INSTITUTO DE ESTUDOS SUPERIORES MILITARES

CURSO DE PROMOÇÃO A OFICIAL SUPERIOR DA FORÇA AÉREA

2009/2010

TII

O TEXTO CORRESPONDE A TRABALHO FEITO DURANTE A FREQUÊNCIA DO CURSO NO IESM SENDO DA RESPONSABILIDADE DO SEU AUTOR, NÃO CONSTITUINDO ASSIM DOUTRINA OFICIAL DA FORÇA AÉREA PORTUGUESA.

A SEGURANÇA DOS DADOS INFORMÁTICOS NA FORÇA AÉREA

MANUEL ANTÓNIO DA COSTA CASTRO
CAP/TINF

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

A SEGURANÇA DOS DADOS INFORMÁTICOS NA FORÇA AÉREA

CAP/TINF Manuel António da Costa Castro

Trabalho de Investigação Individual do CPOS/FA 2009/2010

Lisboa 2010

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

A SEGURANÇA DOS DADOS INFORMÁTICOS NA FORÇA AÉREA

CAP/TINF Manuel António da Costa Castro

Trabalho de Investigação Individual do CPOS/FA 2009/2010

Orientador: TCOR/PILAV João Caldas

Lisboa 2010

Agradecimentos

A todos os meus camaradas de curso que se prontificaram para responder aos inquéritos efectuados.

Aos distintos oficiais que disponibilizaram o seu tempo e a sua experiência para entrevistas que foram da maior importância para a definição da problemática e para a validação da investigação.

Ao meu orientador, Tenente-Coronel João Caldas, pelo indispensável apoio, disponibilidade e interesse demonstrados durante o trabalho.

À minha família pelo apoio e compreensão.

Índice

Índice de Figuras

Índice de Tabelas

Índice de Anexos

Lista de Abreviaturas

ADAL – Administrador de Dados da Área Logística

AFA – Academia da Força Aérea

ARPA –Advanced Research Projects Agency

ARPANET – Advanced Research Projects Agency Network

BA11 – Base Aérea Nº11

BA5 – Base Aérea Nº5

BA6 – Base Aérea Nº6

BBN – Bolt, Beranek and Newman

CA – Comando Aéreo

CAP – Capitão

CFMTFA – Centro de Formação Militar e Técnica da Força Aérea

CNPD – Comissão Nacional de Protecção de Dados

COR – Coronel

CPOS – Curso de Promoção a Oficial Superior

DARPA – Defense Advanced Research Projects Agency

DCSI – Direcção de Comunicações e Sistemas de Informação

ENGEL – Engenheiro Electrotécnico

ENGINF – Engenheiro Informático

EUA – Estados Unidos da América

FAP – Força Aérea Portuguesa

FTP – File Transfer Protocolo

HFA – Hospital da Força Aérea

IDC – International Data Corporation

ISO – International Organization for Standardization

IVE – Instant Virtual Extranet

LAN – Local Area Network

LCD – Liquid Crystal Display

MAC – Media Access Control

MAJ – Major

MIT – Massachusetts Institute of Technology

NASA – National Aeronautics and Space Administration

OSI – Open Systems Interconnection

OTP – One Time Password

PARC – Palo Alto Research Center

PC – Personal Computer

RIGFA – Rede Interna Geral da Força Aérea

RTP – Rádio e Televisão de Portugal

SGH – Sistema de Gestão Hospitalar

SI – Sistema de Informação

SIAGFA – Sistema Integrado de Administração e Gestão da Força Aérea

SIGMA – Sistema de Informação de Gestão de Manutenção e Abastecimento

SPSS – Statistical Package for Social Sciences

SSL – Secure Sockets Layer

STA – Simulador de Tráfego Aéreo

TCOR – Tenente-coronel

TCP/IP – Transmission Control Protocol / Internet Protocol

TEN – Tenente

TI – Tecnologias de Informação

TINF – Técnico de Informática

TMMEL – Técnico de Manutenção de Material Electrotécnico

TTY – Teletypewriter ou Teleimpressor

VPN – Virtual Private Network

WAN – Wide Area Network

WWW – World Wide Web

Resumo

O presente trabalho foi desenvolvido para responder à questão central, inicialmente formulada da seguinte forma: **Quais as implicações de uma eventual maior abertura da RIGFA ao exterior?** Tem como objectivos avaliar a necessidade, importância, benefícios e a percepção que os utilizadores da RIGFA, nas diversas áreas funcionais, têm relativamente ao seu acesso a partir do exterior; fazer uma caracterização dos acessos remotos à RIGFA, nomeadamente em termos das principais necessidades e benefícios; e identificar os riscos associados à abertura da RIGFA ao exterior e forma de mitigação dos mesmos.

Para atingir estes objectivos e responder à questão central fizemos uma revisão de literatura sobre redes, acessos remotos e riscos associados aos mesmos, que norteou a elaboração do nosso modelo de análise[1], que é composto por 5 questões derivadas e 8 hipóteses. Para testar as hipóteses, aplicámos um inquérito por questionário, que obteve 50 respostas. De forma a aprofundar a nossa compreensão dos resultados obtidos pela análise quantitativa, realizamos 10 entrevistas a especialistas sobre o tema.

A combinação da análise quantitativa com a análise qualitativa, permitiu-nos confirmar totalmente 6 das 8 hipóteses formuladas, tendo sido as restantes duas validadas apenas parcialmente. Os resultados obtidos, permitem-nos responder à questão central, indicando que as principais implicações de uma maior abertura da RIGFA ao exterior se prendem essencialmente com a segurança, sendo necessário realizar uma avaliação custo/benefício caso a caso, para as empresas, e definir perfis de acesso, no caso dos utilizadores individuais. As recomendações apresentadas, surgidas em parte pelas lacunas observadas nas hipóteses parcialmente validadas, vão precisamente nesse sentido, afirmando-se a necessidade de definição de políticas de acesso remoto, e operacionalização das mesmas.

1 No anexo A apresenta-se o quadro síntese do modelo de análise.

Abstract

This study was designed to answer the central question, first formulated as follows: **What are the implications of a possible opening up of RIGFA abroad?** The purposes of the study are to assess the need, importance, benefits and the perception that users of RIGFA in several functional areas, have regard to their access from the outside, to make a characterization of remote access to RIGFA, particularly in terms of the main needs and benefits and to identify the risks associated with opening RIGFA abroad and how to mitigate them.

To achieve these objectives and answer the central question we conducted a review of literature on networks, remote access and risks associated with it that guided the development of our analytical model, which consists of 5 derived questions and 8 hypotheses. To test the hypotheses, we applied a questionnaire survey, which received 50 responses. In order to deepen our understanding of the results obtained by quantitative analysis, we conducted 10 interviews with experts on the topic.

The combination of quantitative and qualitative analysis, allowed us to fully validate 6 of 8 assumptions made and the other two were only partially validated. The results allow us to answer the central question, indicating that the main implications of greater openness to the outside of RIGFA relate primarily to safety and is essential to perform a cost / benefit evaluation in each case, for companies, and set access profiles in the case of individual users. The recommendations, which emerged in part by the failure partly on assumptions validated, will do just that, asserting the need to define remote access policies, and operation thereof.

Palavras-chave

Acesso remoto; controlo de acessos; confidencialidade de dados; disponibilidade de dados; integridade de dados; riscos do acesso remoto; segurança de dados; teletrabalho.

Introdução

De acordo com Toffler (1984), o mundo atravessou três grandes transformações na sua estrutura e economia a que ele chama vagas. Cada uma teve uma duração de várias décadas, originando grandes mudanças, por via das quais as sociedades se reorganizaram em termos da sua visão do mundo, dos seus valores fundamentais e das estruturas sociais, politicas e económicas. A primeira vaga, ou revolução agrícola, ocorreu na Mesopotâmia há 10.000 anos *"...com a introdução de técnicas de agricultura que permitiram fixar as populações nómadas, dando origem às primeiras civilizações da história humana"* (Braga, 1989: 95). A segunda foi a revolução Industrial, que aconteceu em finais do século XVIII, inícios do século XIX e durou até aos anos 60 *"...com a invenção das máquinas a vapor, que permitiram a substituição das práticas artesanais pela produção mecanizada em série e em massa*" (Braga, 1989: 95).

A terceira vaga, constitui a revolução da informação, que se iniciou em finais dos anos 40, com a invenção do primeiro computador em 1947, e ganhou maior fulgor a partir dos anos 70 até aos nossos dias, com o surgimento da *internet*, em 1969. Fruto desta revolução, vivemos naquilo que Castells (1999) chama de "*sociedade em rede*", em que, virtualmente, é possível estar em vários tempos e espaços e em permanente produção, circulação e actualização de conhecimento. A informatização e globalização das sociedades, segundo Heidi e Toffler (2007), fazem do conhecimento o cerne fundamental da criação de valor e de poder.

As oportunidades surgidas com esta revolução da informação são enormes, no entanto, os desafios e as ameaças estão também muito presentes, na medida em que, com o acesso generalizado à internet e a interligação entre Redes Locais, "*Local Area Network*" (LAN), se passa de um modelo de redes autónomo, centralizado e delimitado, com um perímetro de segurança perfeitamente definido, para um modelo mais aberto e descentralizado, onde o perímetro de segurança é difuso e de difícil identificação, estando exposto a um número cada vez maior e mais variado de ameaças e vulnerabilidades (http://www.iso.org)[2], que podem colocar em risco o funcionamento, reputação ou mesmo a continuidade de organizações e instituições.

Neste sentido, tendo em conta que os Sistemas de Informação (SI) constituem um património estratégico valioso para uma organização, torna-se essencial garantir a sua

2 http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm

segurança e protecção contra ameaças potenciais, intencionais ou não, *"...by implementing a suitable set of controls, including policies, processes, procedures, organizational structures and software and hardware functions"* (http://www.iso.org).[3]

Este dilema de maior abertura e de riscos de segurança, que ocorre em todo o tipo de organizações, coloca-se com especial incidência na Força Aérea Portuguesa (FAP), que pela natureza específica da sua missão, deve considerar a segurança dos dados informáticos como uma prioridade e garantir que o modelo adoptado é eficaz, eficiente e ajustado à constante evolução dos conceitos de acesso e partilha de informação. Tem sido política da FAP, através da sua Direcção de Comunicações e Sistemas de Informação (DCSI), não permitir acessos à RIGFA a partir do exterior, no entanto, segundo (Chiavenato,1999: 30) *"na era da informação, as organizações requerem agilidade, mobilidade, inovação e mudanças necessárias para enfrentar as novas ameaças e oportunidades num ambiente de intensa mudança e turbulência"*. Este ambiente faz-se sentir no crescente número de utilizadores externos que manifesta necessidades de aceder a serviços e informação da Rede Interna Geral da Força Aérea (RIGFA) a partir do exterior, e também de empresas, que desenvolvem *software* para a FAP em regime de *outsourcing*, que manifestam a intenção de aceder remotamente às aplicações que desenvolvem. Neste contexto, podemos questionarmo-nos se ao restringir os acessos à RIGFA não estaremos a fechar-nos ao mundo sob o pretexto da segurança?

O presente trabalho pretende avaliar a necessidade, importância, benefícios e a percepção que os utilizadores da RIGFA, nas diversas áreas funcionais, têm relativamente ao seu acesso a partir do exterior. Pretende também fazer uma caracterização dos acessos remotos à RIGFA, nomeadamente em termos das principais necessidades e benefícios. E por fim, como consequência de uma eventual maior "abertura" da RIGFA ao exterior, pretende identificar os riscos associados e a forma de mitigação dos mesmos.

Seguindo a metodologia em ciências sociais de Quivy e Campenhoudt (2003), esta investigação é orientada pela seguinte questão central:

Quais as implicações de uma eventual maior abertura da RIGFA ao exterior?

A esta questão estão associadas as seguintes perguntas que dela derivam[4]:

QD1: Em que áreas ou serviços se poderá colocar a necessidade de aceder à informação a partir do exterior da RIGFA?

3 http://www.iso.org/iso/support/faqs/faqs_widely_used_standards/widely_used_standards_other/information_security.htm

4 No anexo A apresenta-se o quadro síntese do modelo de análise.

QD2: Qual a percepção que os utilizadores têm acerca da importância do acesso à RIGFA a partir do exterior?

QD3: Como se caracteriza o acesso à RIGFA a partir do exterior?

QD4: Quais as formas de mitigar os riscos relativos à segurança dos dados informáticos, associados à abertura da RIGFA ao exterior?

QD5: Em que medida a adopção de um plano de segurança e recuperação de dados eficaz permite repor a situação dos dados informáticos em caso de perda provocada pela maior abertura da RIGFA ao exterior?

Face às perguntas derivadas e, para análise e compreensão da questão central, formularam-se as seguintes hipóteses:

H1: Todas as áreas funcionais manifestam de igual modo a necessidade de aceder à informação a partir do exterior da RIGFA. (**QD1**)

H2: Os utilizadores consideram que, tanto eles como o serviço beneficiariam com o acesso remoto. (**QD2**)

H3: Os utilizadores consideram importante o acesso remoto à RIGFA a partir de casa. (**QD2**)

H4: Os utilizadores atribuem um grau de importância diferente ao acesso às várias Aplicações/Serviços a partir de casa. (**QD2**)

H5: A principal necessidade de acesso remoto à RIGFA a partir do exterior refere-se à manutenção, por parte das Empresas, das suas aplicações informáticas. (**QD3**)

H6: Quem beneficia mais do acesso à RIGFA a partir do exterior é a própria FAP. (**QD3**)

H7: As principais formas de mitigar os riscos relativos à segurança são a autenticação, compartimentação e acessos aos serviços/aplicações mediante perfil. (**QD4**)

H8: O actual plano de segurança e recuperação de dados é eficaz para repor a situação dos dados informáticos em caso de perda provocada pela maior abertura da RIGFA ao exterior. (**QD5**)

O trabalho de investigação foi desenvolvido com recurso a técnicas de recolha de dados de natureza quantitativa e qualitativa e a validação das hipóteses foi feita através de inquérito por questionário e também por entrevistas a personalidades com conhecimentos comprovados nas matérias em causa.

No que respeita à organização do trabalho, no primeiro capítulo apresenta-se uma breve perspectiva da evolução das redes informáticas e do acesso remoto. No segundo

capítulo avalia-se a necessidade, importância, benefícios e a percepção que os utilizadores da RIGFA, nas diversas áreas funcionais, têm relativamente ao seu acesso a partir do exterior. No terceiro capítulo caracterizam-se os acessos remotos à RIGFA, destacando as principais necessidades e benefícios. No quarto capítulo identificam-se os riscos associados à abertura da RIGFA ao exterior e a forma de mitigação dos mesmos. Finalmente, far-se-á uma retrospectiva global do trabalho no capítulo das conclusões, onde se incluem alguns contributos e recomendações.

1. Evolução das redes informáticas e acesso remoto

a. Redes informáticas

Antes do advento das redes de computadores, a comunicação entre os computadores era realizada manualmente por operadores humanos que transportavam as instruções entre eles. O transporte de dados era feito através de cartões perfurados, que "*são uma das formas mais lentas, trabalhosas e demoradas de transportar grandes quantidades de informação que se pode imaginar. São, literalmente, cartões de cartolina com furos, que representam os bits um e zero armazenados*" (Marimoto, 2008: 15).

Em Setembro de 1940, George Robert Stibitz[5], um matemático que trabalhava na Bell Telephone Laboratories, demonstrou pela primeira vez a operação remota de um computador digital eléctrico, a que chamou "*Complex Number Calculator*", "...by *typing numbers into a teletype which transmitted the data 250 miles to a calculator. After the calculator had computed the answer, it transmitted the data back to the teletype, which printed the result. The calculator Stibitz construted was an electromechanical system for adding, subtracting, multiplying, and dividing complex numbers*" (Holliday, 2009: 5).

As primeiras ideias para uma rede de computadores, destinada a permitir a comunicação geral entre os utilizadores, foram formuladas pelo cientista de computação Joseph Carl Robnett Licklider, em Agosto de 1962, através de memorandos, discutindo o conceito de uma "*Intergalactic Computer Network*" (Leiner et al, 2003).[6] Essas ideias continham quase tudo o que compõe a actual *Internet*. Em Outubro de 1963 Licklider foi nomeado responsável pelos programas de Ciências Comportamentais e de Comando e Controle, da Defense Advanced Research Projects Agency (DARPA), no Departamento de Defesa dos Estados Unidos e convenceu os seus colaboradores a desenvolverem o seu conceito de rede de computadores. Em Dezembro de 1969 foi então criada a Advanced Research Projects Agency Network (ARPANET), o embrião da actual *Internet* (Ronda, 2001).[7] A rede começou a funcionar inicialmente com quatro nós, localizados no Stanford Research Institute, na Universidade de Santa Barbara, na Universidade da

5 http://www.britannica.com/EBchecked/topic/566105/George-Robert-Stibitz

6 http://www.isoc.org/internet/history/brief.shtml

7 http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt

California e na Universidade de Utah, nos Estados Unidos da América (EUA). Os nós eram interligados através de links de 50 kbps, utilizando linhas telefónicas dedicadas, adaptadas para dados. Esta rede foi criada com objectivos de testes, no entanto cresceu rapidamente e em 1973 interligava já mais de 30 instituições, desde universidades, empresas e instituições militares. Ao permitir o livre tráfego de informações, esta rede levou ao desenvolvimento de ferramentas e recursos que utilizamos ainda hoje, como o correio electrónico, o *File Transfer Protocolo* (FTP) e o *telnet*, que permitem trocar informações, partilhar ficheiros e aceder remotamente a outros computadores.

Outro evento importante teve lugar em 1973 no Palo Alto Research Center (PARC), nos EUA, onde foi feito o primeiro teste de transmissão de dados utilizando o padrão *Ethernet*, que transmitia dados a uma velocidade de 2.94 Mbps por meio de cabo coaxial, permitindo a conexão de até 256 estações de trabalho (Leiner et al, 2003; Weiser, et al, 1999). Tudo isto ocorreu antes do lançamento do primeiro computador pessoal, o que só viria a acontecer em 1981. Os investigadores do PARC desenvolveram vários protótipos de estações de trabalho durante a década de 70, e o padrão *Ethernet* surgiu, então, pela necessidade de ligar em rede essas estações de trabalho. A velocidade de transmissão do *Ethernet* original de 2.94 Mbps era condicionada pelo *clock* de 2.94 MHz utilizado no *mainframe* do PARC, mas rapidamente foi ampliada para 10 Mbps, dando origem, após alguns melhoramentos, aos padrões *Ethernet* utilizados actualmente (Leiner et al, 2003). O padrão *Ethernet* e a ARPANET estiveram na origem, respectivamente, das redes locais e da *Internet*, duas inovações que vieram revolucionar o mundo da computação (Weiser, et al, 1999).

Inicialmente, a ARPANET e o padrão *Ethernet* eram tecnologias usadas de forma autónoma. Enquanto a primeira era usada para interligar servidores em universidades e outras instituições, a segunda servia para criar redes locais, partilhando recursos entre os computadores, facilitando a troca de ficheiros e informações no ambiente do local de trabalho e permitindo um aproveitamento optimizado dos recursos disponíveis (Leiner et al, 2003).

Em finais da década de 1980 as redes internas e as ligações à *Internet* estavam já bastante generalizadas, no entanto estas duas realidades continuavam a coexistir de uma forma compartimentada. Para cada computador, apesar de estar conectado a uma rede interna, era necessária uma ligação à *Internet*. Era muito

comum vermos organizações onde cada computador possuía um *modem* e uma linha telefónica dedicada, o que multiplicava os custos. Foi então, no início da década de 1990, que se adoptou definitivamente o protocolo de comunicação *Internet Protocolo Suite* (TCP/IP), o que veio facilitar a comunicação, e se passaram a conectar todos os computadores das redes internas à *Internet* através de um ponto comum, em vez de cada computador individualmente. Para isto contribuiu também o aumento de largura de banda, permitindo várias ligações em simultâneo sem perda de qualidade do serviço. "*O acesso à internet tornou-se tão ubíquo que é cada vez mais difícil encontrar utilidade para um PC desconectado da rede*" (Marimoto, 2008: 18).

b. Acesso remoto

O acesso remoto é a capacidade de aceder a um computador ou uma rede de computadores a partir de um local distante. Houve tempos em que o simples pensamento de permitir o acesso remoto de utilizadores externos aos recursos internos de Tecnologias de Informação (TI) fazia gelar o sangue nas veias dos Administradores de TI.

