segurança da informação

Quadro 8 - Organização dos Controles da Norma ABNT NBR ISO/IEC 27002:2005 (parcial)

(conclusão)

No.	Seções, categorias e controles
6.2	**Partes externas**
6.2.1	Identificação dos riscos relacionados com partes externas
6.2.2	Identificando a segurança da informação, quando tratando com clientes
6.2.3	Identificando segurança da informação nos acordos com terceiros
7	**Gestão de ativos**
7.1	**Responsabilidade pelos ativos**
7.1.1	Inventário dos ativos
7.1.2	Proprietário dos ativos
7.1.3	Uso aceitável dos ativos
7.2	**Classificação da informação**
7.2.1	Recomendações para classificação
7.2.2	Rótulos e tratamento da informação

Quadro 8 - Organização dos Controles da Norma ABNT NBR ISO/IEC 27002:2005 (parcial)

Para cada controle, a norma ABNT NBR ISO/IEC 27002:2005 apresenta um conjunto de recomendações na forma de diretrizes. O Quadro 9, à guisa de exemplo, apresenta uma relação parcial com alguns dos controles e respectivas diretrizes.

Controles e diretrizes da Norma ABNT NBR ISO/IEC 27002:2005

(continua)

No.	Controles	Diretrizes deste controle
5.1.1	Documento da política de segurança da informação	Definição do documento de políticas da organização contendo as metas globais, escopo e importância da segurança da informação; declaração de comprometimento da direção; estrutura para estabelecer os objetivos de controle incluindo estrutura de análise/avaliação e gerenciamento de risco; políticas, princípios, normas e requisitos de conformidade de segurança da informação; definição das responsabilidades gerais e específicas na gestão da segurança da informação.
5.1.2	Análise crítica da política de segurança da informação	Realização de análise crítica considerando: - Política de segurança tem gestor responsável pela sua manutenção e análise crítica, de acordo com processo de análise definido. - Processo garante que análise crítica ocorra como decorrência de mudança que venha afetar avaliação de risco original.

Quadro 9 - Controles e diretrizes sugeridas na Norma ABNT NBR ISO/IEC 27002:2005 (parcial)

(conclusão)

No.	Controles	Diretrizes deste controle
6.1.2	Coordenação da segurança da informação	Existência de grupo formado por representantes da direção para coordenar a implantação de controles de segurança da informação
6.1.3	Atribuição de responsabilidades para a segurança da informação	Descrição das responsabilidades pela proteção do ativo e processos específicos para tal fim e definição do responsável por esta atividade (Gestor). Combinado com controle 7.1.2.
6.1.4	Processo de autorização para os recursos de processamento da informação	Processo implantado de gestão de autorização para novos recursos de hardware e software para processamento da informação.
6.1.6	Contato com autoridades	São mantidos contatos apropriados com autoridades legais,organismos regulamentadores, provedores de serviço de informação e operadores de telecomunicações, para garantir que ações adequadas e apoio especializado possam ser rapidamente acionados na ocorrência de incidentes de segurança.
6.1.8	Análise crítica independente de segurança da informação	A implementação da política de segurança é analisada criticamente, de forma independente.
6.2.1	Identificação dos riscos relacionados com partes externas	Identificação de características de perfil de uso de usuários de domínios de endereços de entidade externa candidata a utilizar-se da infra-estrutura. Análise dos riscos de concessão de acesso a usuários desta entidade. (Estudo para elaboração de acordo de acesso). Vide nota1.

Quadro 9 - Controles e diretrizes sugeridas na Norma ABNT NBR ISO/IEC 27002:2005 (parcial)

Tendo como referência as recomendações de segurança da informação para a implementação e configuração de redes locais *wireless,* constantes do documento 'Wireless LAN Security Summary' do NIST, apresentado na página 41 (e com cópia no Anexo 4, página 93), selecionou-se os objetivos de controle correspondentes na Norma ABNT NBR ISO/IEC 27002:2005.

A lista resultante, com 57 controles selecionados é complementada com as diretrizes detalhadas na norma ABNT NBR ISO/IEC 27002:2005. O produto final desta etapa é a geração do documento "Lista de controles e diretrizes selecionados (S2)" contendo os controles e diretrizes da norma ABNT NBR ISO/IEC 27002:2005 selecionados para aplicação em componentes de rede *wireless.* O Quadro 10, contém uma visualização parcial do documento. Para visualizar o conjunto total de controles e diretrizes selecionados, consultar o Anexo 3 – Controles e diretrizes selecionados para o *checklist*, na página 85.

Controles da norma ABNT NBR ISO/IEC 27002:2005 aplicáveis a componentes de rede wireless		
No.	**Controle**	**Diretrizes aplicáveis ao componente**
6.1.3	Atribuição de responsabilidades para a segurança da informação	Descrição das responsabilidades pela proteção do ativo e processos específicos para tal fim e definição do responsável por esta atividade (Gestor). Combinado com controle 7.1.2.
6.2.1	Identificação dos riscos relacionados com partes externas	Identificação de características de perfil de uso de usuários de domínios de endereços de entidade externa candidata a utilizar-se da infra-estrutura. Análise dos riscos de concessão de acesso a usuários desta entidade. (Estudo para elaboração de acordo de acesso).
6.2.2	Identificando a segurança da informação, quando tratando com os clientes	Verificação do cumprimento dos requisitos de segurança da informação relacionados com o acesso dos clientes ao ativo.
6.2.3	Identificando segurança da informação nos acordos com terceiros	Formalização de acordo com terceiros (contendo política de segurança, termos de acesso, condições de uso, nível de serviço oferecido, condições de para suspensão do acordo).
7.1.1	Inventário dos ativos	Elaboração do inventário do ativo. Deve conter todas as informações necessárias para uma recuperação de um desastre (tipo de ativo, formato, localização, informações sobre cópia de segurança, licenças e detalhes de configuração).

Quadro 10 – Lista (parcial) de controles e diretrizes selecionados (S2)

A partir deste documento, gerou-se um formulário para preenchimento da seleção de controles dos componentes na etapa seguinte do trabalho. Vide, no Quadro 11, apresentação parcial do modelo de formulário.

Controles da norma ABNT NBR ISO/IEC 27002:2005 aplicáveis a componentes de rede wireless			
No.	**Controle**	**Diretrizes aplicáveis ao componente**	**Tipo: [nome do componente]**
6.1.3	Atribuição de responsabilidades para a segurança da informação	Descrição das responsabilidades pela proteção do ativo e processos específicos para tal fim e definição do responsável por esta atividade (Gestor). Combinado com controle 7.1.2.	
6.2.1	Identificação dos riscos relacionados com partes externas	Identificação de características de perfil de uso de usuários de domínios de endereços de entidade externa candidata a utilizar-se da infra-estrutura. Análise dos riscos de concessão de acesso a usuários desta entidade. (Estudo para elaboração de acordo de acesso).	
6.2.2	Identificando a segurança da informação, quando tratando com os clientes	Verificação do cumprimento dos requisitos de segurança da informação relacionados com o acesso dos clientes ao ativo.	
6.2.3	Identificando segurança da informação nos acordos com terceiros	Formalização de acordo com terceiros (contendo política de segurança, termos de acesso, condições de uso, nível de serviço oferecido, condições de para suspensão do acordo).	
7.1.1	Inventário dos ativos	Elaboração do inventário do ativo. Deve conter todas as informações necessárias para uma recuperação de um desastre (tipo de ativo, formato, localização, informações sobre cópia de segurança, licenças e detalhes de configuração).	

Quadro 11 – Modelo para preenchimento de componente

3.3 CRIAÇÃO DA LISTA DE ITENS DE CONTROLE PARA CADA COMPONENTE SELECIONADO

A proposta nesta etapa é a produção de um modelo preenchido para cada componente. Os componentes utilizados são previstos em redes locais *wireless* corporativas padrão 802.1x (vide capítulos 2.1.4 e 2.1.5). Os onze componentes selecionados (S1) no item 3.1 (Quadro 7, página 46) resultam, portanto, em 11 formulários-modelo.

Para cada componente, estabelece-se quais dos controles selecionados na fase anterior são aplicáveis.

Exemplo: o controle "10.4.1 – Controle contra códigos maliciosos" pode ser aplicável ao componente "RADIUS", que é uma aplicação cliente/servidor implementada sobre hardware e softwares genéricos para instalação e customização de servidor. Porém, não tem sentido se o componente em análise for um produto industrial e customizado (*appliance*) tal como um "Access Point" pois, estes, geralmente não oferecem possibilidade de inserir qualquer conteúdo que não seja através de atualização do firmware ou comandos digitados.

O produto final desta etapa é uma lista de itens para cada componente, composta por controles selecionados, portanto, *checkpoints* ativos, e áreas sombreadas, onde a função de preenchimento estará desativada. Os itens do componente "Access Point" foram preenchidos para efeitos ilustrativos. Vide, no Quadro 12, parte inicial do documento (S3): "Lista de itens do componente Access Point".

Controles da norma ABNT NBR ISO/IEC 27002:2005 aplicáveis a componentes de rede wireless			
No.	**Controle**	**Diretrizes aplicáveis ao componente**	**Tipo: Access Point**
6.1.3	Atribuição de responsabilidades para a segurança da informação	Descrição das responsabilidades pela proteção do ativo e processos específicos para tal fim e definição do responsável por esta atividade (Gestor). Combinado com controle 7.1.2.	X
6.2.1	Identificação dos riscos relacionados com partes externas	Identificação de características de perfil de uso de usuários de domínios de endereços de entidade externa candidata a utilizar-se da infra-estrutura. Análise dos riscos de concessão de acesso a usuários desta entidade. (Estudo para elaboração de acordo de acesso).	X
6.2.2	Identificando a segurança da informação, quando tratando com os clientes	Verificação do cumprimento dos requisitos de segurança da informação relacionados com o acesso dos clientes ao ativo.	X
6.2.3	Identificando segurança da informação nos acordos com terceiros	Formalização de acordo com terceiros (contendo política de segurança, termos de acesso, condições de uso, nível de serviço oferecido, condições de para suspensão do acordo).	X
7.1.1	Inventário dos ativos	Elaboração do inventário do ativo. Deve conter todas as informações necessárias para uma recuperação de um desastre (tipo de ativo, formato, localização, informações sobre cópia de segurança, licenças e detalhes de configuração).	X

Quadro 12 – Lista (parcial) de itens preenchida do componente Access Point (S3)

3.4 MONTAGEM DO REPOSITÓRIO DE ITENS DE CONTROLE DE COMPONENTES

Nesta etapa, os conteúdos de todos os modelos de controles para componentes criados acima são agregados numa única tabela. O propósito desta é ser um repositório das definições dos componentes. Neste ponto, a coluna correspondente a cada componente, contém os *checkpoints* definidos na etapa anterior. No processo de preparação do repositório, os "X" destes *checkpoints* são

substituídos por "caixas de seleção", ou '*checkmarks*' (recurso gráfico específico, que dá um aspecto visual mais formatado ao produto final). Os dois campos superiores da coluna de cada componente recebem etiquetas com as denominações "Cod.:" e "Localização:". Uma visualização parcial do documento (somente com o componente "Access Point") pode ser observada no Quadro 13.

Matriz de componentes para montagem do checklist			Cod.:
			Localização:
Controles da norma ABNT NBR ISO/IEC 27002:2005 aplicáveis a componentes de rede wireless			
No.	**Controle**	**Diretrizes aplicáveis ao componente**	**Tipo: Access Point (AP)**
6.1.3	Atribuição de responsabilidades para a segurança da informação	Descrição das responsabilidades pela proteção do ativo e processos específicos para tal fim e definição do responsável por esta atividade (Gestor). Combinado com controle 7.1.2.	☐
6.2.1	Identificação dos riscos relacionados com partes externas	Identificação de características de perfil de uso de usuários de domínios de endereços de entidade externa candidata a utilizar-se da infra-estrutura. Análise dos riscos de concessão de acesso a usuários desta entidade. (Estudo para elaboração de acordo de acesso). Vide nota1.	☐
6.2.2	Identificando a segurança da informação, quando tratando com os clientes	Verificação do cumprimento dos requisitos de segurança da informação relacionados com o acesso dos clientes ao ativo.	☐
6.2.3	Identificando segurança da informação nos acordos com terceiros	Formalização de acordo com terceiros (contendo política de segurança, termos de acesso, condições de uso, nível de serviço oferecido, condições de para suspensão do acordo).	☐
7.1.1	Inventário dos ativos	Elaboração do inventário do ativo. Deve conter todas as informações necessárias para uma recuperação de um desastre (tipo de ativo, formato, localização, informações sobre cópia de segurança, licenças e detalhes de configuração).	☐
7.1.2	Proprietário dos ativos	Definição da pessoa ou entidade que tenha responsabilidade autorizada para controlar a produção, manutenção, o uso e a segurança do ativo (Proprietário). Combinado com 6.1.3	☐
7.1.3	Uso aceitável dos ativos	Elaboração das regras de uso do ativo (condições, limites e restrições). Combinado com 10.8.1.	☐

Quadro 13 – Repositório de listas de itens de componentes para montagem do *checklist* (S4) - parcial

Em sua forma final, o documento acima contém quatorze colunas: as primeiras três (no. do controle, descrição do controle e descrição das diretrizes do controle), formando o cabeçalho e as onze colunas restantes, correspondentes a cada um dos componentes. O formato resultante do Repositório de listas de itens de componentes (S4) é semelhante ao representado esquematicamente na Figura 7 (página 44). O Apêndice B, na página 72, contém as colunas complementares do Repositório, referentes aos demais dez componentes, preenchidas, para efeito meramente ilustrativo, com *checkmarks* e áreas de sombra (controles selecionados e não selecionados, respectivamente).

