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.

INTERNET LÚDICA NA FORÇA AÉREA

CARLOS MANUEL RAPOSO BONITO

CAP/ENGEL

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

INTERNET LÚDICA NA FORÇA AÉREA

CAP/ENGEL Carlos Manuel Raposo Bonito

Trabalho de Investigação Individual do CPOSFA 09/10

Lisboa 2010

INSTITUTO DE ESTUDOS SUPERIORES MILITARES

INTERNET LÚDICA NA FORÇA AÉREA

CAP/ENGEL Carlos Manuel Raposo Bonito

Trabalho de Investigação Individual do CPOSFA 09/10

Orientador:

TCOR/PILAV João Vicente

Lisboa 2010

Agradecimentos

Agradeço a colaboração dos seguintes militares na elaboração deste documento:

- COR Monteiro do EMGFA
- TCOR Ornelas da DivCSI
- TCOR Frazão do Departamento Jurídico
- TCOR Vicente do IESM
- CAP Fernanda Paulo da DCSI
- CAP Simões da DCSI
- CAP Valente da DCSI
- CAP Trabula da DCSI
- CAP Almeida da DMSA
- CAP Vinagreiro do Regimento de Transmissões do Exército
- 1º TEN Neves da DITIC da Marinha
- ALF Gomes do CPSIFA

Índice

Anexos:

Apêndices:

Índice de Figuras:

Índice de Tabelas:

Índice de Gráficos:

Resumo

A Utilização Lúdica da Internet no Posto de Trabalho é algo tipicamente visto com desconfiança pelos responsáveis das Empresas. Por outro lado, o Empregado vê essa actividade como algo não nocivo para a Empresa, chegando mesmo a ser encarada por parte deste, como um direito que lhe assiste como compensação da sua dedicação ao trabalho. Fica então a questão sobre este dilema. A Utilização Lúdica da Internet no Posto de Trabalho é má para as empresas? É má para a FA? Será que os inúmeros perigos vindos da Internet resultam todos eles dessa Utilização Lúdica? Será que a Utilização Lúdica só traz malefícios? Estudos recentes sugerem ser outro o foco desses males institucionais, o da Utilização Inapropriada da Internet, e que esta não está só presente na componente Lúdica, mas também na componente de Serviço. Assim sendo, que efeitos produzem esse Uso Inapropriado da Internet e quais as suas causas? E o que podem os responsáveis das Empresas fazerem para diminuir esses efeitos? Como está implementado e a funcionar o serviço de Internet na Força Aérea? Que Medidas poderá adoptar para reduzir os malefícios dessa Utilização Inapropriada da Internet? Serão estas as principais questões que este trabalho de investigação pretende responder.

Abstract

The Use of Internet in Workplace for personal reasons is typically seen with suspicion by the company's leaders. Moreover, the employee look at this activity as not being harmful to the Company, and even be seen by him, as his right as a compensation for his dedication to work. So, the question is: The Personal Internet Usage in Workplace is bad for business? Is it bad for the Portuguese Air Force? Are the many dangers arising from the Internet be coming from this kind of utilization? Does the Personal Internet Usage only bring bad things? Recent studies suggest another focus of these institutional evils, the Inappropriate Internet Usage, and that this is not only present in the Personal Internet Usage component, but also in the work related usage component. So, what effects the Inappropriate Use of the Internet produces and what are their causes? And what can the leaders of companies do to reduce these effects? How is Internet service implemented and functioning in the Portuguese Air Force? What measures can be taken to reduce the harm of Inappropriate Internet Usage? These are the main issues of this research work aims to answer.

Palavras-chave

Internet; Internet Lúdica; Utilização Inapropriada da Internet; Posto de Trabalho; Normativo

Lista de abreviaturas

AFA	Academia da Força Aérea
IP	*Internet Protocol*
CE	Correio Electrónico
CNPD	Comissão Nacional de Protecção de Dados
DCSI	Direcção de Comunicações e Sistemas de Informação
DivCSI	Divisão de Comunicações e Sistemas de Informação
DInst	Direcção de Instrução
EE	Entidade Empregadora
EMGFA	Estado-Maior General das Forças Armadas
FA	Força Aérea Portuguesa
UII	Utilização Inapropriada da Internet
ULI	Utilização Lúdica da Internet
WWW	*World Wide Web*

Introdução

"O carácter provisório deste documento justifica-se pela novidade do uso destes produtos [Internet e Correio Electrónico] a nível alargado da Força Aérea, sendo prudente a aquisição de alguma experiência antes de cristalizar as normas definitivas em documento do tipo RFA."

Normas provisórias para a utilização do correio electrónico interno da FAP e da internet no âmbito das redes locais de unidade.
O CEMFA, Manuel José Alvarenga de Sousa Santos, 9 de Outubro de 1998

A Utilização da Internet no seio das Empresas, após uma explosão inicial onde apenas se viam os benefícios daí emanados, tem vindo na última década a ser alvo de uma atenção cada vez maior por parte dos gestores, devido à percepção dos perigos que dela podem surgir (JOHNSON, 2003). São, aliás, vários os estudos que apontam para perdas volumosas de tempo, de recursos, de prestígio e de dinheiro devido a uma Utilização Inapropriada da Internet (UII) (JOHNSON, 2003). Nesse sentido, a Utilização Lúdica da Internet (ULI) tem sido, de uma forma simplista, apontada como a causa de todos esses males. Não será, portanto de estranhar, que se assista em muitas empresas à adopção de Medidas que visam eliminar a ULI. No entanto, esta questão está longe de ser simples. Cada vez mais, os serviços tendem a depender da Internet. O aumento do número de serviços sobre a Rede, associado a um maior número de utilizadores, nem sempre disciplinados, cria uma conjectura de elevado risco, uma vez que a probabilidade e o impacto da ocorrência de incidentes estão a crescer. A Internet na FA, com as suas parcas Medidas, está vulnerável a esses males. Assim, o pensamento que irá orientar este trabalho de investigação será "como pode a Internet Lúdica existir na Força Aérea (FA) sem que represente uma ameaça para a instituição?". De uma forma muito pragmática, a resposta a esta questão é: através da aplicação de Medidas. Que Medidas serão essas e como aplicá-las na FA, constituirá o objectivo de estudo deste trabalho.

Seguindo a proposta metodológica de Quivy e Campenhoudt (1998), esta investigação é orientada pela seguinte pergunta de partida:

De que forma pode a FA regular a utilização da Internet no Posto de Trabalho?
Na busca da resposta à pergunta principal, decorrem três perguntas derivadas:

- ***Será, de facto, importante a adopção de Medidas pelas Empresas?***
- ***Quais as Medidas mais utilizadas, e quais as suas desvantagens?***
- ***Como pode a FA aplicar essas Medidas?***

Com base na problemática e nas perguntas derivadas estabelecidas, constrói-se um modelo de análise, que relaciona conceitos, dimensões e indicadores, assente nas seguintes hipóteses:

H1: A ULI não representa a fonte de todos os malefícios vindos da Internet.
H2: A aplicação de Medidas não apresenta nenhumas contra-indicações.
H3: A FA beneficiará com a implementação de Medidas.

As hipóteses serão testadas e verificadas ao longo dos capítulos, através da análise dos dados recolhidos por consulta bibliográfica, por entrevistas a entidades que, pelas suas funções, têm conhecimento do tema objecto de estudo, e a um inquérito realizado a elementos da FA, na qualidade de Utilizadores.

Ao longo deste estudo foram trabalhados alguns conceitos que importa desde já apresentar para uma melhor compreensão:

Internet nas Empresas: Utilização do serviço Internet nos Postos de Trabalho das Empresas.

Internet na Força Aérea: Utilização do serviço Internet nos Postos de Trabalho da Força Aérea.

Medidas: Acções tomadas por parte da Entidade Empregadora com o objectivo de reduzir a Utilização Inapropriada da Internet nos Postos de Trabalho.

Utilização Lúdica da Internet: Utilização da Internet no Posto de Trabalho sem ser para fins de serviço.

Utilização Inapropriada da Internet: Utilização da Internet no Posto de Trabalho de forma pejorativa para a Entidade Empregadora.

Normativo: Documento com vinculo jurídico que regulariza a utilização da Internet no Posto de Trabalho.

Assim, no primeiro capítulo, será analisada a Internet nas Empresas, nomeadamente o que é que de facto constitui a ameaça, que tipo de efeitos poderão advir da UII, e quais as suas causas. Será feita uma comparação entre a UII e a ULI, para que seja bem entendida a diferença entre ambas, e para que se possa proceder à verificação da primeira hipótese. Antes de se analisar as Medidas, considerou-se importante determinar as causas da UII, pois serão elas que deverão ser tomadas como alvo dessas mesmas Medidas. No segundo capitulo, serão analisadas as Medidas mais utilizadas nas Empresas, caracterizando-as, agrupando-as por tipologia, e descrevendo as respectivas vantagens e desvantagens. Será neste ponto possível efectuar-se a verificação da segunda hipótese. Devido à complexidade e importância da elaboração de um Normativo, Medida considerada como primordial, serão apresentados alguns aspectos importantes para a sua construção. Sobre as restantes Medidas a aplicar, serão tecidas algumas considerações a ter em conta para esse fim. No terceiro capitulo, será analisada a realidade da FA no âmbito da Utilização da Internet no Posto de Trabalho, apresentando-se a estrutura orgânica e operacional que a suporta, e como está a ser usada pelos Utilizadores. Será pois possível testar-se a terceira hipótese, e dessa forma responder-se à pergunta principal. Por fim, serão efectuadas algumas recomendações, nomeadamente com a sugestão de adopção de Medidas, pelos respectivos órgãos competentes da FA, identificados neste trabalho.

1) A Internet nas Empresas

a) A ULI e a UII

Sendo a ULI considerada, no âmbito deste estudo, todo o uso da Internet não relacionado com o serviço, podemos facilmente identificar alguns exemplos que nela se enquadram (GALLETA, 2003): Troca de *mail* pessoal, compras *on-line*, consulta de *sites* de informação ou desportivos (sem ser para serviço), jogos *on-line*, consulta de *sites* pornográficos, uso de salas de conversação, entre outros.

Apesar de, geralmente, a ULI ser associada a uma actividade nociva para a produtividade de uma empresa (GALLETA, 2003), sabe-se também que é comum os Empregados usufruírem da ULI para curtas tarefas pessoais ou durante os intervalos de serviço, sem que tal represente um prejuízo para a Entidade Empregadora (EE), tempo esse que acabaria por ser consumido por outra actividade lúdica caso não estivesse disponível a Internet (UGRIN, 2008). Este uso adequado da ULI irá contribuir para a satisfação do Empregado, para uma boa relação de confiança entre este e a EE (UGRIN, 2008), permite pausas no serviço necessárias para descanso, refrescar as ideias (GALLETA, 2003) e o contacto experimental com novas tecnologias (UGRAY, 2007).

No entanto, o uso abusivo da Internet para fins Lúdicos no serviço, que é uma realidade (JOHNSON, 2003), traz grandes malefícios para a EE, nomeadamente a perda de rendimento do Empregado, a hostilização do ambiente de trabalho, a ocupação de largura de banda e dos meios tecnológicos, o tráfego de conteúdos ilegais, a degradação da imagem da EE (JOHNSON, 2003), etc.

Devido aos efeitos apresentados, é comum as EE apontarem a ULI como a fonte de todos os malefícios vindos da Internet, tentando eliminá-la, recorrendo, essencialmente, a ferramentas tecnológicas (UGRIN, 2008). No entanto, nem a ULI traz só malefícios, nem todos os malefícios da Internet advêm só da ULI. Mesmo quando usada para serviço, a Internet apresenta perigos idênticos aos já anunciados. Usar indisciplinadamente o Correio Electrónico (CE), por exemplo, misturando os *mails* pessoais com os de serviço, ou enviando como anexo uma apresentação de dimensão excessiva, colocando em causa o desempenho da rede, são alguns dos exemplos de Utilização Inapropriada da Internet (UII) (MARKSTEINER, 2008).

Assim sendo, a UII deverá representar o alvo das Medidas a aplicar pela EE, e não a ULI. Numa figura abstracta, poderemos da seguinte forma representar a Utilização da Internet para Serviço, a ULI e a UII:

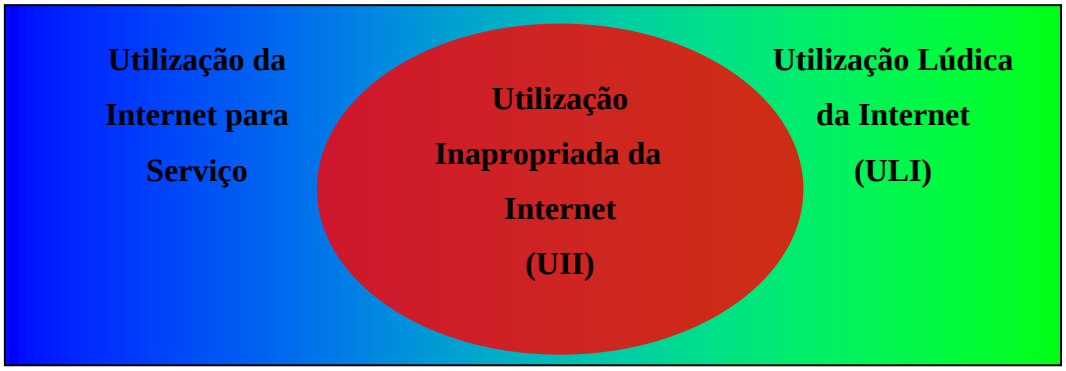


Figura 1 – Utilização da Internet: Serviço / Lúdica / Inapropriada

Será pois importante definirmos as fronteiras entre os conceitos apresentados. Entre a Utilização da Internet para Serviço e a ULI, o que as diferencia é a intenção do Empregado associada a essa actividade. Dois Empregados poderão exibir precisamente o mesmo comportamento na Utilização da Internet, mas um estar a praticar uma actividade lúdica e o outro de serviço. Este factor, o da intencionalidade, torna impossível a eficiência a 100% das ferramentas tecnológicas na restrição dos acessos para uso lúdico do Empregado, uma vez que nenhum algoritmo poderá fazer essa distinção.

A UII pode estar associada à componente lúdica ou de serviço da Internet. Sempre que se mencione o termo: uso abusivo da Internet, estamos perante uma situação de UII, tipicamente associada ao uso excessivo da ULI. A UII que advém da componente de serviço, é geralmente devida à indisciplina do trabalho ou ao desconhecimento e violação das boas práticas para a utilização da Internet. É exemplo desta situação o dedicar um tempo excessivo para pesquisar um assunto de menor importância, ainda que tenha como fim o serviço, resultando num balanço negativo a diferença entre os recursos utilizados e os benefícios daí obtidos.

De uma forma geral, poderemos afirmar que a UII estará presente sempre que um Empregado utiliza a Internet de forma pejorativa para a EE, podendo fazê-lo de forma consciente ou não. Face ao apresentado, é possível verificar-se a primeira hipótese, constatando que ela é verdadeira.

Para melhor entendermos o impacto desta actividade, iremos de seguida analisar os Efeitos da UII.

b) Efeitos da UII

Identificar e compreender a magnitude dos efeitos da UII, permite a EE obter a real percepção do impacto que esta tem sobre o regular desempenho da sua actividade, e assim extrair a devida motivação para empenhar-se no seu combate.

Apresenta-se, como resumo, uma tabela com os efeitos agrupados em três áreas:

Efeitos Humanos
- Desfoco da atenção
- Saúde mental
- Saúde fisica
Efeitos tecnológicos
- Consumo de recursos tecnológicos
- Importação de *softwares* malignos
- Necessidade de tornar seguro
Efeitos organizacionais
- Actividade ilegal
- Processos disciplinares
- Hostilização do ambiente de trabalho
- Degradação da imagem da Empresa
- Perda de produtividade

Tabela 1 – Efeitos

Serão de seguida apresentados os efeitos, com uma breve descrição:

(1) Efeitos Humanos

- Desfoco da atenção: O excesso de informação, principalmente o que chega através do CE, interfere na capacidade de tomada de decisão do Empregado, provocando-lhe um desfoco da sua atenção (MARKSTEINER, 2008).
- Saúde mental: O excesso de informação assimilada através da Internet tem um impacto negativo sobre a personalidade do Empregado, pois irá afectar a sua capacidade de se relacionar e comunicar com os outros. Interfere na sua

capacidade de concentração, prejudicando a execução de tarefas que dela careçam, bem como a capacidade de tomada de decisão[1].

- Saúde física: O manuseamento do teclado ou do rato de forma continuada e repetitiva pode originar Lesões por Esforço Repetitivo, as denominadas doenças da informática[2]. Assim, para quem já no desempenho das suas funções necessita de passar muito tempo em frente a um computador, não aproveitar as pausas de serviço para se aliviar dessa postura, estará a contribuir para o surgimento deste tipo de lesões.

(2) Efeitos Tecnológicos

- Consumo de recursos tecnológicos: A UII contribui para o estrangulamento da largura de banda (UGRIN, 2008), afectando a qualidade do serviço Internet, que provoca o *Web stress*[3] (NUCLEUS RESEARCH, 2009). Da mesma forma, todos os recursos de rede, incluindo o computador do Empregado, são consumidos pela UII, impondo custos volumosos para a sua sustentação.
- Importação de *softwares* malignos: Gravar músicas, filmes e fotos pessoais no computador é visto com desconfiança pelas Empresas. Eles podem trazer vírus informáticos (Ferreira, 2008) ou outros *softwares* malignos que corrompam a informação que circula na rede, ou o seu próprio desempenho.
- Necessidade de tornar seguro: Representando a UII uma ameaça considerável à EE, existe a necessidade de esta ser combatida, o que exige esforços e empenho de recursos nessa actividade.