Nas palavras de Tomás (2006), o conceito de teletrabalho ou trabalho à distância nasce no início da década de 70 do século passado, nos EUA, antes da generalização dos PC's na década de 80 ou da *Internet* na década de 90. Jack Nilles, considerado o "pai do teletrabalho", trabalhava na altura para a *National Aeronautics and Space Administration* (NASA) e vivia em Los Angeles, questionou-se um dia, em pleno trânsito de casa para o trabalho, sobre se não seria mais vantajoso, ao invés de levar os trabalhadores ao trabalho, levar o trabalho aos trabalhadores. Tal seria possível se estes usassem meios de telecomunicação (telefone e fax) para enviar o trabalho processado nos seus computadores, rudimentares na altura. Surge assim o conceito de teletrabalho (literalmente, *trabalho à distância*) e estavam lançadas as sementes do que viria a ser, mais de duas décadas depois, o conceito de acesso remoto a intranets.

Com o avanço tecnológico desenvolveram-se as redes internas de alta velocidade nos locais de trabalho, mas mais especialmente em casa e em espaços públicos. Com isso surgiu um apetite renovado pelo trabalho remoto. Para além da evolução tecnológica das redes, que originou uma maior velocidade de transmissão de dados, mais dois factores foram fundamentais para a consolidação do acesso

remoto. O primeiro foi o aparecimento das *Virtual Private Networks* (VPN) que são redes de comunicações privadas normalmente utilizadas por uma empresa ou um conjunto de empresas e/ou instituições, construídas em cima de uma rede de comunicações pública (como por exemplo, a *Internet*). O tráfego de dados é levado pela rede pública utilizando protocolos padrão, não necessariamente seguros. O segundo factor, que veio de certa forma tranquilizar os Administradores de TI, foi o desenvolvimento de tecnologia *Secure Sockets Layer* (SSL). Com esta tecnologia, os dados que passavam entre os dois computadores eram criptografados e foi essa percepção de confiança e segurança que incentivou a adopção desta tecnologia tão rapidamente.

Começaram por existir várias abordagens ligeiramente diferentes para este tipo de conectividade, mas, no essencial, todas partiram da premissa de que o acesso aos recursos internos, tais como a partilha de ficheiros e o acesso a aplicações baseadas na Web podia ser efectuado através de um "Navegador". E porque a ligação entre o cliente e o servidor era concretizada através de um servidor *proxy*, uma vez definidas as regras de conexão e acesso, poder-se-ia facilmente delimitar onde os utilizadores poderiam chegar. Isto significava também que eventuais vulnerabilidades não poderiam ser exploradas. A Neoteris, empresa pioneira em ligações remotas, adoptou a sigla *Instant Virtual Extranet* (IVE) para descrever a sua filosofia subjacente à funcionalidade. De facto era verdade que o acesso do exterior aos recursos internos podia ser implementado sem fazer quaisquer alterações à rede ou a servidores. Na prática, isso significava que a solução VPN SSL permitia a possibilidade de garantir o acesso remoto, de forma rápida e a um custo reduzido.

Inicialmente, os Administradores de TI, foram cautelosos, mas à medida que a facilidade de utilização, estabilidade e segurança foram sendo comprovadas, várias organizações e empresas de todos os tamanhos começaram a aderir a esta tecnologia e actualmente o acesso remoto permite uma interacção entre os indivíduos e as organizações que há menos de dez anos seria considerada impensável.

(1) Riscos associados ao acesso remoto

Os três vectores da segurança que podem ser postos em causa pelos acessos remotos, quer de empresas quer de utilizadores internos, são a

confidencialidade, a integridade e a disponibilidade. Segundo (Schneier, 2004: 121) "*Confidentiality, availability and integrity all boil down to access control. We want to make sure that authorized people are able to do whatever they are authorized to do, and everyone else is not*". Vamos desenvolver estes três conceitos de confidencialidade, integridade e disponibilidade.

(a) Confidencialidade

De acordo com Schneier (2004), a confidencialidade é entendida no âmbito da segurança informática, como a protecção de dados e informações trocadas entre um emissor e um ou mais destinatários contra terceiros. Isto deve ser feito independentemente da segurança do sistema de comunicação utilizado: de facto, uma questão de grande interesse é o problema de garantir o sigilo de comunicação utilizado quando o sistema é inerentemente inseguro como é o caso da Internet. Num sistema que garanta a confidencialidade, se um terceiro entrar na posse de informações trocadas entre o remetente e o destinatário não é capaz de extrair qualquer conteúdo inteligível. Para garantir isso utilizam-se mecanismos de criptografia e de ocultação de comunicação.

(b) Integridade

Ainda na opinião de Schneier (2004: 122), a integridade é mais difícil de definir com precisão. A melhor definição que ele encontra é a seguinte: "*Every piece of data is as the last authorized modifier left it*", ou seja, no contexto da segurança informática a violação da integridade tem a ver com a eliminação ou alteração dos dados de forma ilícita. Esta definição de integridade ilustra bem o quanto ela está relacionada com a confidencialidade. Enquanto a confidencialidade se refere à leitura de dados de uma forma não autorizada, a integridade refere-se à modificação ou eliminação desses dados. E, de facto, são utilizadas as mesmas técnicas de segurança (criptografia e outras) para atingir os objectivos de confidencialidade e integridade.

(c) Disponibilidade

A disponibilidade é o terceiro pilar tradicional da segurança informática, mas na realidade ela é muito mais ampla do que a segurança informática. A disponibilidade pode ser definida como "*the property that a product's services are accessible when needed and without undue delay, or the property of being accessible and usable upon demand by an authorized entity*" (Schneier, 2004: 123). No contexto da segurança informática, a disponibilidade consiste em garantir que um atacante não pode impedir que utilizadores legítimos tenham acesso razoável aos seus sistemas. Por exemplo, a disponibilidade consiste em garantir que não são possíveis ataques de negação de serviço.

Neste primeiro capítulo procurámos compreender e analisar a evolução das redes informáticas e a tendência para a massificação dos acessos remotos característico da sociedade da informação em que vivemos actualmente, tendo-se verificado que se levantam grandes desafios à gestão das TI, uma vez que as vantagens da produtividade decorrem em paralelo com diversos riscos ao nível da segurança da informação. Nos seguintes capítulos, procuramos analisar e compreender estas problemáticas no terreno, entrevistando e inquirindo aqueles que lidam com a RIGFA, tanto na perspectiva dos responsáveis como dos utilizadores. Com esta abordagem pretendemos responder à questão central e às questões derivadas, testar as hipóteses e alcançar os objectivos definidos.

2. Percepção da necessidade, importância e benefícios que os utilizadores da RIGFA possuem relativamente ao acesso remoto

Para ter uma ideia mais clara e precisa sobre a percepção da necessidade, importância e benefícios que os utilizadores da RIGFA possuem relativamente ao acesso remoto, foi efectuado um inquérito por questionário contendo 11 perguntas fechadas (Anexo B). Relativamente às perguntas Q2 e Q3, não foi definida, no questionário, uma extensão temporal, no entanto, para efeitos do nosso estudo, podemos inferir os últimos 10 anos sem que isso influencie os resultados, uma vez que, antes dessa data, os acessos remotos à RIGFA não eram equacionados. As perguntas foram agrupadas de acordo com as várias dimensões: permanência ou necessidade de se deslocar ao serviço fora do horário normal (Q2, Q3), percepção da importância do acesso remoto ao PC ou serviços de rede e beneficiário do mesmo (Q4, Q5), percepção do grau de importância do acesso remoto às vária aplicações/serviços da RIGFA a partir do exterior (Q6, Q7, Q8, Q9, Q10, Q11). A informação associada à classificação das respostas considera somente a área funcional a que os inquiridos pertencem. A informação relativa ao sexo, idade, nível de escolaridade, etc., não foi recolhida por não ter sido considerada importante para o estudo. A amostra considerada foi o Curso CPOS 2009/10, constituído por 50 utilizadores regulares da RIGFA. A informação foi processada através da aplicação *Statistical Package for Social Sciences* (SPSS), tomando em consideração toda a amostra, e que está distribuída pelas várias áreas funcionais de acordo com o gráfico da figura 1.

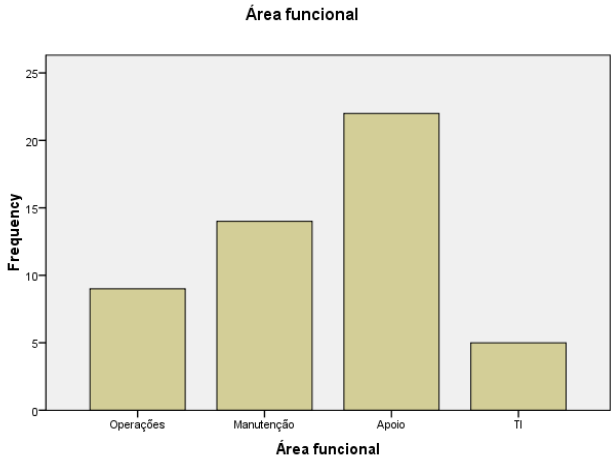


Figura 1 - Área funcional a que pertence. Anexo C Pagina C-6 (Q1)

Além das três áreas funcionais existentes na FAP (Operações, Manutenção e Apoio), considerou-se TI uma área funcional, embora esta esteja incluída na área de Apoio. O objectivo é perceber se existe uma diferente percepção dos profissionais de TI relativamente ao acesso remoto, embora essa não seja uma pergunta derivada e como tal não essencial para o nosso trabalho. A amostra está distribuída da seguinte forma: 9 inquiridos (18%) pertencem à área de operações, 14 (28%) pertencem à manutenção, 22 (44%) pertencem ao apoio e 5 (10%) pertencem às TI.

a. Necessidades de acesso à RIGFA

Para testar a ***Hipótese 1:*** *"Todas as áreas funcionais manifestam de igual modo a necessidade de aceder à informação a partir do exterior da RIGFA" (**H1**)* colocaram-se duas questões no questionário: *"Alguma vez permaneceu no serviço, após o horário normal, para resolver uma situação que poderia resolver a partir de casa se tivesse acesso a uma ligação remota ao seu Posto de Trabalho (PC) ou a Serviços da Rede Interna Geral da Força Aérea (RIGFA)?"* (Q1) *e "Alguma vez se deslocou ou teve* intenção *de se deslocar à Unidade, fora do horário normal, para resolver uma situação que poderia resolver a partir de casa se tivesse aceso a uma ligação remota ao seu PC ou a Serviços da RIGFA?*" (Q2) (Anexo B).

Relativamente à primeira pergunta, o resultado obtido é expresso na figura 2.

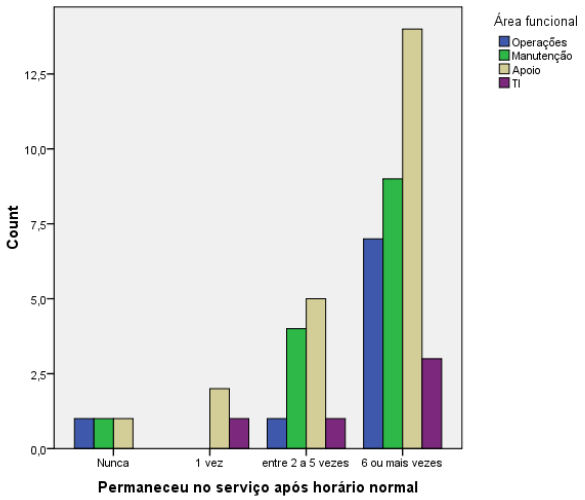


Figura 2- Permaneceu no serviço após o horário normal? Anexo D Pagina D-3 (Q2)

Três inquiridos (6%) responderam "*nunca*", 3 (6%) responderam "*1 vez*", 11 (22%) responderam "*entre 2 e 5 vezes*" e 33 (66%) responderam "*6 ou mais vezes*". De salientar que apenas 6% responderam "*nunca*" e que 66% responderam "*6 ou mais vezes*". Importa referir também que da análise do gráfico, não existem diferenças significativas nas respostas entre as áreas funcionais.

Já em relação à segunda pergunta, a distribuição dos resultados foi ligeiramente diferente, embora se tenha mantido a tendência, como se vê na figura 3. Treze inquiridos (26%) responderam "*nunca*", 3 (6%) responderam "*1 vez*", 11 (22%) responderam "*entre 2 e 5 vezes*" e 23 (46%) responderam "*6 ou mais vezes*". De referir que embora 26% tenha respondido "*nunca*", uma grande percentagem (66%) responderam "*6 ou mais vezes*".

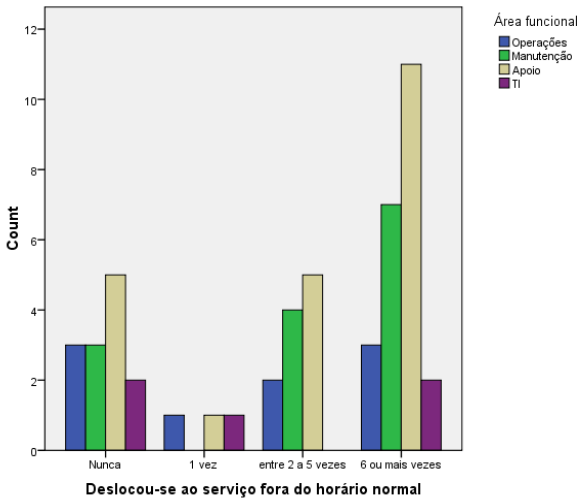


Figura 3 - Deslocou-se ao serviço após o horário normal? Anexo D Pagina D-4 (Q3)

Também pela análise deste gráfico se pode verificar que não existem diferenças percentuais significativas nas respostas, entre as várias áreas funcionais. Estes resultados são evidentes quando fazemos uma análise percentual, usando os indicadores "*entre 2 a 5 vezes*" e "*6 ou mais vezes*", que são os que nos interessam para testar a hipótese, podendo-se verificar nas Tabelas 1 e 2 que, como já tínhamos visto graficamente (Figuras 2 e 3), há uma forte tendência para permanecer no serviço para além do horário normal, e para uma deslocação frequente ao serviço após o horário normal, verificando-se uma grande incidência principalmente no indicador "*6 ou mais vezes*", não se encontram desvios significativos nas necessidades de acesso das diferentes Áreas Funcionais.

			Operações	Manut.	Apoio	TI	Total
Permaneceu no serviço após horário normal	entre 2 a 5 vezes	% within Área funcional	11,1%	28,6%	22,7%	20,0%	22,0%
	6 ou mais vezes	% within Área funcional	77,8%	64,3%	63,6%	60,0%	66,0%

Tabela 1 - (Extracto da Tabela da Página D3 do Anexo D)

			Operações	Manut.	Apoio	TI	Total
Deslocou-se ao serviço fora do horário normal	entre 2 a 5 vezes	% within Área funcional	22,2%	28,6%	22,7%	,0%	22,0%
	6 ou mais vezes	% within Área funcional	33,3%	50,0%	50,0%	40,0%	46,0%

Tabela 2 - (Extracto da Tabela da Página D4 do Anexo D)

Considera-se, por isso, verificada a hipótese H1.

b. Benefícios do acesso remoto à RIGFA

Para testar a ***Hipótese 2***: "*Os utilizadores consideram que, tanto eles como o serviço* beneficiariam *com o acesso remoto*" ***(H2)***, fizemos a seguinte pergunta "*Quem acha que beneficiaria no caso de poder aceder remotamente a partir de casa ao seu PC ou Serviços da RIGFA?*" (Q4). Os resultados apresentados na figura 4, mostram que 7 inquiridos (14%) acham que é a FAP quem fica a ganhar e 43 (86%) são de opinião de que ambos (o próprio e a Organização) beneficiam com o acesso. De destacar o facto de uma elevada percentagem (86%) serem de opinião de que o acesso traz vantagens para ambas as partes. Interessa referir que existiam mais duas opções de resposta ("*O próprio" e "Ninguém*") e que não tiveram ocorrências.

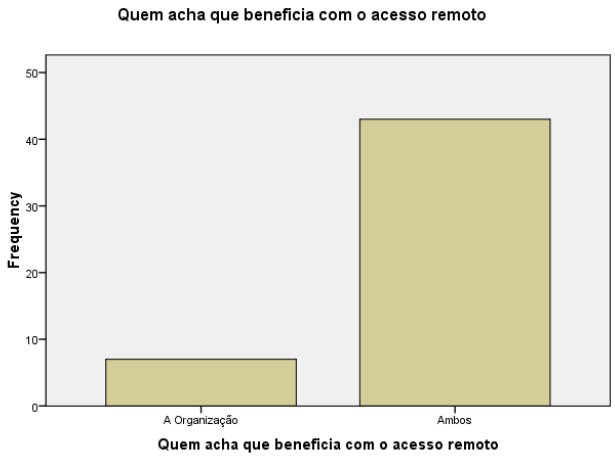


Figura 4 – Quem acha que beneficia com o acesso remoto? Anexo C Pagina C-7 (Q4)

Estes resultados permitem **confirmar a hipótese H2**. Embora 14% dos inquiridos seja da opinião de que só a organização beneficia com o acesso remoto, 86%, a grande maioria, entende que, tanto os próprios utilizadores como a organização beneficiam com o acesso.

c. Importância atribuída ao acesso remoto

Quisemos também saber qual a importância atribuída, de uma forma genérica, ao acesso a serviços da RIGFA ou ao PC e também, mais especificamente, a cada uma das Aplicações ou Serviços, de forma a testar a **Hipótese 3:** "*Os utilizadores consideram importante o acesso remoto à RIGFA a partir de casa"* **(H3)**.

Quando se pede para classificar a importância do acesso remoto ao PC ou a serviços da RIGFA a partir de casa, de uma forma genérica (Q5), o resultado é o que consta no gráfico da figura 5.

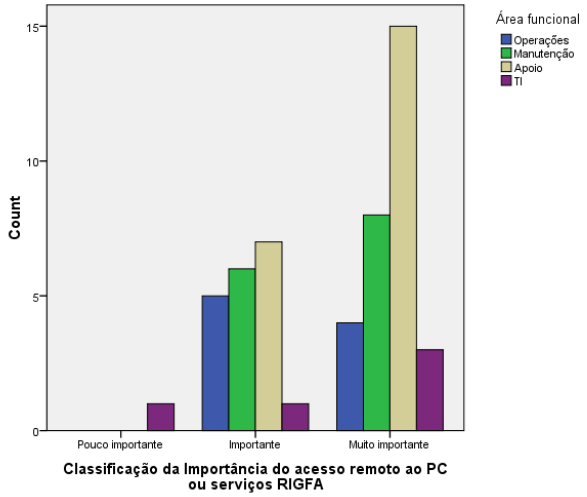


Figura 5 – Classificação da importância do acesso remoto ao PC ou a serviços da RIGFA

Anexo D Pagina D-6 (Q5)

Um inquirido (2%) considera pouco importante o acesso remoto ao PC ou a serviços da RIGFA, 19 (38%) consideram importante e 30 (60%) consideram muito importante. De salientar que a distribuição se encontra entre o "*Importante*" e o "*Muito importante*" com predominância do "*Muito importante*", não tendo ninguém respondido "*Nada importante*". Desta forma, a **hipótese H3 também se confirma através da análise dos resultados expressos no gráfico da figura 5**. Com excepção de um inquirido (2%) todos os outros (98%) consideram importante ou muito importante, o acesso remoto.