3.5 ELABORAÇÃO DO MODELO DE CORPO (ESTRUTURA) DO *CHECKLIST*

Conforme proposto na Figura 8 da página 44, o produto final que é a matriz para o usuário compor seu *checklist* personalizado, ou seja, com os componentes necessários ao trabalho a ser executado, compõe-se de duas partes: cabeçalho e corpo.

A Parte 1 – Cabeçalho (vide Quadro 14), utiliza o mesmo conjunto de colunas (no. do controle, descrição do controle e descrição das diretrizes do controle) do documento anterior (Quadro 13), tendo somente o título principal alterado para "CHECKLIST – Implantação do projeto:"

A Parte 2 – Corpo, é montada conforme a necessidade do projeto a ser avaliado, utilizando-se dos componentes do repositório (S4) pertinentes e nas quantidades necessárias para representar cada um dos elementos da estrutura a ser analisada.

Para ilustrar o uso do *checklist*, utilizando *checkmarks* hipotéticos para as listas de itens de componentes, foi concebida uma situação prática simulada, com dados fictícios, descrita na próxima seção.

CHECKLIST - Implantação do projeto:		
Controles da norma ABNT NBR ISO/IEC 27002:2005 aplicáveis a componentes de rede wireless		
No.	**Controle**	**Diretrizes aplicáveis ao componente**
6.1.3	Atribuição de responsabilidades para a segurança da informação	Descrição das responsabilidades pela proteção do ativo e processos específicos para tal fim e definição do responsável por esta atividade (Gestor). Combinado com controle 7.1.2.
6.2.1	Identificação dos riscos relacionados com partes externas	Identificação de características de perfil de uso de usuários de domínios de endereços de entidade externa candidata a utilizar-se da infra-estrutura. Análise dos riscos de concessão de acesso a usuários desta entidade. (Estudo para elaboração de acordo de acesso). Vide nota1.
6.2.2	Identificando a segurança da informação, quando tratando com os clientes	Verificação do cumprimento dos requisitos de segurança da informação relacionados com o acesso dos clientes ao ativo.
6.2.3	Identificando segurança da informação nos acordos com terceiros	Formalização de acordo com terceiros (contendo política de segurança, termos de acesso, condições de uso, nível de serviço oferecido, condições de para suspensão do acordo).
7.1.1	Inventário dos ativos	Elaboração do inventário do ativo. Deve conter todas as informações necessárias para uma recuperação de um desastre (tipo de ativo, formato, localização, informações sobre cópia de segurança, licenças e detalhes de configuração).

Quadro 14 – Estrutura parcial (cabeçalho) do corpo do *checklist* (S5)

3.6 DESENVOLVIMENTO DE UM CENÁRIO PARA EXEMPLO

Para exemplificar o uso do *checklist* desenvolvido ao longo do capítulo 3, foi utilizada uma versão simples e fictícia de projeto de implementação de rede *wireless* numa instituição universitária. Neste contexto, o projeto completo prevê a implantação de uma grande infra-estrutura de rede local *wireless*, com pontos de presença previstos em todas as edificações, porém, para cobertura parcial da área total ocupada pelo conjunto dos prédios da instituição (o projeto está focado em atender, prioritariamente, usuários nas áreas internas dos prédios). A solução deve contar com autenticação padrão 802.1X e múltiplos domínios poderão vir a ser autenticados. A primeira etapa do projeto restringe-se à implantação de pontos iniciais de presença em três dos prédios (próximo a áreas comunitárias, laboratórios didáticos e algumas salas de aula selecionadas) e uma cobertura básica das áreas administrativas centrais. O desenho desta etapa ficou semelhante ao da Figura 10.

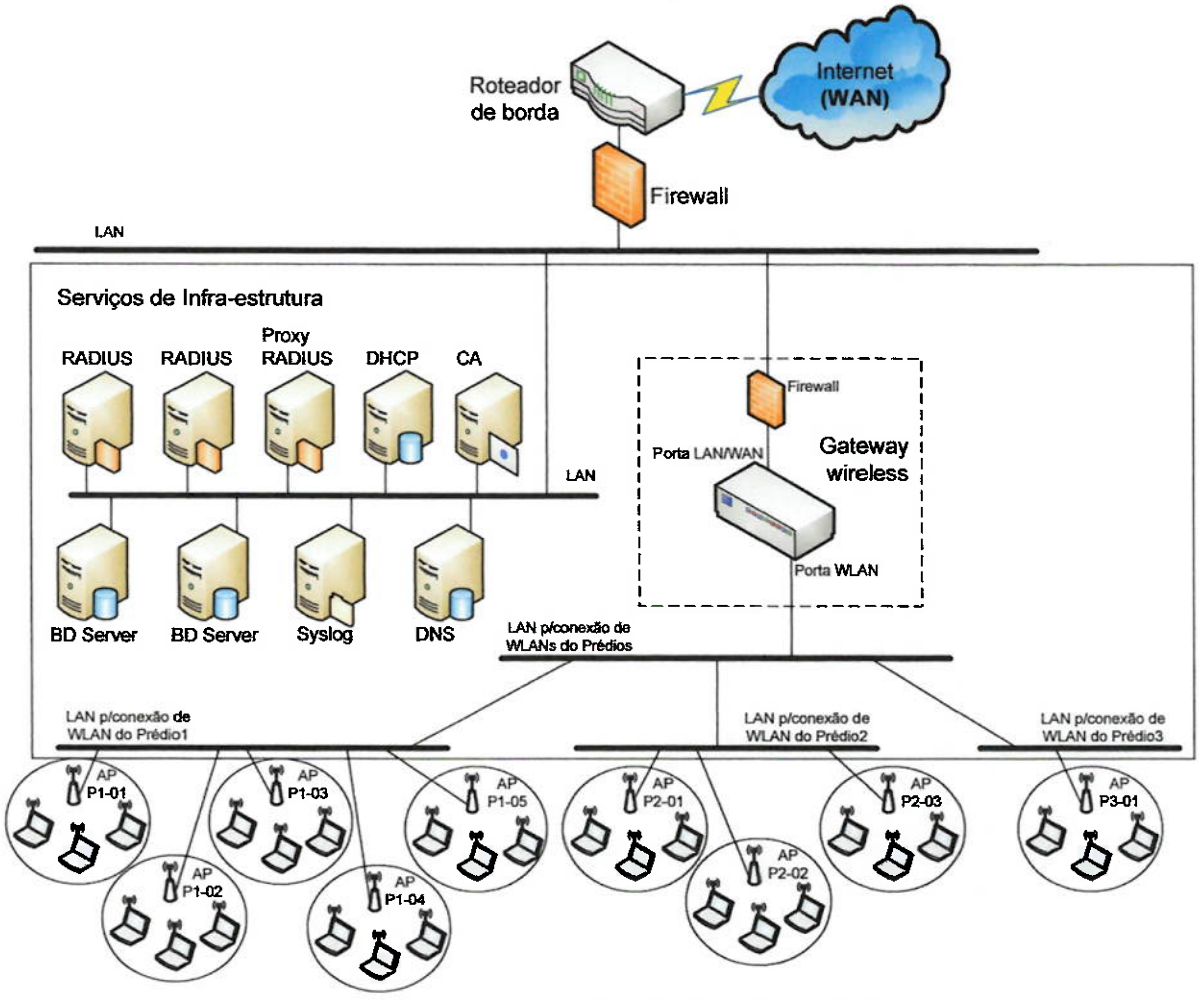


Figura 10 – Esquema físico simplificado do exemplo Projeto EscolaSemFio-2010

Nesta implantação foram projetados, na área "WLAN" (de acordo com o que foi visto, anteriormente, na seção 2.1.5) três conjuntos de APs (no prédio 1, cinco unidades, no prédio2, três unidades e no prédio 3, apenas uma unidade). Na área "Serviços de Infra-estrutura" (instalação central de TI da organização), estão previstos um *gateway wireless*, um servidor ProxyRADIUS transferindo pedidos de autenticação para três diferentes servidores RADIUS e respectivos bancos de dados (dois locais e um remoto, pela Internet), além dos serviços de servidores já disponíveis para as demais atividades relacionadas (DNS, DHCP, CA).

O Quadro 15 contém a distribuição dos componentes apresentados na Figura 10, com sua codificação e localização física nos prédios envolvidos no projeto.

Projeto EscolaSemFio-2010		
Componente	**Código**	**Localização**
Access Point	P1-01	Prédio 1- Hall do Pav. Térreo
Access Point	P1-02	Prédio 1 - Ala dos Laboratórios - Pav. Térreo
Access Point	P1-03	Prédio 1 - Ala dos Laboratórios - Pav. Superior
Access Point	P1-04	Prédio 1 - Centro de Tecnologia (CETEC)
Access Point	P1-05	Prédio 1 - Área de Vivência
Access Point	P2-01	Prédio 2 - Hall do Pav. Térreo
Access Point	P2-02	Prédio 2 - Lanchonete
Access Point	P2-03	Prédio 2 - Biblioteca
Access Point	P3-01	Prédio 3 - Pav. Térreo
Gateway Wireless	GW-P01	TR-IDC Rack-TR08
Open RADIUS	SF-ORAD01	IDC Rack-IDC06
RADIUS	SV-RAD001	IDC Rack-IDC06
RADIUS	SV-RAD002	IDC Rack-IDC02
RADIUS	SR-3rd.001	Fundação Alhures
Certificate Authority - CA	CA-APL2k	IDC Rack-IDC03
DHCP	SV-APL315	IDC Rack-IDC03
SysLog	SV-APL509	IDC Rack-IDC06
BD Server	SV-APL110	IDC Rack-IDC01
BD Server	SV-IVM02	IDC Rack-IDC06
DNS	SV-APL105	IDC Rack-IDC02

Quadro 15 – Componentes da rede wireless do Projeto EscolaSemFio-2010

Com estes dados, o *checklist* para o Projeto EscolaSemFio-2010 gera uma planilha com 20 componentes, portanto, 20 colunas de conteúdo. No Quadro 16, pode ser observada uma visualização parcial do documento, contendo o cabeçalho e o primeiro componente do conjunto da infra-estrutura. Como, por limitações de

formato, não é possível a apresentação do documento em seu formato completo, as demais colunas à direita da planilha foram segmentadas em quatro partes e apresentadas no Apêndice C, a partir da página 74, preenchidas, para efeito meramente ilustrativo.

CHECKLIST - Implantação do projeto: EscolaSemFio-2010			Cod.: P1-01
Controles da norma ABNT NBR ISO/IEC 27002:2005 aplicáveis a componentes de rede wireless			Localização: Prédio 1 Hall-Térreo
No.	**Controle**	**Diretrizes aplicáveis ao componente**	**Tipo: Access Point (AP)**
6.1.3	Atribuição de responsabilidades para a segurança da informação	Descrição das responsabilidades pela proteção do ativo e processos específicos para tal fim e definição do responsável por esta atividade (Gestor). Combinado com controle 7.1.2.	☑
6.2.1	Identificação dos riscos relacionados com partes externas	Identificação de características de perfil de uso de usuários de domínios de endereços de entidade externa candidata a utilizar-se da infra-estrutura. Análise dos riscos de concessão de acesso a usuários desta entidade. (Estudo para elaboração de acordo de acesso). Vide nota1.	☑
6.2.2	Identificando a segurança da informação, quando tratando com os clientes	Verificação do cumprimento dos requisitos de segurança da informação relacionados com o acesso dos clientes ao ativo.	☐
6.2.3	Identificando segurança da informação nos acordos com terceiros	Formalização de acordo com terceiros (contendo política de segurança, termos de acesso, condições de uso, nível de serviço oferecido, condições de para suspensão do acordo).	☐
7.1.1	Inventário dos ativos	Elaboração do inventário do ativo. Deve conter todas as informações necessárias para uma recuperação de um desastre (tipo de ativo, formato, localização, informações sobre cópia de segurança, licenças e detalhes de configuração).	☑
7.1.2	Proprietário dos ativos	Definição da pessoa ou entidade que tenha responsabilidade autorizada para controlar a produção, manutenção, o uso e a segurança do ativo (Proprietário). Combinado com 6.1.3	☑
7.1.3	Uso aceitável dos ativos	Elaboração das regras de uso do ativo (condições, limites e restrições). Combinado com 10.8.1.	☐

Quadro 16 – Trecho inicial do *checklist* do exemplo "Projeto EscolaSemFio-2010"

4 CONCLUSÃO

Numa breve avaliação do produto desenvolvido no decorrer deste trabalho, pergunta-se quais as vantagens mais evidentes quando do uso de *checklist* de múltiplos componentes.