(3) Efeitos Institucionais

- Actividade ilegal: A *UK National High Tech Crime Unit* (2005) (WILLISON, 2009) reportou que 38% dos casos de fraude financeira, 68% de roubo de informação/dados e 100% de sabotagem de dados ou da rede foram cometidos

[1]Estes dados podem ser consultados em <http://www.xerox.com/information-overload/enus.html>

[2]Informação disponível em <http://www.microferas.blogspot.com/2009/03/doencas-da-informatica.html >

[3]Stress provocado nos utilizadores da Rede devido ao mau desempenho da mesma. Estudo realizado pela Foviance em Fevereiro de 2010: <http://www.ca.com/gb/content/campaign.aspx?cid=229165>

por elementos internos à EE. Neste sentido, as organizações têm orientado as suas atenções cada vez mais para a ameaça interna.

- Processos disciplinares: Os casos disciplinares relacionados com o uso abusivo de Internet são mais que a soma da totalidade das restantes ofensas nos locais de trabalho. (MACWORLD, 2002). Um processo disciplinar é sempre penalizador para a EE, pois consome recursos e contribui para a hostilização do ambiente de trabalho.
- Hostilização do ambiente de trabalho: A UII traz problemas relacionados com a divulgação de conteúdos racistas, sexuais e de outros conteúdos ofensivos a serem divulgados pelo CE (UGRIN, 2008). Já em 2000, no Brasil, houve um dos primeiros registos de despedimento por um funcionário ter enviado pelo CE da EE um *mail* com conteúdo sexista (FERREIRA, 2008).
- Degradação da imagem da Empresa: São já muitos os casos de Organizações, Empresas, ou Países mesmo, que viram a sua reputação ser afectada por imagens ou textos publicados na Internet, tipicamente nas redes sociais. Temos como exemplo as fotos de médicos de Porto Rico no Haiti divulgadas no *Facebook*[4], ou o caso dos Pilotos da TAP que escreveram sobre as suas chefias usando termos pouco abonatórios[5], na mesma rede social.
- Perda de produtividade: Uma estimativa apresentada em Novembro de 2002 pela *Business Wire*, aponta que o mau uso da Internet em instituições Americanas custaram, nesse ano, 85 biliões de dólares (BUSINESS WIRE, 2002).

Percebendo-se neste ponto quanto prejudicial pode ser a UII para a EE, iremos de seguida analisar as suas causas.

[4] Notícia da tvi24.iol.pt: "Haiti: médicos publicam fotos polémicas no *Facebook*" publicada em 30 de Janeiro de 2010.

[5] Notícia da ionline.pt: "Conversa entre pilotos no *Facebook* abre guerra na TAP" publicada em 25 de Janeiro de 2010.

c) Causas da UII

Identificar as causas da UII é fundamental para que se possa determinar quais as medidas mais adequadas para o seu combate. Vamos, portanto, apontar aquilo que deverá ser o alvo das medidas de regulamentação do uso da Internet.

(1) Fácil Acessibilidade: "As pessoas irão usar a Internet no serviço, simplesmente porque ela está lá, como o Everest" (MACWORLD, 2002). A fácil acessibilidade a um número ilimitado de serviços e a ilusão de que a Internet não custa (GUPTA, 2004), predispõe o Empregado ao seu consumo sem constrangimentos de consciência.

(2) Hábito: Os comportamentos efectuados de forma repetitiva tendem a tornar-se habituais. Assim, o uso abusivo da Internet, que é, por norma, um comportamento "continuado", verá a influência do hábito sobrepor-se à influência da intenção (WOON, 2004).

(3) Insatisfação no serviço: Galletta e Polak (2003) mostraram que a insatisfação no trabalho é um indicador significativo de uso abusivo de Internet. Do ponto de vista psicológico, quando a produção de uma pessoa é indefinida, ela é menos motivada para desempenhar bem porque pode "escapar" ao trabalho sem que seja criticada ou punida (GALLETA, 2003). Essa desmotivação leva o Empregado a olhar para a Internet como um escape. Nos casos extremos, existem os actos de vingança. Verificou-se que 88% dos casos de sabotagem interna ocorreram após uma situação de divergência profunda entre o Empregado e a EE (WILLISON, 2009).

(4) Vício: Um estudo realizado já em 2009 mostrou que 5,7% dos utilizadores de Internet preenchiam os critérios médicos de uso compulsivo da internet, ultrapassando em 30 horas semanais navegando em *sites* não essenciais (TUMA, 2006). Um pequeno exemplo de um comportamento compulsivo é o facto de a maioria dos trabalhadores terem a tendência para abrir o CE imediatamente após a notificação de aviso de recepção, em vez de esperarem por um intervalo no serviço (MARKSTEINER, 2008).

(5) Socialização: Num ambiente laboral hostil, o Empregado tenderá a optar por estar a "falar" com os seus amigos através da conversação *on-line*, porque mentalmente fá-lo-á sentir-se melhor, funcionando como um escape à realidade,

na medida em que lhes permite aliviar a pressão do dia-a-dia (JOHNSON, 2003).

(6) Sensação de privacidade: Pesquisar na Internet a partir do posto de trabalho, induz no Empregado uma sensação de privacidade que irá potenciar a UII (GUPTA, 2004), pois acredita que a probabilidade de ser apanhado é mínima (GRIFFITHS, 2003). Casanova, no século XVIII, ficou famoso ao frequentar bailes de máscara em Veneza, escondendo a sua identidade e inventando histórias para as suas vítimas femininas que invariavelmente lhe cediam. Esse espírito parece ter reaparecido com a criação de serviços, como as salas de conversações e o *Messenger*, onde se verificam comportamentos idênticos.

(7) Indisciplina de trabalho: Apesar de ser grande o número de Empregados a utilizar a Internet, apenas uma pequena percentagem deles têm alguma formação nesta ferramenta. Assim, será espectável que não seja usada da forma mais eficiente e segura. O excesso de informação a circular na Internet é uma realidade, e exige por parte do navegante ferramentas e métodos cada vez mais poderosos para o seu processamento e filtragem (FREED, 2008). Obter o que se pretende, num curto espaço de tempo e garantindo a qualidade da fonte de informação, é algo que exige conhecimento e treino, havendo, inclusivé, cursos para esse efeito. É também cada vez mais comum os Empregados ficarem até tarde no serviço (GRIFFITHS, 2002), ou até levar serviço para casa. Esta dedicação de muitas horas ao serviço legítima no subconsciente do Empregado a utilização recursos da Empresa para fins pessoais, como forma de compensação. Por sua vez, esse tempo "pessoal" durante o expediente, irá contribuir para o seu pouco rendimento, forçando a permanência pós-horário laboral no serviço, originando um ciclo perversamente auto-alimentado. Esta promiscuidade entre o universo pessoal e de serviço contribui para que os Empregados sejam fracos profissionais, e pessoas com relações familiares fragilizadas.

Identificadas as principais causas da UII, iremos analisar no próximo capítulo as Medidas mais comuns aplicadas pelas Empresas.

2) Medidas

a) Tipo de Medidas

Conhecendo-se os efeitos da UII, será expectável que a EE desenvolva esforços no sentido de os minimizar, através de aplicação de Medidas. Para que as Medidas sejam eficazes, elas devem ter como alvo as causas da UII, e não os seus efeitos. No entanto, há que ter o cuidado no tipo de Medidas a usar, pois em excesso irão contribuir para a degradação da relação entre o Empregado e a EE, no sentido em que provoca insatisfação e desconfiança no ambiente de trabalho (UGRIN, 2008). Poderemos, tendo em conta o seu impacto e método de actuação, agrupar as Medidas em Directas e Indirectas, havendo ainda Medidas que poderão enquadrar-se em ambas as tipologias.

(1) Medidas Directas

As Medidas Directas são aquelas que se baseiam na Teoria Geral da Dissuasão, onde se preconiza que cada pessoa toma as suas decisões avaliando a cada instante os riscos e os benefícios dessa acção (UGRIN, 2008). Considerando o risco como o produto entre a probabilidade e o impacto de ser "apanhado" em infracção, obtemos os três elementos sobre os quais as Medidas deverão incidir para dissuadir da decisão de efectuar uso abusivo da Internet: Probabilidade, Impacto (Sanção) e Beneficio.

$$\text{Decisão de praticar uso abusivo} = \frac{\text{Benefício obtido com a acção}}{\text{Probabilidade de ser "apanhado" em infracção x Sanção a que será sujeito}}$$

Figura 2 – Fórmula da tomada de decisão do Empregado

Apresenta-se de seguida, mediantes os elementos a intervir, as Medidas a aplicar e os seus objectivos:

Elementos a intervir	Medidas utilizadas	Objectivo da Medida
Probabilidade	Monitorização e detecção	Aumentar Probabilidade
Impacto	Aplicação de sanções	Aumentar Impacto
Beneficio	Restrição de acessos	Reduzir Beneficio

Tabela 2 – Elementos / Medidas / Objectivos

Como já referido, será necessário moderação na aplicação deste tipo de Medidas, pois quando aplicadas de forma excessiva irão produzir mais problemas que benefícios. De igual forma, sendo pouco ou nada aplicadas, estaremos perante um cenário de utilização anárquica da Rede, daí resultando todos os efeitos já anteriormente descriminados. As figuras seguintes pretendem representar esses três cenários possíveis:

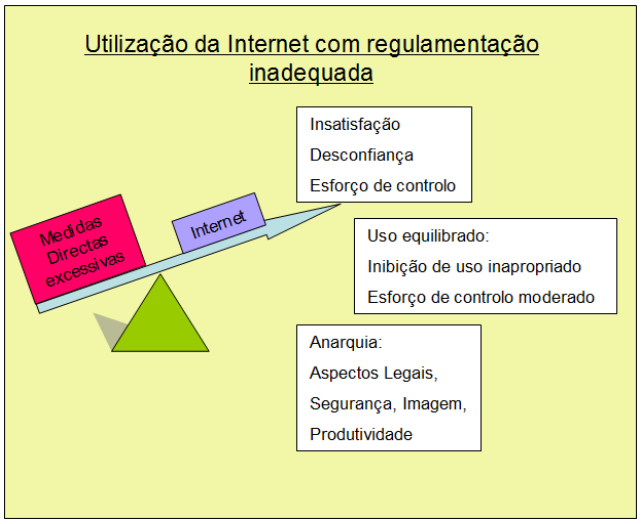


Figura 3 – Excesso de Medidas Directas

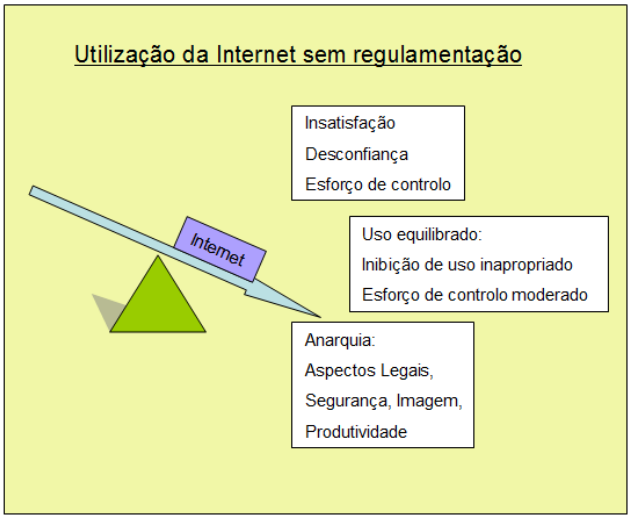


Figura 4 – Poucas ou nenhumas Medidas Directas

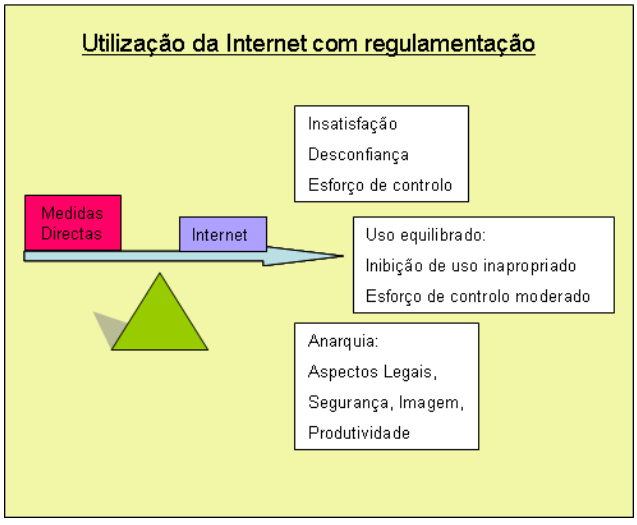


Figura 5 – Quantidade adequada de Medidas Directas

(2) Medidas Indirectas

As Medidas Indirectas são as que actuam sobre a educação e a consciência do Empregado, levando-os, por vontade própria e conhecimento, a adoptarem comportamentos mais responsáveis na utilização da Internet. Têm a vantagem de não provocarem insatisfação nos Empregados, embora não seja espectável que produzam resultados a curto prazo, uma vez que se trata de um processo de aculturação, por norma demorado. Neste âmbito, inserem-se, por exemplo, as acções de formação e de sensibilização para as boas práticas da utilização da Internet.

Existirão também Medidas que têm efeitos Directos e Indirectos em simultâneo, tal como o bloqueio de determinados tipos de acesso por períodos horários, onde o objectivo será não só restringir a utilização da Internet, mas principalmente disciplinar e educar o Empregado, para que este estabeleça hábitos de trabalho mais saudáveis e adequados.

Apresenta-se de seguida, as Medidas mais utilizadas pelas Empresas, relacionando-as com as causas sobre as quais produzirão efeitos:

Causas / Medidas	Fácil Acessibilidade	Hábito	Insatisfação no serviço	Vicio	Sensação de privacidade	Indisciplina de trabalho
Elaboração e divulgação de um Normativo		x			x	x
Controlo de acessos	x					
Monitorização e detecção de actividade irregular		x			x	
Divulgação sanções		x		x		
Fomentar trabalho por objectivos		x	x	x		
Formação		x	x			x
Campanhas de sensibilização: Seminários, Conferências…		x		x		
Restrições por horário ou por dias	x	x		x		
Quiosques			x			
Grupos de acesso diferenciados	x					

Tabela 3 – Relação: Medidas / Causas

Apresenta-se de seguida, as mesmas Medidas caracterizadas pela sua forma de implementação e quanto ao efeito:

Medidas \ Forma x Efeito	Quanto à forma de implementação				Quanto ao efeito	
	Regulamentação	Tecnológico	Procedimento	Outras actividades	Directo	Indirecto
Elaboração, divulgação e aplicação de um Normativo	x				x	
Controlo de acessos	x	x			x	
Monitorização e detecção de actividade irregular	x	x			x	
Divulgação sanções			x		x	
Fomentar trabalho por objectivos		x	x		x	
Formação				x		x
Campanhas de sensibilização: Seminários, Conferências…				x		x
Restrições por horário ou por dias		x			x	x
Quiosques		x			x	x
Grupos de acesso diferenciados		x	x		x	

Tabela 4 – Medidas / Forma de implementação / Efeitos

Atendendo que a Medida de fomentar o trabalho por objectivos será uma preocupação natural de qualquer Empresa, e certamente discutida em âmbitos mais alargados do que a sua contribuição para a redução da UII, não será mais analisada neste trabalho. Fica apenas o registo que a gama alargada de causas da UII, levará a que Medidas aparentemente não relacionadas com a utilização da Internet, possam e devam ser aplicadas. Entre elas poderemos ter, por exemplo, o incentivo a práticas desportivas.

De forma a compreendermos melhor as vantagens a desvantagens de cada uma das Medidas, apresenta-se um resumo das mesmas na seguinte Tabela:

Medidas	Vantagens	Desvantagens
Elaboração e divulgação de um Normativo	Saber que existem regras para utilização da Internet. Espera-se que afecte os hábitos e discipline o Empregado nesta actividade.	Insatisfação por parte de alguns Empregados, dependendo da agressividade das Normas.
Controlo dos acessos	Bloqueio inequívoco de domínios cujos conteúdos explicitamente não se relacionam com a missão da FA, ou que sejam susceptíveis de conterem *software* malicioso.	O carácter dinâmico da Internet exige um esforço contínuo na actualização das listagens. Existem vários domínios que apenas ocasionalmente poderão ser uma mais-valia para o serviço.
Monitorização e detecção de actividade irregular	Afectar a sensação de privacidade do empregado, de forma a dissuadi-lo de efectuar um uso abusivo da Internet. Permite apurar responsáveis de acções ilícitas na rede.	Exige rigor na aplicação da Lei e um grande cuidado na utilização da informação que daí provenha.
Divulgação de sanções	Efeito dissuasor extremamente eficaz no uso abusivo da Internet. Poderá ser omitida a identificação do autor da sanção, que não afectará o efeito desejado.	Sensação de repressão caso não seja esclarecido o objectivo da divulgação.
Formação	Contribui para um Empregado mais culto, e portanto mais consciente.	Difícil formar um grande número de Empregados, e a tecnologia evolui também muito rapidamente.
Campanhas de sensibilização	Contribui para um Empregado mais consciente.	Dificuldade em chegar a todos os Empregados e a motivá-los para esta causa.
Restrições de acessos por horário ou por dias	Força um uso mais disciplinado da Internet, dividindo claramente os horários de lazer e de serviço.	Resistência às restrições de acessos.
Quiosques de acesso livre à Internet	Permite compensar a agressividade de algumas Medidas mais "polémicas".	Difícil de controlar e de responsabilizar os Empregados. Só por si não alteram em nada a problemática da UII.
Grupos de acesso diferenciados	Permite que cada tipo de Empregado tenha um acesso mais personalizado, e portanto adaptado às suas necessidades, optimizando o serviço em geral.	Difícil de definir por grupos os acessos permitidos, bem como as prioridades entre eles.

Tabela 5 – Medidas / Vantagens / Desvantagens

Tendo em conta que o excesso de Medidas Directas contribui para uma insatisfação no serviço, entre outros malefícios, e que mesmo as Medidas Indirectas apresentam desvantagens, verifica-se que a segunda hipótese é falsa.

Sendo que no Normativo estará reflectido o pensamento da EE sobre de que forma a utilização da Internet deverá ser efectuada, iremos no próximo subcapítulo debruçar-nos, em exclusivo, sobre esse assunto.

b) Elaboração de um Normativo

A elaboração de um Normativo será a principal Medida, uma vez que servirá de referência para as demais Medidas a aplicar. O Normativo é um documento que define qual a postura e comportamentos esperados pelos Empregados aquando da utilização da Internet no Posto de Trabalho (Ferreira, 2008). Será também este documento que criará um vínculo jurídico com o Empregado, incutindo-lhe os deveres inerentes ao direito da utilização da Internet.