De forma a testar a ***Hipótese 4***: "*Os utilizadores atribuem um grau de importância diferente ao acesso às várias aplicações/serviços a partir de casa" **(H4)***, solicitou-se aos inquiridos que avaliassem a importância específica do acesso remoto às várias Aplicações/Serviços da RIGFA (Q6, Q7, Q8, Q9, Q10, Q11). Devido à quantidade de informação contida no gráfico da figura 6, não vamos analisá-lo aqui em detalhe, passando a destacar simplesmente os aspectos mais importantes. Só relativamente a duas aplicações, o Portal FAP e o SIAGFA, existem inquiridos, mais especificamente 1 (2%) em cada caso, que consideram não ser importante o seu acesso remoto. Também em relação a estas duas Aplicações/Serviços existe um número considerável que entende ser pouco importante o acesso remoto: 12 inquiridos (24%) relativamente ao acesso ao Portal FAP e 15 (30%) em relação ao SIAGFA.

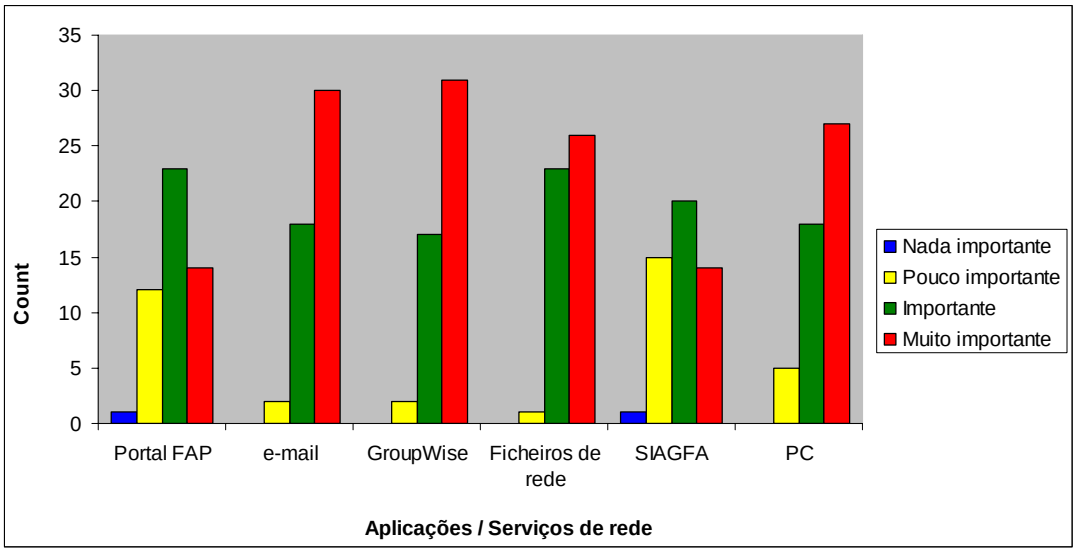


Figura 6 – Classificação da importância específica do acesso remoto às Aplicações/Serviços da RIGFA. (Q6, Q7, Q8, Q9, Q10, Q11)

Já no que diz respeito às restantes Aplicações/Serviços (e-mail, GroupWise, acesso a ficheiros de rede e acesso ao PC) as escolhas recaem nas opções "*Muito importante*" em primeiro lugar e "*Importante*" em segundo, sendo a preferência pela opção "*Pouco importante*" insignificante e a escolha da opção "*Nada importante*" nula.

Estes resultados permitem **confirmar a hipótese H4**. Das cinco Aplicações/Serviços identificados, dois (SIAGFA e Portal FAP) são considerados menos importantes relativamente ao acesso remoto, já que, se englobarmos as opções "Importante" e "Muito importante", essas Aplicações/Serviços atingem uma percentagem de 68% e 74%, respectivamente, enquanto as restantes (acesso ao PC, e-mail, GroupWise e acesso a ficheiros de rede) obtém, respectivamente, percentagens de 90%, 96%, 96% e 98%. Para tentar entender a diferente importância atribuída no acesso remoto às várias Aplicações/Serviços de rede, voltámos a questionar alguns dos inquiridos e concluímos que a menor importância considerada se deve ao facto de essas Aplicações/Serviços serem, também, por eles menos utilizadas habitualmente.

3. Caracterização dos acessos remotos à RIGFA: principais necessidades e benefícios

De forma a compreender em maior profundidade os dados analisados de forma quantitativa, sentimos necessidade de realizar entrevistas pessoais com diversos especialistas. Destas entrevistas resultou o alargamento do conceito de utilizadores para incluir também as empresas que prestam diversos serviços na área de informática que requerem acesso remoto à RIGFA.

Para testar a ***Hipótese 5****: "A principal necessidade de acesso remoto à RIGFA a partir do exterior refere-se à manutenção, por parte das empresas, das suas aplicações informáticas" (**H5**)* e a ***Hipótese 6****: "Quem beneficia mais do acesso à RIGFA a partir do exterior é a própria FAP" (**H6**),* fizeram-se diversas questões aos entrevistados. Da análise das respostas, foi possível identificar vários tipos e necessidades de acesso à RIGFA a partir do exterior; alguns já implementados oficialmente, outros oficiosamente e outros ainda que se prevê, venham a ser implementados devido a "pressões cada vez maiores, quer internas, quer externas", como nos afirmou Rato (2010). Quando perguntámos a Gorgulho (2010) se entende que deve haver abertura por parte da FAP relativamente a acessos remotos, ele *responde* que "existem ainda alguns fantasmas do passado mas devem ser combatidos e, o que é necessário é, caso a caso, quando se justifique e for vantajoso para a FAP, estudar e implementar soluções técnicas para permitir esses acessos, nunca esquecendo a componente da segurança". Os diversos tipos de acesos identificados são:

a. *Software* de Sistemas de armas

Como foi referido por Rato (2010), todos os Sistemas de Armas modernos possuem as suas aplicações informáticas logísticas específicas e existe a necessidade de acesso pelo fabricante, a partir do exterior, para efeito de carregamento de dados e manutenção das mesmas. Segundo ele, "não faz sentido colocar restrições a esses acessos, até porque, as vantagens *são* mútuas. Devemos é, encarar isso como uma realidade e assegurar mecanismos de segurança e, para isso, a DCSI deve ser envolvida nestes projectos o mais a montante possível para garantir que a solução técnica é a mais adequada".

b. Empresas de outsourcing

Existem já, neste momento, empresas externas a desenvolver *software* para a FAP, como é o caso do Sistema de Gestão Hospitalar (SGH) e, como nos informou Reis (2010), essas situações irão ser cada vez mais frequentes no futuro. Nas situações em que as empresas *desenvolvem* o *software*, utilizando os recursos informáticos da FAP, é conveniente, na opinião de Oliveira (2010), que esse desenvolvimento seja feito e o acesso remoto seja dado a uma área restrita que ele denomina "laboratório" ou "pré-produção" e, só após testes de aceitação, por parte de técnicos da DCSI, esse software seja colocado em produção. No entanto, existem outras situações em que é do interesse da própria FAP, o acesso a equipamentos em ambiente de produção e Cordeiro (2010) aponta-nos o exemplo do SGH que esteve inoperativo durante um dia, até chegar um técnico da Siemens vindo propositadamente da Alemanha, quando poderia ter resolvido rapidamente a situação se existisse um acesso remoto. E aqui, Cordeiro (2010) identifica duas vantagens que justificam a existência de acessos remotos: a maior margem, para a FAP, na negociação dos contractos de manutenção e a rapidez na resolução de problemas. Manteigas (2010) aponta-nos também um exemplo em que o acesso remoto poderá trazer vantagens: "a empresa "Roche" calibra os equipamentos do laboratório de análises clínicas do Hospital da Força Aérea (HFA) uma vez por mês, por exemplo. Se eles tivessem acesso remoto, a calibração poderia ser feita todos os dias, melhorando a qualidade do serviço.

c. Missões, destacamentos e teletrabalho

Como referiu Faria (2010), e nos confirmou Silva (2010), cada vez existem mais pedidos, à DCSI, de acessos remotos para situações de missões e destacamentos. Existem pedidos do Administrador de Dados da Área Logística (ADAL), por exemplo, para consulta e actualização do Sistema de Informação de Gestão de Manutenção e *Abastecimento* (SIGMA) em situações de missão ou destacamento e, a DCSI não tem capacidade de resposta porque os 25 acessos existentes para "testes" já foram todos distribuídos, como refere Faria (2010), embora este seja um projecto que ainda nem sequer está em produção, uma vez que não existe, oficialmente, uma política de segurança relativa a acessos remotos. Falámos com o ADAL, Silva (2010), que confirma que existem, de facto, mais necessidades que ele está a identificar para reportar à DCSI, e salienta as vantagens

de se poder aceder, em *real-time*, ao SIGMA a partir de qualquer ponto e em qualquer situação. Existem ainda, para além das missões e destacamentos, outros tipos de acessos, em áreas ou serviços, com um volume de trabalho intenso em determinados períodos e em que, trabalhar a partir de casa se revela uma grande mais-valia. No fundo é, como nos diz Faria (2010), "*a criação de um posto de trabalho móvel e remoto que as pessoas podem levar para casa, mantendo todas as funcionalidades que teriam se estivessem a trabalhar, no seu posto de trabalho, na FAP*".

As entrevistas demonstraram que, efectivamente, o maior peso actual dos acessos externos é relativo a acções de manutenção por parte de empresas fornecedoras de software, em particular nas áreas dos Sistemas de armas. No entanto, o acesso externo não se limita a empresas, sendo também efectuado por utilizadores individuais de cariz oficial como missões e destacamentos, e ao nível do teletrabalho. A utilização dos acessos remotos como teletrabalho tem vindo a crescer significativamente, prevendo-se que venha a ser a principal forma de acesso remoto num futuro próximo. Esta tendência constitui um enorme desafio, na medida em que permite obter enormes ganhos em termos de produtividade mas, por outro lado, levanta problemas ao nível da segurança como se irá analisar no capítulo seguinte. **Fica assim comprovada a hipótese H5**.

Relativamente aos benefícios do acesso remoto à RIGFA, os entrevistados foram unânimes em considerar que as vantagens são mútuas, sobretudo ao nível da eficiência do serviço e da produtividade do trabalho. Na medida em que todos estes serviços são, em última instância prestados à FAP, conclui-se que quem mais beneficia com os acessos remotos à RIGFA é a própria FAP, **comprovando-se deste modo a hipótese H6**.

4. Riscos associados à abertura da RIGFA ao exterior e forma de mitigação dos mesmos

Para testar a **Hipótese 7**: "*As principais formas de mitigar os riscos relativos à segurança são a autenticação, compartimentação e acessos aos serviços/aplicações mediante o perfil* (***H7***), pretendemos entender quais os riscos associados à abertura da RIGFA ao exterior e quais as medidas de segurança que existem ou poderão vir a ser adoptadas no futuro. Neste contexto, entrevistámos várias individualidades da DCSI, responsáveis pela segurança dos dados informáticos na FAP. Como nos referiu Manteigas (2010), não existe nenhum mecanismo de segurança absolutamente eficaz e a melhor forma de manter segura a informação de um computador é não o ligar à rede; e mais seguro ainda, é não o ligar de todo. Extrapolando, poderíamos dizer que a melhor forma de manter a informação da RIGFA segura seria não permitir a sua abertura ao exterior, no entanto, essa não parece ser uma alternativa. De acordo com a teoria, e confirmado pelo por Valente (2010), os três vectores da segurança que importa manter garantidos na RIGFA e que podem ser postos em causa pelos acessos remotos, quer de empresas quer de utilizadores internos, são a confidencialidade, a integridade e a disponibilidade.

Relativamente à confidencialidade, tanto Reis (2010) como Gorgulho (2010) alertam para o facto de que existem SI mais sensíveis do que outros. O caso do SGH é apontado como um exemplo em que a confidencialidade tem que ser garantida a todo o custo, uma vez que estes SI possuem dados relativos aos pacientes e aos militares da FA. E é a própria Comissão Nacional de Protecção de Dados (CNPD), na voz do seu presidente, Luís Silveira, em entrevista à Rádio e Televisão de Portugal (RTP)[8], que coloca reservas inclusive na substituição dos processos clínicos em papel por *dossiers* informatizados. Estas situações devem, portanto, ser analisadas cuidadosamente, não só à luz dos imperativos de segurança da FAP, mas também da lei geral, nomeadamente a Lei nº 67/98[9] que regula a protecção de dados pessoais.

Os riscos associados aos acessos remotos à RIGFA, quer seja por empresas quer seja por utilizadores existem mas, no entanto, podem ser mitigados numa relação custo/benefício. Oliveira (2010) dá-nos um exemplo: "*Vamos partir do princípio que temos um Sistema completamente aberto, com acesso a todas as funcionalidades, sem*

8 http://ww1.rtp.pt/wportal/acessibilidades/legendagem/pecas.php?data=2010-02-02&fic=jtarde_1_20100202&peca=11&tvprog=1098 (acedido em Março de 2010)

9 http://www.pofc.qren.pt/ResourcesUser/Legislacao/Lei%2067_98.pdf (acedido em Março de 2010)

restrições de segurança e em que, obviamente, o risco é máximo. Se quisermos diminuir o risco temos duas opções: ou vamos restringindo funcionalidades até deixarmos de ter acessos ou vamos implementando medidas de segurança diminuindo os riscos mas mantendo os acessos". Se nos decidirmos pela primeira opção este trabalho deixa de fazer sentido, por isso iremos escolher a segunda e tentar identificar quais as medidas de segurança que poderão ser implementadas para a diminuição dos riscos dos acessos remotos. Da análise das várias entrevistas, da literatura consultada e da Lei nº 67/98, nomeadamente no seu artº 14º, referente à segurança e tratamento de dados pessoais, classificamos as formas de mitigação dos riscos associados ao acesso remoto à RIGFA nas seguintes categorias: autenticação, compartimentação e acesso aos serviços/aplicações mediante perfil.

a. Autenticação

A DCSI iniciou um projecto-piloto para acessos remotos há cerca de dois anos. Valente (2010) explicou-nos como funciona: "*a solução implementa uma tecnologia, comummente usada, denominada One Time Password (OTP). Existe um servidor na RIGFA que gera uma palavra passe aleatória a cada período de tempo predefinido. Adicionalmente, existem Tokens*[10]*, que estão na posse dos utilizadores que pretendem conectar-se à rede remotamente, e que estão sincronizados com o servidor, ou seja, o software instalado no servidor possui a informação que um Token com um determinado número de série gera uma palavra passe num determinado momento e que no momento seguinte ela deixa de ser válida*". Como ele nos diz, a autenticação pode ser verificada de um modo independente ou complementar através de três formas: "*what you have, what you know and what you are*". *What you are* refere-se à autenticação biométrica como o reconhecimento de voz e leitura da retina ou da impressão digital. Os *Tokens* implementam as outras duas formas de autenticação: *what you have* e *what you know*. Este projecto de acessos remotos começou por ser restrito e limitado à utilização por técnicos da DCSI, para efeitos de testes, com ligações esporádicas e, portanto, com riscos assumidamente baixos, na opinião de Oliveira (2010). No

10 Token é um dispositivo electrónico gerador de senhas, geralmente sem ligação física com o computador. O modelo OTP (One Time Password) pode ser baseado em tempo (time based), que gera senhas dinâmicas a cada fracção de tempo previamente determinada, ou ainda baseado em evento (event based), que gera senhas a cada click do botão, sendo essa senha válida até ao momento da sua utilização.

entanto o projecto cresceu devido às necessidades que existem de acesso à RIGFA em missões ao estrangeiro e outras que, na visão de Rato (2010), é necessário e urgente implementar todas as outras medidas complementares de segurança que os *Tokens*, por si só, não garantem. Este foi, aliás, um dos pontos da agenda de uma das últimas reuniões semanais da DCSI como nos disse Rato (2010).

b. Compartimentação

Uma situação em que é necessário aceder remotamente à RIGFA, ou a determinada áreas da RIGFA, coloca-se no caso das empresas que fornecem e sustentam Sistemas da armas utilizados pela FAP, como são os exemplos do EH101 e do C295. Como foi referido por Rato (2010), ao contrário do que acontecia anteriormente, hoje em dia, todos os Sistemas de armas possuem as suas próprias aplicações informáticas logísticas e faz parte do contracto entre a FAP e essas empresas garantir um acesso remoto para que elas possam actualizar software ou dados. A solução encontrada para minimizar os riscos associados a estes acessos, como nos diz Faria (2010), foi isolar zonas dentro da RIGFA onde essas aplicações estão instaladas e, adicionalmente, criar uma VPN segura para acesso remoto. Assim, as empresas conseguem aceder aos Sistemas a partir da *Internet*, utilizando a RIGFA, mas não conseguem aceder a mais nada para além disso. Existem cada vez mais sistemas já implementados com acesso remoto como o Simulador de Tráfego Aéreo (STA) no Centro de Formação Militar e Técnica da Força Aérea (CFMTFA) e outros ainda em fase de implementação como os sistemas de radar da Base Aérea Nº5 (BA5) e Base Aérea Nº11 (BA11). No entanto Gorgulho (2010), embora não apresentando valores, adverte para o facto de que implementar uma solução técnica para permitir acessos remotos de uma forma segura tem custos elevados e que cada situação deve ser analisada em função dos factores custo/benefício.

c. Acesso a Serviços/Aplicações mediante perfil

Na opinião de Rato (2010), é urgente definir políticas de aceso à informação da RIGFA a partir do exterior. Segundo ele, não é necessário, nem conveniente, disponibilizar toda a informação para o exterior; “existem necessidades focalizadas como é o caso das missões e destacamentos em que é necessário aceder a áreas como o SIAGFA, que inclui o SIGMA, para efeitos de consulta e actualização de

dados. Esse levantamento de necessidades de acesso está neste momento a ser efectuado pelo ADAL, como o próprio nos referiu. Farinha (2010) adverte-nos para o facto de que a solução implementada neste momento, para acessos a partir do exterior, quer para missões, destacamentos ou a partir de casa, comporta elevados riscos uma vez que, segundo ele, "é como se estivéssemos a dar uma tomada de rede remota para as pessoas acederem à RIGFA a partir de casa, sem quaisquer restrições". Uma solução apontada por Oliveira (2010), uma vez feito o levantamento de necessidades de acesso, é a definição de perfis de utilizadores remotos. Assim, cada utilizador remoto teria acesso a uma página *Web* na qual apareceriam só as Aplicações/Serviços a que estaria autorizado a aceder. Isso é, aliás, o que acontece com os utilizadores internos; quando um utilizador acede ao SIAGFA, só lhe aparecem disponíveis as funcionalidades definidas no seu perfil.

Estes resultados obtidos permitem-nos constatar que existe uma consciência, por parte dos responsáveis, das medidas técnicas a implementar para mitigar os riscos de acesso à RIGFA a partir do exterior, devendo essas medidas ser aplicadas caso a caso e numa óptica custo/benefício. **A hipótese H7 foi confirmada parcialmente**, na medida em que a autenticação e a compartimentação estão a ser implementadas, faltando ainda a definição e operacionalização consistentes de medidas de acesso à informação da RIGFA a partir do exterior.

d. Backups

Para testar a nossa **Hipótese 8***: "O actual plano de segurança e recuperação de dados é eficaz para repor a situação dos dados informáticos em caso de perda provocada pela maior abertura da RIGFA ao exterior" **(H8)***, colocamos questões relacionadas com os planos se segurança e recuperação de dados existentes e a sua fiabilidade. A este respeito, foram abordadas questões relacionadas com os *backups.* Até hoje, como nos refere Manteigas (2010), "nunca foi necessário utilizar os *backups* para recuperar ficheiros corrompidos por falha de segurança devida a acessos remotos, mas pode acontecer e é para situações como essa que eles existem; e quando fizerem falta, deverão estar actualizados". O sistema de *backups* da FAP é descentralizado, ou seja, cada Unidade ou LAN possui o seu sistema autónomo de *backup*.