Conforme visto nos conceitos na seção 2.3, um *checklist* deve procurar proporcionar facilidade de interpretação. Na planilha preenchida na seção 3.6 (Quadro 16, página 59, e nos seus segmentos do Apêndice C, a partir da página 74)[15], pode-se observar, visual e rapidamente, a situação do estado de atendimento a um determinado item de controle, mesmo que se esteja trabalhando com muitos componentes. Como cada item de controle ocupa uma linha na planilha e, nas respostas das questões o *checklist* desenvolvido aceita apenas entradas do tipo "atende" (*checkmark* selecionado) ou "não atende" (*checkmark* não selecionado), a percepção é direta pela simples observação da proporção de *checkmarks* selecionados em relação aos não selecionados na linha de interesse.

No exemplo citado, isto pode ser ilustrado na linha correspondente ao item de controle 6.1.3 (Atribuição de responsabilidades para a segurança da informação). Observando-se esta linha completa (no *checklist* do Quadro 16 e em seus respectivos complementos nas páginas 74 a 77 do Apêndice C), pode-se notar que, após o preenchimento, 25% dos componentes avaliados no projeto não atendem ao quesito. Este quesito, na norma ABNT NBR ISO/IEC 27002:2005, refere-se à definição do que se entende por responsabilidade pela proteção do componente e respectivos procedimentos necessários para o exercício desta atribuição e, também, da definição do indivíduo que será responsável pela atividade. Observando-se os campos "Cod." e "Localização" das etiquetas de identificação dos componentes (primeira e segunda linhas superiores de cada componente)[16], das colunas de componentes representadas no Quadro 16 e em seus respectivos complementos nas páginas 74 a 77 do Apêndice C, percebe-se que a totalidade dos componentes

---

[15] Conforme informado na página 59, por limitações de formato, não é possível a apresentação do documento em seu formato completo, portanto, as colunas de componentes à direita da planilha foram segmentadas em quatro partes e apresentadas no Apêndice C, a partir da página 74.

[16] "Cod." (código do componente) e "Localização" (localização física na instalação), conforme visto na página 54.

cujo quesito não foi atendido, encontra-se na área de TI central da organização (esta cumpriu o quesito em somente 50% dos componentes sob sua responsabilidade).

Além da observação, como visto acima, de "regiões/localidades (etiquetas de identificação dos componentes) que estão com problemas de atendimento de um quesito (ou conjunto de quesitos)", outras interpretações podem, também, ser feitas, como "quesitos com grande número de pendências" (eventualmente indicando a existência de um problema para sua efetiva aplicação). No exemplo em uso, o item de controle 6.2.2 (nenhum *checkmark* selecionado), poderia ilustrar esta situação. Outra leitura pode ser "tipos de componentes com maus resultados" (podendo indicar problemas para implementação do quesito naquele tipo de componente). No exemplo, tanto "Gateway Wireless", como "Servidor RADIUS" estão sem nenhum *checkmark* selecionado, o que pode demandar uma ação de verificação específica.

Desta forma, os registros no *checklist* de múltiplos componentes, além de um retrato instantâneo da situação de aplicação dos controles, geram informações que servem de base para disparar outras ações posteriores, sejam elas de verificação/confirmação da situação, sejam corretivas ou o que for aplicável.

A aplicação de *checklist* em auditorias de conformidade e *gap analysis* de sistemas de informação e tecnologia de informação não é uma atividade nova. O *gap analysis* é feito para se identificar o hiato entre o estado "em que as coisas estão", em relação ao estado "em que elas deveriam estar". Neste contexto, o *checklist* contribui com o primeiro passo, que é o levantamento da situação atual. Este é o sentido principal de se aplicar este tipo de ferramenta. Embora o *checklist* possa ser adaptado para acompanhar o andamento de uma implementação, a função mais clássica, na acepção direta do termo, é checar, verificar e apontar "como ela está".

Tomando por base, ainda, as definições da seção 2.3 para o uso de *checklists*, pode-se dizer que:

- É um recurso "mnemônico" e, conforme for feita sua diagramação, facilita a visualização e observação de tendências e comportamentos. Numa rede, por exemplo, com algumas dezenas de componentes e cerca de cinco dezenas de itens de verificação (controles da norma) para cada um deles, uma ferramenta deste tipo pode ser de grande ajuda.

- A assimilação do recurso por um novo profissional é algo muito simples. Ele tem de se concentrar no domínio do conteúdo tratado, despendendo um mínimo de tempo para conhecer a ferramenta em si. Os registros preenchidos por um profissional (apenas seleção de *checkmarks*) não geram dúvida[17] se outro for interpretá-los.

- É um recurso flexível, facilmente adaptável, que permite alterar facilmente o número de quesitos ou itens de verificação e realizar inclusões e alterações sem grande dificuldade. Dada a dinâmica das atualizações das normas, tanto as relacionadas às tecnologias de redes locais (IEEE, série 802), como as relacionadas à segurança da informação (ISO/IEC, série 27000), considera-se importante a revisão constante dos itens de *checklist* a serem utilizados.

Resumindo o visto na seção 2.3, não custa relembrar algumas das finalidades básicas do *checklist:* manter o usuário no foco/objetivo, servir de guia para o profissional que o está utilizando, reduzir as chances da ocorrência de esquecimento de algo importante, garantindo que os itens/eventos importantes tenham sido considerados. Muitos processos não requerem um *checklist*, entretanto, ele é muito útil nas situações em que se tenham operações complexas, com muitos itens, em que partes podem ser esquecidas [33][34][35][36][37].

Para a realização do presente trabalho fez-se um instantâneo ('*snapshot*') de um momento da realidade, mas sem perder de vista que a definição e aplicação de controles aconteçam como parte de um processo e que este deva ser cíclico e permanentemente revisado. Isto está previsto na norma ABNT NBR ISO/IEC 27001:2006, que estabelece o ciclo PDCA para a atualização e aperfeiçoamento constantes do modelo.

4.1 CONSIDERAÇÕES FINAIS

A implementação correta e segura de uma rede local wireless pressupõe que a configuração de seus elementos cumpre as determinações e recomendações

[17] Os registros, não o conteúdo (este deve fazer parte do domínio de conhecimento de quem vai interpretá-los).

constantes nas normas estabelecidas para a tecnologia. Esta conformidade é uma garantia de que o ambiente irá se comportar conforme especificado.

Outrossim, o atendimento às determinações das normas de segurança da informação, acrescenta complexidade na medida que passa-se a tratar, também, aspectos relacionados a processos e políticas e não apenas à tecnologia e seu detalhamento operacional.

A aplicação de um *checklist* sobre cada elemento componente de uma rede local *wireless* pode parecer improdutivo quando se está lidando com uma pequena rede, com poucos itens de configuração. Neste caso, um *checklist* único para a WLAN, nos moldes do '*Wireless LAN Security Summary*', abordado na página 41 da seção 2.3.1 pode atender plenamente as necessidades do profissional encarregado de garantir a conformidade com as normas.

O *checklist* de atividades necessárias ao cumprimento dos requisitos de segurança de informação quando de projeto e implantação de redes locais *wireless* foi concebido com o intuito de facilitar o controle do atendimento de requisitos de segurança da informação quando o número de componentes ativos do sistema e/ou aplicação ou, a área geográfica envolvida for grande e isto dificultar o processo.

Conforme visto na página 47, é importante lembrar que a norma não delimita o nível de detalhamento em que deve se analisar os recursos de processamento de informação (qualquer sistema de processamento de informação, serviço ou infra-estrutura, ou as instalações físicas que os abriguem), mas orienta o interessado a procurar o nível mais significativo para suas necessidades de forma a obter, como resultado, o controle efetivo da segurança da informação como um todo. O problema é que ao aumentar o detalhamento dos controles começa-se a entrar nas particularidades de cada componente envolvido. Com isso, a construção destes controles implica conhecimento e experiência tanto nas demandas (requisitos) do ambiente de segurança da informação, como dos recursos da tecnologia.

Uma possibilidade aberta para futuros trabalhos é a categorização e inclusão de novos componentes. Por exemplo, a inclusão de ativos como os *switches* (L2 ou L3), cujos detalhes de configuração, dependendo dos recursos embarcados, podem ser muito significativos em termos de segurança de informação para contextos como os abordados no presente trabalho.

REFERÊNCIAS

[1] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27002:2005**: Tecnologia de segurança – Técnicas de segurança: Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005. 120 p.

[2] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR ISO/IEC 27001:2006**: Tecnologia da informação – Técnicas de segurança – Sistemas de gestão da segurança da informação – Requisitos. Rio de Janeiro, 2006. 34 p.

[3] Universidad De Granada. Departamento de Electrónica y Tecnologia de Computadores. **Infrared Data Communications with IrDA**. Disponível em: <http://electronica.ugr.es/~amroldan/modulos/temas_tecnicos/irda/infrared_data_communications_with_irda.pdf>. Acesso em: 19 jan. 2010.

[4] Bluetooth. **Fast Facts – Bluetooth Technology 101**. Disponível em: <http://bluetooth.com/Bluetooth/Fast_Facts.htm>. Acesso em: 03 jan. 2010.

[5] **Wi-Fi Alliance**. Disponível em: <http://www.wi-fi.org>. Acesso em: 03 jan. 2010.

[6] Kioskea.net. **Redes sem fio – Wireless Networks**. Disponível em: <http://pt.kioskea.net/contents/wireless/wlintro.php3>. Acesso em: 03 jan. 2010.

[7] elektrorevue. **Bandwidth Efficiency of Wireless Networks of WPAN, WLAN, WMAN and WWAN**. Disponível em: <http://www.elektrorevue.cz/en/articles/analogue-technics/0/bandwidth-efficiency-of-wireless-networks-of-wpan--wlan--wman-and-wwan-1/>. Acesso em: 20 jan. 2010.

[8] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEEE 802.11-2007**: 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. New York, 2007. 1183 p. Disponível em: <http://standards.ieee.org/getieee802/download/802.11-2007.pdf>. Acesso em: 03 jan. 2010.

[9] BreezeCOM. **A Technical Tutorial on the IEEE 802.11 Protocol**. Disponível em:<http://sss-mag.com/pdf/802_11tut.pdf>. Acesso em: 20 jan. 2010.

[10] SANS Institute. **The evolution of wireless security in 802.11networks**: WEP, WPA and 802.11 standards. Disponível em: <http://www.sans.org/reading_room/whitepapers/wireless/the_evolution_of_wireless_security_in_802_11_networks_wep_wpa_and_802_11_standards_1109?show=1109.php&cat=wireless>. Acesso em: 07 jan. 2010.

[11] Microsoft TechNet. **Wireless Networking Security**. Disponível em: <http://technet.microsoft.com/en-us/library/bb457019(printer).aspx#EGAA>. Acesso em: 07 jan. 2010

[12] Microsoft TechNet. **Noções básicas sobre autenticação 802.1X para redes sem fio**. Disponível em:<http://technet.microsoft.com/pt-br/library/cc759077(WS.10,printer).aspx>. Acesso em: 28 dez. 2009.

[13] INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERS. **IEE 802.1x-2004**: 802.1X IEEE Standard for Local and metropolitan area networks. Port-Based Network Access Control. New York: IEEE Computer Society, 2004. 169 p.

[14] Allied Telesis. **802.1x White Paper**. Disponível em: <http://www.alliedtelesis.com/media/pdf/8021x_wp.pdf>. Acesso em: 19 jan. 2010.

[15] CISCO. **How Does RADIUS Work?** Disponível em: <http://www.cisco.com/en/US/tech/tk59/technologies_tech_note09186a00800945cc.shtml>. Acesso em: 21 jan. 2009.

[16] SANS Institute. **802.11i (How we got here and where are we headed)**. Disponível em: <http://www.sans.org/reading_room/whitepapers/wireless/802_11i_how_we_got_here_and_where_are_we_headed_1467>. Acesso em: 28 nov. 2009.

[17] AWIN - Advanced Wireless Networks Research Lab. **Mesh WLAN Networks**: Concept and System Design. Disponível em: <http://awin.cs.ccu.edu.tw/magazine/IEEE_Wireless/2006/April/01632476.pdf>. Acesso em 28 jan. 2010.

[18] Microsoft TechNet. **Securing Wireless LANs with Certificate Services**. Disponível em: <http://technet.microsoft.com/en-us/library/cc527055.aspx>. Acesso em: 04 jan. 2010.