Para a sua elaboração, deverão ser respeitados os seguintes princípios:

- Estar de acordo com a Lei, de preferência referenciado na Comissão Nacional de Protecção de Dados (CNPD);
- Ser claro e exemplificativo de forma a não suscitar duplas interpretações;
- Ser curto e de fácil leitura;
- Referir a monitorização;
- Prever a evolução tecnológica dos equipamentos e serviços, de forma a não ficar desactualizado rapidamente;
- Ser abrangente no sentido de incluir todas as áreas que se pretende regular: Uso da Internet e da Rede local, actividade computacional local, plataformas tecnológicas portáteis (caso existam), etc.;
- Descriminar as sanções aplicáveis em caso de infracção.

Tipicamente, um Normativo é constituído pelas seguintes partes (UGRIN, 2008):

- Explicação da extensão das normas: o objectivo, a quem se aplica e em que situações;
- Normas definindo o uso apropriado;
- Exemplos de uso apropriado vs uso não apropriado;
- Descrição das sanções aplicáveis em caso de infracção;
- Informar sobre a monitorização efectuada pela EE;
- Espaço para assinatura do utilizador onde dará conhecimento que leu, compreendeu, e que aceita as regras de utilização.

Apesar de ser fundamental a existência de um Normativo para a utilização de Internet, espera-se que a sua simples implementação tenha um impacto pouco significativo na redução da UII (UGRIN, 2008). Terá que haver um empenho no cumprimento das regras nele contido para que se possa obter resultados efectivos (UGRIN, 2008).

O primeiro passo após a sua elaboração, é submetê-lo a assinatura por todos os Empregados, de forma a divulgar o seu conteúdo, e torná-lo legalmente efectivo. A utilização do CE de serviço deverá ser claramente mencionado com regras específicas.

Paralelamente ao Normativo, é recomendável a existência de um Manual de Boas Práticas para a utilização da Internet e do CE, preferencialmente *on-line*, com a capacidade de periodicamente apresentar aos Empregados, através do seu computador, sugestões e dicas. Sobre as redes sociais, caso a Empresa pretenda fazer um uso institucional das mesmas, deverá produzir um Normativo específico para o efeito, uma vez que exigirá cuidados especiais e específicos devido aos seus potenciais efeitos negativos já descritos.

Em relação à legalidade do documento, existe todo um pacote legislativo que balanceia os legítimos interesses da EE em controlar os acessos à Internet dos seus Empregados e os direitos, liberdades e garantias dos titulares dos dados. Sobre este assunto, o TCOR Frazão elaborou um resumo (Anexo B) dessa legislação, de onde se destaca os seguintes princípios:

- A EE deve assegurar-se que os trabalhadores estão claramente informados e que estão conscientes dos limites estabelecidos em relação à utilização de Internet para fins privados e que conhecem as formas de controlo que podem ser adoptadas;
- Deve ser admitido um certo grau de tolerância em relação ao acesso para fins privados, nomeadamente se este decorrer fora do horário de trabalho;
- O controlo dos *mails* – a realizar de forma aleatória e não persecutória – deve ter em vista, essencialmente, garantir a segurança do sistema e a sua performance;
- Os responsáveis pelo tratamento de dados pessoais devem fazer a respectiva notificação junto da CNPD (artigo 27.º da Lei 67/98), a qual será formulada em impresso próprio.

O COR Monteiro do Estado-Maior General das Forças Armadas (EMGFA), em entrevista, disponibilizou um documento que é uma proposta para o Normativo do EMGFA, que se considera ser uma boa referência (Apêndice A).

Sendo fundamental a elaboração do Normativo, é também importante o processo de selecção das restantes Medidas a aplicar, bem como o modo de aplicá-las. Será pois, esse o tema do próximo subcapítulo.

c) Considerações para a aplicação de Medidas

Para se determinar as melhores Medidas a aplicar, será importante ter em conta determinadas considerações. Um delas, será a de verificar de que forma o Empregado percepciona a sua utilização da Internet no Posto de Trabalho (UGRIN, 2008):

- A ULI, efectuada ocasionalmente é algo aceitável;

  Significa que será visto como uma acção agressiva a proibição total da ULI;

- A pornografia não deve ser tolerada;

  Não haverá resistência ao bloqueio de sites pornográficos e será encarada com naturalidade a proibição desses conteúdos no Posto de Trabalho;

- A dedicação exigida ao trabalho força o Empregado a tratar de assuntos pessoais no serviço;

  A ULI pode ser mesmo encarada como um direito;

- O sentimento que a ULI não é um assunto preocupante;

  Existe pouca consciencialização, por parte dos Empregados, da amplitude dos efeitos da UII, e da sua relação com a ULI;

- Mesmo não sendo a ULI um grande problema, a existência de normas é aceitável;

  Aceita-se a existência de Normas para a utilização da Internet.

Os dados até este ponto apresentados sugerem que proibir a ULI não será uma boa Medida, uma vez que trará insatisfação ao Empregado e não resolverá muitos dos efeitos mencionados que ocorrem na utilização da Internet para serviço. Deverá mesmo a EE assumir a responsabilidade de satisfazer as necessidades sociais dos seus Empregados (GUPTA, 2004), antecipando essa procura que invariavelmente ocorrerá, nem sempre da forma mais correcta.

Existem porém, outros factores a ter em conta para a escolha das Medidas a adoptar (UGRIN 2008):

- Que tipo de Empregado a Empresa tem? Será possível restringir o acesso à Internet?
- Qual é a cultura da Empresa? Aceitará as Medidas?
- As sanções deverão ser proporcionais aos crimes.

- Todas as infracções deverão ficar registadas.
- Quanto custarão as Medidas?

Será igualmente importante verificar alguns outros aspectos. A dimensão da Empresa influência a tendência para uma maior ou menor prática da UII. As Empresas de maior dimensão (considerando acima de 250 Empregados como grande), são mais propícias para a UII, verificando-se que o Empregado representa a sua maior ameaça à segurança da informação em rede (WILLISON, 2009). Verifica-se também que o sector Público apresenta uma maior incidência de utilização de ferramentas de monitorização (GUPTA, 2004), indiciando essa necessidade uma maior tendência para a existência de UII nesse sector.

No entanto, a responsabilidade de reduzir a UII não é só das Empresas, é dos Empregados também. Importa pois saber quais as linhas de pensamento que deverão ser incutidas nos Empregados (GUPTA, 2004):

- A ULI é para ser minimizada: Os Empregados precisam de compreender que a ULI em excesso corresponde a um uso abusivo da Internet, e que o motivo da sua existência é o serviço;
- Realçar os ganhos de produtividade: É necessário relembrar, continuadamente, os motivos pelos quais a EE contratou o Empregado, que é o da produção. Deverá haver a percepção do trabalho por objectivos, e que o serviço de Internet é propriedade da Empresa, e que por isso tem todo o direito a controlá-la;
- Manter os interesses da Empresa em mente: Atendendo a que a Empresa permite a ULI, deverá ser estabelecido uma relação de confiança entre a mesma e o Empregado. Esse ambiente promoverá uma relação de respeito mútuo entre as duas entidades, fazendo com que os Empregados, de própria vontade, defendam os interesses da sua Empresa, limitando dessa forma as acções que possam resultar em seu prejuízo.

Estando apresentadas as Medidas mais aplicadas pelas Empresas, bem como as considerações a ter em conta para a sua aplicação, veremos de seguida qual o ponto de situação da FA em termos de utilização da Internet, para que se perspective quais as Medidas mais adequadas para a sua realidade.

3) A Internet na FA

a) Como está implementada a Internet na FA?

Apresenta-se o enquadramento orgânico dos órgãos com responsabilidade directa sobre o funcionamento da Internet na FA, que são a Direcção de Comunicações e Sistemas de Informação (DCSI) e a Divisão de Comunicações e Sistemas de Informação (DivCSI):

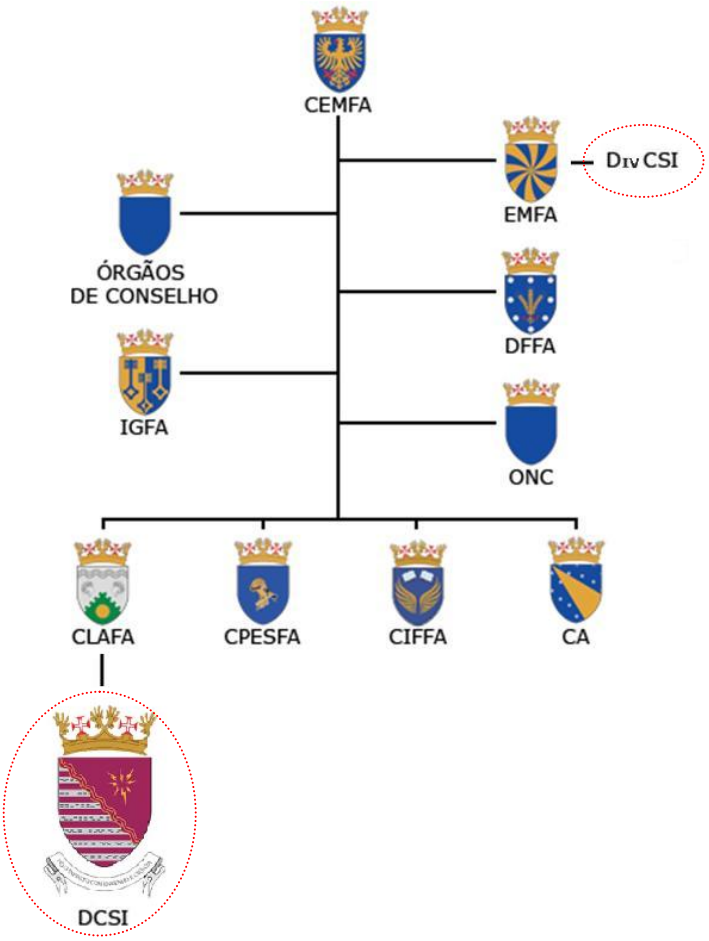


Figura 6 – Estrutura orgânica da FA[6]

A DCSI tem a responsabilidade de administrar o serviço de Internet, enquanto a DivCSI tem o dever de emanar as directivas que orientam essa administração.

[6] Informação extraída do Portal Externo da FA.

(1) Normativo actual

Existe um documento com o título: "Normas provisórias para a utilização do CE interno da FAP e da internet no âmbito das redes locais de unidade", que data de 1998 e que está disponibilizado no portal interno da FA (Apêndice B).

Como o próprio título indica, trata-se de Normas provisórias, o que sugere ser uma primeira aproximação a um segundo documento final, ainda por elaborar.

Analisando o documento, destacam-se os seguintes aspectos:

- Tem a assinatura do CEMFA, o que demonstra o reconhecimento da importância do assunto em causa;

- Permite a ULI, desde que não "represente prejuízo sensível para o serviço.";

- É vago, usa linguagem técnica e não está exclusivamente dedicado ao Utilizador;

- Não prevê monitorização nem sanções;

- Não prevê assinatura por parte do utilizador, pelo que não tem valor legal nem será espectável que seja do conhecimento geral.

Atendendo às características necessárias a um Normativo, apresentadas no capítulo anterior, verifica-se que não será espectável que o presente documento esteja a produzir qualquer tipo de efeito. A DivCSI reconheceu a importância de se elaborar rapidamente um Normativo[7], para que se colmate esta necessidade de regulamentação.

(2) Quem está a usar o serviço?

A FA tem cerca de 8.681 elementos (SIGAP 26/02/10), dos quais 4.422 têm computador no seu Posto de Trabalho (Anuário 2008) e 3.296 são Utilizadores.

[7] Tópico de entrevista ao TCOR Ornelas da DivCSI.

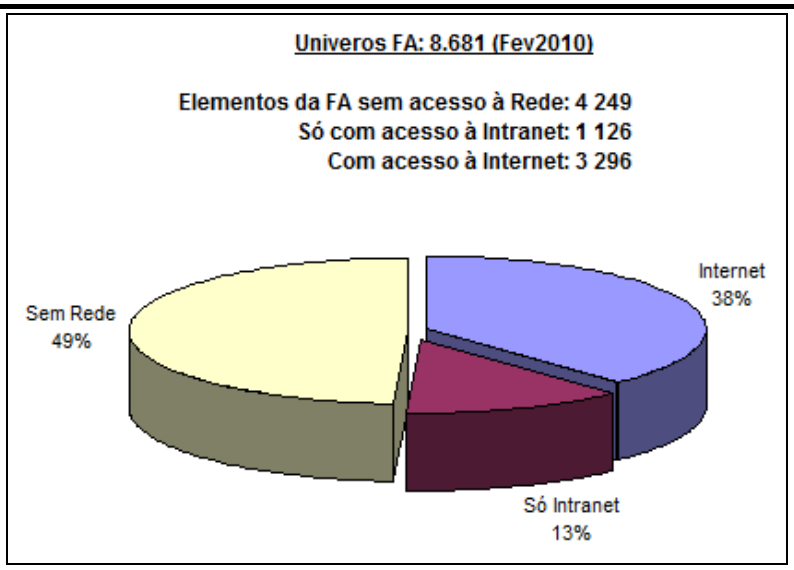


Figura 7 – Universo da FA / Utilizadores da Rede FA / Utilizadores da Internet

Existem cerca de 2.357 endereços de serviço na FA, que se dividem em 1.617 endereços nominais e 740 endereços institucionais[8]. Todos os Utilizadores têm um endereço nominal, existindo ainda 740 endereços institucionais. Apesar de haver uma percentagem significativa de endereços institucionais (46%), o que é positivo, pois a sua utilização dissuade um comportamento abusivo, cerca de 41% dos Utilizadores reconhecem que do CE enviado, menos de 10% são para endereços institucionais[9].

(3) Ferramentas tecnológicas

Existem várias páginas de Internet que estão bloqueadas, por se considerarem ofensivas ou maliciosas para a FA[10]. Para os acessos realizados a páginas com exibição de vídeos, é utilizado um sistema de degradação de sinal[11], o que se considera ser uma técnica bastante perspicaz, uma vez dissuade o Utilizador de aceder ao serviço sem que fique com a sensação de impedimento de utilização.

A monitorização é efectuada através de sistemas automáticos que procuram comportamentos anómalos na Rede, o que, uma vez detectados, motivará posteriormente uma intervenção humana. No entanto, os acessos à Internet estão a ser atribuídos,

[8] Dados fornecidos por ALF Afonso e CAP Simões da DCSI.

[9] Inquérito realizado a 649 Utilizadores.

[10] Tópico de entrevista com CAP Valente, da DCSI.

[11] Tópico de entrevista com TEN Rodrigues, da DCSI.

tecnicamente, aos computadores e não aos Utilizadores (através de uma conta e respectiva senha). Apenas efectuando a associação entre o computador e o Utilizador, o que nem sempre é linear, se poderá identificar o autor de determinada acção na rede[12].

O *software Zen Works* (instalado na DCSI) não está a fazer uso de todas as suas capacidades, o que permitiria monitorizar e gerir remotamente as aplicações instaladas nos computadores da FA, o que tornaria possível, de uma forma simples, o controlo centralizado dos aplicativos instalados nos mesmos[13], suprimindo parte dos efeitos da UII.

A largura de banda de Internet contratada para a FA tem 40Mb/s, de *Download* e *Upload* (acesso empresarial sem taxa de contenção). No entanto, nem toda essa gama se destina a ser usada no Posto de Trabalho, sendo uma parte dela destinada ao portal da FA, a acessos do exterior à rede (para pessoal em missão, por exemplo), para algumas representações de empresas aeronáuticas na FA (no âmbito de contrato FISS do EH101 e do C-295), e ainda se espera que venha a servir a rede de alunos da AFA que se encontra em fase de projecto[14].

Pelo referido, é notório que com um universo tão alargado de utilizadores, para uma largura de banda tão diminuta, se espere que a sua utilização seja tão racional, equilibrada e eficiente quanto possível. Será pois esse o tópico do próximo subcapítulo.

b) Como é utilizada a Internet na FA?

Será descrito de seguida, de que forma o serviço Internet é utilizado na FA, recorrendo ao Inquérito efectuado aos seus Utilizadores (Anexo C) e a dados fornecidos pela DCSI.

(1) Tipologia de Utilização

Foi solicitada à DCSI[15] uma listagem dos dez domínios mais visitados (Anexo D), num período de 24 Horas, bem como dos Utilizadores que mais ligações à Internet estabeleceram nesse mesmo período (Anexo E). Dos dez domínios mais visitados, os primeiros oito, que totalizaram 89% dos acessos totais, não são relacionados com o

[12] Tópico de entrevista com o CAP Valente da DCSI.

[13] Tópico de entrevista com o CAP Trabula da DCSI.

[14] Tópico de entrevista com o MAJ Ferreira da DCSI.