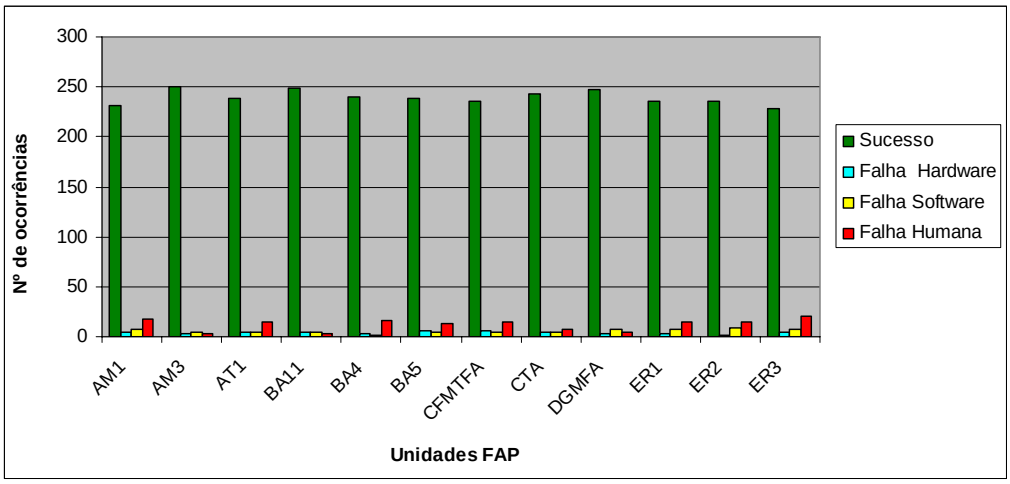


Figura 7 – Resultado dos backups das LAN's da FAP, com sistema de Backup Manual, durante o ano de 2009

As falhas na execução do *backup* devem-se a três factores (*hardware*, *software* ou falha humana). Nas LAN de maior dimensão (Alfragide, CA, Lumiar, BA6, AFA) estão já instalados, ou em fase de instalação sistemas de *backup* automatizados que não requerem intervenção humana, o que reduz significativamente as falhas, já que, as causas humanas, nos sistemas em que a sua intervenção é requerida, são as mais significativas como se pode verificar no gráfico da figura 7. Do total das 3132 ocorrências de operações de *backup*, em todas as Unidades da FAP que não possuem sistema automático, durante o ano de 2009, 2870 (91,7%) tiveram sucesso, 49 (1,6%) falharam por motivos de *hardware*, 68 (2,1%) falharam por motivos de *software* e 145 (4,6%) não tiveram sucesso devido a falha humana.

Uma das formas de eliminar as falhas humanas seria implementar sistemas automatizados em todas as LAN, no entanto, o custo de tal solução não se justifica nalgumas Unidades da FAP devido ao reduzido número de servidores que possuem. Como alternativa, como nos explica Manteigas (2010), os *backups* dos servidores das Unidades mais pequenas poderão passar a ser efectuados pelos sistemas de *backup* das Unidades em que essas soluções estiverem implementadas caso a velocidade de tráfego entre essas Unidades seja suficiente.

As opiniões manifestadas nas entrevistas e as avaliações efectuadas vão no sentido de **confirmar parcialmente a hipótese H8**, uma vez que existe a consciência de que o

sistema não é perfeito, por não estar totalmente automatizado, estando sujeito a falha humana.

Conclusões

O presente trabalho foi concebido para responder à questão central "**Quais as implicações de uma eventual maior abertura da RIGFA ao exterior**?", tendo sido definidos três objectivos fundamentais: (i) avaliar a necessidade, importância, benefícios e a percepção que os utilizadores da RIGFA, nas diversas áreas funcionais, têm relativamente ao seu acesso a partir do exterior; (ii) fazer uma caracterização dos acessos remotos à RIGFA, nomeadamente em termos das principais necessidades e benefícios; (iii) identificar os riscos associados à abertura da RIGFA ao exterior e forma de mitigação dos mesmos.

No decurso do trabalho utilizamos o método de investigação em Ciências Sociais proposto por Quivy e Campenhoudt (2003). Foram definidas 5 questões derivadas e 8 hipóteses. Para testar as hipóteses, realizamos um inquérito a uma amostra de 50 utilizadores regulares da RIGFA e 10 entrevistas a especialistas. A combinação da análise quantitativa com a análise qualitativa, permitiu-nos validar totalmente seis das hipóteses e parcialmente as restantes duas.

As hipóteses totalmente validadas são as seguintes: "Todas as áreas funcionais manifestam de igual modo a necessidade de aceder à informação a partir do exterior da RIGFA" (**H1)**; **"**Os utilizadores consideram que, tanto eles como o serviço beneficiariam com o acesso remoto" (**H2)**; **"**Os utilizadores consideram importante o acesso remoto à RIGFA a partir de casa" (**H3)**; **"**Os utilizadores atribuem um grau de importância diferente ao acesso às várias Aplicações/Serviços a partir de casa" (**H4**); "A principal necessidade de acesso remoto à RIGFA a partir do exterior refere-se à manutenção, por parte das Empresas, das suas aplicações informáticas" (**H5**); **"**Quem beneficia mais do acesso à RIGFA a partir do exterior é a própria FAP" (**H6**).

As duas hipóteses validadas parcialmente são: "As principais formas de mitigar os riscos relativos à segurança são a autenticação, compartimentação e acessos aos serviços/aplicações mediante perfil" (**H7**); "O actual plano de segurança e recuperação de dados é eficaz para repor a situação dos dados informáticos em caso de perda provocada pela maior abertura da RIGFA ao exterior" (**H8**).

Os resultados obtidos, permitem-nos alcançar os propósitos definidos e responder à questão central, podendo-se concluir que: por um lado, há uma grande necessidade de aceder remotamente à RIGFA, dado que a maior parte dos utilizadores tem que trabalhar

fora do horário normal, quer ficando no local de trabalho, quer deslocando-se ao mesmo fora das horas de expediente; o acesso remoto é considerado importante e muito importante; os benefícios do acesso remoto são mútuos, embora, quem beneficie mais seja a FAP.

Por outro lado, existem certas limitações desta abertura ao exterior, nomeadamente ao nível da segurança. Há uma consciência por parte dos especialistas para este problema, estando a ser implementadas procedimentos ao nível da autenticação, com uma solução *One Time Password*. No entanto, face à crescente necessidade de acesso remoto, este sistema não garante totalmente a segurança, estando a ser discutidas medidas complementares de segurança. Ao nível da compartimentação, estão também a ser implementadas medidas de segurança, com acessos por parte das empresas delimitados através de VPN segura. No entanto, esta medida é limitada, estando a ser implementadas e em fase de implementação outras medidas mais adequadas. As soluções a implementar devem passar sempre por uma avaliação custo/benefício tendo em conta cada caso específico. No que respeita aos acessos aos serviços/aplicações mediante perfil, as medidas implementadas são reconhecidamente insuficientes, existindo a consciência de que é necessário a criação de medidas consistentes de acesso à informação através da definição de perfis de utilizadores remotos com níveis diferenciados de acesso, tal como já existe com os utilizadores internos.

Em termos globais, os resultados obtidos, permitem-nos responder à nossa questão central, indicando que as principais implicações de uma maior abertura da RIGFA ao exterior se prendem essencialmente com a segurança. Ao longo do trabalho, tornou-se evidente que não existem soluções perfeitas, sendo necessário fazer uma avaliação sistemática e cuidada dos custos/benefícios desta abertura. Se por um lado, é desejável e vantajoso uma maior abertura ao exterior, por outro lado, existem riscos associados que devem ser mitigados, através de medidas e procedimentos de segurança. Desta forma, os riscos não devem ser interpretados como impeditivos da abertura ao exterior.

O principal contributo deste trabalho é o facto de se ter analisado as duas partes do complexo problema relacionado com a abertura da RIGFA ao exterior, tendo-se identificado algumas necessidades dos utilizadores que vão no sentido da maior abertura, e também identificado no ponto de vista dos especialistas, os principais desafios que esta abertura levanta. Esta dupla perspectiva é importante na definição de politicas de

segurança e, sobretudo, de adequação dessas mesmas politicas à realidade, que passa por uma análise custo/benefício tendo em conta cada caso concreto.

As recomendações apresentadas, surgem em parte, da identificação de lacunas nas duas últimas hipóteses, indo precisamente neste sentido, de se afirmar a necessidade de definição de políticas de acesso remoto, e operacionalização das mesmas.

AO EMFA/DIVCSI – Definir políticas de acesso remoto, tanto para as empresas, como para os utilizadores, ao nível das missões, destacamentos e do teletrabalho;

AO CLAFA/DCSI – Implementar soluções técnicas de gestão de perfis de utilizadores remotos; implementar medidas de segurança para cada projecto que implique necessidades de acesso remoto por parte de empresas; diminuir ou eliminar a intervenção humana nos *backups* de forma a reduzir as falhas;

Aos Administradores de Dados – Quantificar o número de acessos necessários; identificar as aplicações/serviços a disponibilizar para o exterior; e definir os perfis de utilizadores remotos, em função das aplicações/serviços a que cada utilizador pode aceder;

Aos Gestores de projectos – Envolver a DCSI o mais possível nas fases iniciais de aquisição de Sistemas de armas e outros, de forma a que logo a montante seja possível a adaptação dos sistemas informáticos às políticas de segurança da FAP, e também de forma a garantir a máxima compatibilidade e interoperabilidade com os SI da FAP.

Glossário

Acesso remoto – Conexão à distância entre um dispositivo isolado (terminal ou computador) e uma rede.

Advanced Research Projects Agency Network – A ARPANET foi criada pela *Defense Advanced Research Projects Agency* (DARPA) do Departamento de Defesa dos Estados Unidos, foi a primeira rede de comutação de pacotes de dados operacional do mundo e a antecessora da Internet global contemporânea.

Aplicação web – Na engenharia de software, uma aplicação web é uma aplicação que é acedida por um navegador da Web através de uma rede como a Internet ou uma intranet

Ataque de negação de serviço – (Denial-of-Service) é uma tentativa para tornar os recursos de um sistema indisponíveis para os seus utilizadores legítimos. Os alvos típicos são os servidores WEB e o ataque tenta tornar indisponíveis na Internet as páginas hospedadas. Não se trata de uma invasão do sistema, mas sim da sua invalidação por sobrecarga. Os ataques de negação de serviço forçam o sistema vítima a reinicializar ou consumir todos os recursos como a memória ou a capacidade de processamento. Isso é conseguido através de pedidos contínuos, executados de forma automática por programas maliciosos, a partir de diversas localizações, ao sistema vítima.

Bell Telephone Laboratories ou Bell Labs – Era originalmente o braço de pesquisa e de desenvolvimento AT&T dos Estados Unidos, desenvolvendo uma série de tecnologias consideradas revolucionárias desde comutadores telefónicos, cabos de telefone, transístores, LEDs, lasers, a linguagem de programação C e o sistema operativo Unix

Bolt, Beranek and Newman – A BBN é uma empresa de alta tecnologia que fornece serviços de investigação e desenvolvimento. A BBN situa-se em Cambridge, Massachusetts, EUA. É talvez mais conhecida pelo seu trabalho pioneiro no desenvolvimento de transmissão de pacotes de dados (incluindo a ARPANET e a Internet)

Browser – Programa informático que habilita seus utilizadores a interagirem com documentos virtuais da Internet e Intranet, também conhecidos como páginas da Web.

Criptografia – (Do Grego *kryptós*, "escondido", e *gráphein*, "escrita") é o estudo dos princípios e técnicas pelas quais a informação pode ser transformada da sua forma original para outra ilegível, de forma que possa ser conhecida apenas pelo seu destinatário (detentor

da "chave secreta"), o que a torna difícil de ser lida por alguém não autorizado. Assim sendo, só o receptor da mensagem pode ler a informação com facilidade.

Defense Advanced Research Projects Agency – A DARPA é uma agência do Departamento de Defesa dos Estados Unidos, responsável pelo desenvolvimento de novas tecnologias para uso militar. O seu nome original era simplesmente Advanced Research Projects Agency (ARPA), mas foi renomeado para DARPA (de Defesa) durante Março de 1972. Em Fevereiro de 1993 volta a designar-se ARPA e, finalmente, é renomeada DARPA em Março de 1996.

Ethernet – É uma tecnologia de interconexão de computadores para redes locais (LANs). O nome vem do conceito físico de éter. Ela define o tipo de cabo e os sinais eléctricos para a camada física, e também o formato dos pacotes e protocolos para a camada Media Access Control (MAC) do modelo OSI. A partir da década de 1990, ela passou a ser a tecnologia de Local Área Network (LAN) mais utilizada.

George Stibitz (1904 – 1995) – Foi um investigador americano cujos trabalhos mais conhecidos foram realizados nas décadas de 1930 e 1940 e eram sobre circuitos digitais baseados em lógica booleana, usando relés electromecânicos como comutadores. No ano de 1937, George Stibitz constrói no "Bell Telephone Laboratories" o primeiro calculador binário. No ano de 1940 Ainda no "Bell Telephone Laboratories", ele demonstrou o "Complex Number Calculator" que deve ter sido o primeiro computador digital. E nesse ano foi também criado o primeiro terminal

International Data Corporation – A IDC é uma empresa de pesquisa de mercado e de análise, especializada em tecnologias de informação e telecomunicações.

Internet – Rede global que conecta milhares de redes independentes.

Intranet – Rede privada que usa as mesmas tecnologias da Internet, funciona dentro de uma LAN ou WAN de uma organização.

Joseph Carl Robnett Licklider (1915 – 1990) – Conhecido simplesmente como JCR ou "Lick" foi um cientista da computação norte-americano, considerado uma das figuras mais importantes na história da ciência da computação e informática em geral. Estudou matemática e física e recebeu um doutoramento em psicologia da Universidade de Rochester (NY). Leccionou na Universidade de Harvard antes de ingressar na faculdade no MIT (1949-57, 1966-85). Como líder do grupo na Advanced Research Projects Agency

(ARPA), em 1960, incentivou a pesquisa em time-sharing e ajudou a lançar as bases para redes de computadores e ARPANET, a antecessora da Internet.

Mainframe – É um computador de grande porte, dedicado normalmente ao processamento de um grande volume de informações. Os mainframes são capazes de oferecer serviços de processamento a milhares de utilizadores através de milhares de terminais ligados directamente ou através de uma rede.

Navegador – Um navegador, também conhecido pelos termos ingleses *web browser* ou simplesmente *browser*, é um programa de computador que permite aos utilizadores interagirem com documentos virtuais da Internet, também conhecidos como páginas de Web

One Time Password – A senha única (OTP) é uma senha que só é válida para uma única sessão de login. A senha única evita uma série de deficiências que estão associados às tradicionais senhas estáticas. A lacuna mais importante que é colmatada pelas OTP's é que, ao contrário das senhas estáticas, elas não são vulneráveis a ataques de repetição. Isto significa que, se um potencial intruso conseguir gravar uma OTP que já foi usada para fazer *login* num serviço ou para realizar uma transacção, ele não será capaz de a reutilizar, uma vez que a OTP deixará de ser válida.

Palo Alto Research Center – O PARC é uma empresa de investigação e desenvolvimento, em Palo Alto, Califórnia, com uma excelente reputação pela sua contribuição para as tecnologias da informação. Fundada em 1970 como uma divisão da Xerox Corporation, o PARC foi responsável pelo desenvolvimento de tecnologias importantes das quais se destacam a impressão a laser, a Ethernet e o *interface* gráfico do moderno computador pessoal.

Secure Sockets Layer – É uma tecnologia de segurança que é utilizada para codificar os dados transferidos entre o computador de um utilizador e um website. O protocolo SSL, através de um processo de encriptação dos dados, previne que os dados transmitidos possam ser interceptados, ou mesmo alterados no seu percurso entre o navegador (browser) do utilizador e o site com o qual ele está ligado, garantindo desta forma a troca de informações confidenciais como os dados de cartão de crédito.

Servidor – Máquina computacional com grande capacidade de armazenamento e processamento de dados.

Servidor *proxy* – Em redes de computadores, um servidor *proxy* é um servidor que actua como um intermediário para solicitações de clientes que procuram recursos de outros servidores. Um cliente conecta-se ao servidor *proxy*, solicitando algum serviço, como um ficheiro, uma página *web* ou outro recurso disponível a partir de um servidor diferente. O servidor *proxy* avalia o pedido, de acordo com suas regras de filtragem, e se este for validado pelo filtro, o *proxy* efectua a conexão com o servidor em causa e solicita o serviço em nome do cliente

Teletrabalho – Trabalho que é realizado quando se está a utilizar equipamentos que permitem que o trabalho efectivo tenha efeito num lugar diferente do que é ocupado pela pessoa que o está a realizar. O teletrabalho foi um conceito referido pela 1ª vez por Jack Nilles em 1973 e, genericamente, refere-se ao trabalho que é levado a cabo numa localização afastada dos escritórios centrais ou da fábrica, onde o trabalhador não tem qualquer contacto pessoal com os seus colegas de trabalho, mas pode comunicar com eles através da utilização das novas tecnologias, logo a única diferença entre o trabalho tradicional e o teletrabalho, é que este é feito à distância e recorre ás tecnologias de informação para comunicar.

Teletypewriter ou Teleimpressor – é uma máquina de escrever electromecânica que pode ser usada para enviar mensagens dactilografadas de um ponto a outro através de uma variedade de canais de comunicação que vão desde uma simples ligação eléctrica com um par de fios até à utilização de sinais de rádio e microondas como meio de transmissão.

Telnet – É um protocolo de login remoto, "cliente-servidor", usado para permitir a comunicação entre computadores ligados numa rede (exemplos: rede local / LAN, Internet), baseado em TCP.

Token – É um dispositivo electrónico gerador de senhas, geralmente sem ligação física com o computador. O modelo OTP (One Time Password) pode ser baseado em tempo (time based), que gera senhas dinâmicas a cada fracção de tempo previamente determinada, ou ainda baseado em evento (event based), que gera senhas a cada click do botão, sendo essa senha válida até ao momento da sua utilização.

Transmission Control Protocol / Internet Protocol – O Internet Protocol Suite (normalmente conhecido por TCP/IP) é um conjunto de protocolos de comunicação utilizado na Internet e na generalidade das redes. O seu nome deriva dos dois mais importantes protocolos que o compõem: o Transmission Control Protocol (TCP) e o

Internet Protocol (IP), que foram os dois primeiros protocolos de rede definidos neste padrão. Actualmente, as redes de IP representam uma síntese de vários desenvolvimentos que começaram nos anos de 1960 e 1970, nomeadamente a Internet e LAN's (Local Area Networks) e que tiveram um enorme desenvolvimento em finais da década de 1980, juntamente com o advento da World Wide Web (WWW) no início de 1990.

Virtual Private Network – É uma rede de comunicações privada normalmente utilizada por uma empresa ou um conjunto de empresas e/ou instituições, construída em cima de uma rede de comunicações pública (como por exemplo, a Internet).

Virtual Private Network Segura – As VPN's seguras usam protocolos de criptografia por tunelamento que garantem a confidencialidade, autenticação e integridade necessárias para garantir a privacidade das comunicações. Quando implementados adequadamente, estes protocolos podem assegurar comunicações seguras através de redes inseguras.

World Wide Web – A WWW (que em português significa, "Rede de alcance mundial"; também conhecida como Web) é um sistema de documentos interligados e executados na Internet.