[19] International Organization of Standardization. **ISO/IEC 27000**: Information technology — Security techniques — Information security management systems — Overview and vocabulary. Geneva, 2009. 19 p.

[20] Audit – Information Systems. **ISO 27002 Overview**. Disponível em: <http://www.audit-is.com/bestpractice/iso27002.htm>. Acesso em: 28 nov. 2009.

[21] ISO 27001 Security home. **ISO/IEC 27002**. Disponível em: <http://www.iso27001security.com/html/27002.html>. Acesso em: 28 nov. 2009.

[22] ISO - International Standardization Organization. Products. **ISO/IEC 27001:2005**. Disponível em: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=42103>. Acesso em: 10 jan. 2010.

[23] ISO - International Standardization Organization. Products. **ISO/IEC 27002:2005**. Disponível em: <http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=50297>. Acesso em: 10 jan. 2010.

[24] Gamma. **History of 27000**. Disponível em: <http://www.gammassl.co.uk/bs7799/history.html>. Acesso em: 10 jan. 2010.

[25] The ISO 27000 Directory. **A Short History of the ISO 27000 Standards**. Disponível em: <http://www.27000.org/thepast.htm>. Acesso em 11 jan. 2010.

[26] Microsoft TechNet. Academia Latino-Americana de Segurança da Informação. **Entendendo e implementando a Norma ABNT NBR ISO/IEC 17799:2005**. Disponível em: <http://www.technetbrasil.com.br/academia/provas/materiais/Apostila_ISO17799_Modulo1.pdf>. Acesso em 12 jan. 2010.

[27] GSeTI – Grupo de Segurança em TI – USP. **Alinhando NBR-ISO/IEC 17799 e 27001 na Administração Pública – USP**. Disponível em: <http://www.security.usp.br/palestras/Normas-Encontro-USP-Seguranca-Computacional-II-V-1-02.pdf>. Acesso em: 12 jan. 2010.

[28] ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT Catálogo**. Disponível em: <http://www.abnt.org.br/catalogo>. Acesso em 12 jan. 2010.

[29] BIS – Department of Business Innovations & Skills. **ISO/IEC 27002 Explained.** Disponível em: <http://www.berr.gov.uk/whatwedo/sectors/infosec/infosecadvice/legislationpolicystandards/securitystandards/isoiec27002/page33370.html>. Acesso em: 13 jan. 2010.

[30] OECD - ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. **OECD Guidelines for the Security of Information Systems and Networks**: Towards a Culture of Security, 2002. Disponível em: < http://www.oecd.org/dataoecd/16/22/15582260.pdf>. Acesso em: 15 jan. 2010.

[31] **PMBOK**: Um Guia do Conjunto de Conhecimentos em Gerenciamento de Projetos. 3ª. Edição. Newtown Square: Project Management Institute, 2004. 388 p.

[32] U.S. Department of Transportation. Federal Aviation Administration. **Human Performance Considerations in the Use and Design of Aircraft Checklists.** Disponível em: <http://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afs/afs200/branches/afs210/training_aids/media/checklist.doc>. Acesso em: 25 nov. 2009.

[33] ProductiveWise. **How to Use Checklists to Deliver High Quality Outputs**. Disponível em: <http://www.productivewise.com/checklists-deliver-high-quality-outputs/>. Acesso em: 26 nov. 2009.

[34] TaleWins. **Checklists and how to use them**. Disponível em: <http://www.talewins.com/homepreneurs/7.htm>. Acesso em: 25 nov. 2009.

[35] PAIVA, L. de. **Listas de verificação**. Disponível em: <http://ogerente.com/congestionado/2009/06/29/listas-de-verificacao/>. Acesso em: 23 nov. 2009.

[36] SCRIVEN, M. **The Logic And Methodology Of Checklists**. Disponível em: <http://www.wmich.edu/evalctr/checklists/papers/logic&methodology_dec07.pdf>. Acesso em: 25 nov. 2009.

[37] Ergonomics 4 Schools. Learning Zone. **What is a checklist?** Disponível em: <http://www.ergonomics4schools.com/lzone/checklists.htm>. Acesso em: 25 nov. 2009.

[38] Florida State University. Learning Systems Institute. **How do I use a checklist?** Disponível em: <http://www.lpg.fsu.edu/charting/InstructionalStrategies/howto-tactics/ht-k5elist.asp>. Acesso em: 25 nov. 2009.

[39] STUFFLEBEAM, D.L. **Guidelines for developing evaluation checklists**: the checklists development checklist (CDC).Disponível em: <http://www.wmich.edu/evalctr/checklists/guidelines.htm>. Acesso em 31 jan. 2010.

[40] BICHELMEYER, B. A. **Checklist For Formatting Checklists.** Disponível em: <http://www.wmich.edu/evalctr/checklists/cfc.pdf>. Acesso em: 31 jan. 2010.

[41] SANS Institute. **Audit Check List for ISO 17999:2005**. Disponível em: <http://www.sans.org/score/checklists/ISO-17799_2005.doc>. Acesso em: 05 jan. 2010.

[42] ISO 27001 Security home. **Router Technical Audit Checklist**. Disponível em: <http://www.iso27001security.com/ISO27k_router_security_audit_checklist.rtf>. Acesso em: 05 jan. 2010.

[43] DesktopAuditing. **ISO 27001 27002**.Disponível em: <http://www.desktopauditing.com/tag/iso-27001-27002>. Acesso em: 07 jan. 2010.

[44] ControlSCADA. **ISO 27001/ISO17799**. Disponível em: <http://www.controlscada.com/tag/iso-17799>. Acesso em: 07 jan. 2010.

[45] KARYGIANNIS, T; OWENS, L. **Wireless Network Security**: 802.11, Bluetooth and Handheld Devices. Recommendations of the National Institute of Standards and Technology. Gaithersburg: NIST – National Institute of Standards and Technology, 2002. 115 p. (Special Publication 800-48).

[46] SCARFONE, K. et al. **Guide to Securing Legacy IEEE 802.11 Wireless Networks:** Recommendations of the National Institute of Standards and Technology. Gaithersburg: NIST – National Institute of Standards and Technology, 2008. 50 p. (Special Publication 800-48 Ver.1). Disponível em: <http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf>. Acesso em: 25 jan. 2010.

GLOSSÁRIO

Access Point (AP) – ponto de acesso para redes locais *wireless* (estação-base)

Appliance – equipamento desenvolvido e configurado para executar uma função específica dentro de um sistema

Backbone – espinha dorsal de uma rede ou sistema. Tronco principal de conexões

Basic Service Set (BSS) – conjunto básico de serviço (em redes sem fio, o conjunto formado por uma ou mais estações sem fio e uma estação-base central)

Certificate Authority (CA) – entidade numa rede que emite e gerencia chaves públicas e credenciais de segurança para encriptação de mensagens

Challenge-do-verify (CDV) – *checklist* aplicado como "desafio-resposta". A cada item lido, uma ação (utilizado em aviação)

Checklist – lista de verificação

Checkmark – caixa de seleção em formulários

Checkpoint – ponto de verificação em listas de verificação

Compliance - conformidade

Dynamic Host Configuration Protocol (DHCP) - protocolo que fornece endereços IP e outros parâmetros de configuração para clientes de rede*

Dynamic Name System (DNS) - sistema de gerenciamento de nomes que tem por função resolver nomes de domínios em endereços de rede (IPs)*

Do-list – lista "atividades a fazer"

Do-verify (DV) – checklist aplicado como verificação posterior, após um fluxo de ações ter sido praticado (utilizado em aviação)

Embbeded (software) – software embutido (pré-gravado) em hardware*

Firewall – dispositivo de uma rede de computadores com a função de regular o tráfego de dados entre redes distintas e impedir a transmissão e/ou recepção de acessos nocivos ou não autorizados de uma rede para outra*

Gap analysis – análise da diferença entre a situação atual e a almejada

Hotspot – ponto de acesso onde a tecnologia Wi-Fi está disponível*

Local Area Network (LAN) – rede local

Mesh network – rede em malha. Ver ***Wireless Mesh Network****

Plain-Do-Check-Act (PDCA) – ciclo de Deming, ou ciclo PDCA

Proxy – servidor que atende a requisições repassando os dados do cliente*

Remote Authentication Dial In User Service (RADIUS) – servidor de autenticação utilizado para controlar acesso de usuários de redes remotas

Roaming – recurso que permite que um usuário de uma rede mantenha conectividade mesmo após mudar para outra rede e/ou localidade geográfica

Syslog - denomina o padrão para a transmissão de mensagens de log em redes IP e, também, a aplicação ou biblioteca de envio de mensagens no protocolo syslog*

STA – station. Em redes sem fio, designação do *host* (hospedeiro de sistemas finais)

Wi-Fi – marca licenciada originalmente pela Wi-Fi alliance para descrever a tecnologia de redes sem fio baseada no padrão IEEE 802.11*

Wide Area Network (WAN) – sinônimo de Internet

Wired – "cabeado". Conectado em rede através de cabos*

Wireless – rede sem fio. Usa comunicação via radiofreqüência ou via infravermelho*

Wireless Gateway – dispositivo de rede que roteia pacotes de uma rede local wireless para outra rede, tipicamente para uma rede WAN cabeada*

Wireless Internet Service Provider (WISP) – provedor de acesso wireless à Internet

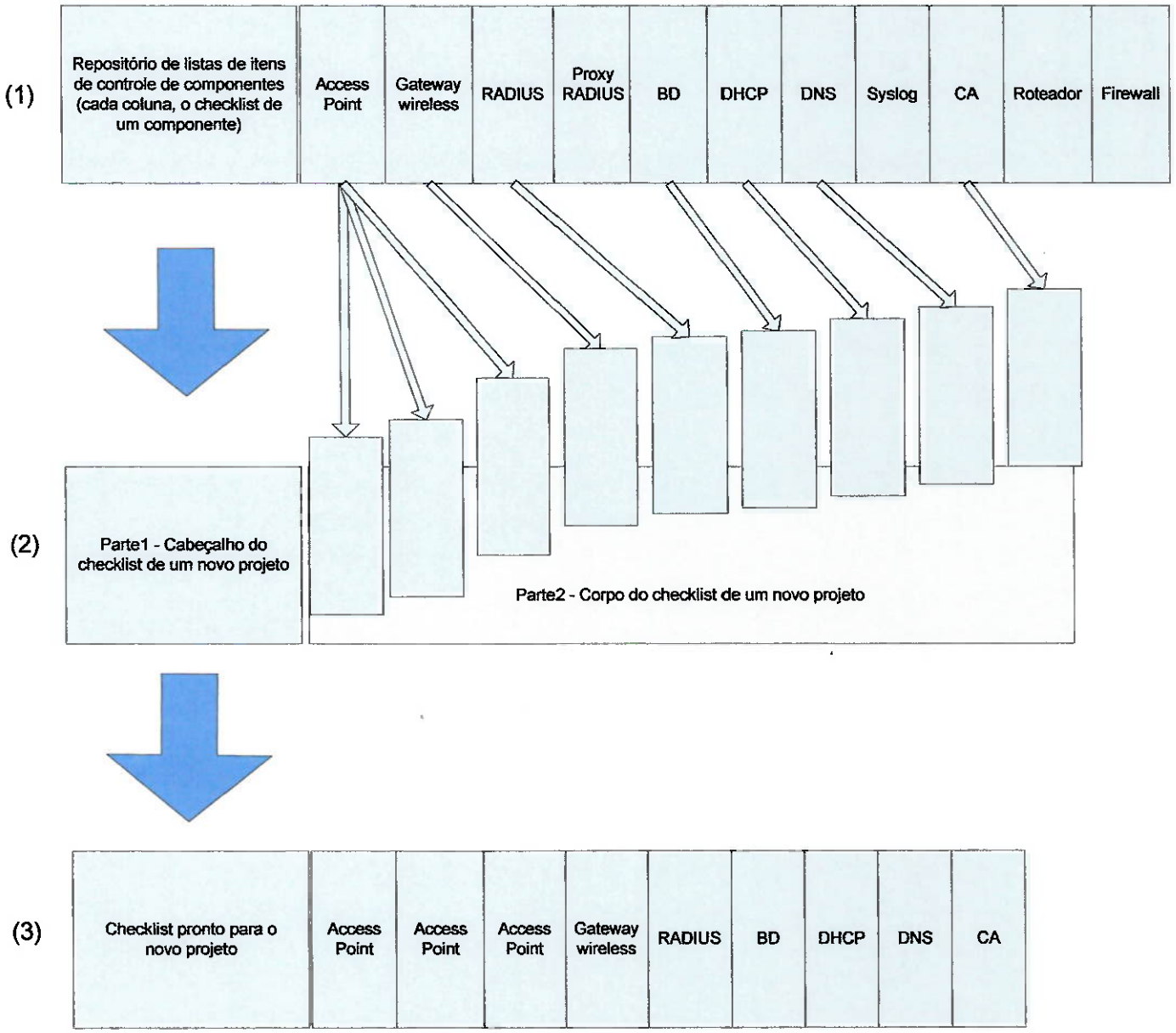
Wireless Local Area Network (WLAN) – rede local sem fio

Wireless Mesh Network – infra-estrutura de comunicação wireless com um alto nível de cooperação entre (grande quantidade de) estações wireless individuais*

(*) Fonte das definições: Wikipedia. Disponível em: <http://en.wikipedia.org>

APÊNDICE A

Ilustração: Exemplo de montagem de *checklist* para um novo projeto utilizando o repositório de componentes



Legenda:

(1) – Repositório de listas de itens de controle de componentes

(2) – Montagem de um novo *checklist*: Parte1- Cabeçalho + Parte2- Corpo (com os componentes selecionados de acordo com as características do projeto)

(3) – *Checklist* do novo projeto

APÊNDICE B

Colunas complementares do documento "Repositório de listas de itens de componentes para montagem do *checklist* (S4) – parcial (Figura 22, página 54)

(continua)

No.*	Cod.:	Cod.:	Cod.:	Cod.:	Cod.:
	Localização:	Localização:	Localização:	Localização:	Localização:
	Tipo: Gateway wireless	**Tipo: Open RADIUS**	**Tipo: RADIUS**	**Tipo: Certificate Authority - CA**	**Tipo: DHCP**
6.1.3	☐	☐	☐	☐	☐
6.2.1		☐			☐
6.2.2	☐	☐	☐	☐	☐
6.2.3		☐			☐
7.1.1	☐	☐	☐	☐	☐
7.1.2	☐	☐	☐	☐	☐
7.1.3	☐	☐	☐	☐	☐

(*) A coluna "No." (controle) à esquerda é apenas uma guia, não pertence a esta parte do formulário.