[15] Dados fornecidos por CAP Valente da DCSI.

serviço. Neste grupo encontra-se o *Gmail*, com 43% dos acessos, um domínio de jogos, outro de encontros sociais (logon2.clubenet.com), um de redes sociais (hi5) e *banners* (acessos involuntários devido a publicidade por navegar em páginas com esses mecanismos instalados). O acesso ao motor de pesquisa *Google*, que entra no âmbito de serviço (embora não necessariamente), surge no 9º e 10º lugar (Google.com e Google.pt). De facto, mais de 25% dos Utilizadores assumem efectuarem a ULI com muita frequência, e mais 35% refere fazê-lo com alguma frequência (I: Pergunta 5):

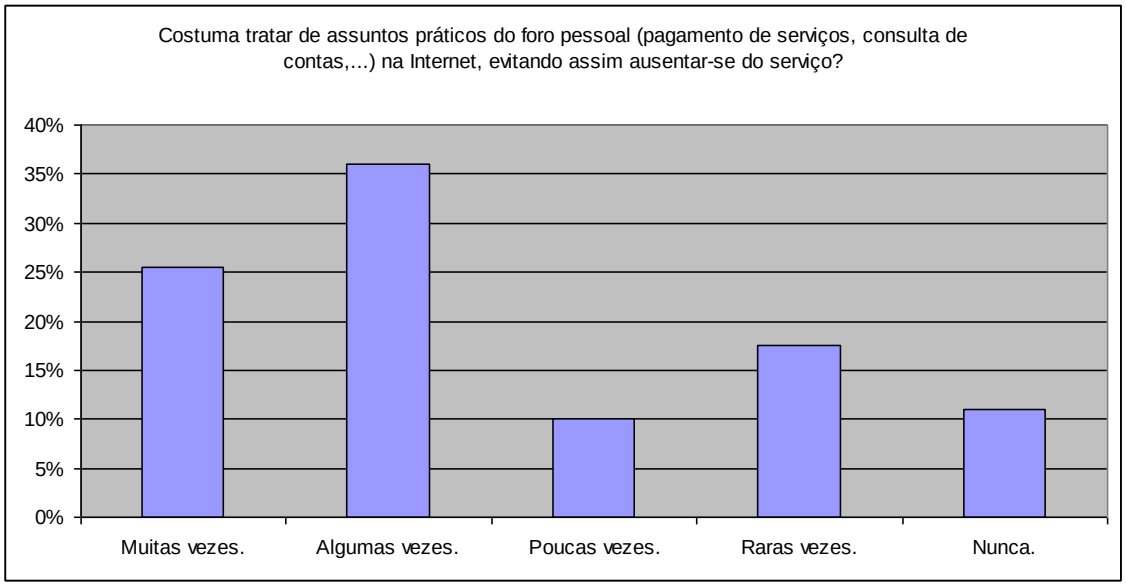


Gráfico 1 - Pergunta 5

No entanto, quando questionados sobre qual a percentagem do tempo lúdico que é consumido a navegar na Internet, dois em cada três Utilizadores referem ser menos de 10% (I: Pergunta 6):

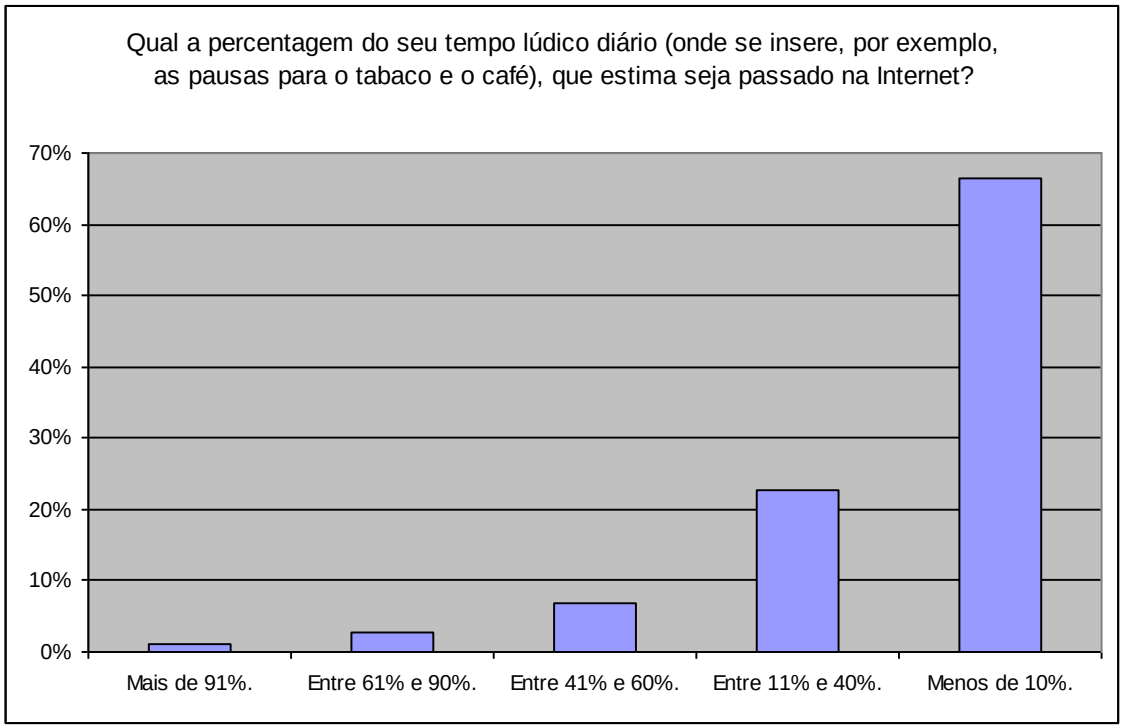


Gráfico 2-Pergunta 6

Estes dados aparentam uma contradição, que pode ser justificada por alguma da utilização se realizar em horário pós laboral, mas será principalmente pela dificuldade que cada um tem em medir o seu tempo real de utilização da Internet. É comum um Utilizador ao navegar na Internet dispersar-se na sua pesquisa, e, ao fim de algum tempo, quando por exemplo convidado para ir beber um café, ele sentir que só a partir desse instante entrou no seu período lúdico, não contabilizando interiormente as divagações que preconizou.

Em relação ao *Messenger* (que não entra na tabela anterior por não ser um domínio, mas sim uma ligação ponto a ponto), verificou-se que um em cada três Utilizadores faz uso deste serviço no seu Posto de Trabalho (I: Pergunta 6). Sendo o *Messenger* amplamente conhecido pelo seu carisma de socialização, há também quem defenda a sua versatilidade para tratar de assuntos de serviço.

Em relação à lista dos Utilizadores que mais acessos fizeram, é possível verificar que os primeiros dez (de um universo de 3.296 utilizadores) foram responsáveis por cerca de 96% dos acessos totais da FA no período mencionado. Os números falam por si.

(2) Qualidade do Serviço

De uma forma geral, os Utilizadores mostram-se satisfeitos com a qualidade do serviço de Internet (I: Pergunta 1), apesar de a maioria reportar um significativo impacto

nas suas funções devido à ocorrência de falhas ou mau desempenho do mesmo (I: Pergunta 2).

(3) Importância da Internet

Perante uma falha do serviço de Internet, a maioria dos Utilizadores revela ficar com restrições no cumprimento da sua missão (40% com algumas restrições, 36% com fortes restrições). Cerca de 17% indica que teriam poucas ou nenhumas restrições e 7% refere que impediria o cumprimento da sua missão (I: Pergunta 3).

(4) Aderência a acções de formação e de sensibilização

De uma forma geral, os Utilizadores sentem-se bem informados sobre os aspectos legais e de segurança relacionados com a Internet (I: Pergunta 10), e sobre as boas práticas do uso do CE (I: Pergunta 11). Apesar do aspecto positivo desta tendência, será de esperar que suscite alguma resistência na adesão a acções de formação e sensibilização para estes temas.

(5) Aceitabilidade de Medidas

Quando confrontados com a possibilidade de divulgação de informação relacionada com os acessos individuais à Internet, é curioso verificar uma grande dispersão de opiniões (I: Pergunta 12), como se pode ver no seguinte gráfico:

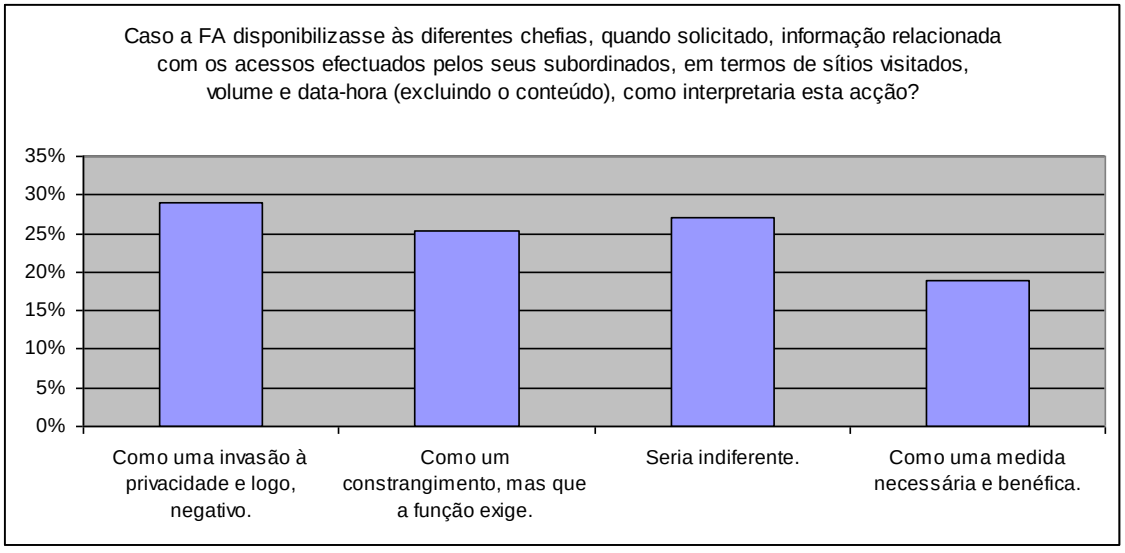


Gráfico 3 – Pergunta 12

(6) Formação

Analisando a Lista de Cursos da Direcção de Instrução (DInst) para 2010[16] (Anexo F), verifica-se que não existe nenhuma formação relacionada com a utilização da Internet. Considera-se, ainda assim, que o curso de Gestão do Tempo poderá ajudar a ultrapassar algumas dificuldades geradas pela UII.

Atendendo aos efeitos da UII, e conhecendo a realidade da utilização da Internet na FA, efectuaremos, no próximo subcapítulo, uma análise de situação focando as Medidas existentes.

c) A Internet na FA: Análise de situação

(1) Normativo

A ausência de um Normativo eficaz torna difícil os Utilizadores terem a percepção do que a FA espera deles ao fazerem uso da Internet, além de que não ficam informados das acções de monitorizações então levadas a cabo, o que resulta num sentimento de impunidade aquando das suas acções.

(2) Ferramentas tecnológicas

A não associação do Utilizador ao acesso à Internet e a falta de enquadramento legal por um Normativo, torna praticamente impossível qualquer acção sancionatória sobre as infracções detectadas.

(3) Formação / Acções de campanhas

O não desenvolvimento de acções de formação e de acções de campanha, no sentido de uma utilização mais apropriada da Internet, impede o "despertar" dos Utilizadores para esta temática.

(4) Grupos de acesso diferenciados

A falta de associação das funções de cada Utilizador ao tipo de acesso à Internet requerido para as mesmas, bem como do seu grau de prioridade[17], impede a diferenciação dos acessos atribuídos, impossibilitando a optimização na distribuição de um bem escasso.

[16] Lista retirada do portal interno da FA.

[17] Tópico de entrevista com CAP Trabula, da DCSI.

Tendo em conta a clara insuficiência de Medidas na FA, que em parte explicarão a tipologia de utilização da Internet apresentada, pode-se concluir que se comprova a terceira hipótese.

Sobre os efeitos que a UII terá na FA, poder-se-á depreender, ainda que não tenham sido quantificados, que eles estão presentes em toda a sua gama.

Conclusão

Para a execução deste trabalho, considerou-se importante começar por identificar porque é que a utilização da Internet no Posto de Trabalho apresenta diversos perigos para a Entidade Empregadora (EE). Verificou-se que é da Utilização Inapropriada da Internet (UII) que surgem os malefícios da Internet, e que esta tanto poderá estar presente na Utilização Lúdica da Internet (ULI) como na utilização com fins de Serviço. A ULI, moderada e consciente, poderá mesmo apresentar benefícios para a EE, no sentido em que contribui para um ambiente de confiança entre esta e o Empregado. Note-se, no entanto, que a fronteira entre a ULI e a utilização com fins de serviço pode ser difusa em determinadas situações, uma vez que apenas a intenção do Empregado fará essa distinção. A UII pode ser efectuada de uma forma consciente ou não, e esta poder-se-á caracterizar como sendo aquela que representa sempre um prejuízo para a EE.

Para que se possa entender os perigos a que a EE está sujeita pela UII, descreveu-se os seus efeitos, reflectindo-se eles nos aspectos Humanos, Tecnológicos e Organizacionais. A UII pode provocar perdas significativas à Empresa em termos de consumo de recursos, tanto materiais como humanos, implicar processos jurídicos, perda ou fuga de informação sensível da Empresa, degradação da imagem institucional e em ultima instância, perdas de produtividade, entre outros aspectos. Uma boa percepção dos perigos resultantes da UII servirá de motivação no esforço de implementação de Medidas.

Percebendo os perigos, procurou-se entender quais as causas dessa UII, uma vez que serão sobre elas que as Medidas deverão actuar. Servirá também para uma melhor compreensão sobre o porquê da existência da UII. Este poderá ser um dos aspectos mais difíceis e sensíveis de analisar e compreender, uma vez que procura explicar porque motivo uma elevada percentagem de Empregados faz UII de forma continuada. As causas são várias: a fácil acessibilidade, o hábito, a insatisfação no serviço, o vicio, a socialização, a sensação de privacidade e a indisciplina de trabalho. Poderiam se apontar outras causas, mas estas foram as consideradas mais importantes.

Conhecendo as causas da UII, procurou-se determinar quais as Medidas mais aplicadas pelas Empresas para as inibir. As Medidas podem ser agrupadas em dois tipos: as Directas, que são as que se baseiam na dissuasão, produzindo efeitos imediatos, mas que induzem insatisfação no Empregado se usadas em excesso, e as Indirectas, que actuam sobre a consciência do Empregado, baseando-se essencialmente na formação e sensibilização do mesmo. Reconhecendo-se como principal Medida a existência de um

Normativo, uma vez que nele deverão estar contidas as regras para a utilização da Internet no Posto de Trabalho, deu-se especial ênfase sobre alguns aspectos a ter em conta aquando da sua elaboração. Destacou-se a importância de se seguir o preconizado na legislação sobre esta matéria, bem como a necessidade de o documento ficar vinculado ao Empregado através da sua assinatura. Apresentaram-se de seguida algumas considerações a ter em conta para a implementação de Medidas. Existem certos aspectos que são necessários ter em conta para a escolha das Medidas a adoptar, tais como a cultura da Empresa, a dimensão da Empresa e o ser privada ou pública.

Conhecendo-se o fenómeno da UII, e a forma de combatê-la, procurou-se de seguida saber como está implementada a Internet na FA, analisando-se o Normativo actual, quem usa esse serviço e as ferramentas tecnológicas implementadas como Medidas. Para se determinar como é utilizada a Internet na FA, recorreu-se a um inquérito realizado a 649 Utilizadores e a dados fornecidos pela DCSI. Dessa forma, apurou-se a tipologia de utilização e outros factores, como a importância e a qualidade da Internet. Verificou-se a existência de uma elevada percentagem de utilização da Internet para fins Lúdicos (89%) e uma distribuição pelos Utilizadores manifestamente desequilibrada (10 dos 3.296 Utilizadores são responsáveis por 96% dos acessos efectuados). Estes dados sugerem uma grande exposição da FA aos efeitos da UII descritos no capítulo 1. Por fim, efectuou-se uma breve análise do ponto de situação actual da Internet na FA.

Com a realização desta investigação, considera-se que as mais-valias resultantes do mesmo são:

- Identificação e caracterização do Conceito UII, em vez de Uso Abusivo da Internet e Actividade Computacional Não Relacionada com o Serviço, que são os termos mais frequentes nos trabalhos de Investigação sobre esta temática;
- Análise dividida em efeitos e causas da UII, uma vez que estes dois aspectos contribuem de forma diferente para a selecção das Medidas a adoptar;
- Identificação da Necessidade de tornar Seguro como um Efeito da UII;
- Caracterização das Medidas em Directas e Indirectas, para uma melhor orientação na selecção das Medidas, mediante os efeitos que se pretendam obter.

- Foi traçado o quadro geral da utilização da Internet na FA, o que poderá auxiliar estudos posteriores, nomeadamente para o processo de implementação de Medidas, caso surja essa decisão.

Por fim, apresenta-se um conjunto de recomendações:

Para a DivCSI:

- A Elaboração de um Normativo, utilizando os princípios apresentados no capitulo 2;
- Propor à DInst a inclusão de acções de formação relacionadas com o uso apropriado da Internet;
- Promover campanhas de sensibilização junto dos órgãos competentes para que os Utilizadores sejam mais conscientes dos perigos da Internet;
- Estudar e propor a implementação de Medidas, tais como as restrições por horário ou por dias;
- Desenvolver estudo que associe, por grupos, as funções dos Utilizadores com as suas reais necessidades de acessos à Internet para serviço, bem como o seu grau de importância.

Para a DCSI:

- Sobre o Controlo dos acessos, recomenda-se uma maior envolvência política na definição dos critérios de bloqueio dos acessos à Internet, bem como a activação de todas as capacidades do *software Zen Works*;
- Associar o Utilizador ao respectivo acesso de Internet e procurar uma solução que permita a monitorização 24 Horas por dia;
- Determinar, juntamente com a DivCSI, procedimentos para actuar aquando da detecção de violações de normas estipuladas.

Este trabalho permite concluir que a UII é um problema de grandes dimensões, e que o seu combate não é simples nem óbvio. Para que surjam resultados efectivos de redução da UII, o assunto deverá ser tratado com seriedade e dedicação ao mais alto nível da FA. Verificou-se também que não é um problema exclusivamente informático, mas bem mais abrangente, uma vez que o espectro dos efeitos é bastante alargado. A ULI, apesar de não representar necessariamente uma actividade nociva, deverá ser limitada à sua menor expressão possível. Em última análise, todos os esforços efectuados pela FA deverão contribuir para que o Utilizador seja mais consciente dos seus deveres e responsabilidades, de forma a torná-lo mais apto e eficiente na utilização da Internet.

Bibliografia

FERREIRA, Lilian (2008): ***O que você pode fazer no computador do trabalho?*** UOL Tecnologia.

Disponível na Internet em:

<http://tecnologia.uol.com.br/dicas/ultnot/2008/04/07/ult2665u272.jhtm>

FREED, Michael, at al. (2008): ***RADAR: A Personal Assistant that Learns to Reduce Email Overload***. Association for the Advancement of Artificial Intelligence

Disponível na Internet em:

<http://iorgforum.org/>

GALLETTA, Dennis, POLAK, Peter (2003): ***An Empirical Investigation of Antecedents of Internet Abuse in the Workplace***. SIGHCI 2003 Proceedings. Paper 14.