Bibliografia

Livros/Artigos

- BRAGA, Carlos A. P. (1989). A economia mundial e a revolução dos serviços. Revista de Economia Política, Vol. 9, Nº2, Abril-Junho/1989 p. 94-107.
- CASTELLS, Manuel (1999). A sociedade em rede. São Paulo: Paz e Terra.
- CHIAVENATO, Idalberto (1999). Gestão de Pessoas. 1ª ed., Rio de Janeiro: Editora Campus.
- FICHER, Royal P. (1994). Information Systems Security. New Jersey: Prentice-Hall, Inc., Englewood Cliffs.
- MORIMOTO Carlos E. (2008). Redes, Guia Prático, São Paulo: GDH Press e Sul Editores
- NILLES, Jack M. (1997). Fazendo do Teletrabalho uma Realidade. São Paulo: Editora Futura
- QUIVY, Raymond, CAMPENHOUDT, Luc Van (2003). Manual de Investigação em Ciências Sociais. 3ª Ed., Lisboa: Gradiva - Publicações, Lda.
- SCHNEIER, Bruce (2004). Secrets & Lies. Didital Security in a Networked World. Indianápolis, Indiana: Wiley Publishing, Inc.
- TOFFLER, Alvin (1984). A Terceira Vaga, Lisboa: Edições Livros do Brasil.
- TOFFLER, Alvin, TOFFLER Heidi (2007). A revolução da riqueza: como será criada e como alterará as nossas vidas. 3ª ed., Lisboa: Actual Editora.
- VAZ, Ana (2007). Segurança da Informação, Protecção da Privacidade e dos Dados Pessoais. NAÇÃO & DEFESA, Verão 2007, Nº117, 3ª Série p. 35-63.
- WALDROP, Mitchell M. (2001). The Dream Machine: J. C. R. Licklider and the Revolution That Made Computing Personal. New York, NY: Viking Penguin.
- WEISER, Mark David; GOLD, Rich, BROWN, John Seely (2001). The origins of ubiquitous computing research at PARC in the late 1980s. IBM Systems Journal, Vol 38, Nº4, p.693 - 696

Internet

- DIÁRIO DA REPÚBLICA – I SÉRIE-A Nº 247 – 26-10-1998. Lei nº 67/98 de 26 de Outubro. *Lei da Protecção de Dados Pessoais*, [referência de 02 de Abril de 2010]. Disponível na Internet em: <http://www.pofc.qren.pt/ResourcesUser/Legislacao/Lei%2067_98.pdf>
- HOLLIDAY, Mark A. (2009). History of Information Technology, [referência de 24 de Abril de 2010]. Disponível na Internet em: < http://polaris.cs.wcu.edu/~holliday/teaching/fall09/cs210.02/lectureNotes/LectureChapter1.pdf >.
- ISEP, DEI (2006). Análise e *benchmarking* de plataformas tecnológicas de suporte a ambientes de Teletrabalho, [referência de 02 de Fevereiro de 2010]. Disponível na Internet em: <http://www.dei.isep.ipp.pt/paf/proj/Jan2006/PROJCS_teletrabalho_1970336.pdf>.
- KENNY, Brian J., LIPSCHUTZ, Robert P. (2003). Secure Remote Access, [referência de 18 de Fevereiro de 2010]. Disponível na Internet em: <http://www.pcmag.com/article2/0,2817,981215,00.asp>.
- LEINER, Barry M., CERF, Vinton G.; CLARK, David D.; KAHN, Robert E.; KLEINROCK, Leonard; LYNCH, Daniel C.; POSTEL, ROBERTS, Larry G.; WOLFF, Stephen (2003). A Brief History of the Internet, [referência de 23 de Abril de 2010]. Disponível na Internet em: <http://www.isoc.org/internet/history/brief.shtml>.
- NATRAJAN, Jayanthy (2007). Evolution of Computer Networks, [referência de 24 de Abril de 2010]. Disponível na Internet em: <http://networking.ittoolbox.com/documents/evolution-of-computer-networks-12521>.
- Revolução da Informação. In Infopédia [Em linha]. Porto: Porto Editora, 2003-2010. [referência de 20 de Abril de 2010]. Disponível na Internet em: <http://www.infopedia.pt/$revolucao-da-informacao>.
- RONDA, Hauben (2001). From the ARPANET to the Internet [referência de 24 de Abril de 2010]. Disponível na Internet em: <http://www.columbia.edu/~rh120/other/tcpdigest_paper.txt>.
- SILVEIRA, Luís (2010). *Entrevista ao Jornal da tarde da RTP*, [referência de 02 de Abril de 2010]. Disponível na Internet em:

<http://ww1.rtp.pt/wportal/acessibilidades/legendagem/pecas.php?data=2010-02-02&fic=jtarde_1_20100202&peca=11&tvprog=1098>.

– TOMÁS, João (2006). Análise e *brenchmarking* de plataformas tecnológicas de suporte a ambientes de Teletrabalho, [referência de 16 de Fevereiro de 2010]. Disponível na Internet em: <http://www.dei.isep.ipp.pt/~paf/proj/Jan2006/PROJCS_teletrabalho_1970336.pdf>.

Entrevistas

– CAP/ENGEL Farinha, João. (Março de 2010). *Direcção de Comunicações e Sistemas de Informação*. *Repartição de Comunicações, Sensores e Navegação*. Alfragide.

– CAP/TINF Valente, António. (Março de 2010). *Direcção de Comunicações e Sistemas de Informação*. *Repartição de Tecnologias de Informação*. Alfragide.

– COR/TINF Rato, Moreira. (Março de 2010). *Subdirector da Direcção de Comunicações e Sistemas de Informação*. Alfragide.

– MAJ/ENGEL Faria, Elisabete. (Março de 2010). *Direcção de Comunicações e Sistemas de Informação*. *Chefe da Repartição de Comunicações, Sensores e Navegação*. Alfragide.

– MAJ/ENGINF Gorgulho, José. (Março de 2010). *Direcção de Comunicações e Sistemas de Informação*. *Chefe da Repartição de Tecnologias de Informação*. Alfragide.

– MAJ/TINF Cordeiro, Miguel. (Janeiro de 2010). *Hospilal da Força Aérea*. *Chefe do Centro de Informática*. Lumiar.

– TCOR/TINF Manteigas, Jorge. (Março de 2010). *Direcção de Comunicações e Sistemas de Informação*. *Gabinete da Direcção*. Alfragide.

– TCOR/TINF Reis, Filipe. (Março de 2010). *Direcção de Comunicações e Sistemas de Informação*. *Chefe da Repartição de Sistemas de Informação*. Alfragide.

– TCOR/TMMEL Silva, Gustavo. (Março de 2010). *Comando Logistico e Administrativo da Força Aérea. Administrador de Dados da Área Logística*. Alfragide.

– TEN/TINF Oliveira, António. (Março de 2010). *Direcção de Comunicações e Sistemas de Informação*. *Repartição de Comunicações, Sensores e Navegação*. Alfragide.

ANEXO A

Quadro síntese do modelo de análise

Perguntas derivadas	Hipóteses	Conceitos	Dimensões	Componentes	Indicadores
Em que áreas ou serviços se poderá colocar a necessidade de aceder à informação a partir do exterior da RIGFA? (**QD1**)	Todas as áreas funcionais manifestam de igual modo a necessidade de aceder à informação a partir do exterior da RIGFA (**H1**)	Áreas funcionais			– Operações – Manutenção – Apoio – Tecnologias de Informação
		Necessidades de acesso à informação	Permanecer no serviço após horário normal	Frequência de permanência	– Nunca – 1 vez – Entre 2 e 5 vezes – 6 vezes ou mais
			Deslocar-se ou ter intenção de se deslocar à Unidade fora do horário normal	Frequência de deslocação ou intenção de se deslocar	– Nunca – 1 vez – Entre 2 e 5 vezes – 6 vezes ou mais
		– Acesso à RIGFA a partir do exterior	– Acesso remoto	– Acesso seguro – Acesso não seguro	
Qual a percepção que os utilizadores têm acerca da importância do acesso à RIGFA a partir do exterior? (**QD2**)	Os utilizadores consideram que, tanto eles como o serviço beneficiariam com o acesso remoto (**H2**)	Áreas funcionais			– Operações – Manutenção – Apoio – Tecnologias de Informação
		Percepção		Beneficiário do acesso	– O próprio – A Organização – Ambos – Ninguém
		Acesso à RIGFA a partir do exterior			
	Os utilizadores consideram importante o acesso remoto à RIGFA a partir de casa (**H3**)	Áreas funcionais			– Operações – Manutenção – Apoio – Tecnologias de Informação
		Percepção		Grau de importância do acesso remoto aos PC's	– Nada importante – Pouco importante – Importante – Muito importante
		– Acesso à RIGFA a partir do exterior	– Acesso remoto	– Acesso seguro – Acesso não seguro	–
	Os utilizadores atribuem um grau de importância diferente ao acesso às várias Aplicações/ serviços a partir de casa (**H4**)	Áreas funcionais			– Operações – Manutenção – Apoio – Tecnologias de Informação
		Percepção		Grau de importância do acesso às Aplicações/ serviços da RIGFA a partir do exterior	– Nada importante – Pouco importante – Importante – Muito importante
		Acesso às Aplicações/ serviços da RIGFA a partir do exterior		Tipologia de aplicações/ serviços	– Portal FAP – E-mail – GroupWise – Ficheiros de rede – SIAGFA Acesso ao PC

Perguntas derivadas	Hipóteses	Conceitos	Dimensões	Componentes	Indicadores
Como se caracteriza o acesso à RIGFA a partir do exterior? (**QD3**)	A principal necessidade de acesso remoto à RIGFA a partir do exterior refere-se à manutenção, por parte das Empresas, das suas aplicações informáticas (**H5**)	– Necessidades de acesso	– Tipo de aplicações	– Aplicações hospitalares	– Sistema de patologia clínica – Sistema de gestão de doentes – Sistema de arquivo de imagem – Sistema de cuidados intensivos
				– Aplicações de gestão	– Bibliotecas – Gestão documental
				– Aplicações da área operacional	– C295 – EH101 – Simulador de tráfego Aéreo – Sistemas de radar
			– Frequência de acesso		– Diária – Semanal – Mensal
		– Acesso à RIGFA a partir do exterior	– Acesso remoto	– Acesso seguro – Acesso não seguro	
		– Entidades que acedem à RIGFA a partir do exterior	– Empresas		– Siemens – Roche – Glint – Papelaco – Eurocontrol – EADS CASA – Augusta Westland
			– Utilizadores		– Em missões – Teletrabalho
	Quem beneficia mais do acesso à RIGFA a partir do exterior é a própria FAP (**H6**)	– Acesso à RIGFA a partir do exterior	– Acesso remoto	– Acesso seguro – Acesso não seguro	–
		Benefícios do acesso à RIGFA a partir do exterior	– Vantagens nos contractos de manutenção	– Vantagens financeiras – Qualidade do serviço – Flexibilidade de acesso	
			– Tempos de resposta na resolução de problemas mais curtos	– Service Level Agreement (SLA)	– 4 horas – 24 horas

Perguntas derivadas	Hipóteses	Conceitos	Dimensões	Componentes	Indicadores
Quais as formas de mitigar os riscos relativos à segurança dos dados informáticos, associados à abertura da RIGFA ao exterior? (**QD4**)	As principais formas de mitigar os riscos relativos à segurança são a autenticação, compartimentação e acessos aos serviços/aplicações mediante perfil (**H7**)	Riscos associados à abertura da RIGFA ao exterior)			– Confidencialidade – Integridade – Disponibilidade
		Medidas de segurança dos dados informáticos			– Autenticação – Compartimentação – Acessos aos serviços/aplicações mediante o perfil
		– Acesso à RIGFA a partir do exterior	– Acesso remoto	– Acesso seguro – Acesso não seguro	
Em que medida a adopção de um plano de segurança e recuperação de dados eficaz permite repor a situação dos dados informáticos em caso de perda provocada pela maior abertura da RIGFA ao exterior? (**QD5**)	O actual plano de segurança e recuperação de dados é eficaz para repor a situação dos dados informáticos em caso de perda provocada pela maior abertura da RIGFA ao exterior (**H8**)	Plano de segurança e recuperação de dados.	Procedimentos de segurança e recuperação de dados		– Backup – Recuperação
			Execução dos procedimentos de segurança e recuperação de dados	Falhas nos procedimentos de segurança e recuperação de dados	– Humanas – Software – Hardware
		Recuperação de dados informáticos	Tempo		– 15 minutos – 30 minutos – 1 hora – 24 horas
			Conteúdo		– Total – Parcial
		– Acesso à RIGFA a partir do exterior	– Acesso remoto	– Acesso seguro – Acesso não seguro	

ANEXO B

QUESTIONÁRIO SOBRE ACESSO REMOTO À RIGFA

1. Área funcional a que pertence: **(Q1)**

1	Operações	
2	Manutenção	
3	Apoio	
4	Tecnologias de Informação	

2. Alguma vez permaneceu no serviço, após o horário normal, para resolver uma situação que poderia resolver a partir de casa se tivesse aceso a uma ligação remota ao seu Posto de Trabalho (PC) ou a Serviços da Rede Interna Geral da Força Aérea (RIGFA)? **(Q2)**

1	Nunca	
2	1 vez	
3	Entre 2 e 5 vezes	
4	6 vezes ou mais	

3. Alguma vez se deslocou ou teve intenção de se deslocar à Unidade, fora do horário normal, para resolver uma situação que poderia resolver a partir de casa se tivesse aceso a uma ligação remota ao seu PC ou a Serviços da RIGFA? **(Q3)**

1	Nunca	
2	1 vez	
3	Entre 2 e 5 vezes	
4	6 vezes ou mais	

4. Quem acha que beneficiaria no caso de poder aceder remotamente a partir de casa ao seu PC ou Serviços da RIGFA? **(Q4)**

1	O próprio	
2	A Organização	
3	Ambos	
4	Ninguém	

5. Classifique a importância do acesso remoto a PC's ou a Serviços da RIGFA a partir de casa, de uma forma genérica: **(Q5)**

Nada importante	Pouco importante	Importante	Muito importante

6. Classifique o acesso remoto às seguintes Aplicações/Serviços da RIGFA a partir de casa:

		Nada importante	Pouco importante	Importante	Muito importante
1	Portal FAP **(Q6)**				
2	E-mail **(Q7)**				
3	GroupWise **(Q8)**				
4	Ficheiros de rede **(Q9)**				
5	SIAGFA **(Q10)**				
6	Acesso ao seu PC **(Q11)**				

ANEXO C

Tratamento dos dados dos Inquéritos (Frequências)

FREQUENCIES VARIABLES=area_funcional permaneceu_servico deslocou_se_unidade quem_beneficia importancia_acesso_remoto acesso_portal_f ap acesso_email acesso_groupwise acesso_ficheiros_rede acesso_siagfa acesso_pc /BARCHART FREQ /ORDER=ANALYSIS.

Frequencies

Notes

	Output Created	28-Fev-2010 19:00:16
	Comments	
Input	Data	E:\CPOS0910\WORK\Trabalho\spss_tratados\questionario.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	50
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics are based on all cases with valid data.
	Syntax	FREQUENCIES VARIABLES=area_funcional permaneceu_servico deslocou_se_unidade quem_beneficia importancia_acesso_remoto acesso_portal_fap acesso_email acesso_groupwise acesso_ficheiros_rede acesso_siagfa acesso_pc /BARCHART FREQ /ORDER=ANALYSIS.
Resources	Processor Time	0:00:04.172
	Elapsed Time	0:00:04.235

[DataSet1] E:\CPOS0910\WORK\Trabalho\spss_tratados\questionario.sav

Statistics

	N	
	Valid	Missing
Área funcional	50	0
Permaneceu no serviço após horário normal	50	0
Deslocou-se ao serviço fora do horário normal	50	0
Quem acha que beneficia com o acesso remoto	50	0
Classificação da Importância do acesso remoto ao PC ou serviços RIGFA	50	0
Classificação da importância do acesso remoto ao Portal FAP	50	0
Classificação da importância do acesso remoto ao e-mail	50	0
Classificação da importância do acesso remoto ao GroupWise	50	0
Classificação da importância do acesso remoto aos ficheiros de rede	50	0
Classificação da importância do acesso remoto ao SIAGFA	50	0
Classificação da importância do acesso remoto ao PC	50	0

Frequency Table

Área funcional

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Operações	9	18,0	18,0	18,0
	Manutenção	14	28,0	28,0	46,0
	Apoio	22	44,0	44,0	90,0
	TI	5	10,0	10,0	100,0
	Total	50	100,0	100,0	

Permaneceu no serviço após horário normal

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nunca	3	6,0	6,0	6,0
	1 vez	3	6,0	6,0	12,0
	entre 2 a 5 vezes	11	22,0	22,0	34,0
	6 ou mais vezes	33	66,0	66,0	100,0
	Total	50	100,0	100,0	

Frequency Table (cont.)

Deslocou-se ao serviço fora do horário normal

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nunca	13	26,0	26,0	26,0
	1 vez	3	6,0	6,0	32,0
	entre 2 a 5 vezes	11	22,0	22,0	54,0
	6 ou mais vezes	23	46,0	46,0	100,0
	Total	50	100,0	100,0	

Quem acha que beneficia com o acesso remoto

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	O próprio	0	0,0	0,0	0,0
	A Organização	7	14,0	14,0	14,0
	Ambos	43	86,0	86,0	100,0
	Ninguém	0	0,0	0,0	100,0
	Total	50	100,0	100,0	

Classificação da Importância do acesso remoto ao PC ou serviços RIGFA

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nada importante	0	0,0	0,0	0,0
	Pouco importante	1	2,0	2,0	2,0
	Importante	19	38,0	38,0	40,0
	Muito importante	30	60,0	60,0	100,0
	Total	50	100,0	100,0	

Frequency Table (cont.)

Classificação da importância do acesso remoto ao Portal FAP

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nada importante	1	2,0	2,0	2,0
	Pouco importante	12	24,0	24,0	26,0
	Importante	23	46,0	46,0	72,0
	Muito importante	14	28,0	28,0	100,0
	Total	50	100,0	100,0	

Classificação da importância do acesso remoto ao e-mail

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nada importante	0	0,0	0,0	0,0
	Pouco importante	2	4,0	4,0	4,0
	Importante	18	36,0	36,0	40,0
	Muito importante	30	60,0	60,0	100,0
	Total	50	100,0	100,0	

Classificação da importância do acesso remoto ao GroupWise

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nada importante	0	0,0	0,0	0,0
	Pouco importante	2	4,0	4,0	4,0
	Importante	17	34,0	34,0	38,0
	Muito importante	31	62,0	62,0	100,0
	Total	50	100,0	100,0	

Frequency Table (cont.)