APÊNDICE B

Colunas complementares do documento "Repositório de listas de itens de componentes para montagem do *checklist* (S4) – parcial

(conclusão)

No.*	Cod.:	Cod.:	Cod.:	Cod.:	Cod.:
	Localização:	Localização:	Localização:	Localização:	Localização:
	Tipo: **SysLog**	Tipo: **BD Server**	Tipo: **DNS**	Tipo: **Firewall**	Tipo: **Roteador**
6.1.3	☐	☐	☐	☐	☐
6.2.1		☐	☐	☐	
6.2.2		☐	☐	☐	☐
6.2.3		☐	☐	☐	
7.1.1	☐	☐	☐	☐	☐
7.1.2	☐	☐	☐	☐	☐
7.1.3	☐	☐	☐	☐	☐

(*) A coluna "No." (controle) à esquerda é apenas uma guia, não pertence a esta parte do formulário.

APÊNDICE C

Colunas complementares do exemplo parcial de *checklist* "Projeto EscolaSemFio-2010" – (Continuação da página 59)

(continua)

No.*	Cod.: P1-02 Localização: Prédio 1 Labs-Térreo Tipo: **Access Point (AP)**	Cod.: P1-03 Localização: Prédio 1 Labs-Sup Tipo: **Access Point (AP)**	Cod.: P1-04 Localização: Prédio 1 CETEC Tipo: **Access Point (AP)**	Cod.: P1-05 Localização: Prédio 1 Vivência Tipo: **Access Point (AP)**	Cod.: P2-01 Localização: Prédio 2 Hall-Térreo Tipo: **Access Point (AP)**
6.1.3	☑	☑	☑	☑	☑
6.2.1	☑	☑	☐	☐	☐
6.2.2	☐	☐	☐	☐	☐
6.2.3	☐	☐	☐	☐	☐
7.1.1	☑	☑	☑	☑	☑
7.1.2	☑	☑	☑	☑	☐
7.1.3	☐	☐	☐	☐	☐

(*) A coluna "No." (controle) à esquerda é apenas uma guia, não pertence a esta parte do formulário.

APÊNDICE C

Colunas complementares do exemplo parcial de *checklist* "Projeto EscolaSemFio-2010"

(continuação)

No.*	Cod.: P2-02 Localização: Prédio 2 Lanchonete Tipo: **Access Point (AP)**	Cod.: P2-03 Localização: Prédio 2 Biblioteca Tipo: **Access Point (AP)**	Cod.: P3-01 Localização: Prédio 3 Térreo Tipo: **Access Point (AP)**	Cod.: GW-P01 Localização: TR-IDC Rack-TR08 Tipo: **Gateway wireless**	Cod.: SF-ORAD01 Localização: IDC Rack-IDC06 Tipo: **Open RADIUS**
6.1.3	☑	☑	☑	☐	☐
6.2.1	☐	☐	☐		☑
6.2.2	☐	☐	☐	☐	☐
6.2.3	☐	☐	☐		☐
7.1.1	☑	☑	☑	☐	☐
7.1.2	☐	☐	☑	☐	☐
7.1.3	☐	☐	☐	☐	☐

(*) A coluna "No." (controle) à esquerda é apenas uma guia, não pertence a esta parte do formulário.

APÊNDICE C

Colunas complementares do exemplo parcial de *checklist* "Projeto EscolaSemFio-2010"

(continuação)

No.*	Cod.: SV-RAD001 Localização: IDC Rack-IDC06 Tipo: **RADIUS**	Cod.: SV-RAD002 Localização: IDC Rack-IDC02 Tipo: **RADIUS**	Cod.: SR-3rd.001 Localização: Fundação Alhures Tipo: **RADIUS**	Cod.: CA-APL2k Localização: IDC Rack-IDC03 Tipo: **Certificate Authority - CA**	Cod.: DV-APL315 Localização: IDC Rack-IDC03 Tipo: **DHCP**
6.1.3	☐	☐	☑	☐	☑
6.2.1					☐
6.2.2	☐	☐	☐	☐	☐
6.2.3					☐
7.1.1	☐	☑	☐	☑	☑
7.1.2	☐	☐	☐	☑	☑
7.1.3	☐	☐	☐	☑	☑

(*) A coluna "No." (controle) à esquerda é apenas uma guia, não pertence a esta parte do formulário.

APÊNDICE C

Colunas complementares do exemplo parcial de *checklist* "Projeto EscolaSemFio-2010"

(conclusão)

No.*	Cod.: DV-APL509 Localização: IDC Rack-IDC06 Tipo: **SysLog**	Cod.: SV-APL110 Localização: IDC Rack-IDC01 Tipo: **BD Server**	Cod.: SV-IVM02 Localização: IDC Rack-IDC06 Tipo: **BD Server**	Cod.: SV-APL105 Localização: IDC Rack-IDC02 Tipo: **DNS**
6.1.3	☑	☑	☑	☑
6.2.1		☐	☐	☐
6.2.2		☐	☐	☐
6.2.3		☐	☐	☐
7.1.1	☑	☑	☑	☑
7.1.2	☑	☑	☑	☑
7.1.3	☑	☑	☑	☑

(*) A coluna "No." (controle) à esquerda é apenas uma guia, não pertence a esta parte do formulário.

ANEXO 1 – Família de Normas ISO27K

Norma	Função	Situação
ISO/IEC 27000:2009	Visão geral e vocabulário - Sistemas de gestão da segurança da informação	Publicada
ISO/IEC 27001:2005	Requisitos para sistema de gestão da segurança da informação	Publicada
ISO/IEC 27002:2005	Código de prática para a gestão da segurança da informação	Publicada
ISO/IEC FDIS 27003	Diretrizes para implementação de sistemas de gestão da segurança da informação	Em desenv.
ISO/IEC 27004:2009	Padrão de medição para a gestão da segurança da informação	Publicada
ISO/IEC 27005:2008	Padrão de gestão de riscos da segurança da informação	Publicada
ISO/IEC 27006:2007	Requisitos para corpos de auditoria e certificação de sistemas de gestão da segurança da informação	Publicada
ISO/IEC CD 27007	Diretrizes para auditoria de sistemas de gestão da segurança da informação	Em desenv.
ISO/IEC WD 27008	Diretrizes para auditores em controles de ISMS	Em desenv.
ISO/IEC NP 27010	Diretrizes para gestão da segurança da informação para comunicações inter-setores	Em desenv.
ISO/IEC 27011:2008	Diretrizes para gestão da segurança da informação para organizações de telecomunicações baseada em ISO/IEC 27002	Publicada
ISO/IEC 27013	Diretrizes para implementação integrada de ISO/IEC 20000-1 e 27001	Não disp.
ISO/IEC 27014	Governança da segurança da informação	Não disp.
ISO/IEC 27015	Diretrizes de sistemas de gestão da segurança da informação para organizações de serviços financeiros	Não disp.
ISO/IEC CD 27031	Padrão para continuidade de negócios	Em desenv.
ISO/IEC WD 27032	Diretrizes para cibersegurança	Em desenv.
ISO/IEC 27033-1:2009	Segurança de redes de TI	Publicada
ISO/IEC CD 27034-1	Diretrizes para segurança de aplicações	Em desenv.
ISO/IEC CD 27035	Gestão de incidentes de segurança da informação	Em desenv.
ISO/IEC NP TR 27036	Diretrizes para auditores em controles de ISMS - Técnicas de segurança	Em desenv.
ISO/IEC NP 27037	Diretrizes para evidência digital	Em desenv.
ISO/IEC 27799:2008	Gestão da segurança da informação em saúde usando ISO/IEC 27002	Publicada

Fontes:

ISO International Standardization Organization (http://www.iso.org/iso/search.htm?qt=27003&published=on&active_tab=standards)

ISO 27001 Security home. About the ISO27K standards. (http://www.iso27001security.com/html/iso27000.html)

The ISO 27000 Directory (http://www.27000.org/index.htm)

ANEXO 2 - Lista de controles* da norma ABNT NBR ISO/IEC 27002:2005

(continua)

No.**	Seções, categorias e controles
5	**Política de segurança da informação**
5.1	**Política de segurança da informação**
5.1.1	Documento da política de segurança da informação
5.1.2	Análise crítica da política de segurança da informação
6	**Organizando a segurança da informação**
6.1	**Infra-estrutura da segurança da informação**
6.1.1	Comprometimento da direção com a segurança da informação
6.1.2	Coordenação da segurança da informação
6.1.3	Atribuição de responsabilidades para a segurança da informação
6.1.4	Processo de autorização para os recursos de processamento da informação
6.1.5	Acordos de confidencialidade
6.1.6	Contato com autoridades
6.1.7	Contato com grupos especiais
6.1.8	Análise crítica independente de segurança da informação
6.2	**Partes externas**
6.2.1	Identificação dos riscos relacionados com partes externas
6.2.2	Identificando a segurança da informação, quando tratando com clientes
6.2.3	Identificando segurança da informação nos acordos com terceiros
7	**Gestão de ativos**
7.1	**Responsabilidade pelos ativos**
7.1.1	Inventário dos ativos
7.1.2	Proprietário dos ativos
7.1.3	Uso aceitável dos ativos
7.2	**Classificação da informação**
7.2.1	Recomendações para classificação
7.2.2	Rótulos e tratamento da informação
8	**Segurança em recursos humanos**
8.1	**Antes da contratação**
8.1.1	Papéis e responsabilidades
8.1.2	Seleção
8.1.3	Termos e condições de contratação
8.2	**Durante a contratação**
8.2.1	Responsabilidades da direção
8.2.2	Conscientização, educação e treinamento em segurança da informação
8.2.3	Processo disciplinar

(*) Lista compilada com dados extraídos da Norma Brasileira ABNT NBR ISO/IEC 27002:2005
(**) Legenda: n = seção, n.n = categoria, n.n.n = controle

ANEXO 2 - Lista de controles* da norma ABNT NBR ISO/IEC 27002:2005

(continuação)

No.**	Seções, categorias e controles
8.3	**Encerramento ou mudança da contratação**
8.3.1	Encerramento de atividades
8.3.2	Devolução de ativos
8.3.3	Retirada de direitos de acesso
9	**Segurança física e do ambiente**
9.1	**Áreas seguras**
9.1.1	Perímetro de segurança física
9.1.2	Controles de entrada física
9.1.3	Segurança em escritórios, salas e instalações
9.1.4	Proteção contra ameaças externas e do meio ambiente
9.1.5	Trabalhando em áreas seguras
9.1.6	Acesso do público, áreas de entrega e de carregamento
9.2	**Segurança de equipamentos**
9.2.1	Instalação e proteção do equipamento
9.2.2	Utilidades
9.2.3	Segurança do cabeamento
9.2.4	Manutenção dos equipamentos
9.2.5	Segurança dos equipamentos fora das dependências da organização
9.2.6	Reutilização e alienação de equipamentos
9.2.7	Remoção de propriedade
10	**Gerenciamento das operações e comunicações**
10.1	**Procedimentos e responsabilidades operacionais**
10.1.1	Documentação dos procedimentos de operação
10.1.2	Gestão de mudanças
10.1.3	Segregação de funções
10.1.4	Separação dos recursos de desenvolvimento, teste e de produção
10.2	**Gerenciamento de serviços terceirizados**
10.2.1	Entrega dos serviços
10.2.2	Monitoramento e análise crítica de serviços terceirizados
10.2.3	Gerenciamento de mudanças para serviços terceirizados
10.3	**Planejamento e aceitação dos sistemas**
10.3.1	Gestão de capacidade
10.3.2	Aceitação de sistemas
10.4	**Proteção contra códigos maliciosos e códigos móveis**
10.4.1	Controles contra códigos maliciosos
10.4.2	Controles contra códigos móveis