Disponível na Internet em:

< http://aisel.aisnet.org/sighci2003/14>

GRIFFITHS, Mark (2003): ***Internet abuse in the workplace: issues and concerns for employers and employment counsellors,*** Journal of Employment Counseling.

Disponível na Internet em:

<http://www.allbusiness.com/technology/internet-technology/585920-1.html>

GUPTA, Jatinder (2004): ***Improving workers' productivity and reducing internet abus,*** The Journal of Computer Information Systems.

Disponível na Internet em:

<http://www.allbusiness.com/technology/internet-technology/932035-1.html>

HEARTS, Jack (2002): ***Web tops workplace disciplinary procedure league,*** IT-Director.

Disponível na Internet em:

<http://www.it-director.com/content.php?cid=3119>

JOHNSON, Jeffrey, UGRAY, Zsolt (2007): ***Employee Internet abuse: Policy versus reality,*** Issues in Information Systems.

Disponível na Internet em:

<http://www.iacis.org/iis/2007_iis/PDFs/Johnson_Ugray.pdf>

JOHNSON, Pamela, INDVIK, Julie (2003): ***The organizational benefits of reducing cyberslacking in the workplace.*** Business Services Industry.

Disponível na Internet em:

<http://findarticles.com/p/articles/mi_m1TOT/is_2_8/ai_n25102519/>

MACWORLD (2002): ***Internet abuse is top reason for workplace discipline.***

Disponível na Internet em:

<http://www.macworld.com/article/6745/2002/09/internet.html>

MARKSTEINER, COL. Peter (2008): ***The threat from within, E-mail overload degrades military decision-making,*** *Armed Forces Journal.*

Disponível na Internet em:

<http://www.armedforcesjournal.com/2008/09/3640424/>

NUCLEUS RESEARCH (2009): ***Facebook: Measuring the cost to business of social Notworking.*** Nucleus Research.

Disponível na Internet em:

<http://nucleusresearch.com/research/notes-and-reports/facebook-measuring-the-cost-to-business-of-social-notworking/>

QUIVY, Raymond, CAMPENHOULDT, LucVan (1998): ***Manual de investigação em ciências sociais,*** 2ª ed., Lisboa: Gradiva.

TUMA, Rogério (2006): ***A Internet e a Compulsão***, Carta Capital.

Disponível na Internet em:

<http://cartacapital.com.br/2006/10/5470>

UGRIN, Joseph, PEARSON, Michael (2008): ***Exploring Internet abuse in the workplace: how can we maximize deterrence efforts?*** Review of Business.

Disponível na Internet em:

<http://www.entrepreneur.com/tradejournals/article/184710901_1.html>

WEBSENSE (2002): ***Workplace Web Abuse Costs Corporate America $85 Billion This Year, Reports Websense Inc.,*** Websense.

Disponível na Internet em:

<http://investor.websense.com/releasedetail.cfm?ReleaseID=285842>

WILLISON, Robert (2009): ***Motivations for Employee Computer Crime: Understanding and Addressing Workplace Disgruntlement through the Application of Organisational Justice.*** Copenhagen Business School.

Disponível na Internet em:

<http://openarchive.cbs.dk/handle/10398/7759>

WOON, Irene, PEE, Loo (2004): ***Behavioral Factors Affecting Internet Abuse in the Workplace – An Empirical Investigation.*** CiteSeerx.

Disponível na Internet em:

<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.118.547>

Glossário

Empregado – Funcionário de uma Empresa que Utiliza o serviço de Internet no seu Posto de Trabalho. É usada a expressão de "Empregado" sempre que se estiver a referir a dados recolhidos à bibliografia que dessa forma descreve o Utilizador de Internet.

Empresas – Entidade mais comummente referenciada na bibliografia consultada, podendo representar também uma organização ou instituição.

Entidade Empregadora – Órgão de uma Empresa com competência e responsabilidade sobre o serviço de Internet nos seus postos de trabalho.

Posto de Trabalho – Conjunto de meios necessários a um Empregado para o desempenho das suas funções.

Utilizador – Elemento da Força Aérea que no seu Posto de Trabalho faz uso do serviço de Internet.

Internet – Rede global de computadores e de Rede de Computadores, baseados no protocolo TCP/IP, sobre a qual correm diversos tipo de serviços:

- World Wide Web (URL, HTTP, HTML).
- CE;
- Transferência de ficheiros (FTP);
- Chats (IRC);
- Sessão remota;

Anexo A - Quadro Conceptual

Conceitos	Dimensões	Indicadores
Internet nas Empresas	**A ULI e a UII**	Semelhanças
		Diferenças
	Efeitos da UII	Efeitos Humanos
		Efeitos Tecnológicos
		Efeitos Organizacionais
	Causas da UII	Fácil Acessibilidade
		Hábito
		Insatisfação no serviço
		Vicio
		Socialização
		Sensação de privacidade
		Indisciplina de trabalho
Medidas de Combate à UII	**Tipologia**	Tempo de produção de efeitos
		Agressividade das medidas
	Normativo	Princípios a respeitar
		Sentimento do Utilizador
		Aspectos legais
	Vantagens / Desvantagens	Tipo de efeito produzido
		Agressividade da medida
		Dificuldade de implementação
Internet na FA	**Como está**	Quem usa o serviço
		Órgãos competentes
		Normativo existente
		Ferramentas tecnológicas
	Como é usada	Sites mais acedidos na FA
		Utilizadores com mais acessos
		Uso Lúdico x Uso de serviço
		Qualidade do serviço
		Importância do Serviço
		Aceitabilidade das Medidas

Anexo B - Pacote Legislativo fornecido por TCOR Frazão

1. Princípios específicos em relação ao e-mail

- O facto de a entidade empregadora proibir a utilização do e-mail para fins privados não lhe dá o direito de abrir, automaticamente, o e-mail dirigido ao trabalhador.
- A entidade empregadora – enquanto responsável pelo tratamento (cf. art. 3.º al. d) da Lei 67/98) – tem legitimidade para tratar os dados, na sua vertente de «registo, organização e armazenamento», com fundamento no disposto no artigo 6.º al. a) da Lei 67/98.
- As condições de legitimidade do tratamento – na vertente de «acesso» – devem obedecer à previsão do artigo 6.º al. e) da Lei 67/98, a qual aponta para a necessidade de ser feita uma ponderação entre os "interesses legítimos do responsável" e os "interesses ou os direitos liberdades e garantias do titular dos dados".
- Os poderes de controlo da entidade empregadora – que não podem ser postos em causa – devem ser compatibilizados com os direitos dos trabalhadores, assegurando-se que devem ser evitadas intrusões. A entidade empregadora deve, por isso, escolher metodologias de controlo não intrusivas, que estejam de acordo com os princípios previamente definidos e que sejam do conhecimento dos trabalhadores.
- A entidade empregadora não deve fazer um controlo permanente e sistemático do e-mail dos trabalhadores. O controlo deve ser pontual e direccionado para as áreas e actividades que apresentem um maior "risco" para a empresa.
- O grau de autonomia do trabalhador e a natureza da actividade desenvolvida, bem como as razões que levaram à atribuição de um e-mail ao trabalhador devem ser tomadas em conta, decisivamente, em relação à forma como vão ser exercidos os poderes de controlo. O segredo profissional específico que impende sobre o empregado (vg. sigilo médico ou segredo das fontes) deve ser preservado.
- As razões determinantes da entrada na caixa postal dos empregados, com fundamento em ausência prolongada (férias, doença), devem ser claramente explicitadas e do seu conhecimento prévio.

- Deve ser claramente diferenciado o grau de exigência e de rigor em relação ao controlo dos e-mails expedidos e recebidos, sendo facultados ao trabalhador meios expeditos e eficazes para assegurar a eliminação imediata dos e-mails recebidos e cuja entrada na sua caixa de correio ele não pode controlar.
- O controlo dos e-mails – a realizar de forma aleatória e não persecutória – deve ter em vista, essencialmente, garantir a segurança do sistema e a sua performance.
- Para assegurar estes objectivos a entidade empregadora pode adoptar os procedimentos necessários para – sempre com o conhecimento dos trabalhadores – fazer uma «filtragem» de certos ficheiros que, pela natureza da actividade desenvolvida pelo trabalhador podem indiciar, claramente, não se tratar de e-mails de serviço (vg. ficheiros «.exe», .mp3 ou de imagens).
- A necessidade de detecção de vírus não justifica, só por si, a leitura dos e-mails recebidos.
- À constatação da utilização desproporcionada deste meio de comunicação – que será comparada com a natureza e tipo de actividade desenvolvida – deve seguir-se um aviso do trabalhador e, se possível, o controlo através de outros meios alternativos e menos intrusivos.
- Eventuais controlos fundamentados na prevenção ou detecção da divulgação de segredos comerciais deve ser direccionado, exclusivamente, para as pessoas que têm acesso a esses segredos e apenas quando existam fundadas suspeitas.
- Os prazos de conservação dos dados de tráfego devem ser limitados em função de razões relacionadas com a organização da actividade e gestão da correspondência e nunca em razão de quaisquer objectivos de controlo ou organização de perfis comportamentais dos trabalhadores.
- O acesso ao e-mail deverá ser o último recurso a utilizar pela entidade empregadora, sendo desejável que esse acesso seja feito na presença do trabalhador visado e, de preferência, na presença de um representante da comissão de trabalhadores. O acesso deve limitar-se à visualização dos endereços dos destinatários, o assunto, a data e hora do envio, podendo o trabalhador – se for o caso – especificar a existência de alguns e-mails de natureza privada e que não pretende que sejam lidos pela entidade empregadora.

- Perante tal situação a entidade empregadora deve abster-se de consultar o conteúdo do e-mail, em face da oposição do trabalhador.

2. Princípios relativos à Internet

- A entidade empregadora deve assegurar-se que os trabalhadores estão claramente informados e que estão conscientes dos limites estabelecidos em relação à utilização de Internet para fins privados e que conhecem as formas de controlo que podem ser adoptadas.
- Deve ser admitido um certo grau de tolerância em relação ao acesso para fins privados, nomeadamente se este decorrer fora do horário de trabalho.
- Qualquer decisão sobre a realização de controlo deve ser criteriosa, evitando-se que os benefícios que a entidade empregadora pretende obter sejam desproporcionados em relação ao grau de lesão que vai ser causada à privacidade e à autonomia dos empregados.
- Devem ser consideradas as vantagens – quer para a empresa quer para os trabalhadores – que o acesso à Internet traz para o desenvolvimento da capacidade de investigação, autonomia e iniciativa do trabalhador, aspectos que podem ser capitalizados em benefício da empresa.
- A entidade empregadora não deve fazer um controlo permanente e sistemático do acesso à Internet. O controlo dos acessos à Internet – a ser decidido – deve ser feito de forma não individualizada, e global, em relação a todos os acessos na empresa, com referência ao tempo de conexão na empresa.
- A realização de estudos estatísticos pode ser suficiente para a entidade empregadora se poder aperceber do grau de utilização da Internet no local de trabalho e em que medida o acesso compromete a dedicação às tarefas profissionais ou a produtividade. Admite-se que seja feito um tratamento dos sítios mais consultados na empresa, sem identificação dos postos de trabalho.
- Se estiverem em causa razões de custos ou de produtividade, o controlo do trabalhador deve ser feito, num primeiro momento, através da contabilização do tempo médio de conexão, independentemente dos sítios consultados. Perante a

verificação de acessos excessivos e desproporcionados deste meio de comunicação deve seguir-se um aviso do trabalhador em relação ao grau de utilização.

- O controlo em relação ao tempo de acesso diário e aos sítios consultados por cada trabalhador só deverá ser realizado em circunstâncias excepcionais, nomeadamente quando, no contexto da sua advertência, o trabalhador duvidar das indicações da empresa e quiser conferir a realização de tais acessos.
- Em particular, poderá ser necessário verificar as horas de conexão (início e fim) para comprovar que o acesso para fins privados ocorreu fora do horário de trabalho.

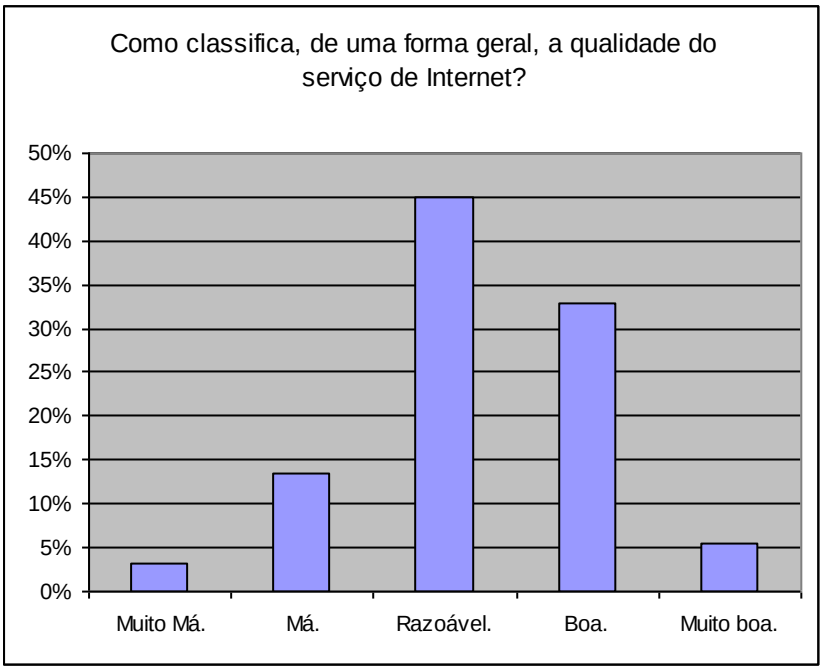
3. Procedimentos a adoptar pelas entidades empregadoras

- O grau de utilização dos meios da empresa para fins privados, a delimitação das condições de tratamento e a especificação das formas de controlo adoptadas devem constar de Regulamento Interno o qual, nos termos legais, deverá ser submetido a parecer da Comissão de Trabalhadores e aprovado pelo IDICT.
- A entidade empregadora deve publicitar o conteúdo dos regulamentos internos, designadamente afixando-os na sua sede e nos locais de trabalho, de modo que os trabalhadores possam deles tomar conhecimento.
- Os responsáveis pelo tratamento de dados pessoais devem fazer a respectiva notificação junto da CNPD (artigo 27.º da Lei 67/98), a qual será formulada em impresso próprio (disponível em http://www.cnpd.pt).
- Com a notificação à CNPD as entidades responsáveis devem juntar o Regulamento Interno e especificar as formas como publicitaram as condições de tratamento de dados junto dos trabalhadores.

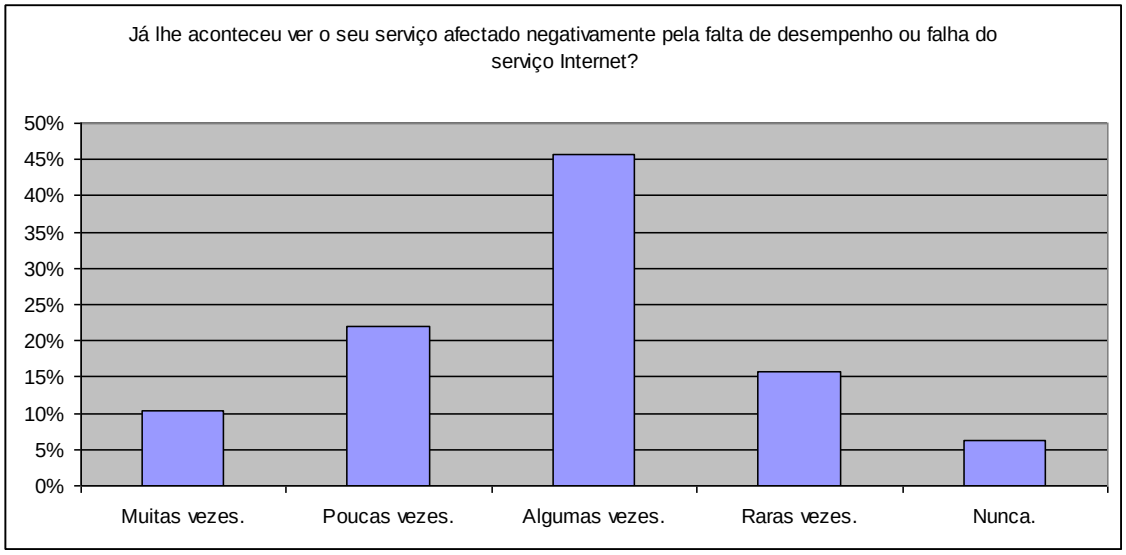
Anexo C - Inquérito realizado na FA

Inquérito realizado a 649 Utilizadores de Internet na FA, em Janeiro de 2010, através da Internet.