Classificação da importância do acesso remoto aos ficheiros de rede

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nada importante	0	0,0	0,0	0,0
	Pouco importante	1	2,0	2,0	2,0
	Importante	23	46,0	46,0	48,0
	Muito importante	26	52,0	52,0	100,0
	Total	50	100,0	100,0	

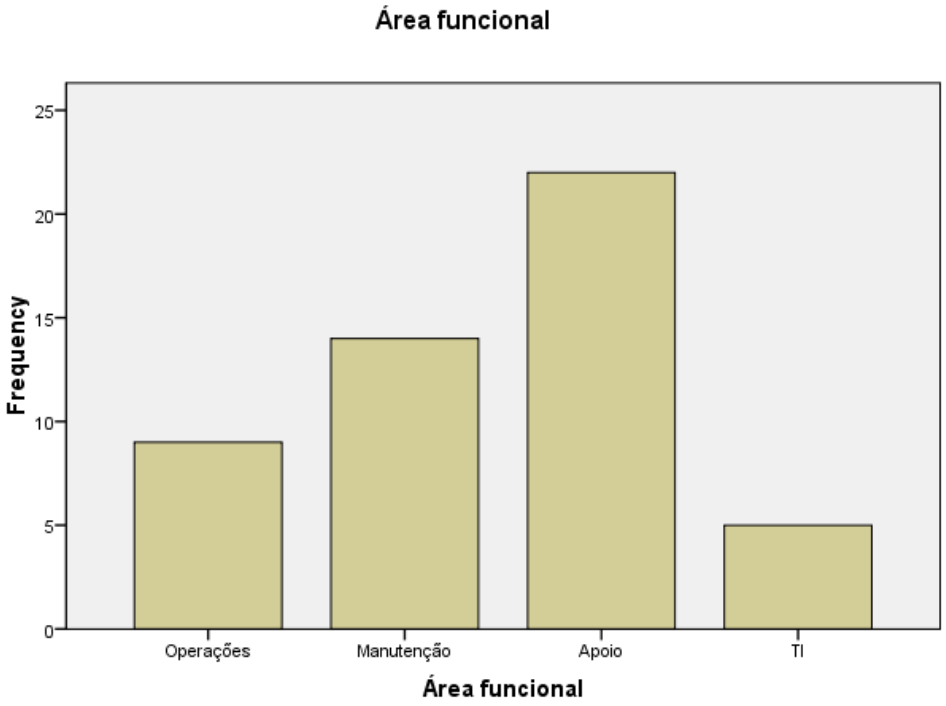
Classificação da importância do acesso remoto ao SIAGFA

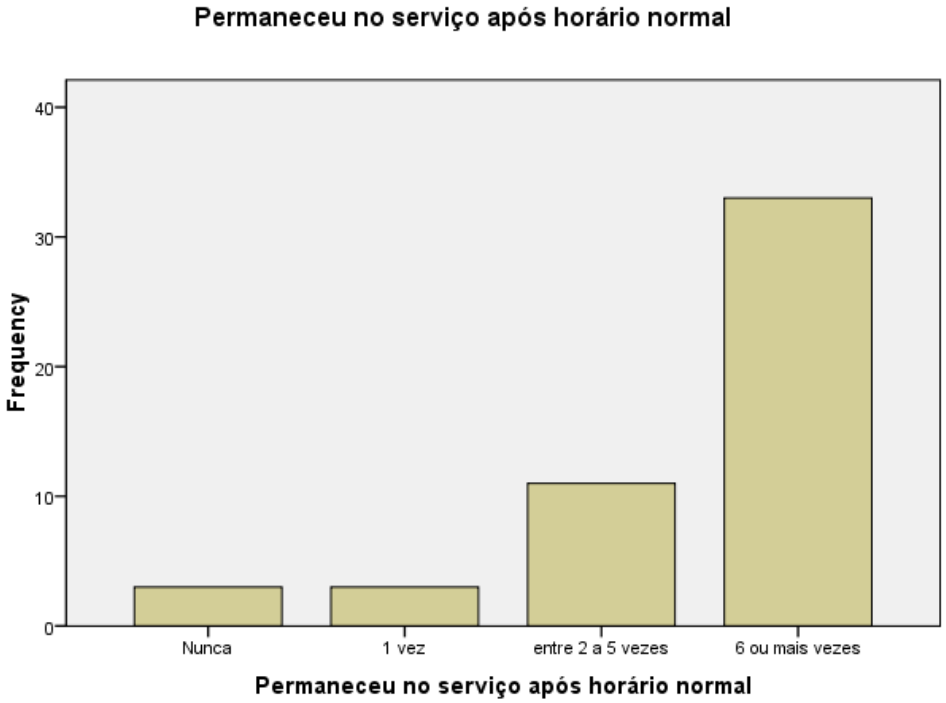
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nada importante	1	2,0	2,0	2,0
	Pouco importante	15	30,0	30,0	32,0
	Importante	20	40,0	40,0	72,0
	Muito importante	14	28,0	28,0	100,0
	Total	50	100,0	100,0	

Classificação da importância do acesso remoto ao PC

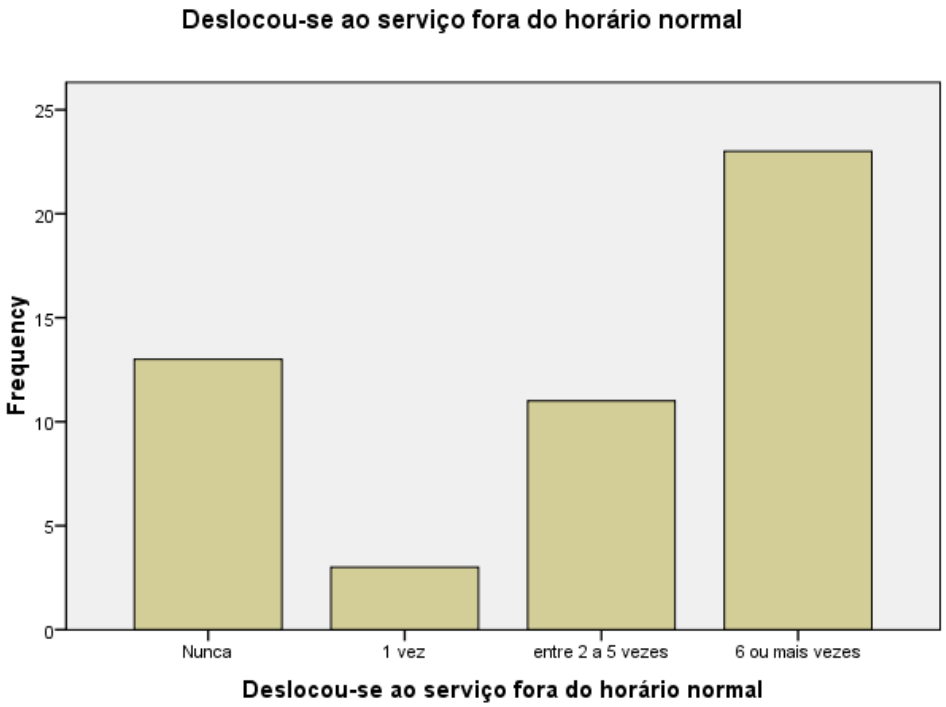
		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	Nada importante	0	0,0	0,0	0,0
	Pouco importante	5	10,0	10,0	10,0
	Importante	18	36,0	36,0	46,0
	Muito importante	27	54,0	54,0	100,0
	Total	50	100,0	100,0	

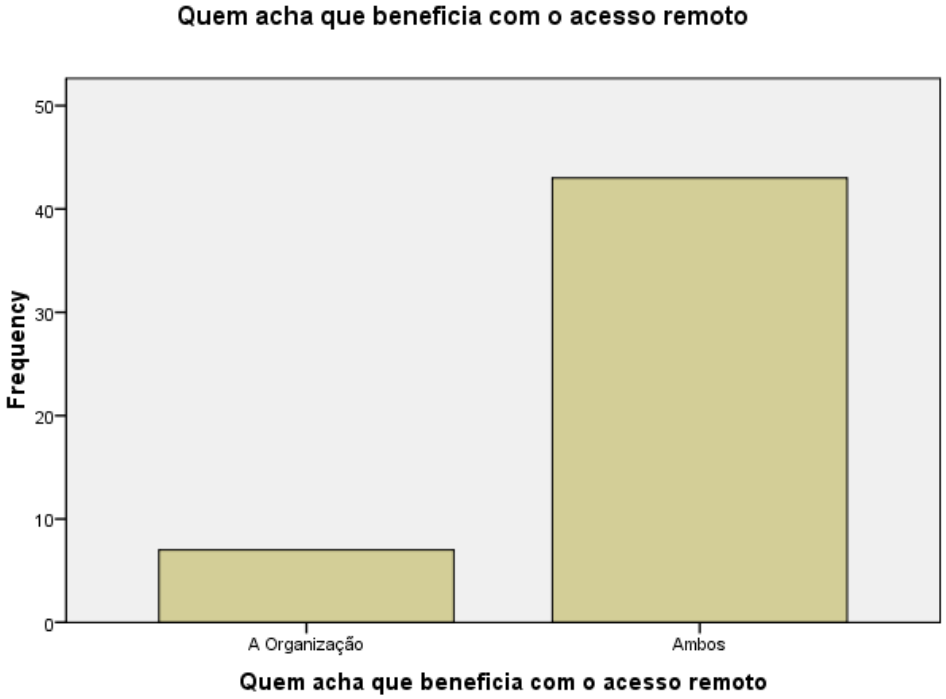
Bar Chart

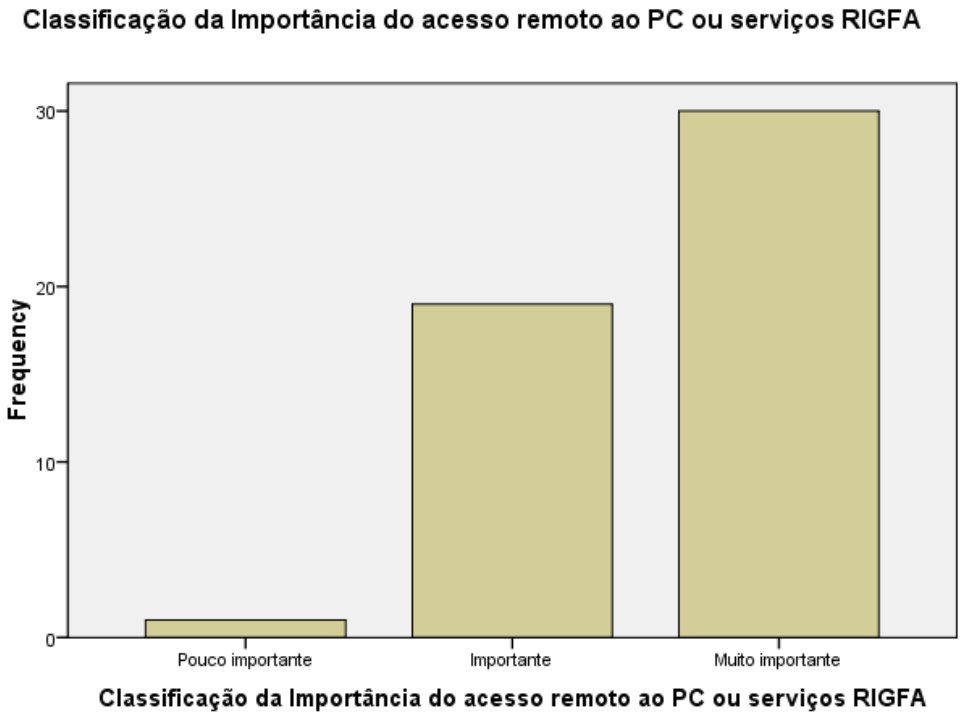

Área funcional
Frequency
25
20
15
10
5
0
Operações
Manutenção
Apoio
TI
Área funcional

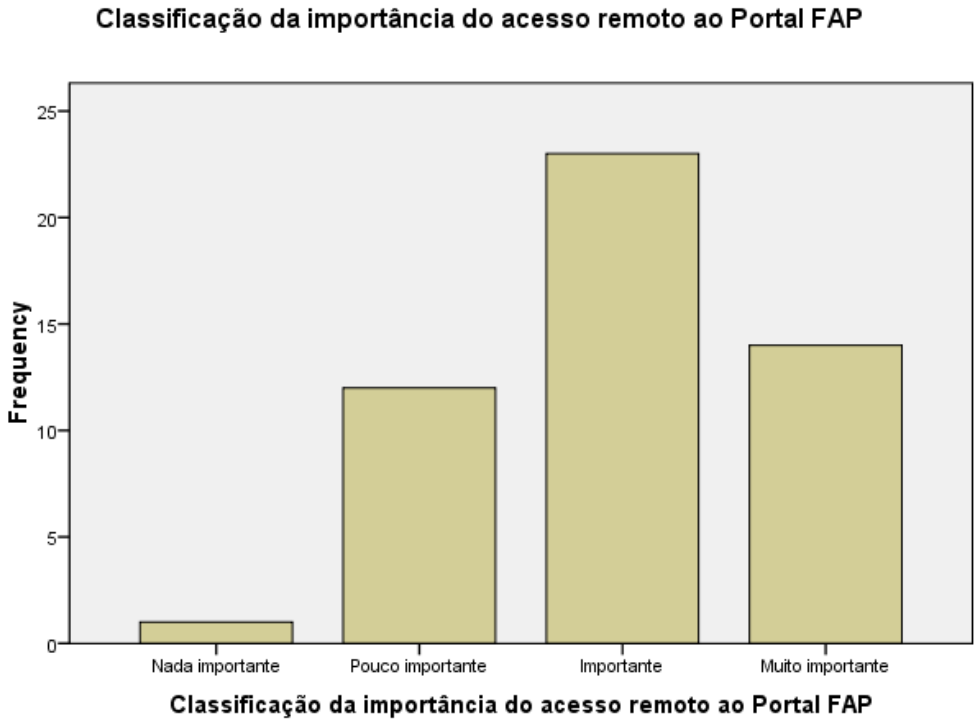

Permaneceu no serviço após horário normal
Frequency
40
30
20
10
0
Nunca
1 vez
entre 2 a 5 vezes
6 ou mais vezes
Permaneceu no serviço após horário normal

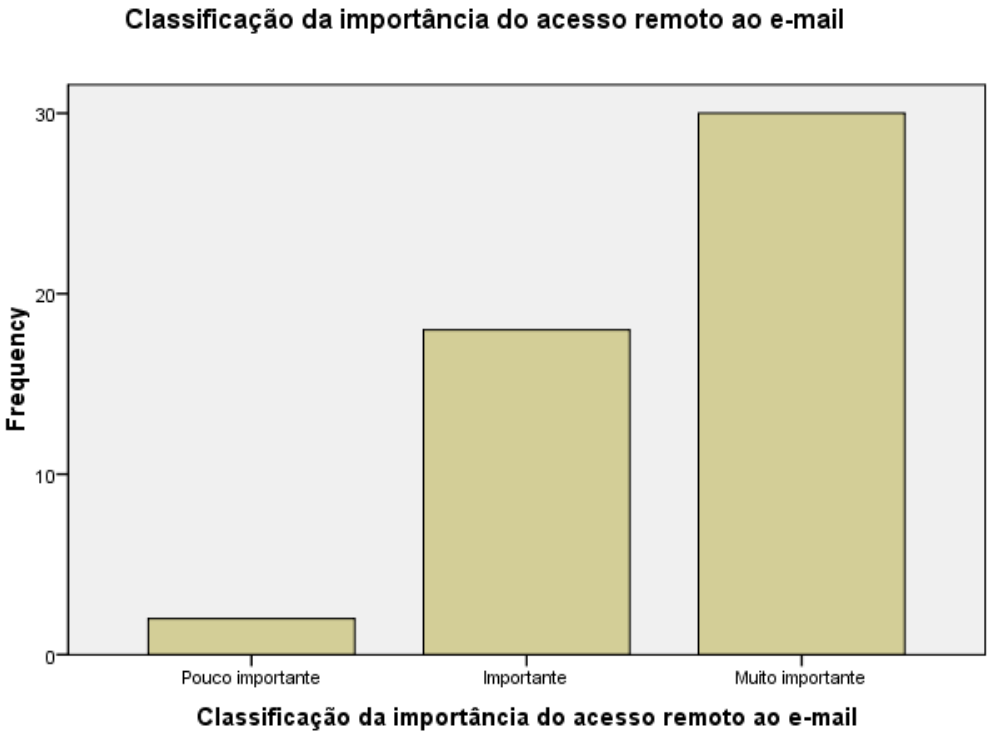
Bar Chart (cont.)

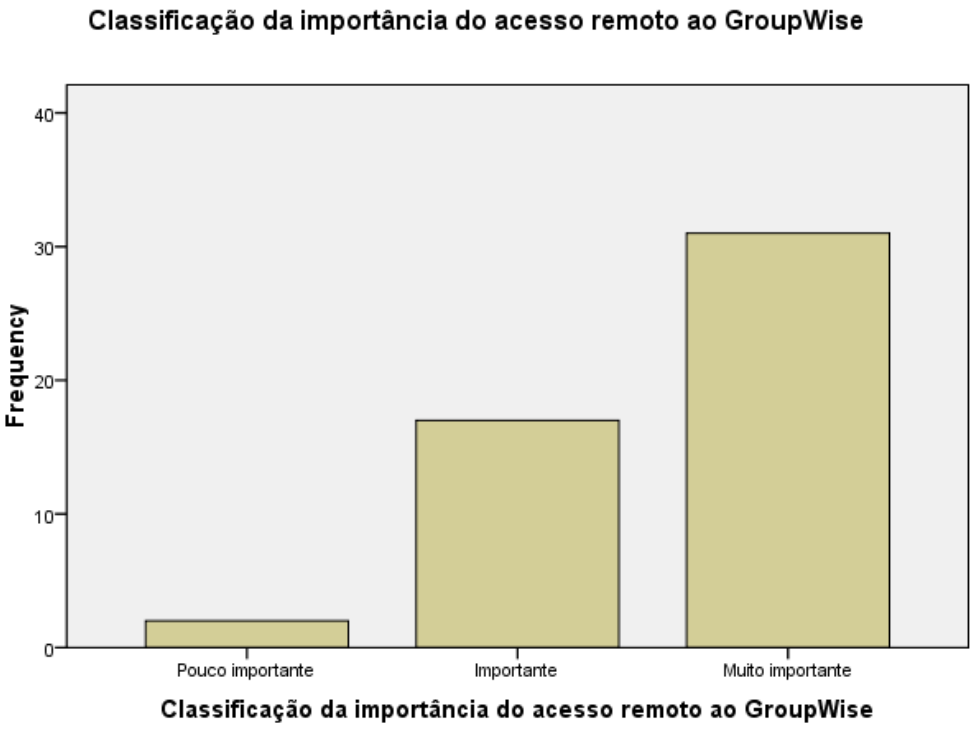


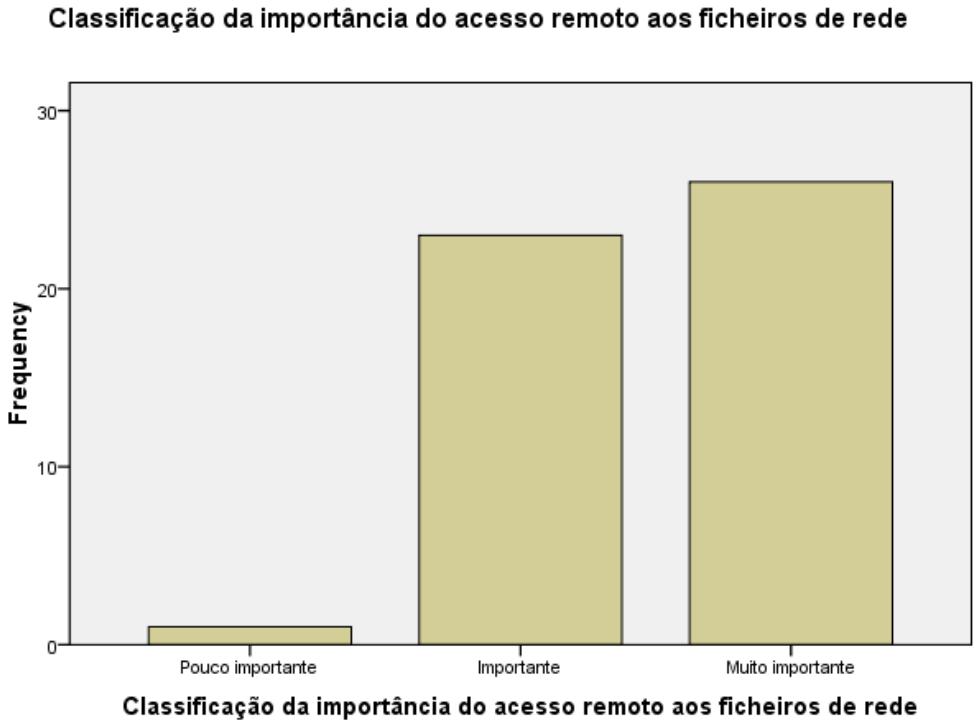


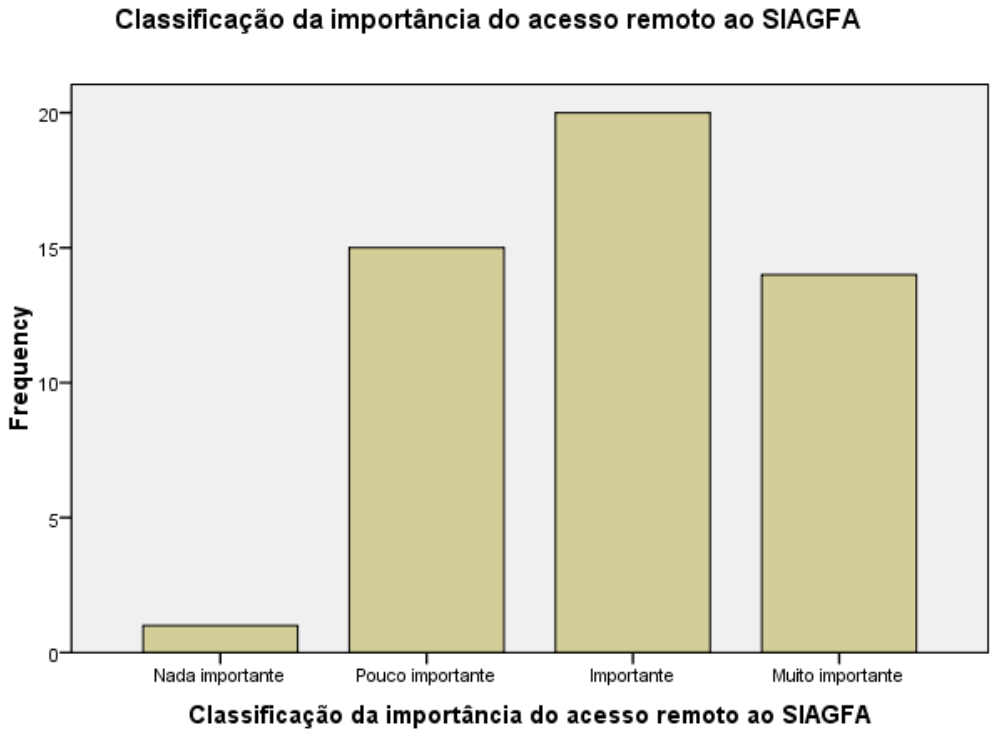

Classificação da Importância do acesso remoto ao PC ou serviços RIGFA
Frequency
30
20
10
0
Pouco importante
Importante
Muito importante
Classificação da Importância do acesso remoto ao PC ou serviços RIGFA