(*) Lista compilada com dados extraídos da Norma Brasileira ABNT NBR ISO/IEC 27002:2005
(**) Legenda: n = seção, n.n = categoria, n.n.n = controle

ANEXO 2 - Lista de controles* da norma ABNT NBR ISO/IEC 27002:2005

(continuação)

No.**	Seções, categorias e controles
10.5	**Cópias de segurança**
10.5.1	Cópias de segurança das informações
10.6	**Gerenciamento da segurança em redes**
10.6.1	Controles de redes
10.6.2	Segurança dos serviços de rede
10.7	**Manuseio de mídias**
10.7.1	Gerenciamento de mídias removíveis
10.7.2	Descarte de mídias
10.7.3	Procedimentos para tratamento de informação
10.7.4	Segurança da documentação dos sistemas
10.8	**Troca de informações**
10.8.1	Políticas e procedimentos para troca de informações
10.8.2	Acordos para a troca de informações
10.8.3	Mídias em trânsito
10.8.4	Mensagens eletrônicas
10.8.5	Sistemas de informações do negócio
10.9	**Serviços de comércio eletrônico**
10.9.1	Comércio eletrônico
10.9.2	Transações *on-line*
10.9.3	Informações publicamente disponíveis
10.10	**Monitoramento**
10.10.1	Registros de auditoria
10.10.2	Monitoramento do uso do sistema
10.10.3	Proteção das informações dos registros (*log*)
10.10.4	Registros (*log*) de administrador e operador
10.10.5	Registros (*log*) de falhas
10.10.6	Sincronização dos relógios
11	**Controle de acessos**
11.1	**Requisitos de negócio para controles de acesso**
11.1.1	Política de controle de acesso
11.2	**Gerenciamento de acesso do usuário**
11.2.1	Registro de usuário
11.2.2	Gerenciamento de privilégios
11.2.3	Gerenciamento de senha do usuário
11.2.4	Análise crítica dos direitos de acesso de usuário
11.3	**Responsabilidades dos usuários**
11.3.1	Uso de senhas

(*) Lista compilada com dados extraídos da Norma Brasileira ABNT NBR ISO/IEC 27002:2005
(**) Legenda: n = seção, n.n = categoria, n.n.n = controle

ANEXO 2 - Lista de controles* da norma ABNT NBR ISO/IEC 27002:2005

(continuação)

No.**	Seções, categorias e controles
11.3.2	Equipamentos de usuário sem monitoração
11.3.3	Política de mesa limpa e tela limpa
11.4	**Controle de acesso à rede**
11.4.1	Política de uso dos serviços de rede
11.4.2	Autenticação para conexão externa do usuário
11.4.3	Identificação de equipamentos em redes
11.4.4	Proteção e configuração de portas de diagnóstico remotas
11.4.5	Segregação de redes
11.4.6	Controle de conexão de rede
11.4.7	Controle de roteamento de redes
11.5	**Controle de acesso ao sistema operacional**
11.5.1	Procedimentos seguros de entrada no sistema (*log-on*)
11.5.2	Identificação e autenticação de usuário
11.5.3	Sistema de gerenciamento de senha
11.5.4	Uso de utilitários de sistema
11.5.5	Desconexão de terminal por inatividade
11.5.6	Limitação de horário de conexão
11.6	**Controle de acesso à aplicação e à informação**
11.6.1	Restrição de acesso à informação
11.6.2	Isolamento de sistemas sensíveis
11.7	**Computação móvel e trabalho remoto**
11.7.1	Computação e comunicação móvel
11.7.2	Trabalho remoto
12	**Aquisição, desenvolvimento e manutenção de sistemas de informação**
12.1	**Requisitos de segurança de sistemas de informação**
12.1.1	Análise e especificação dos requisitos de segurança
12.2	**Processamento correto nas aplicações**
12.2.1	Validação dos dados de entrada
12.2.2	Controle do processamento interno
12.2.3	Integridade de mensagens
12.2.4	Validação de dados de saída
12.3	**Controles criptográficos**
12.3.1	Política de uso de controles criptográficos
12.3.2	Gerenciamento de chaves
12.4	**Segurança dos arquivos do sistema**
12.4.1	Controle de *software* operacional
12.4.2	Proteção dos dados para teste de sistema

(*) Lista compilada com dados extraídos da Norma Brasileira ABNT NBR ISO/IEC 27002:2005
(**) Legenda: n = seção, n.n = categoria, n.n.n = controle

ANEXO 2 - Lista de controles* da norma ABNT NBR ISO/IEC 27002:2005

(continuação)

No.**	Seções, categorias e controles
12.4.3	Controle de acesso ao código-fonte de programa
12.5	**Segurança em processos de desenvolvimento e de suporte**
12.5.1	Procedimentos para controle de mudanças
12.5.2	Análise crítica técnica das aplicações após mudanças no sistema operacional
12.5.3	Restrições sobre mudanças em pacotes de software
12.5.4	Vazamento de informações
12.5.5	Desenvolvimento terceirizado de software
12.6	**Gestão de vulnerabilidades técnicas**
12.6.1	Controle de vulnerabilidades técnicas
13	**Gestão de incidentes de segurança da informação**
13.1	**Notificação de fragilidades e eventos de segurança da informação**
13.1.1	Notificação de eventos de segurança da informação
13.1.2	Notificando fragilidades de segurança da informação
13.2	**Gestão de incidentes de segurança da informação e melhorias**
13.2.1	Responsabilidades e procedimentos
13.2.2	Aprendendo com os incidentes de segurança da informação
13.2.3	Coleta de evidências
14	**Gestão de continuidade do negócio**
14.1	**Aspectos da gestão da continuidade do negócio, relativos à segurança da informação**
14.1.1	Incluindo segurança da informação no processo de gestão da continuidade de negócio
14.1.2	Continuidade de negócios e análise/avaliação de riscos
14.1.3	Desenvolvimento e implementação de planos de continuidade relativos à segurança da informação
14.1.4	Estrutura do plano de continuidade do negócio
14.1.5	Testes, manutenção e reavaliaçãods planos de continuidade do negócio
15	**Conformidade**
15.1	**Conformidade com os requisitos legais**
15.1.1	Identificação da legislação vigente
15.1.2	Direitos de propriedade intelectual
15.1.3	Proteção dos registros organizacionais
15.1.4	Proteção dos dados e privacidade de informações pessoais
15.1.5	Prevenção de mau uso de recursos de processamento de informação
15.1.6	Regulamentação de controles de criptografia

(*) Lista compilada com dados extraídos da Norma Brasileira ABNT NBR ISO/IEC 27002:2005
(**) Legenda: n = seção, n.n = categoria, n.n.n = controle

ANEXO 2 - Lista de controles* da norma ABNT NBR ISO/IEC 27002:2005

(conclusão)

No.**	Seções, categorias e controles
15.2	**Conformidade com normas e políticas de segurança da informação e conformidade técnica**
15.2.1	Conformidade com as políticas e normas de segurança da informação
15.2.2	Verificação da conformidade técnica
15.3	**Considerações quanto à auditoria de sistemas de informação**
15.3.1	Controles de auditoria de sistemas de informação
15.3.2	Proteção de ferramentas de auditoria de sistemas de informação

(*) Lista compilada com dados extraídos da Norma Brasileira ABNT NBR ISO/IEC 27002:2005
(**) Legenda: n = seção, n.n = categoria, n.n.n = controle

ANEXO 3 - Controles e diretrizes da norma ABNT NBR ISO/IEC 27002:2005 selecionados para o *checklist*

(continua)

No.	Controle	Diretrizes aplicáveis ao componente
6.1.3	Atribuição de responsabilidades para a segurança da informação	Descrição das responsabilidades pela proteção do ativo e processos específicos para tal fim e definição do responsável por esta atividade (Gestor). Combinado com controle 7.1.2.
6.2.1	Identificação dos riscos relacionados com partes externas	Identificação de características de perfil de uso de usuários de domínios de endereços de entidade externa candidata a utilizar-se da infra-estrutura. Análise dos riscos de concessão de acesso a usuários desta entidade. (Estudo para elaboração de acordo de acesso).
6.2.2	Identificando a segurança da informação, quando tratando com os clientes	Verificação do cumprimento dos requisitos de segurança da informação relacionados com o acesso dos clientes ao ativo.
6.2.3	Identificando segurança da informação nos acordos com terceiros	Formalização de acordo com terceiros (contendo política de segurança, termos de acesso, condições de uso, nível de serviço oferecido, condições de para suspensão do acordo).
7.1.1	Inventário dos ativos	Elaboração do inventário do ativo. Deve conter todas as informações necessárias para uma recuperação de um desastre (tipo de ativo, formato, localização, informações sobre cópia de segurança, licenças e detalhes de configuração).
7.1.2	Proprietário dos ativos	Definição da pessoa ou entidade que tenha responsabilidade autorizada para controlar a produção, manutenção, o uso e a segurança do ativo (Proprietário). Combinado com 6.1.3
7.1.3	Uso aceitável dos ativos	Elaboração das regras de uso do ativo (condições, limites e restrições). Combinado com 10.8.1.
9.2.1	Instalação e proteção do equipamento	Cumprimento das condições para proteção física do equipamento. Proteção contra riscos e ameaças do meio ambiente (furto, fumaça, água, poeira, vibração, interferência elétrica/eletromagnética/comunicações, vandalismo, temperatura, umidade, proteção contra raios ou outras situações pertinentes). Minimização do risco de acesso físico não autorizado (local protegido e/ou de difícil acesso, quando possível e aplicável).
9.2.2	Utilidades	Provisionamento de utilidades necessárias para o recurso (suprimento de energia elétrica, ventilação, ar-condicionado, umidificador, UPS, gerador de energia, meio de suprimento combustível para o gerador, chaves de emergência para desligamento de energia, luzes de emergência e/ou outros recursos necessários). Plano de contingência em caso de falha (quando de recursos para sistema crítico).

Fonte: Diretrizes baseadas nas recomendações da Norma ABNT NBR ISO/IEC 27002:2005

ANEXO 3 - Controles e diretrizes da norma ABNT NBR ISO/IEC 27002:2005 selecionados para o *checklist*

(continuação)

No.	Controle	Diretrizes aplicáveis ao componente
9.2.3	Segurança do cabeamento	Verificação da correta instalação do cabeamento necessário, tanto de energia, como de comunicações (caminhamento, ativação, homologação, identificação, documentação das conexões, isolamento).
9.2.5	Segurança dos equipamentos fora das dependências da organização	Efetivação de medidas de segurança necessárias para equipamentos que operam fora do local, levando em conta os diferentes riscos decorrentes de se trabalhar em localidades remotas, ou fora das dependências centrais da organização.
10.1.1	Documentação dos procedimentos de operação	Elaboração da documentação dos procedimentos de operação (especificação detalhada das instruções para execução de cada tarefa).
10.1.3	Segregação de funções	Descrição da segregação de funções. Se não praticável, verificação da pertinência de mecanismos de monitoração, trilhas de auditoria, acompanhamento gerencial, para reduzir as oportunidades de modificação ou uso indevido não autorizado ou não intencional do ativo.
10.1.4	Separação dos recursos de desenvolvimento, teste e de produção	Confirmação de que o ativo não permanece com dados de teste, nem que compiladores, editores ou outras ferramentas de desenvolvimento ou utilitários de sistema permaneçam acessíveis quando este estiver em produção.
10.4.1	Controles contra códigos maliciosos	Aplicação de proteção contra códigos maliciosos baseada em softwares de detecção de códigos maliciosos e reparo. Configuração e ativação de sistema de atualização automática desta aplicação.
10.5.1	Cópias de segurança das informações	Configuração e ativação de sistema automático de cópias de segurança (conteúdo). Processamento da copia de segurança da configuração do startup (configuraçao baseline, ou inicial, da aplicação). Teste do procedimento de copia automática e certificação de sua execução de acordo. Execuçao de procedimento de recuperação para teste de confiabilidade.
10.6.1	Controles de redes	Efetivação do registro e demais providências relacionadas para entrada do ativo em operação em rede (pedido e registro de endereço de rede, cadastro em servidor de nomes e outros itens relacionados).
10.6.2	Segurança dos serviços de rede	Aplicação de parâmetros requeridos para segurança de serviços de rede e conexão segura, de acordo com a segurança e regra de conexões de redes da instituição.