Qualidade do serviço

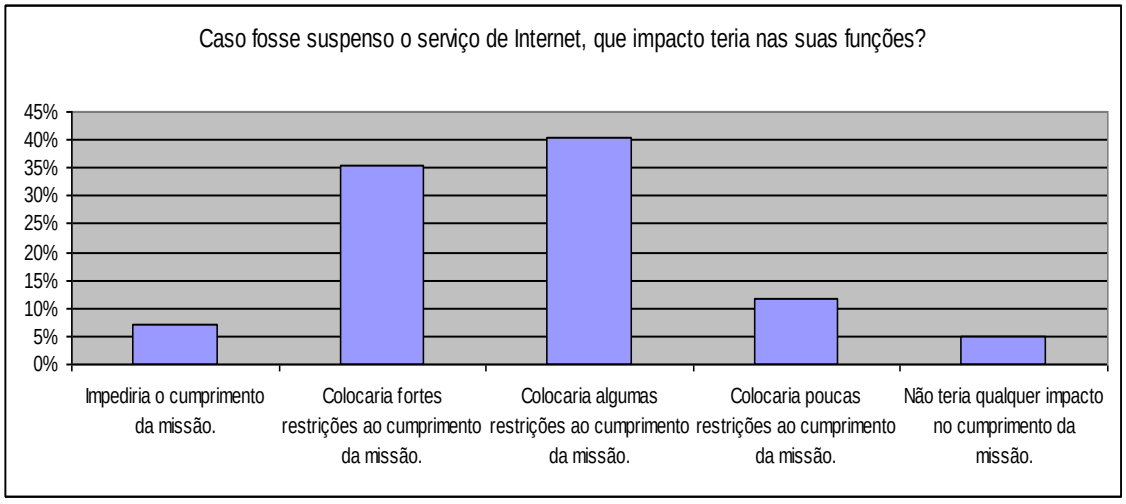


Pergunta 1

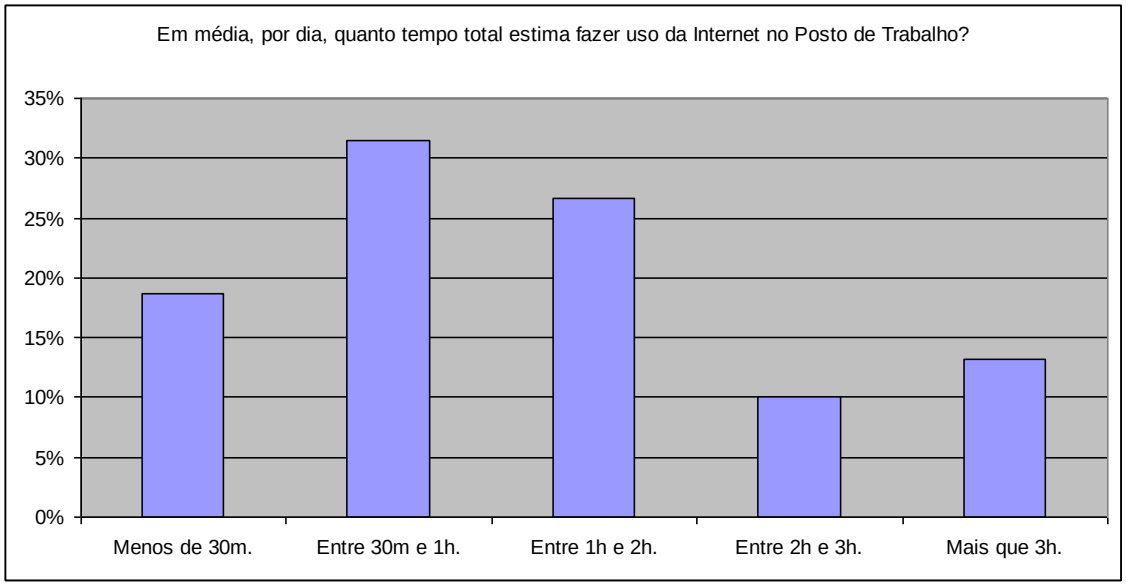


Pergunta 2

Importância do Serviço

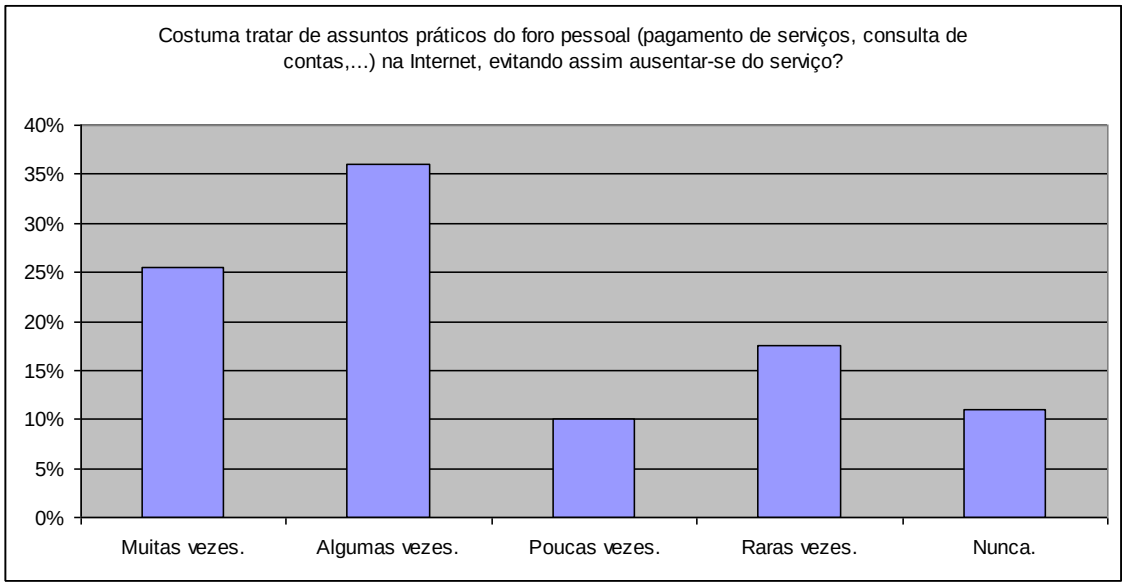


Pergunta 3

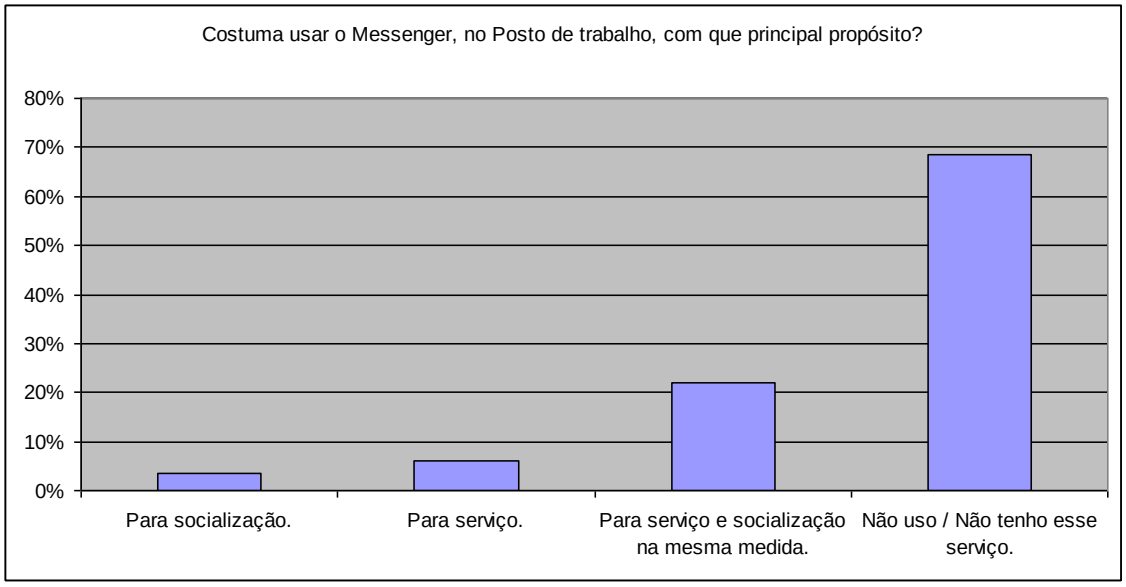


Pergunta 2

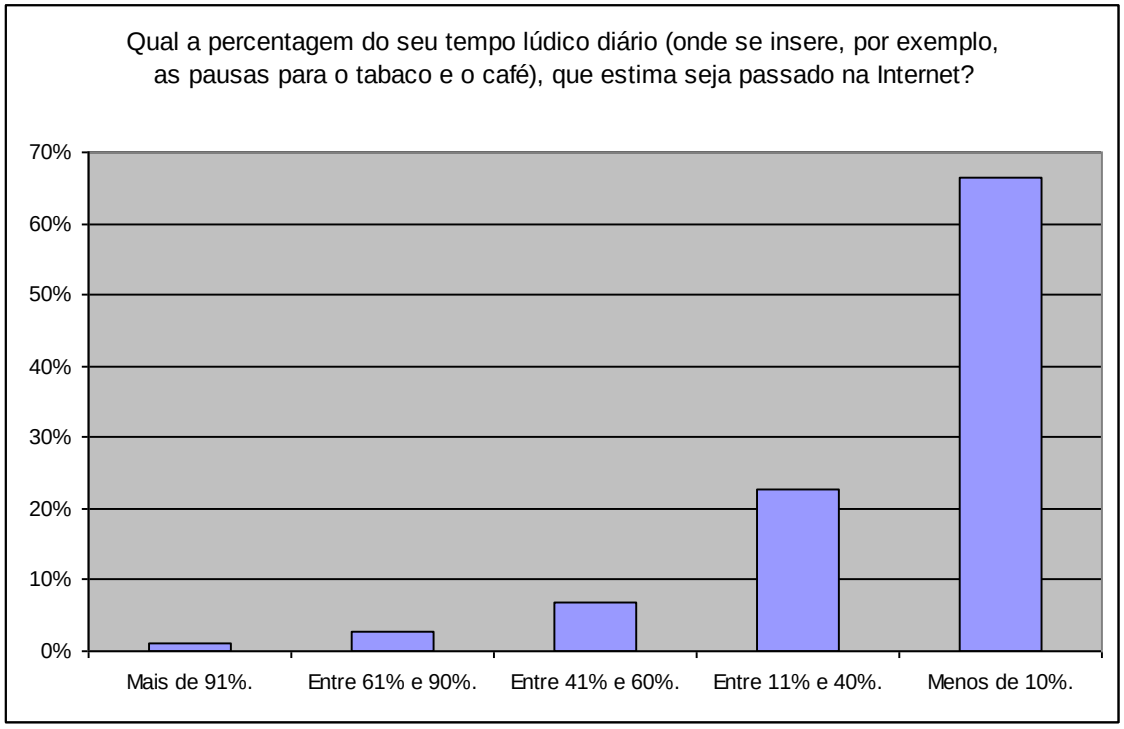
Tipologia da utilização



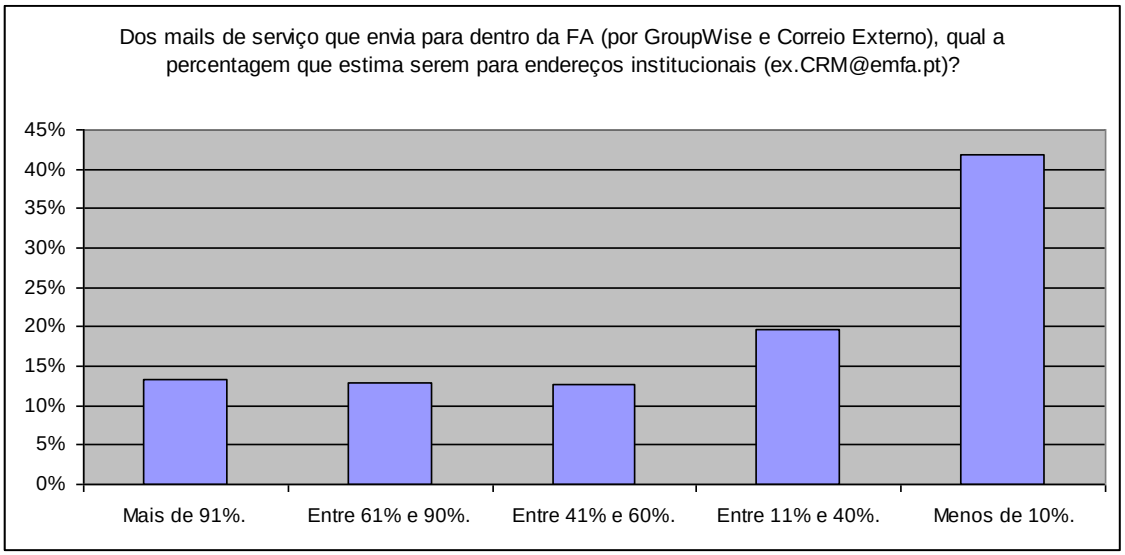
Pergunta 3



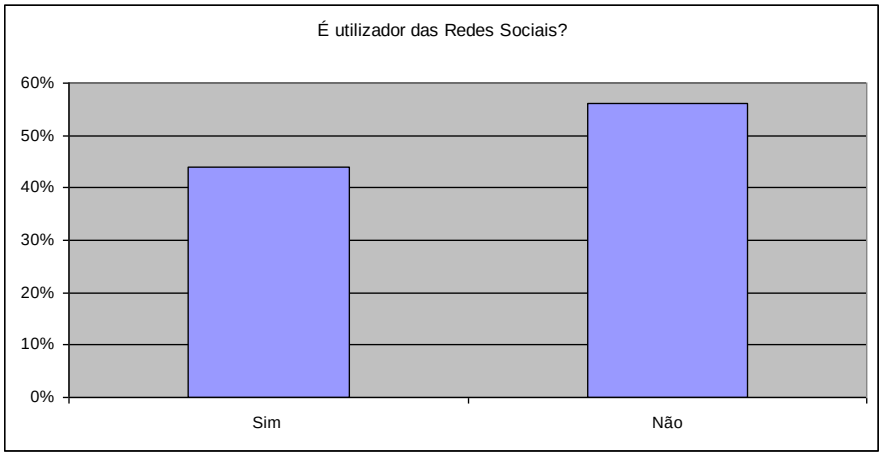
Pergunta 4



Pergunta 7

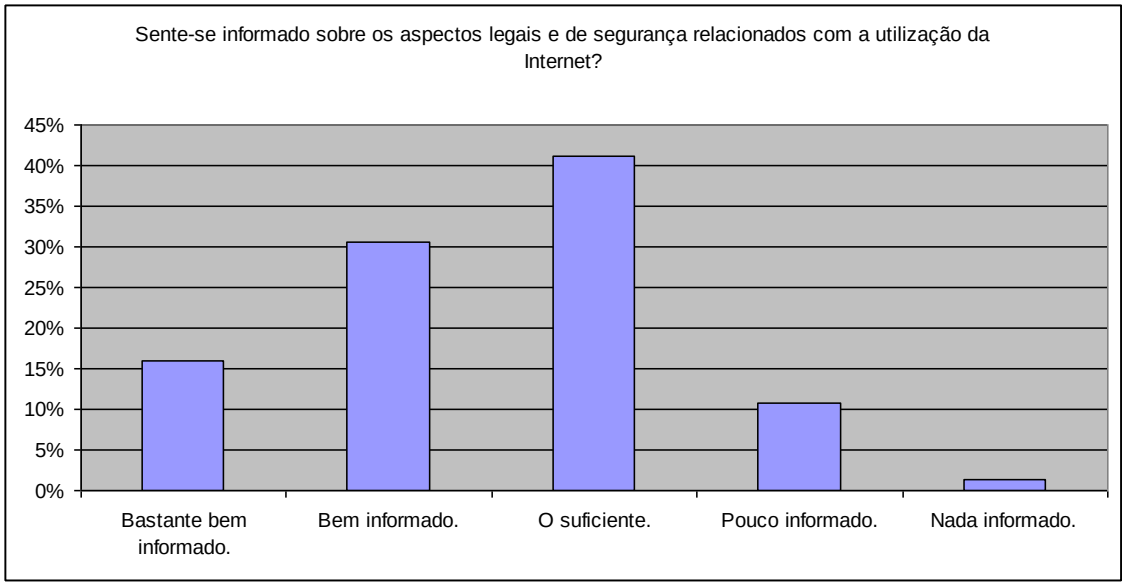


Pergunta 8

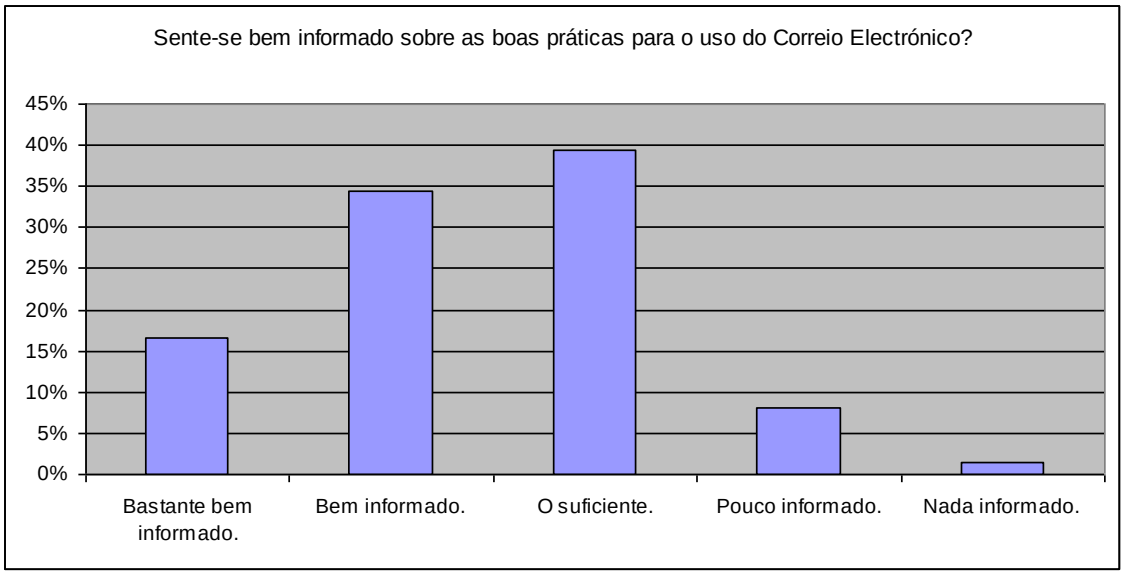


Pergunta 9

Aceitabilidade de acções de formação / sensibilização

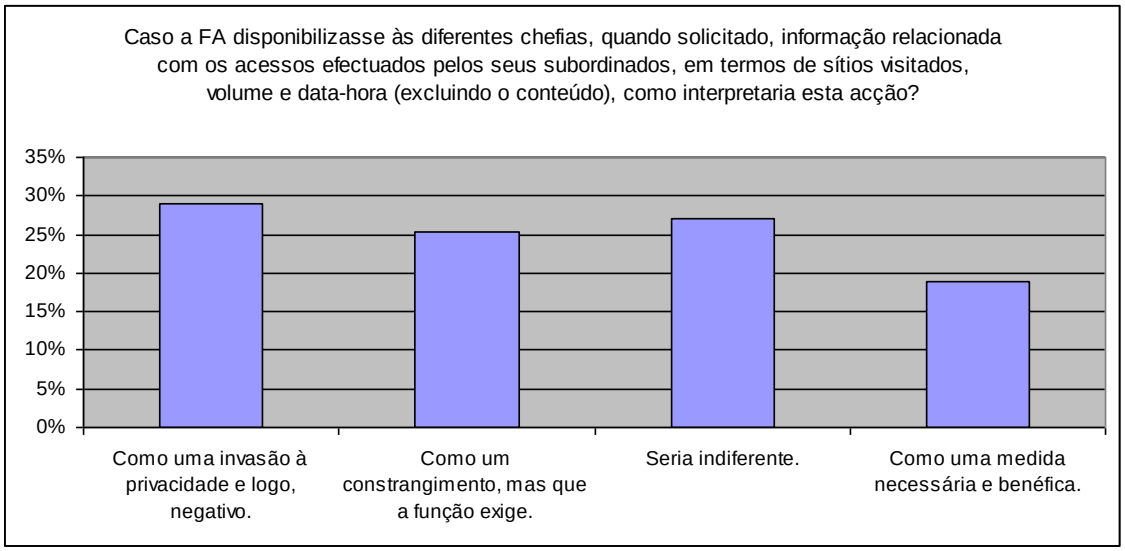


Pergunta 10



Pergunta 11

Aceitabilidade de Medidas de Controlo dos acessos


Caso a FA disponibilizasse às diferentes chefias, quando solicitado, informação relacionada com os acessos efectuados pelos seus subordinados, em termos de sítios visitados, volume e data-hora (excluindo o conteúdo), como interpretaria esta acção?
35%
30%
25%
20%
15%
10%
5%
0%
Como uma invasão à privacidade e logo, negativo.
Como um constrangimento, mas que a função exige.
Seria indiferente.
Como uma medida necessária e benéfica.