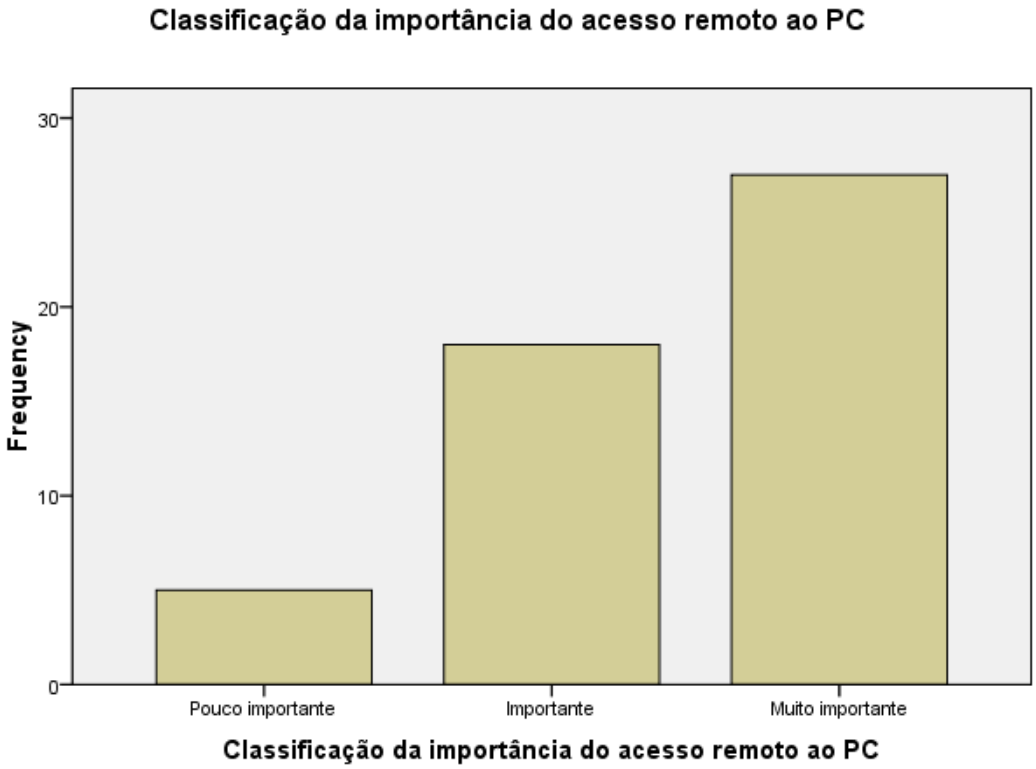

Classificação da importância do acesso remoto ao Portal FAP
Frequency
25
20
15
10
5
0
Nada importante
Pouco importante
Importante
Muito importante
Classificação da importância do acesso remoto ao Portal FAP


Classificação da importância do acesso remoto ao e-mail
Frequency
30
20
10
0
Pouco importante
Importante
Muito importante
Classificação da importância do acesso remoto ao e-mail


Classificação da importância do acesso remoto ao GroupWise
Frequency
40
30
20
10
0
Pouco importante
Importante
Muito importante
Classificação da importância do acesso remoto ao GroupWise


Classificação da importância do acesso remoto aos ficheiros de rede
Frequency
30
20
10
0
Pouco importante
Importante
Muito importante
Classificação da importância do acesso remoto aos ficheiros de rede


Classificação da importância do acesso remoto ao SIAGFA
Frequency
20
15
10
5
0
Nada importante
Pouco importante
Importante
Muito importante
Classificação da importância do acesso remoto ao SIAGFA


Classificação da importância do acesso remoto ao PC
Frequency
30
20
10
0
Pouco importante
Importante
Muito importante
Classificação da importância do acesso remoto ao PC

ANEXO D

Tratamento dos dados dos Inquéritos (Cross tabulation)

CROSSTABS /TABLES=permaneceu_servico deslocou_se_unidade quem_beneficia importancia_acesso_remoto acesso_portal_fap acesso_email acesso_grou pwise acesso_ficheiros_rede acesso_siagfa acesso_pc BY area_funcional /FORMAT=AVALUE TABLES /CELLS=COUNT COLUMN /COUNT ROUND CELL /BARCHART.

Crosstabs

Notes

	Output Created	28-Fev-2010 18:41:37
	Comments	
Input	Data	E:\CPOS0910\WORK\Trabalho\spss_tratados\questionario.sav
	Active Dataset	DataSet1
	Filter	<none>
	Weight	<none>
	Split File	<none>
	N of Rows in Working Data File	50
Missing Value Handling	Definition of Missing	User-defined missing values are treated as missing.
	Cases Used	Statistics for each table are based on all the cases with valid data in the specified range(s) for all variables in each table.
	Syntax	CROSSTABS /TABLES=permaneceu_servico deslocou_se_unidade quem_beneficia importancia_acesso_remoto acesso_portal_fap acesso_email acesso_groupwise acesso_ficheiros_rede acesso_siagfa acesso_pc BY area_funcional /FORMAT=AVALUE TABLES /CELLS=COUNT COLUMN /COUNT ROUND CELL /BARCHART.
Resources	Processor Time	0:00:03.954
	Elapsed Time	0:00:04.000
	Dimensions Requested	2
	Cells Available	174762

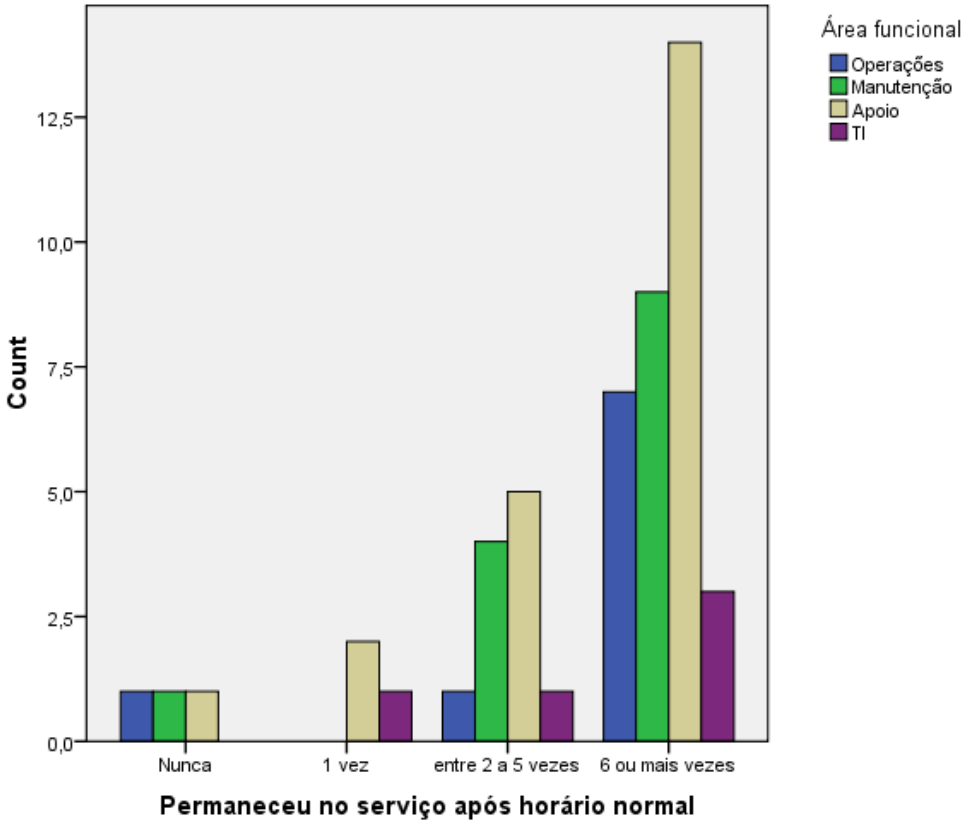
[DataSet1] E:\CPOS0910\WORK\Trabalho\spss_tratados\questionario.sav

Case Processing Summary

	Cases					
	Valid		Missing		Total	
	N	Percent	N	Percent	N	Percent
Permaneceu no serviço após horário normal * Área funcional	50	100,0%	0	,0%	50	100,0%
Deslocou-se ao serviço fora do horário normal * Área funcional	50	100,0%	0	,0%	50	100,0%
Quem acha que beneficia com o acesso remoto * Área funcional	50	100,0%	0	,0%	50	100,0%
Classificação da Importância do acesso remoto ao PC ou serviços RIGFA * Área funcional	50	100,0%	0	,0%	50	100,0%
Classificação da importância do acesso remoto ao Portal FAP * Área funcional	50	100,0%	0	,0%	50	100,0%
Classificação da importância do acesso remoto ao e-mail * Área funcional	50	100,0%	0	,0%	50	100,0%
Classificação da importância do acesso remoto ao GroupWise * Área funcional	50	100,0%	0	,0%	50	100,0%
Classificação da importância do acesso remoto aos ficheiros de rede * Área funcional	50	100,0%	0	,0%	50	100,0%
Classificação da importância do acesso remoto ao SIAGFA * Área funcional	50	100,0%	0	,0%	50	100,0%
Classificação da importância do acesso remoto ao PC * Área funcional	50	100,0%	0	,0%	50	100,0%

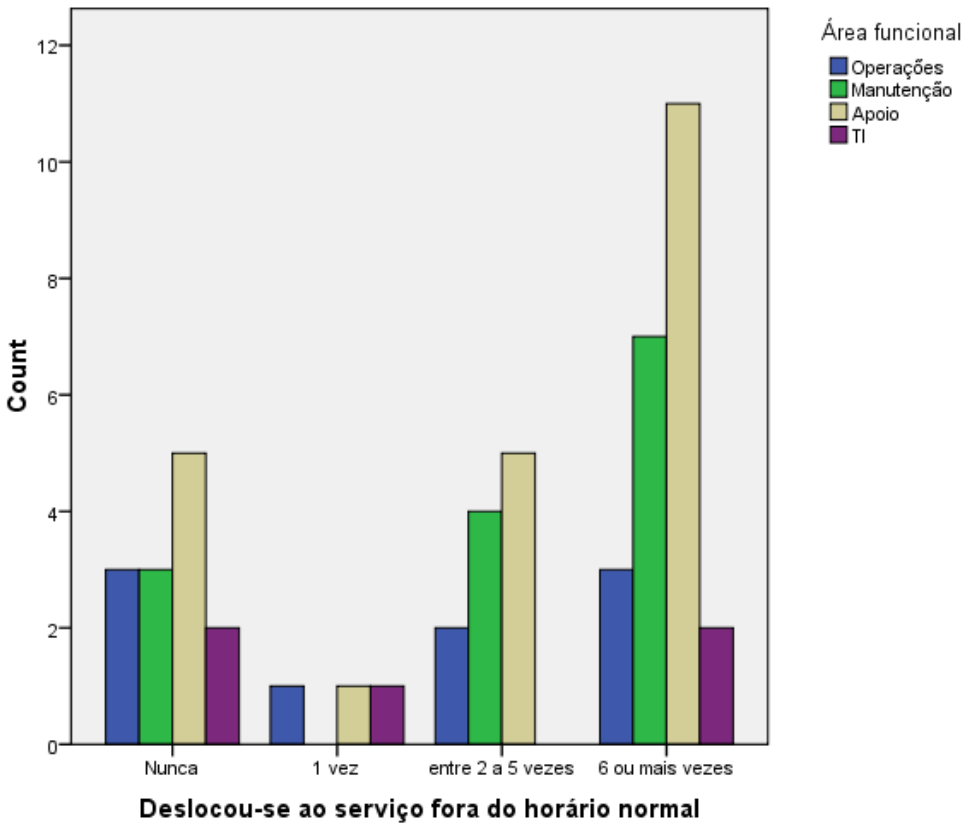
Permaneceu no serviço após horário normal * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Permaneceu no serviço após horário normal	Nunca	Count	1	1	1	0	3
		% within Área funcional	11,1%	7,1%	4,5%	,0%	6,0%
	1 vez	Count	0	0	2	1	3
		% within Área funcional	,0%	,0%	9,1%	20,0%	6,0%
	entre 2 a 5 vezes	Count	1	4	5	1	11
		% within Área funcional	11,1%	28,6%	22,7%	20,0%	22,0%
	6 ou mais vezes	Count	7	9	14	3	33
		% within Área funcional	77,8%	64,3%	63,6%	60,0%	66,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



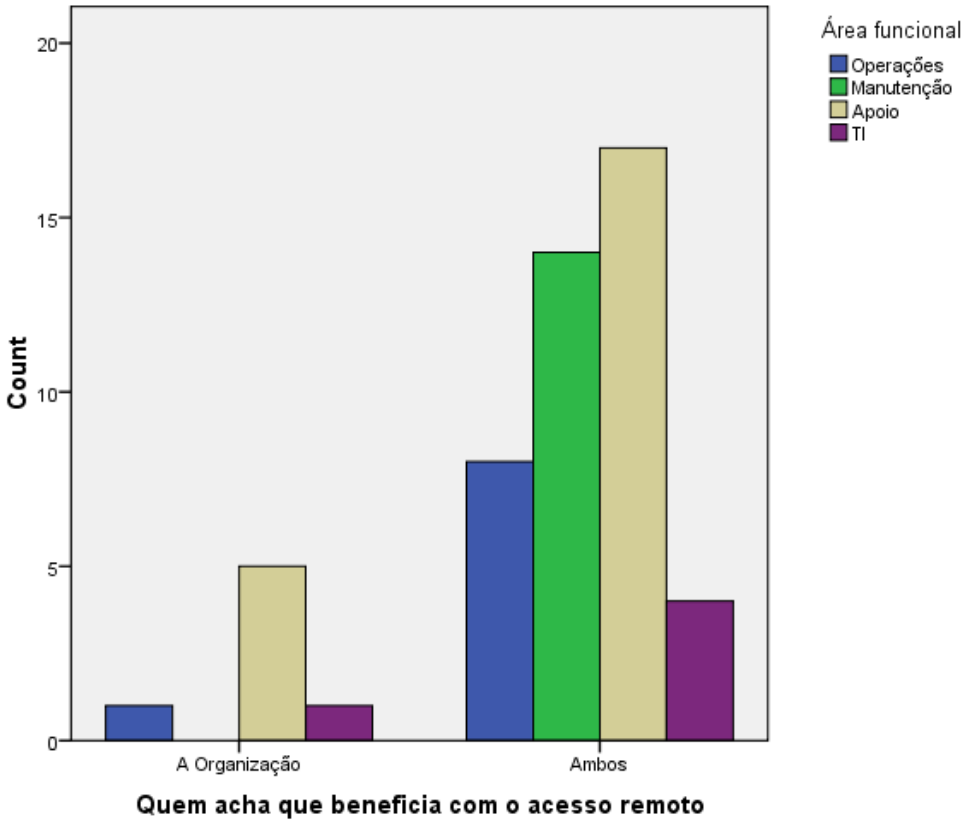
Deslocou-se ao serviço fora do horário normal * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Deslocou-se ao serviço fora do horário normal	Nunca	Count	3	3	5	2	13
		% within Área funcional	33,3%	21,4%	22,7%	40,0%	26,0%
	1 vez	Count	1	0	1	1	3
		% within Área funcional	11,1%	,0%	4,5%	20,0%	6,0%
	entre 2 a 5 vezes	Count	2	4	5	0	11
		% within Área funcional	22,2%	28,6%	22,7%	,0%	22,0%
	6 ou mais vezes	Count	3	7	11	2	23
		% within Área funcional	33,3%	50,0%	50,0%	40,0%	46,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



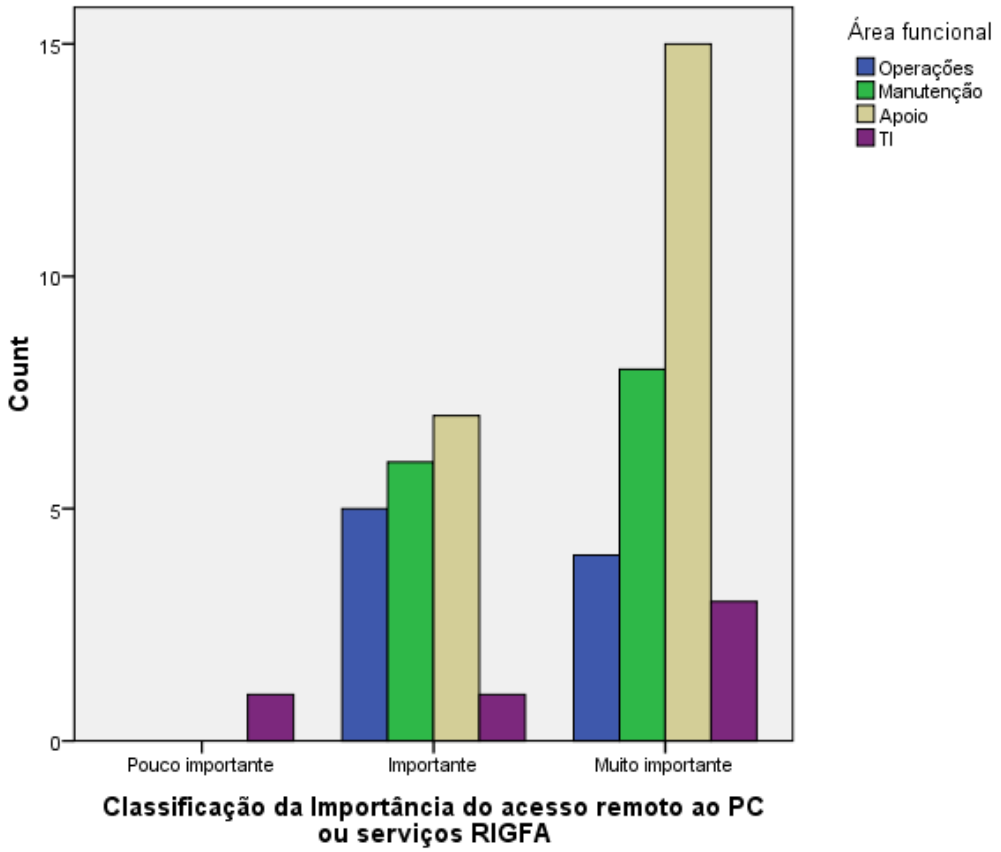
Quem acha que beneficia com o acesso remoto * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Quem acha que beneficia com o acesso remoto	O próprio	Count	0	0	0	0	0
		% within Área funcional	,0%	,0%	,0%	,0%	,0%
	A Organização	Count	1	0	5	1	7
		% within Área funcional	11,1%	,0%	22,7%	20,0%	14,0%
	Ambos	Count	8	14	17	4	43
		% within Área funcional	88,9%	100,0%	77,3%	80,0%	86,0%
	Ninguém	Count	0	0	0	0	0
		% within Área funcional	,0%	,0%	,0%	,0%	,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