Fonte: Diretrizes baseadas nas recomendações da Norma ABNT NBR ISO/IEC 27002:2005

ANEXO 3 - Controles e diretrizes da norma ABNT NBR ISO/IEC 27002:2005 selecionados para o *checklist*

(continuação)

No.	Controle	Diretrizes aplicáveis ao componente
10.7.1	Gerenciamento de mídias removíveis	Certificação da não existência de mídias removíveis instaladas e habilitadas (salvo nos casos em que estas sejam expressamente requeridas).
10.7.4	Segurança da documentação dos sistemas	Certificação de que a documentação do sistema/aplicação esteja protegida contra acessos não autorizados, esteja guardada de forma segura e a relação de pessoas com acesso autorizado a esta seja a menor possível e autorizada pelo proprietário do sistema (7.1.2).
10.8.1	Políticas e procedimentos para troca de informações	Ativação de recursos de criptografia quando da necessidade de proteção da confidencialidade, integridade e autenticidade das informações. Ativação de recursos adicionais de segurança, se disponíveis, quando na atuação em segmentos de comunicação sem fio (7.1.3).
10.10.1	Registros de auditoria	Ativação de logs de auditoria, quando disponíveis e pertinentes, apontando para dispositivos centrais de armazenamento de logs (integrando-os como parte da política de retenção de registros da infra-estrutura de TI da organização como um todo).
10.10.2	Monitoramento do uso do sistema	Ativação de sistema de monitramento de uso dos recursos de processamento, quando disponível e pertinente.
10.10.3	Proteção das informações dos registros (*log*)	Ativação da proteção dos registros de log contra falsificação e acesso não autorizado, quando disponível
10.10.4	Registros (*log*) de administrador e operador	Ativação do registro de log dos administradores e operadores, quando disponível e, se possível, sem que estes tenham a opção de exclusão ou desativação dos registros.
10.10.5	Registros (*log*) de falhas	Ativação do registro de log de falhas e erros e certificação de que este esteja configurado para encaminhamento ao solucionador competente.
10.10.6	Sincronização dos relógios	Ativação do relógio do sistema, apontando para um relógio ou servidor ntp de referência que atende a infra-estrutura de TI da organização como um todo.
11.1.1	Política de controle de acesso	Verificação se há condições específicas de controle de acesso, se há contas privilegiadas compartilhadas ou exclusivas.

Fonte: Diretrizes baseadas nas recomendações da Norma ABNT NBR ISO/IEC 27002:2005

ANEXO 3 - Controles e diretrizes da norma ABNT NBR ISO/IEC 27002:2005 selecionados para o *checklist*

(continuação)

No.	Controle	Diretrizes aplicáveis ao componente
11.2.1	Registro de usuário	Verificação, para cadastramento de usuários, se há autorização expressa do proprietário do sistema/recurso para o uso ou aprovação separada para direitos de acesso dada pelo gestor do sistema/recurso. Verificação se o nível de acesso concedido é consistente com o perfil do usuário e finalidade do recurso e se não compromete a segregação de funções. Fornecimento ao usuário de uma declaração por escrito de seus direitos de acesso e obtendo, em contrapartida, seu aceite das condições de acesso. Manutenção de um registro formal de todas as pessoas registradas para usar/acessar o recurso (administrativamente).
11.2.2	Gerenciamento de privilégios	Concessão de privilégios controlada por sistema de autorização formal. Os privilégios devem ser atribuídos a um identificador de usuário (ID) diferente do utilizado por este normalmente em atividades corriqueiras (de "usuário final"). O uso inadequado de privilégios de administrador pode ser um grande fator de contribuição para falhas ou violações de sistemas.
11.2.3	Gerenciamento de senha do usuário	Certificação de que as senhas-padrão sejam alteradas logo após a instalação de sistema ou software. Verificação de identidade do usuário antes de fornecer senha de acesso. Conveniente que a senha seja enviada de maneira segura (convém que o uso de mensagens de e-mail, em texto claro, seja evitado para tal fim. Certificação de que as senhas nunca sejam armazenadas nos sistemas de um computador/sistema de forma desprotegida. Procurar estabelecer, quando necessário, senhas de qualidade (não sujeitas a ataque de dicionário, isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos, não óbviamente relacionadas à pessoa, como nome, número de telefone ou data de aniversário).
11.3.1	Uso de senhas	Orientação ao usuário (gestor ou operador designado), principalmente se este for acessar múltiplos sistemas ou recursos e necessitar de múltiplas senhas para isso, para selecionar uma senha única de qualidade (não sujeita a ataque de dicionário, isentas de caracteres idênticos consecutivos, todos numéricos ou todos alfabéticos sucessivos, não óbviamente relacionadas à pessoa, como nome, número de telefone ou data de aniversário) para estes fins administrativos e não utilizar mesma também para finalidades pessoais ("usuário final").

Fonte: Diretrizes baseadas nas recomendações da Norma ABNT NBR ISO/IEC 27002:2005

ANEXO 3 - Controles e diretrizes da norma ABNT NBR ISO/IEC 27002:2005 selecionados para o *checklist*

(continuação)

No.	Controle	Diretrizes aplicáveis ao componente
11.4.1	Política de uso dos serviços de rede	Certificação de que usuários somente recebam acesso para os serviços que tenham sido especificamente autorizados a usar.
11.4.2	Autenticação para conexão externa do usuário	Certificação de que controles adicionais de autenticação para controlar o acesso a redes sem fio tenham sido estabelecidos e encontrem-se ativos. Especial atenção para o estabelecimento destes controles em função das oportunidades de não detecção de interceptação e inserção de tráfego de rede que surgem neste tipo de ambiente.
11.4.3	Identificação de equipamento em redes	Certificação de que a identificação automática de equipamentos esteja ativada, caso disponível, como um meio de autenticar conexões vindas de localizações e equipamentos específicos, de forma a controlar se a comunicação está sendo iniciada de origem esperada.
11.4.4	Proteção e configuração de portas de diagnóstico remotas	Certificação de que portas, serviços e similares de diagnóstico remoto, não requeridos especificamente para a funcionalidade do recurso, sejam desabilitados ou removidos, pois podem proporcionar meios de acesso não autorizado.
11.4.5	Segregação de redes	Certificação de que os segmentos de redes conectados ao recurso estão devidamente segregados e que os endereços IP para cada interface estão corretamente atribuídos (segmentos LAN, WAN e WLAN).
11.4.6	Controle de conexão de rede	Certificação de que recurso como "traffic shapping" e filtros, se disponíveis e aplicáveis, estejam corretamente configurados.
11.4.7	Controle de roteamento de redes	Certificação de que os endereços de faixas e blocos de endereços estejam corretamente configurados, se aplicável.
11.5.1	Procedimentos seguros de entrada no sistema (*log-on*)	Certificação de que o processo de log-on esteja configurado (para as situações disponíveis) para não exibir a senha que está sendo informada (caracteres da senha ocultos por símbolos), não transmita senha em texto claro pela rede, seja estabelecida limitação de três tentativas de entrada (log-on).

Fonte: Diretrizes baseadas nas recomendações da Norma ABNT NBR ISO/IEC 27002:2005

ANEXO 3 - Controles e diretrizes da norma ABNT NBR ISO/IEC 27002:2005 selecionados para o *checklist*

(continuação)

No.	Controle	Diretrizes aplicáveis ao componente
11.5.2	Identificação e autenticação de usuário	Certificação de que os usuários tenham um identificador único para o sistema de autenticação e que haja um mecanismo de autenticação adequado para validar sua identidade. Salvo em casos excepcionais (e com aprovação pelo gestor do recurso), evitar sempre o uso de um único identificador (ID) por um grupo de usuários. Quando necessário, liberar identificador (ID) de "usuário genérico" somente para casos onde não seja necessário o rastreamento e para funções só de leitura.
11.5.3	Sistema de gerenciamento de senha	Certificação de que aplicações com gerenciamento de senhas assegurem senhas de qualidade e com procedimentos de validade, atualização e reutilização aceitáveis.
11.5.4	Uso de utilitários de sistema	Certificação de que todos os softwares utilitários e sistemas desnecessários tenham sido removidos ou desabilitados. Em sistemas com segregação de funções estabelecidos, não deixar utilitários de sistema disponíveis para acesso geral aos usuários.
11.5.5	Desconexão de terminal por inatividade	Certificação, quando aplicável e disponível, de que mecanismos de encerramento de sessão inativa estejam ativados, visando prevenir acesso não autorizado e ataques de negação de serviço.
11.6.1	Restrição de acesso à informação	Certificação de que o acesso de usuários e pessoal de suporte à informação, ACLs da estrutura de diretório e funções dos sistemas de aplicação sejam restritos e condicionados à navegação por menus controlados.
11.6.2	Isolamento de sistemas sensíveis	Certificação de que se o recurso/aplicação é um sistema sensível, esteja instalado para ser executado a partir de um computador dedicado e/ou apenas compartilhando recursos com sistemas de aplicação confiáveis.
11.7.1	Computação e comunicação móvel	Certificação de que, caso aplicável, tenham sido incluídos nos textos gerais de orientação ao usuário, recomendações para que este mantenha em seu equipamento móvel, devidamente atualizados, recursos de proteção física (firewall), técnicas criptográficas, cópias de segurança e anti-vírus.
12.1.1	Análise e especificação dos requisitos de segurança	Certificação de que, no caso de produto comprado, um processo formal de testes seja efetuado. Nas situações em que as funcionalidades adicionais incorporadas acarretem riscos à segurança, convém que estas sejam desativadas (pelo menos até que se tenha determinado que haja vantagens na utilização das funcionalidades em questão).

Fonte: Diretrizes baseadas nas recomendações da Norma ABNT NBR ISO/IEC 27002:2005

ANEXO 3 - Controles e diretrizes da norma ABNT NBR ISO/IEC 27002:2005 selecionados para o *checklist*

(continuação)

No.	Controle	Diretrizes aplicáveis ao componente
12.3.1	Política de uso de controles criptográficos	Certificação de que, quando necessário, seguiu a política de uso de controles criptográficos da instituição.
12.3.2	Gerenciamento de chaves	Certificação de que tenha obtido as chaves necessárias através da coordenação infra-estrutura de TI da organização, responsável pelas atividades relacionadas ao gerenciamento de chaves na instituição (geração e obtenção de certificados de chaves públicas, armazenagem de chaves, distribuição de chaves para os usuários/aplicações em que se faça necessário).
12.4.1	Controle de *software* operacional	Certificação de que os sistemas operacionais e aplicações somente contenham código executável e aprovado e não contenham códigos em desenvolvimento e compiladores. Certificação de que tenha utilizado o sistema de controle de configuração da instituição para manter controle da implementação do software assim como da documentação do sistema.
12.4.3	Controle de acesso ao código-fonte de programa	Certificação de que todo código-fonte de programas envolvido está armazenado na biblioteca central de código-fonte da instituição. Certificação de que não há bibliotecas de programa-fonte no mesmo ambiente dos sistemas operacionais. Certificação de que o pessoal operacional não tenha acesso irrestrito às bibliotecas de programa-fonte.
12.5.1	Procedimentos para controle de mudanças	Certificação de que mudanças sejam efetuadas somente por usuários autorizados, está sendo efetuada a manutenção do controle de versão em toda atualização efetuada assim como a documentação operacional e procedimentos de usuários estejam sendo mantidos de acordo.
15.1.1	Identificação da legislação vigente	Certificação de que os controles regulatórios (ex. potência máxima de sinal permitida) estão sendo cumpridos.
15.1.2	Direitos de propriedade intelectual	Certificação de que estão devidamente registradas as licenças de uso necessárias para o recurso e que documento comprobatório de propriedade esteja arquivado de acordo com o padrão da coordenaçãode TI da instituição.
15.1.3	Proteção dos registros organizacionais	Certificação de que foi verificada a correta transmissão e armazenamento dos registros de auditoria gerados pelo recurso, assim como o procedimento de organização e identificação do conteúdo para permitir, caso necessário, capacidade de acesso posterior de leitura dos dados (mídia e formato).

Fonte: Diretrizes baseadas nas recomendações da Norma ABNT NBR ISO/IEC 27002:2005

ANEXO 3 - Controles e diretrizes da norma ABNT NBR ISO/IEC 27002:2005 selecionados para o *checklist*

(conclusão)

No.	Controle	Diretrizes aplicáveis ao componente
15.1.5	Prevenção de mau uso de recursos de processamento de informação	Certificação de que, caso aplicável (caso de "captive portal"), tenham sido incluída, quando da conexão inicial do usuário, uma mensagem de advertência para indicar que o recurso de processamento da informação que está sendo usado é de propriedade da organização e que não são permitidos acesso não autorizados. O usuário tem de confirmar e reagir adequadamente à mensagem na tela para continuar com o processo de conexão.