Pergunta 12

Anexo D - Top 10 Sites mais visitados na FA

IM/P2P application and Web filtering protection

View selection

Protocol	Value format	Period
HTTP	Percentage	Last 24 hours

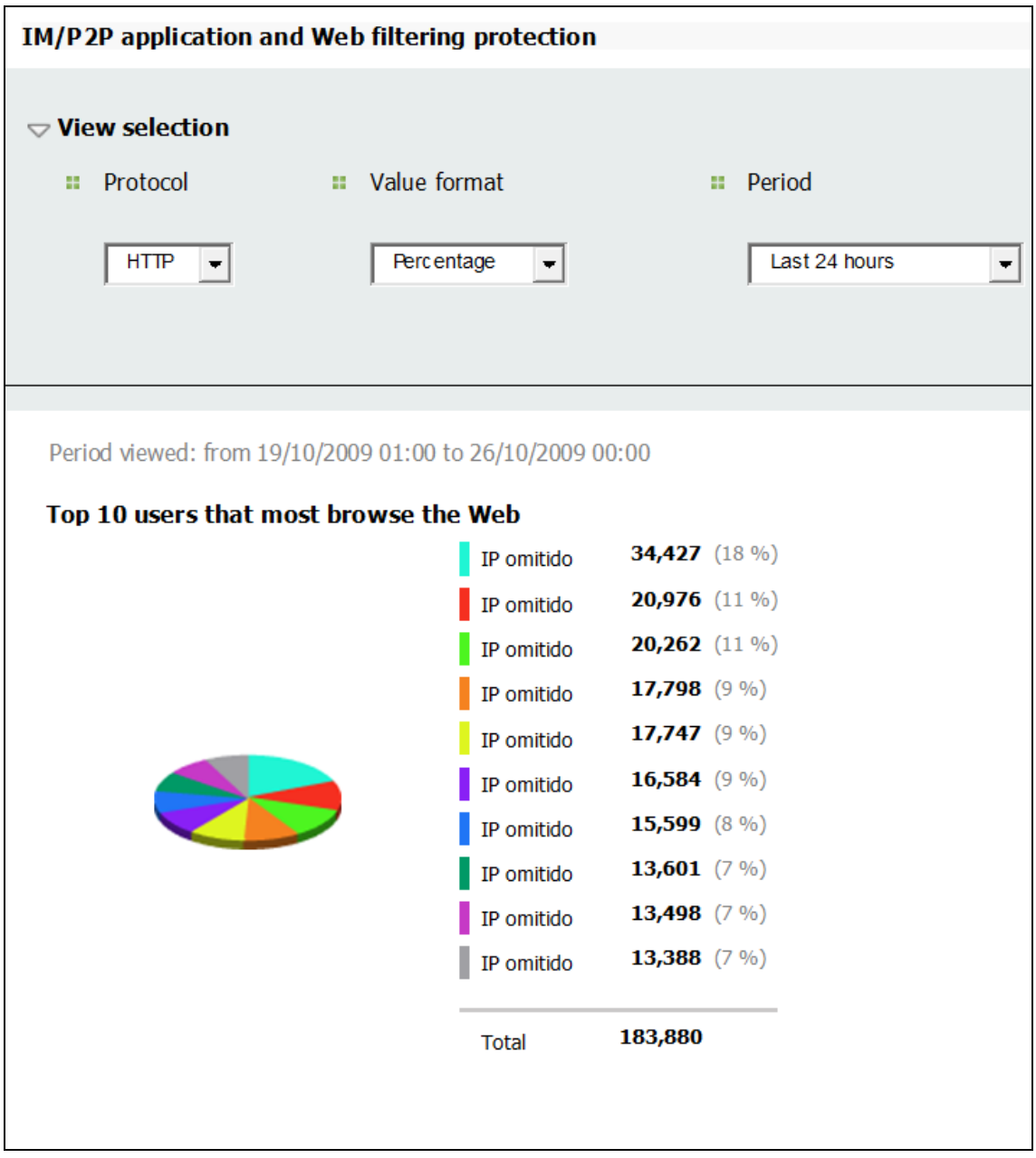
Period viewed: from 19/10/2009 01:00 to 26/10/2009 00:00

Top 10 most visited domains

mail.google.com (White list)	**18,615**	(23 %)
b.mail.google.com (White list)	**16,284**	(20 %)
www.google-analytics.com (Software / Hardware)	**9,265**	(11 %)
ads.sapo.pt (Search Engines / Web Catalogues / Portals)	**7,483**	(9 %)
active.imediata.pt (No categorized)	**7,382**	(9 %)
http://mwfb.static.zynga.com/mwfb/graphics/spac... (Computer Games)	**6,153**	(7 %)
www.hi5.com (Social Media)	**4,492**	(5 %)
logon2.clubenet.com (No categorized)	**4,049**	(5 %)
www.google.com (Search Engines / Web Catalogues / Portals)	**3,168**	(3 %)
www.google.pt (Search Engines / Web Catalogues / Portals)	**2,696**	(3 %)
Total	**79,587**	

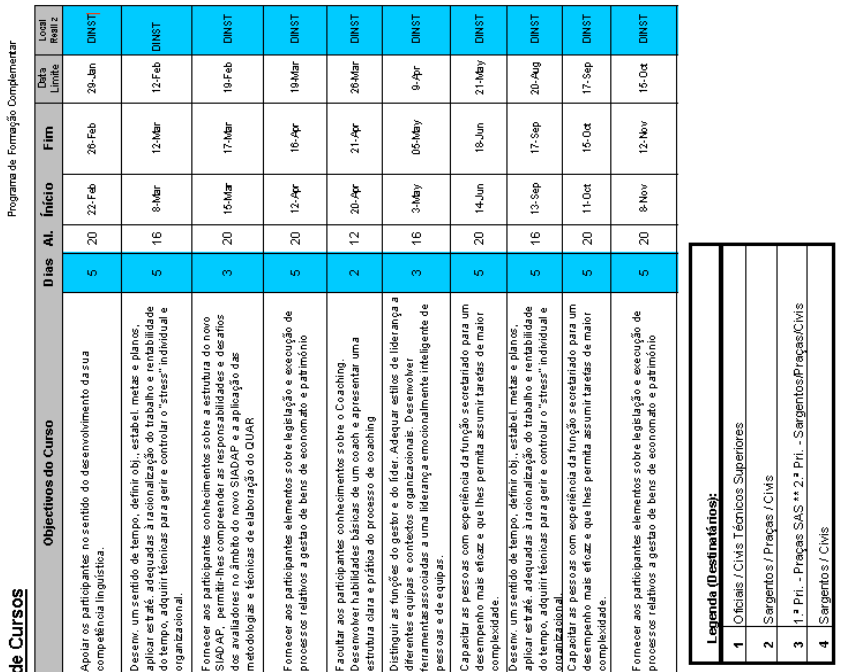
Dados fornecidos pela DCSI, correspondendo os dados a um registo verificado num período de 24 Horas, entre o dia 25 e 26 de Outubro de 2009.

Anexo E - Top 10 Utilizadores



Dados fornecidos pela DCSI, correspondendo os dados a um registo verificado num período de 24 Horas, entre o dia 25 e 26 de Outubro de 2009.

Anexo F -Lista Cursos DINST 2010



FAP - CIFFA/DINST / 2.ª REP

PFC 2010 - Planeamento de Cursos

Programa de Formação Complementar

N.º	Curso	Formador	Dest.	Objectivos do Curso	Dias	Al.	Início	Fim	Data Limite	Local Realiz
1	COMUNICAÇÃO ORAL E ESCRITA 01/10	Dr.ª Fernanda Vilas	2	Apoiar os participantes no sentido do desenvolvimento da sua competência linguística.	5	20	22-Feb	26-Feb	29-Jan	DINST
2	GESTÃO DO TEMPO 01/10	Dr.ª Inês Lourenço	3	Desenv. um sentido de tempo, definir obj., estabel. metas e planos; aplicar estratég. adequadas à racionalização do trabalho e rentabilidade do tempo, adquirir técnicas para gerir e controlar o "stress" individual e organizacional.	5	16	8-Mar	12-Mar	12-Feb	DINST
3	SIADAP P/ DIRIGENTES	Dr. Manuel Afonso Diniz	1	Fornecer aos participantes conhecimentos sobre a estrutura do novo SIADAP, permitir-lhes compreender as responsabilidades e desafios dos avaliadores no âmbito do novo SIADAP e a aplicação das metodologias e técnicas de elaboração do QUAR	3	20	15-Mar	17-Mar	19-Feb	DINST
4	ECONOMATO E PATRIMÓNIO 01/10	Eng. Silva Santos	3	Fornecer aos participantes elementos sobre legislação e execução de processos relativos a gestão de bens de economato e património	5	20	12-Apr	16-Apr	19-Mar	DINST
5	TÉCNICAS DE LIDERANÇA - COACHING 01/10	Dr. Eduardo Torgal(BE COACH)	1	Facultar aos participantes conhecimentos sobre o Coaching. Desenvolver habilidades básicas de um coach e apresentar uma estrutura clara e prática do processo de coaching	2	12	20-Apr	21-Apr	26-Mar	DINST
6	LIDERAR C INTELIGÊNCIA EMOCIONAL	Dr.ª. Teresa Oliveira	1	Distinguir as funções do gestor e do líder. Adequar estilos de liderança a diferentes equipas e contextos organizacionais. Desenvolver ferramentas associadas a uma liderança emocionalmente inteligente de pessoas e de equipas.	3	16	3-May	05-May	9-Apr	DINST
7	SECRETARIADO AVANÇADO 01/10	Dr.ª Carmen Almeida	3	Capacitar as pessoas com experiência da função secretariado para um desempenho mais eficaz e que lhes permita assumir tarefas de maior complexidade.	5	20	14-Jun	18-Jun	21-May	DINST
8	GESTÃO DO TEMPO 02/10	Dr.ª Inês Lourenço	3	Desenv. um sentido de tempo, definir obj., estabel. metas e planos; aplicar estratég. adequadas à racionalização do trabalho e rentabilidade do tempo, adquirir técnicas para gerir e controlar o "stress" individual e organizacional.	5	16	13-Sep	17-Sep	20-Aug	DINST
9	SECRETARIADO AVANÇADO 02/09	Dr.ª Carmen Almeida	3	Capacitar as pessoas com experiência da função secretariado para um desempenho mais eficaz e que lhes permita assumir tarefas de maior complexidade.	5	20	11-Oct	15-Oct	17-Sep	DINST
10	ECONOMATO E PATRIMÓNIO 02/10	Eng. Silva Santos	3	Fornecer aos participantes elementos sobre legislação e execução de processos relativos a gestão de bens de economato e património	5	20	8-Nov	12-Nov	15-Oct	DINST

Legenda (Destinatários):	
1	Oficiais / Civis Técnicos Superiores
2	Sargentos / Praças / Civis
3	1.º Pri. - Praças SAS ** 2.º Pri. - Sargentos/Praças/Civis
4	Sargentos / Civis

Lista retirada do Portal Interno da FA.

Apêndice A

Normas provisórias para a utilização do CE interno da FAP e da Internet no âmbito das redes locais de unidade

NORMAS PROVISÓRIAS
PARA A UTILIZAÇÃO DO CORREIO ELECTRÓNICO INTERNO DA FAP E DA INTERNET
NO ÂMBITO DAS REDES LOCAIS DE UNIDADE

ÍNDICE

OBJECTIVO

- O presente documento apresenta um enquadramento normativo provisório para a exploração das facilidades de Correio Electrónico Interno na FAP, dentro e entre as Unidades ou Órgãos que dispõem de Redes Internas, bem como do acesso à rede mundial conhecida como INTERNET, incluindo as respectivas facilidades de Correio Electrónico internacional, de âmbito externo à FAP. Visa-se estabelecer princípios básicos para o comportamento dos respectivos utilizadores destes produtos, fixando-se também a responsabilidade pela atribuição e cancelamento do direito individual ao seu uso.


Visto. Distribuir às Unidades e Órgãos dotados de redes informáticas internas interligadas à RIALFA
Em 05 / 10 / 1998
O Chefe do Estado-Maior da Força Aérea
Manuel José Alvarenga de Sousa Santos
GENQE

- O carácter provisório deste documento justifica-se pela novidade do uso destes produtos a nível alargado da Força Aérea, sendo prudente a aquisição de alguma experiência antes de cristalizar as normas definitivas em documento do tipo RFA.

TOPO DA PÁGINA

DEFINIÇÕES

- Neste documento são referidos alguns conceitos que em seguida se caracterizam :
    - **Correio Electrónico Interno da FAP (CEI)** . Facilidade de comunicação escrita interpessoal de carácter informal e não classificada, com âmbito interno à FAP, que utiliza um suporte lógico comercial sobre uma infra-estrutura de redes internas das Unidades / Órgãos da FAP, interligadas entre si .

Cada utilizador desta facilidade possuirá um endereço próprio, único na FAP.

- **INTERNET (WWW**) .Facilidade de acesso à rede mundial de informação World Wide Web (WWW) a partir de um posto de trabalho de uma rede interna de Unidade / Órgão, usando o canal alugado existente em Alfragide. Esta facilidade inclui a consulta (visualização no écran) de informação existente em todo o Mundo, a importação de ficheiros de dados e , normalmente (mas não obrigatoriamente) um serviço de Correio Electrónico mundial. Este objectivo é conseguido instalando um suporte lógico especial no posto de trabalho, designado por "Browser" ou "Navegador" (equivalente em Português).
- **Correio Electrónico INTERNET**. Facilidade de comunicação escrita interpessoal de carácter informal e não classificada, de âmbito exterior à FAP, e à escala mundial, que utiliza a ligação à INTERNET. Essa comunicação funciona nos dois sentidos, sendo fornecido um endereço pessoal de correio INTERNET, único no Mundo, a cada utilizador autorizado. Este endereço é diferente do utilizado no Correio Electrónico Interno.
  Embora tal seja possível, a comunicação entre pessoal da FAP não deve fazer-se por esta via mas sim pela do Correio Electrónico Interno.

TOPO DA PÁGINA

ÂMBITO E FINALIDADE DO CORREIO ELECTRÓNICO INTERNO DA FAP (CEI)

- O correio electrónico interno da FAP (CEI) abrange todas as Unidades dotadas com Rede Local nos postos de trabalho onde esta funcionalidade esteja implementada.

- A finalidade deste meio de comunicação é a de fomentar as relações de serviço de carácter informal e com conteúdos sem classificação de segurança. Contudo, é possível incluir as mensagens do Correio Electrónico interno no sistema de controlo e arquivo de correspondência em uso na Unidade/Órgão, desde que se imprima uma cópia da mensagem enviada ou recebida, tratando então essa cópia como qualquer outro documento.

- A pertinência de um correio electrónico deste tipo será reanalisada quando for implementado o novo Sistema de Mensagens Militares (MMHS) em estudo na FAP.

TOPO DA PÁGINA

DISCIPLINA DE UTILIZAÇÃO DO CEI

- A lista de endereços é geral na FAP, tendo em conta o ponto 4., sendo possível a qualquer utilizador enviar uma mensagem para qualquer um dos endereços constantes dessa lista. Esta característica não é tecnicamente modificável, com os suportes lógicos disponíveis. Contudo, todas as mensagens identificam claramente o seu autor.

- A decisão de enviar uma mensagem por esta via para um qualquer destinatário, dentro ou fora da mesma Unidade, é uma questão de bom senso e espírito de disciplina, não sendo ética e disciplinarmente admissível o acesso por esta via a Entidades com as quais não haja normalmente contacto directo, ou cujo contacto directo implique uma quebra das normas de relacionamento institucional.

- O correio electrónico deve funcionar como uma alternativa ao formalismo e demora na comunicação escrita normal, mas não como uma via de anarquizar e destruir os canais normais de informação e comando.

- Embora sejam admissíveis mensagens com um conteúdo pessoal não directamente relacionado com assuntos de serviço, tal só deve acontecer em grau moderado e na medida em que essas relações interpessoais favoreçam a coesão e a eficácia de grupo.

- No conteúdo das mensagens e dos respectivos anexos não é admissível o uso de formas de expressão menos correctas ou educadas.