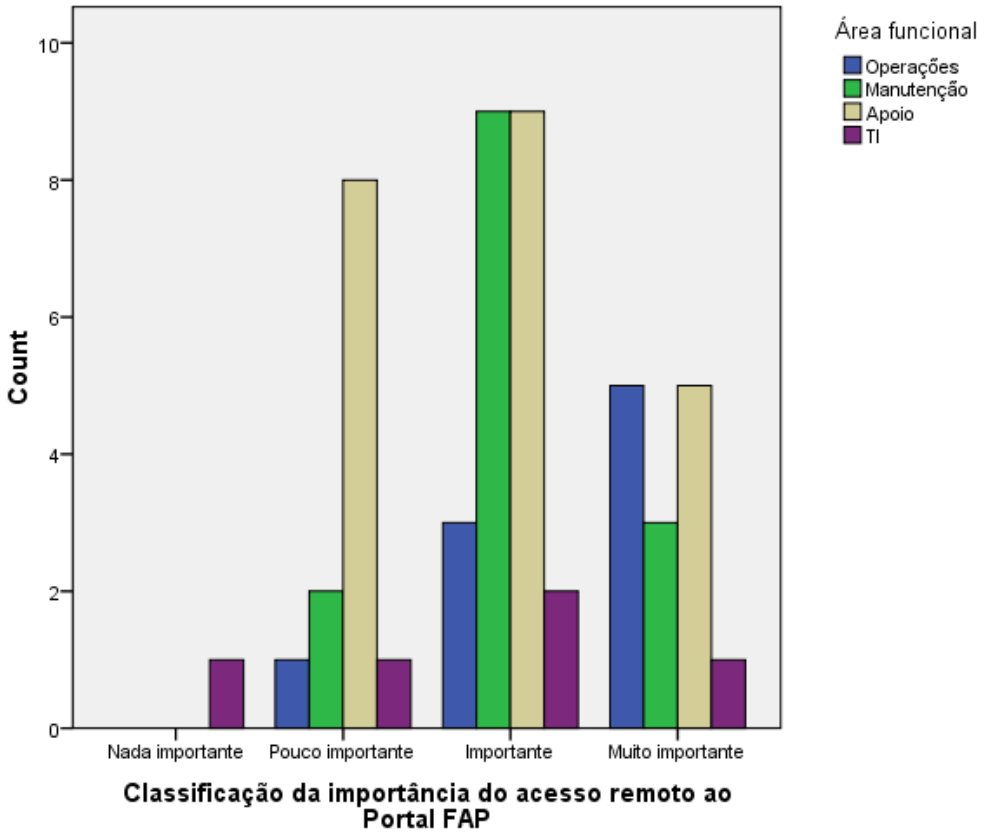
Importância do acesso remoto ao PC ou serviços RIGFA * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Classificação da Importância do acesso remoto ao PC ou serviços RIGFA	Nada importante	Count	0	0	0	0	0
		% within Área funcional	,0%	,0%	,0%	,0%	,0%
	Pouco importante	Count	0	0	0	1	1
		% within Área funcional	,0%	,0%	,0%	20,0%	2,0%
	Importante	Count	5	6	7	1	19
		% within Área funcional	55,6%	42,9%	31,8%	20,0%	38,0%
	Muito importante	Count	4	8	15	3	30
		% within Área funcional	44,4%	57,1%	68,2%	60,0%	60,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



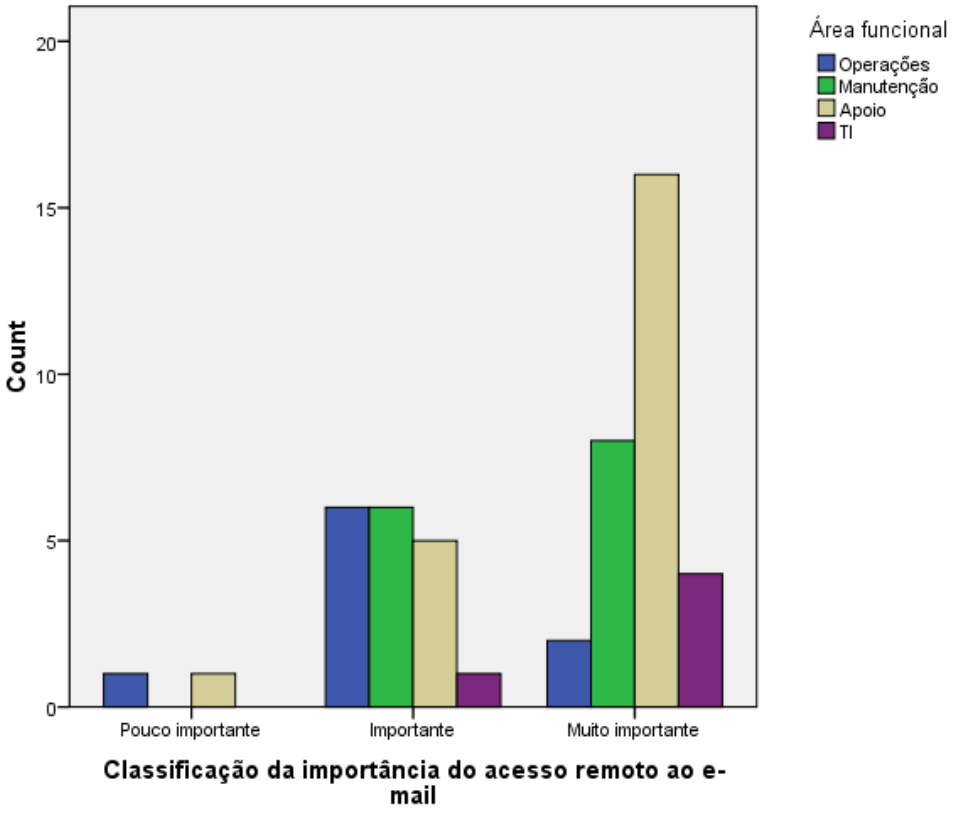
Classificação da importância do acesso remoto ao Portal FAP * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Classificação da importância do acesso remoto ao Portal FAP	Nada importante	Count	0	0	0	1	1
		% within Área funcional	,0%	,0%	,0%	20,0%	2,0%
	Pouco importante	Count	1	2	8	1	12
		% within Área funcional	11,1%	14,3%	36,4%	20,0%	24,0%
	Importante	Count	3	9	9	2	23
		% within Área funcional	33,3%	64,3%	40,9%	40,0%	46,0%
	Muito importante	Count	5	3	5	1	14
		% within Área funcional	55,6%	21,4%	22,7%	20,0%	28,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



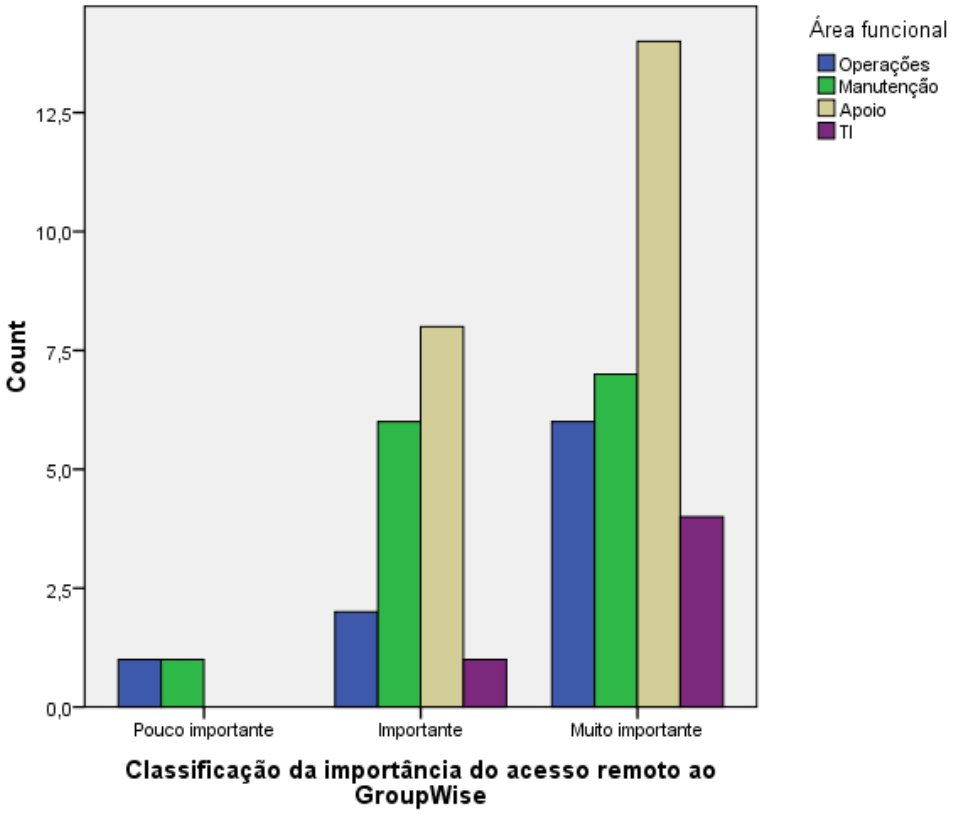
Classificação da importância do acesso remoto ao e-mail * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Classificação da importância do acesso remoto ao Portal FAP	Nada importante	Count	0	0	0	0	0
		% within Área funcional	,0%	,0%	,0%	,0%	,0%
	Pouco importante	Count	1	0	1	0	2
		% within Área funcional	11,1%	,0%	4,5%	,0%	4,0%
	Importante	Count	6	6	5	1	18
		% within Área funcional	66,7%	42,9%	22,7%	20,0%	36,0%
	Muito importante	Count	2	8	16	4	30
		% within Área funcional	22,2%	57,1%	72,7%	80,0%	60,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



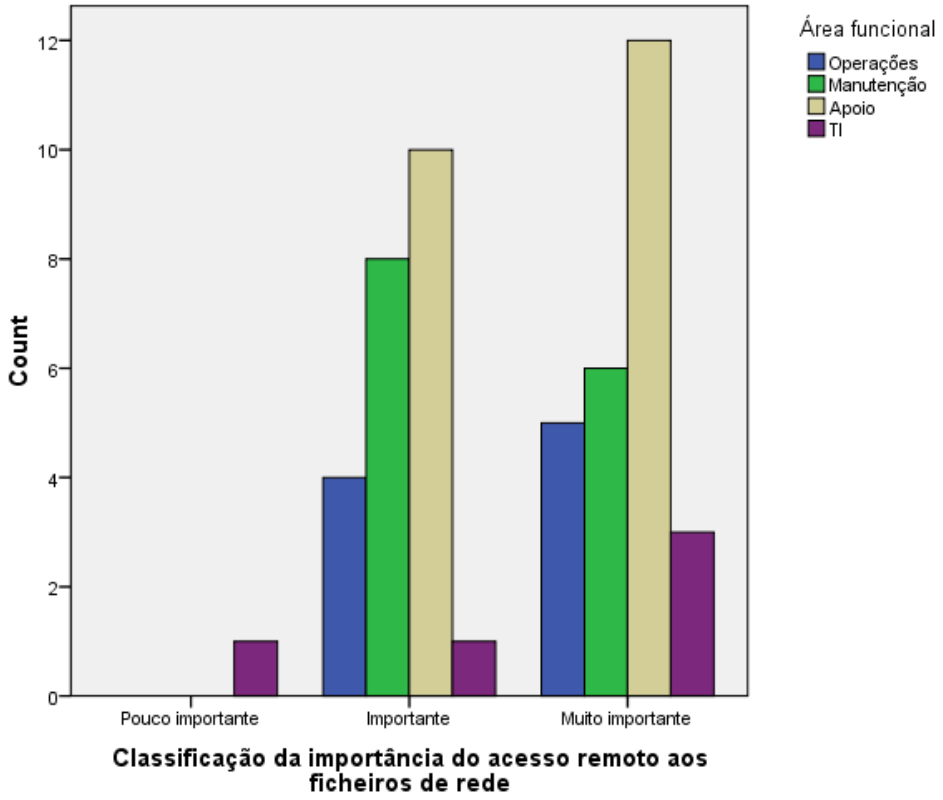
Classificação da importância do acesso remoto ao GroupWise * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Classificação da importância do acesso remoto ao GroupWise	Nada importante	Count	0	0	0	0	0
		% within Área funcional	,0%	,0%	,0%	,0%	,0%
	Pouco importante	Count	1	1	0	0	2
		% within Área funcional	11,1%	7,1%	,0%	,0%	4,0%
	Importante	Count	2	6	8	1	17
		% within Área funcional	22,2%	42,9%	36,4%	20,0%	34,0%
	Muito importante	Count	6	7	14	4	31
		% within Área funcional	66,7%	50,0%	63,6%	80,0%	62,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



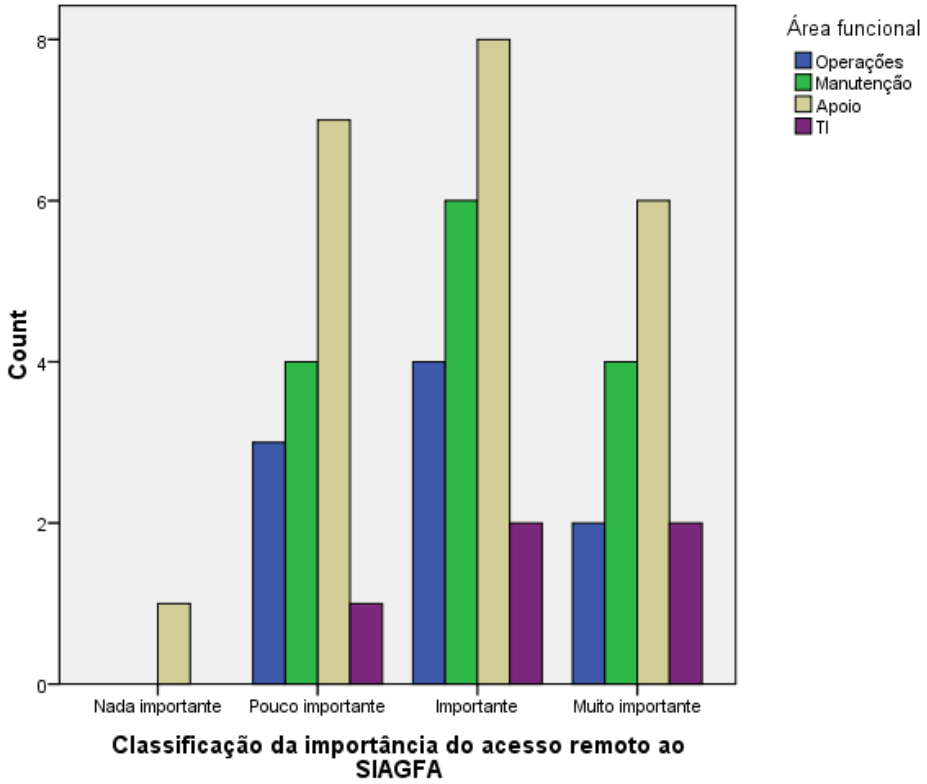
Classificação da importância do acesso remoto aos ficheiros de rede * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Classificação da importância do acesso remoto aos ficheiros de rede	Nada importante	Count	0	0	0	0	0
		% within Área funcional	,0%	,0%	,0%	,0%	,0%
	Pouco importante	Count	0	0	0	1	1
		% within Área funcional	,0%	,0%	,0%	20,0%	2,0%
	Importante	Count	4	8	10	1	23
		% within Área funcional	44,4%	57,1%	45,5%	20,0%	46,0%
	Muito importante	Count	5	6	12	3	26
		% within Área funcional	55,6%	42,9%	54,5%	60,0%	52,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



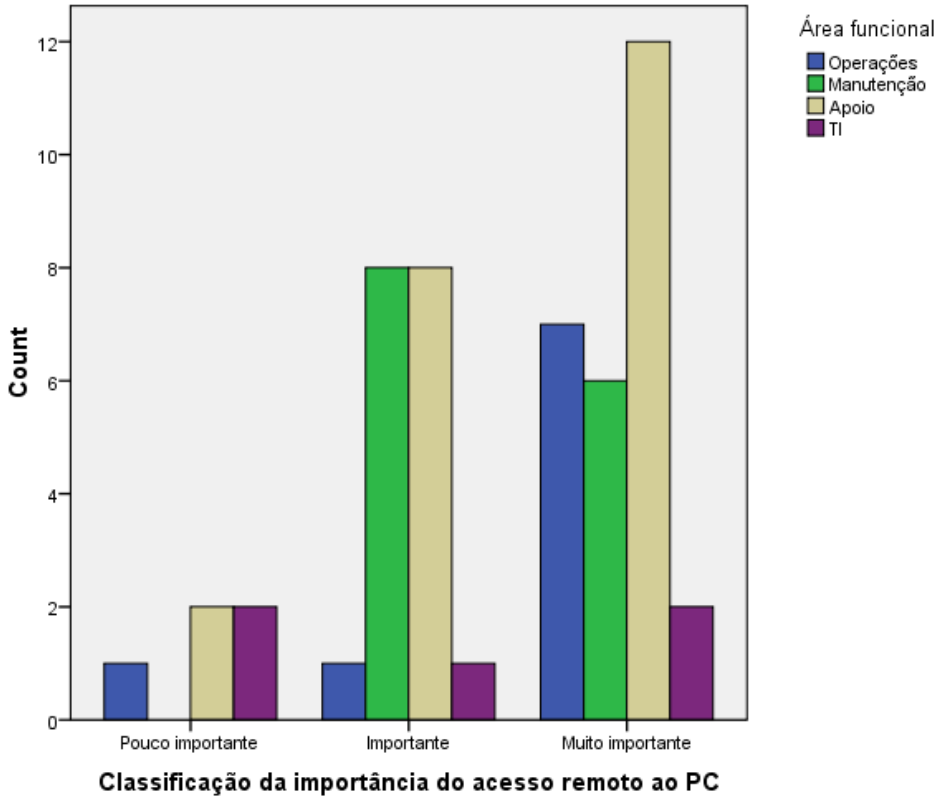
Classificação da importância do acesso remoto ao SIAGFA * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Classificação da importância do acesso remoto ao SIAGFA	Nada importante	Count	0	0	1	0	1
		% within Área funcional	,0%	,0%	4,5%	,0%	2,0%
	Pouco importante	Count	3	4	7	1	15
		% within Área funcional	33,3%	28,6%	31,8%	20,0%	30,0%
	Importante	Count	4	6	8	2	20
		% within Área funcional	44,4%	42,9%	36,4%	40,0%	40,0%
	Muito importante	Count	2	4	6	2	14
		% within Área funcional	22,2%	28,6%	27,3%	40,0%	28,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



Classificação da importância do acesso remoto ao PC * Área funcional Crosstabulation

			Área funcional				
			Operações	Manutenção	Apoio	TI	Total
Classificação da importância do acesso remoto ao PC	Nada importante	Count	0	0	0	0	0
		% within Área funcional	,0%	,0%	,0%	,0%	,0%
	Pouco importante	Count	1	0	2	2	5
		% within Área funcional	11,1%	,0%	9,1%	40,0%	10,0%
	Importante	Count	1	8	8	1	18
		% within Área funcional	11,1%	57,1%	36,4%	20,0%	36,0%
	Muito importante	Count	7	6	12	2	27
		% within Área funcional	77,8%	42,9%	54,5%	40,0%	54,0%
Total		Count	9	14	22	5	50
		% within Área funcional	100,0%	100,0%	100,0%	100,0%	100,0%



ANEXO E

Lista de Servidores de *Backup* da RIGFA

Unidade/Complexo	Sistema de Backup	Nº de Servidores a que é efectuado backup
Alfragide Complexo)	Automático	24
COFA	Automático	12
Lumiar (Complexo)	Automático	13
BA4/CZAA	Manual	2
BA5	Manual	3
BA6	Automático	11
BA11	Manual	2
AFA	Automático	11
CFMTFA	Manual	2
Alverca (Complexo)	Manual	3
AT1	Manual	2
AM1	Manual	2
AM3	Manual	1
CTA	Manual	2
ER1	Manual	1
ER2	Manual	1
ER3	Manual	1