Fonte: Diretrizes baseadas nas recomendações da Norma ABNT NBR ISO/IEC 27002:2005

ANEXO 4 – *Wireless LAN Security Summary* (Table 3-4)

(continua)

	Security Recommendation	**Security Needs, Requirements, or Justification**
1	Develop an agency security policy that addresses the use of wireless technology, including 802.11.	A security policy is the foundation on which other countermeasures—the operational and technical ones—are rationalized and implemented. A documented security policy allows an organization to define acceptable architecture, implementation, and uses for 802.11 wireless technologies.
2.	Ensure that users on the network are fully trained in computer security awareness and the risks associated with wireless technology (e.g., 802.11).	A security awareness program helps users to establish good security practices to prevent inadvertent or malicious intrusions into an organization's information systems.
3.	Perform a risk assessment to understand the value of the assets in the agency that need protection.	Understanding the value of organizational assets and the level of protection required is likely to enable more cost-effective wireless solutions that provide an appropriate level of security.
4.	Ensure that the client NIC and AP support firmware upgrades so that security patches may be deployed as they become available (prior to purchase).	Wireless products should support upgrade and patching of firmware to be able to take advantage of wireless security enhancements and fixes.
5.	Perform comprehensive security assessments at regular and random intervals (including validating that rogue APs do not exist in the 802.11 WLAN) to fully understand the wireless network security posture.	Security assessments, or audits, are an essential tool for checking the security posture of a WLAN and for determining corrective action to make sure it stays secure. Random checks ensure that the security posture is maintained beyond periods of assessment.
6.	Ensure that external boundary protection is in place around the perimeter of the building or buildings of the agency.	The external boundaries should be secured to prevent malicious physical access to an organization's information system infrastructure such as a fence or locked doors.
7.	Deploy physical access controls to the building and other secure areas (e.g., using photo IDs or card badge readers).	Identification badges or physical access cards help to ensure that only authorized personnel have access to gain entry to a facility.
8.	Complete a site survey to measure and establish the AP coverage for the agency.	Proper placement of Access Points will help ensure that there is adequate wireless coverage of the environment while minimizing exposure to external attack. The site survey should result in a report that proposes AP locations, determines coverage areas, and assigns radio channels to each AP and that ensures that the coverage range does not expose APs to potential malicious activities.
9.	Take a complete inventory of all APs and 802.11 wireless devices.	A complete inventory list of APs and 802.11 wireless devices can be referenced when conducting an audit for unauthorized use of wireless technologies.
10.	Ensure that wireless networks are not used until they comply with the agency's security policy.	Security policy enforcement is vital for ensuring that only authorized APs and 802.11 wireless devices are operating in compliance with the organization's wireless security policy.
11.	Locate APs on the interior of buildings instead of near exterior walls and windows.	Locating APs near exterior walls and windows provides a better range of access to potential external malicious users. Choosing the location wisely to balance security and coverage should be considered.

Fonte: NIST SP 800-48.Wireless Network Security.802.11, Bluetooth and Handheld Devices [45]

ANEXO 4 – *Wireless LAN Security Summary* (Table 3-4)

(continuação)

	Security Recommendation	**Security Needs, Requirements, or Justification**
12.	Place APs in secured areas to prevent unauthorized physical access and user manipulation.	Physically securing the APs, putting them "out of reach," prevents unauthorized access by potential malicious users.
13.	**Empirically test AP range boundaries to determine the precise extent of the wireless coverage.**	**By empirically testing the AP coverage range for an agency, a level of risk associated with the access range by potential malicious users can be better understood.**
14.	Make sure that APs are turned off while they are not being used (e.g., after hours, weekends).	Shutting down APs when not in use minimizes potential exposure to malicious activity.
15.	Make sure that the reset function on APs is being used only when needed and is only invoked by an authorized group of people.	The reset function allows an individual to negate any security settings administrators have configured on an access point.
16.	Restore the APs to the latest security settings when the reset functions are used.	Security settings are lost after a reset function. Therefore, the appropriate personnel should restore the latest security settings after a reset.
17.	Change the default SSID in the APs.	Many default SSIDs used by vendors are published and well known. Malicious users often try to connect to 802.11 networks using the default SSID.
18.	Disable the broadcast SSID feature so that the client SSID must match that of the AP.	Malicious users can more easily detect and exploit APs that are broadcasting the SSID. Disabling the broadcast SSID feature minimizes exposure of the AP to malicious users.
19.	Validate that the SSID character string does not reflect the agency's name (division, department, street, etc.) or products.	The SSID should be somewhat difficult for malicious users to use to determine the organization or agency that owns the AP. The SSID should also be long and difficult to guess.
20.	Ensure that AP channels are at least five channels different from any other nearby wireless networks to prevent interference.	Radio interference between APs can result in a denial of service. So, using channels in a different range ensures service availability.
21.	Understand and make sure that all default parameters are changed.	Because default settings are generally known and not secure, these settings should be changed and should comply with organizational security policy.
22.	Disable all insecure and nonessential management protocols on the APs.	Management protocols that are enabled on APs but not used present a potential avenue of attack. Disabling all insecure and nonessential management protocols minimizes potential methods that a hostile entity can use when attempting to compromise an access point.
23.	Enable all security features of the WLAN product, including the cryptographic authentication and WEP privacy features.	Enabling built-in security features provides greater security than the default settings.
24.	Ensure that encryption key sizes are at least 128 bits or as large as possible.	Brute force attacks on encryption key sizes become more difficult as the key sizes increase. The addition of a single bit doubles the key space. A 128-bit provides an "intractable" key space against cryptanalysis, if the algorithm and implementation are sound.

Fonte: NIST SP 800-48.Wireless Network Security.802.11, Bluetooth and Handheld Devices [45]

ANEXO 4 – *Wireless LAN Security Summary* (Table 3-4)

(continuação)

	Security Recommendation	**Security Needs, Requirements, or Justification**
25.	Make sure that default shared keys are periodically replaced by more secure unique keys.	Changing default shared keys periodically decreases the likelihood that a malicious user can exploit a compromised key. A changed key increases the adversary's difficulty.
26.	Install a properly configured firewall between the wired infrastructure and the wireless network (AP or hub to APs).	A firewall can enforce a security policy on the information flow between the wired network and the wireless network.
27.	Install antivirus software on all wireless clients.	Antivirus software helps ensure that the wireless client does not introduce known worms and viruses to the wired network while protecting the wireless client from viruses that originate on the wired network.
28.	Install personal firewall software on all wireless clients.	Personal firewalls help to protect against wireless network attacks.
29.	Disable file sharing on wireless clients (especially in untrusted environments).	Malicious users can potentially exploit wireless clients enabled for file sharing.
30.	Deploy MAC access control lists.	The use of access control lists based on MAC hardware addresses provides a layer of security that ensures that only authorized wireless devices are allowed to connect to the wired network.
31.	Consider installation of Layer 2 switches in lieu of hubs for AP connectivity.	The use of layer 2 switches segments network traffic and minimizes potential for a hostile user to monitor traffic by connecting to a hub.
32.	Deploy IPsec-based Virtual Private Network (VPN) technology for wireless communications.	The use of IPsec-based VPN provides an overlay protection to the standard link encryption (e.g., WEP) provided by the wireless connecting hosts.
33.	Ensure that encryption being used is sufficient with the sensitivity of the data on the network and the processor speeds of the computers.	Sensitive data transmission should be encrypted. The level of encryption provided must be balanced between data security requirement and overhead cost related to processor capability.
34.	Fully test and deploy software patches and upgrades regularly.	Newly discovered security vulnerabilities of vendor products should be patched to prevent malicious and inadvertent exploits. Patches should also be fully tested before implementation to ensure that they work.
35.	Ensure that all APs have strong administrative passwords.	Administrator passwords on APs should not be easy to guess. This minimizes the risk of an unauthorized user gaining access by guessing or cracking administrative passwords.
36.	Ensure that all passwords are being changed regularly.	Passwords should changed regularly to reduce the risk of a compromised password being exploited.
37.	Deploy user authentication such as biometrics, smart cards, two-factor authentication, or PKI.	Implementing strong or two-factor authentication whenever possible minimizes the vulnerabilities associated with simple username and password authentication.
38.	Ensure that the "ad hoc mode" for 802.11 has been disabled unless the environment is such that the risk is tolerable.	Note: some products do not allow disabling this feature; use with caution or use a different vendor. The "ad hoc mode" for 802.11 can be exploited. Users of hosts with "ad hoc mode" enabled may unintentionally allow users to inadvertently or maliciously connect to those systems.
39.	Use static IP addressing on the network.	Using static IP addressing makes it more difficult for a hostile user to connect to the network.

Fonte: NIST SP 800-48.Wireless Network Security.802.11, Bluetooth and Handheld Devices [45]

ANEXO 4 – *Wireless LAN Security Summary* (Table 3-4)

(continuação)

	Security Recommendation	**Security Needs, Requirements, or Justification**
40.	Disable DHCP.	If DHCP is disabled, then hosts are forced to use a static IP address.
41.	Enable user authentication mechanisms for the management interfaces of the AP.	User authentication mechanisms should be enabled to ensure that only authenticated users are allowed access to the management interfaces of an AP.
42.	Ensure that management traffic that is destined for APs is on a dedicated wired subnet.	Passing management traffic over an "out of band' network or management subnet protects management traffic, interfaces, and passwords from organizational and outside users.
43.	Use SNMPv3 and/or SSL/TLS for Web-based management of APs.	SNMPv3 has enhanced security features relative to its predecessor SNMP protocol. SNMPv3 and SSL/TLS provide for secure authentication and encryption for Web-based management access of APs.
44.	Configure SNMP settings on APs for least privilege (i.e., read only). Disable SNMP if it is not used.	SNMPv1 and SNMPv2 are not recommended. Company that require SNMP should change the default community string, as often as needed, to a strong community string. Privileges should be set to "read only" if that is the only access a user requires. SNMPv1 and SNMPv2 message wrappers support only trivial authentication based on plain-text community strings and so are fundamentally insecure and not recommended. Agencies should use SNMPv3.
45.	Enhance AP management traffic security by using SNMPv3 or equivalent cryptographically protected protocol.	AP management traffic should be cryptographically protected. SNMPv3 provides cryptographic mechanisms to provide strong security.
46.	Use a local serial port interface for AP configuration to minimize the exposure of sensitive management information.	By using a local serial port interface for AP configuration ensures that sensitive management information do not traverse the network as well as minimizing the risk of unauthorized users gaining access via a network protocol used to manage the AP.
47.	Consider other forms of authentication for the wireless network such as RADIUS and Kerberos.	Use of authentication mechanisms such as RADIUS and Kerberos can improve the security and simplify user management.
48.	Deploy intrusion detection agents on the wireless part of the network to detect suspicious behavior or unauthorized access and activity.	Intrusion detection agents (e.g., host-based or networkbased agents) deployed on the wireless network can detect and respond to potential malicious activities.
49.	Deploy auditing technology to analyze the records produced by RADIUS for suspicious activity.	If RADIUS is used, the audit records should be manually or automatically processed to determine if malicious activity has been directed at the authentication server.
50.	Deploy an 802.11 security product that offers other security features such as enhanced cryptographic protection or user authorization features.	During product selection, ensure that the product provides enhanced cryptographic protection or user authorization features.
51.	Enable use key-mapping keys rather than default keys so that sessions use distinct WEP keys.	The use of distinct WEP keys provides more security than default keys and reduces the risk of key compromise.

Fonte: NIST SP 800-48.Wireless Network Security.802.11, Bluetooth and Handheld Devices [45]

ANEXO 4 – *Wireless LAN Security Summary* (Table 3-4)

(conclusão)

	Security Recommendation	**Security Needs, Requirements, or Justification**
52.	Fully understand the impacts of deploying any security feature or product prior to deployment.	To ensure a successful deployment, an organization should fully understand the technical, security, operational, and personnel requirements before implementation.
53.	Designate an individual to track the progress of 802.11 security products and standards (IETF, IEEE, etc.) and the threats and vulnerabilities with the technology.	An appointed individual designated to track the latest technology enhancements, standards, and risks will help to ensure the continued secure implementation of wireless technology.
54.	Wait for future releases of 802.11 WLAN technologies that incorporate fixes to the security features, or provide enhanced security features.	Upgrade to the latest versions and avoid purchasing the versions of the 802.11 products with major security vulnerabilities that have not been fixed.
55.	When disposing of access points that will no longer be used by the agency, clear access point configuration to prevent disclosure of network configuration, keys, passwords, etc.	Sensitive or proprietary configuration settings should be cleared from access points before removing them from use or disposing to prevent inadvertent disclosure of the information to potentially malicious users.
56.	If the access point supports logging, turn it on and review the logs on a regular basis.	Ensure that the APs are set to perform logging. Also, review of audit and logging data helps to ensure user accountability.
57.	If the access point supports logging, turn it on and review the logs on a regular basis.	Access point logs should be enabled and regularly reviewed for malicious activity.

Fonte: NIST SP 800-48.Wireless Network Security.802.11, Bluetooth and Handheld Devices [45]