- Para que o CEI tenha credibilidade e constitua de facto uma ferramenta de produtividade de grupo é indispensável que os seus utilizadores adquiram o hábito de ligar os seus equipamentos logo que chegam ao seu posto de trabalho e verifiquem a sua Caixa de Correio, respondendo atempadamente a toda a correspondência recebida e verificando, para a correspondência expedida, se os seus destinatários já a abriram e leram.

- Anexam-se às presentes normas (Anexo A) indicações auxiliares para a localização dos endereços do CEI na FAP.

TOPO DA PÁGINA

SEGURANÇA NO USO DO CEI

- Embora as mensagens do CEI não sejam encriptadas, nenhum utilizador tem acesso à caixa de correio de um outro (incluindo o pessoal técnico de informática responsável pelo sistema), a menos que o faça fraudulentamente, utilizando a identificação pessoal (User_ID) e a palavra-chave (Password) de acesso à rede dessa outra pessoa.

  Para além desse primeiro nível de protecção de uma caixa de correio individual (User_ID e Password de acesso à rede), cada utilizador pode usar uma outra palavra-chave específica para a sua caixa de correio.

TOPO DA PÁGINA

CRITÉRIOS E COMPETÊNCIA DE ATRIBUIÇÃO DAS FACILIDADES DE CEI

- Como norma tendencialmente comum a toda a Força Aérea, deve ser autorizado o acesso ao Correio Electrónico interno da FAP a todo o pessoal, militar ou civil detentor de uma função de chefia ou comando, ou que, por qualquer outro motivo, represente uma vantagem funcional para a Unidade/Órgão , desde que disponha de um posto de trabalho ligado à rede interna.

- A decisão de conferir e/ou retirar o acesso a esta funcionalidade a cada militar ou civil em serviço numa determinada Unidade ou Órgão cabe em ultima instância ao respectivo Comandante, Director ou Chefe, sendo executada através do pessoal técnico do Centro de Informática da respectiva Unidade/Órgão.

TOPO DA PÁGINA

O ACESSO À INTERNET (incluindo Correio Electrónico Externo à FAP)

- O acesso à funcionalidade designada por INTERNET abrange a consulta a todos os elementos existentes a nível mundial, a importação de ficheiros e, habitualmente, o envio e recepção de mensagens de correio electrónico de âmbito geográfico mundial.

- O acesso à INTERNET existente nos postos de trabalho ligados a uma Rede Local de Unidade/Órgão processa-se através de um canal de acesso alugado a uma firma fornecedora deste serviço e de um dispositivo de segurança (Firewall), ambos existentes na DINFA, em Alfragide, visando impedir o acesso não autorizado, proveniente do exterior, a dados existentes a nível interno da FAP, quer a nível central quer a nível local.

- Dado que o canal de acesso à INTERNET está defendido por um "Firewall", a utilização da INTERNET a nível da Unidade / Órgão processa-se de uma forma segura contra acessos exteriores.

TOPO DA PÁGINA

CRITÉRIOS E COMPETÊNCIA DE ATRIBUIÇÃO DO ACESSO À INTERNET

- O acesso à INTERNET (bem como ao serviço de Correio Electrónico Exterior) deve ser mais restringido do que o do Correio Electrónico Interno da FAP, pelas características desta funcionalidade que implica, para além de outros aspectos, um aumento significativo do fluxo de dados nas redes e exige um grande auto controlo e disciplina de utilização. Assim, o acesso deve ser autorizado apenas até ao nível funcional a que corresponde o posto de Major, ou em outros casos a título excepcional.

- Compete igualmente ao Comando de Unidade/Órgão a decisão de atribuir ou retirar o acesso a esta funcionalidade, de acordo com o critério estabelecido no ponto anterior. A execução prática desta medida deve ser solicitada à DINFA, uma vez que tal só é possível a nível central.

- Em casos onde se verifiquem motivos técnicos que impeçam novos acessos ou aconselhem maiores restrições, a DINFA informará do facto o Comando da Unidade/Órgão respectivo, aconselhando as medidas adequadas.

TOPO DA PÁGINA

DISCIPLINA DE UTILIZAÇÃO DO ACESSO À INTERNET e DO CORREIO EXTERIOR

- São aplicáveis aos acessos INTERNET e ao uso do respectivo Correio as normas anteriores , nas partes onde tal seja possível e designadamente quanto ao conteúdo das mensagens de correio e à escolha das entidades destinatárias.

- Não é admissível a utilização desta funcionalidade (INTERNET) para fins de diversão ou outros de natureza estritamente pessoal por forma que represente prejuízo sensível para o serviço.

- É vedado a qualquer utilizador expedir qualquer mensagem para o exterior em nome oficial da sua Unidade / Órgão / Subunidade ou da Força Aérea Portuguesa, a menos que esteja devidamente autorizado para tal, ao nível hierárquico competente.

TOPO DA PÁGINA

SEGURANÇA NO USO DO CORREIO EXTERIOR INTERNET

- A caixa do correio exterior INTERNET de cada utilizador apenas pode ser lida pelo próprio, estando protegida em primeira instância pelo acesso à rede (está ligada à identificação pessoal de cada utilizador - User_ID - e à respectiva palavra-chave) e , adicionalmente, por uma palavra-chave específica deste correio INTERNET .
  Existe uma opção (No Netscape , em Options / News and Mail Preferences / Remember Password) que permite que a palavra-chave específica do correio INTERNET não seja solicitada quando se abre o Correio ; esta opção é desaconselhada se pretender um nível de segurança superior ao que é dado pela Identificação Pessoal + Palavra-Chave do acesso à rede.

TOPO DA PÁGINA

ENDEREÇOS INSTITUCIONAIS DA UNIDADE / ORGÃO ou SUBUNIDADE

- É possível, e aconselha-se fortemente, o uso de endereços institucionais para a Unidade, Órgão ou Subunidade, que passam a representar não uma pessoa mas uma organização, e que podem ser utilizados por mais que uma pessoa, em nome dessa organização, possuindo para tal uma chave secreta de acesso.
  Esses endereços são úteis para efeitos de ligações institucionais, com mais algum formalismo e controlo, sendo exemplo o endereço das Relações Públicas da FAP : relpublic@emfa.pt

  Estes endereços, à semelhança dos restantes, devem ser solicitados à DINFA.

ALFRAGIDE, 01 de OUTUBRO de 1998

O Director

Vitor Manuel Graça Cunha

Brig ENGAED

TOPO DA PÁGINA

ANEXO A — Sugestões para facilitar a consulta do address book do groupwise 5.2

Para facilidade na consulta da Lista de Endereços siga os seguintes procedimentos (consulte a figura 1, abaixo):

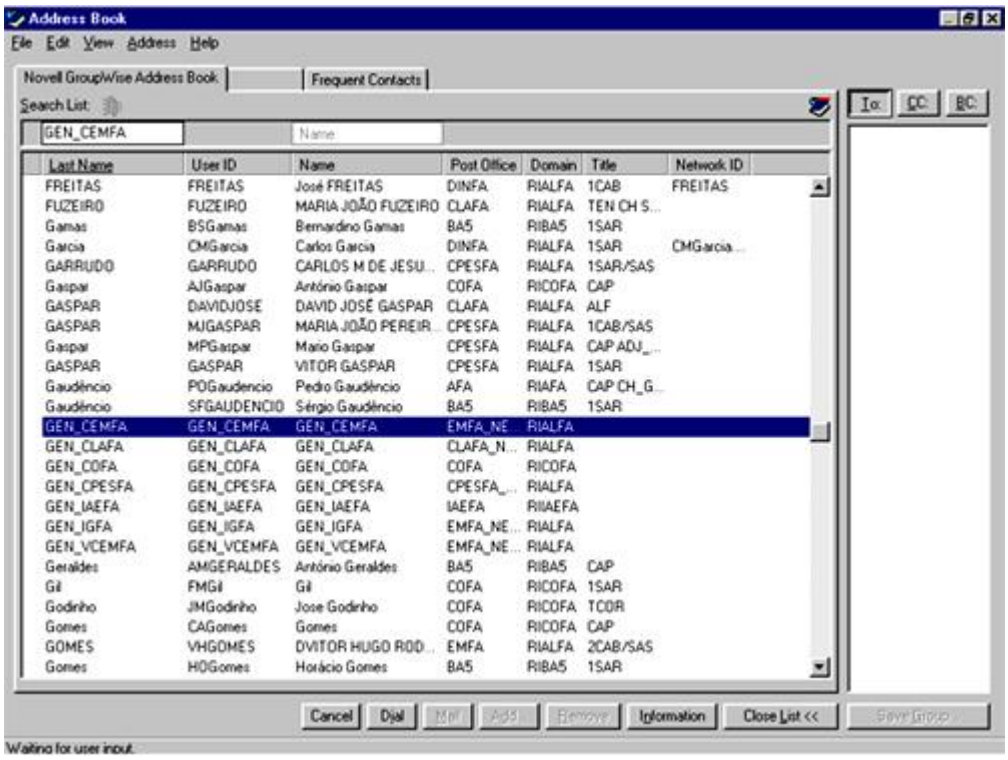


Figura 1 - Organização recomendada para o Address Book do E-Mail (Groupwise versão 5.2)

- Organize a sua Lista de Endereços (Adress Book) de forma a incluir, pelo menos, os seguintes items (em inglês) e atente sempre no seu conteúdo em caso de ambiguidade na identificação dos endereços:

    - **LastName** — indica-lhe o apelido do utilizador com acesso a este Correio
    - **PostOffice** — indica-lhe a Unidade/Órgão (EMFA , CLAFA , BA5 , etc...)
    - **Department** — indica-lhe a Subunidade (DMA , GO , etc...)
    - **Title** — indica-lhe o Posto e Função (TCOR CMD GA ...)

- No que respeita ao "LastName", existem alguns casos especiais, surgindo a função institucional em vez do apelido, designadamente:

    - Generais — começam por GEN (GEN_CEMFA, GEN_CPESFA, etc)
    - Brigadeiros — começam por BRIG (BRIG_DMA, BRIG_GABCEMFA, etc)
    - Chefes de Divisão do EMFA, Chefes de Serviço, Comandantes e 2º Comdt de Unidade, Comandantes de Grupo — começam com a indicação da Unidade / Órgão (BA5_CMDTE , BA5_GO , EMFA_1ªDIV , CLAFA_SA , etc.)

- A pesquisa é facilitada uma vez que este campo é ordenado alfabeticamente, e basta começar a digitar GEN, BRIG ou a Unidade , para se ficar adequadamente situado na lista, pelo menos para um conjunto significativo de Entidades destinatárias.

- Em todo o caso, os diferentes destinatários usados por um determinado utilizador são automaticamente escritos numa lista especial designada "Frequent Contacts" (ver figura seguinte) o que facilitará o envio das mensagens.

 TOPO DA PÁGINA

Apêndice B

Regras de utilização do acesso à internet e ao Correio Electrónico na rede de dados do EMGFA

ESTADO-MAIOR-GENERAL DAS FORÇAS ARMADAS

Divisão de Comunicações e Sistemas de Informação

REGRAS DE UTILIZAÇÃO DO ACESSO À INTERNET e ao CORREIO ELECTRÓNICO NA REDE DE DADOS DO EMGFA

Os utilizadores da rede de dados do EMGFA (incluindo os subdomínios do COA, COM, NPQGOE e Anel de Bruxelas) dispõem de acesso à Internet e de serviços de correio electrónico externo, como suporte às suas actividades profissionais, cuja utilização está sujeita às seguintes regras:

1. ACESSO À INTERNET

1.1. O acesso à Internet destina-se a suportar a actividade profissional, enquadrando-se nesta classificação a exploração com fins de aprendizagem e de desenvolvimento de capacidades pessoais (através da busca de fontes alternativas de informação ou utilização de serviços). É tolerada a sua utilização com fins particulares, por períodos curtos, desde que esta prática não ponha em causa a produtividade do trabalho, devendo a sua utilização ter lugar, preferencialmente, fora das horas normais de serviço.

1.2. Sem aviso prévio, poderão ser bloqueados acessos a sítios cujo conteúdo seja considerado ofensivo, ilegal, ou do âmbito dos caracterizados no parágrafo “Actividades interditas”, etc.

1.3. A participação de carácter profissional em qualquer “forum de discussão”, “newsgroup”, ou a utilização de programas de comunicação tipo “CHAT”, “IRC”, “ICQ”, carece de autorização superior.

1.4. Todos os acessos e ficheiros transferidos são monitorizados em termos de sítios visitados, data-hora, tamanho dos ficheiros transferidos, sendo estes dados distribuídos em formato electrónico a pedido do dirigente de topo de cada organismo utilizador. As cópias de segurança dos ficheiros de monitorização são guardadas por um período de 6 meses.

1.5. Recorda-se que a maioria dos sítios visitados regista todos os acessos, guardando inclusive a identidade electrónica do visitante.

2. CORREIO ELECTRÓNICO

2.1. O sistema de correio electrónico destina-se a suportar a actividade profissional através de mensagens formais e informais. É tolerada a sua

utilização ocasional em mensagens pessoais curtas, desde que esta prática não ponha em causa a produtividade do trabalho, devendo a sua utilização ter lugar, preferencialmente, fora das horas normais de serviço.

2.2. São consideradas mensagens formais as que responsabilizam directamente o organismo expedidor perante terceiros, sendo remetidas a partir do endereço oficial de correio electrónico do organismo em causa, tal como consta no Roteiro da Administração Pública ou no sítio oficial, na Internet.

2.3. São consideradas mensagens informais as que se destinam a agilizar um determinado assunto de serviço, sendo remetidas a partir de qualquer um dos endereços de correio electrónico do organismo em causa, à excepção do endereço oficial. Responsabilizam indirectamente o organismo expedidor perante terceiros, e, como tal, estas mensagens devem ser do conhecimento da estrutura superior hierárquica.

2.4. É da responsabilidade do expedidor obter a confirmação da recepção da mensagem enviada.

2.5. Todo o tráfego de mensagens é monitorizado em termos de remetentes, destinatários, data-hora, assunto, tamanho da mensagem e de ficheiros anexados, sendo estes dados distribuídos em formato electrónico a pedido do dirigente de topo de cada organismo utilizador. As cópias de segurança dos ficheiros de monitorização são guardadas por um período de 6 meses.

2.6. A inspecção dos conteúdos de mensagens pessoais só poderá ter lugar mediante consentimento do utilizador expedidor ou receptor da rede de dados do EMGFA à excepção de solicitação de autoridade competente no âmbito do quadro legal em vigor.

2.7. Sublinha-se que:

2.7.1. Numa mensagem enviada por correio electrónico, sem recurso à assinatura electrónica, não pode ser garantida a sua origem (autenticação), bem como se foi eventualmente alvo de alterações (integridade). A confidencialidade dos dados só é garantida através da utilização de técnicas criptográficas adequadas.

2.7.2. Uma mensagem apagada pelo utilizador pode permanecer *off-line* nos arquivos de segurança do administrador do sistema.

2.7.3. Informação classificada só pode ser enviada através de meios aprovados para cada nível de segurança ou fazendo-se uso de técnicas e procedimentos aprovados para o grau de classificação do documento.

3. ACTIVIDADES INTERDITAS

3.1. É interdita a utilização do sistema de correio electrónico e do acesso à Internet para fins não conformes com o normativo em vigor (designadamente normas, regulamentos, Código Penal e Lei da Criminalidade Informática) ou que se não coadunem com os princípios aceites da moral individual, social e profissional, nomeadamente:

3.1.1. Difundir ou telecarregar conteúdos protegidos pelo direito de autor, nomeadamente software, música ou filmes.

3.1.2. Aceder ou armazenar informações de páginas *hacker/cracker.*

3.1.5. Consultar sítios de carácter erótico ou pornográfico, mesmo que legalmente tolerados.

3.1.3. Exercer actividades com fins lucrativos.

3.1.4. Enviar mensagens pessoais para um conjunto indeterminado de destinatários que as não tenham solicitado, ou com fins de perturbar, hostilizar, difamar e injuriar, ou transmitir pornografia.

3.1.6. Subscrever informação de forma automática não relacionada com o serviço.

4. DEVERES E OBRIGAÇÕES

4.1. É da responsabilidade do Utilizador:

4.1.1. O conteúdo da sua caixa de correio electrónico bem como a sua gestão.

4.1.2. Manter no acesso à Internet e na utilização dos serviços de correio electrónico externo os padrões de comportamento exigíveis no local de trabalho.

4.2. É da responsabilidade do órgão de gestão da rede de dados:

4.2.1. Divulgar *on-line* normas técnicas detalhadas de aplicação geral, respeitando os princípios consagrados nas presentes regras, por forma a garantir níveis de serviço adequados, designadamente na vertente de *performance* e segurança, no acesso à Internet e utilização dos serviços de correio electrónico externo.

4.2.2. Dar a conhecer estas normas aos novos utilizadores, quando da criação das respectivas contas de acesso à REDEMGFA.

4.2.3. Configurar o *software* de filtragem de acessos à Internet e conteúdos do correio electrónico externo de acordo com as normas técnicas divulgadas.

4.2.4. Produzir relatórios no âmbito do referido nos parágrafos 1.4 e 2.5, salvaguardar o conteúdo das mensagens enquadradas no disposto no parágrafo 2.6 e notificar a Comissão Nacional de Protecção de Dados nos termos da legislação em vigor.

4.2.5. Salvaguardar a privacidade das mensagens pessoais existentes no sistema ou em arquivos de segurança do EMGFA.

5. DIVERSOS

5.1. O não cumprimento deste regulamento por parte dos utilizadores da rede de dados do EMGFA poderá ser objecto, sem aviso prévio, de imediata restrição à sua utilização e, eventualmente, à elaboração de procedimento disciplinar. Este facto não impede eventual responsabilidade civil ou criminal.

5.2 Os utilizadores da rede de dados do EMGFA tomarão conhecimento de forma explícita destas regras.

5.3. As presentes regras serão objecto de reavaliação sempre que necessário, tendo por base os contributos dos utilizadores, transmitidos pela via hierárquica.

EMGFA, 07 de Julho de 2008

O CHEFE DA DIVISÃO

Edorindo dos Santos Ferreira

Major-General