

Estudo da percepção dos utilizadores em relação à utilização de tecnologias de autenticação biométrica no acesso aos serviços de saúde

CAPSI'2011

Paulo Rodrigues¹, Henrique Santos²

1) Universidade do Minho, Guimarães, Portugal
paulomrrodrigues@yahoo.com

2) Universidade do Minho, Guimarães, Portugal
hsantos@dsi.uminho.pt

Resumo

Assiste-se a uma massificação do conceito de identidade digital nos dias que correm devido à disseminação das tecnologias de informação. Da perspectiva dos administradores de sistemas, os utilizadores constituem o elo mais fraco da cadeia de segurança. Os utilizadores mostram geralmente preocupação com as questões de segurança e privacidade, mas ao mesmo tempo anseiam por mecanismos de utilização simples que lhes facilite o processo de autorização perante um determinado serviço. As tecnologias de autenticação com recurso à biometria já desempenham um papel preponderante no contexto da segurança de sistemas informáticos. Algumas técnicas são utilizadas em diversos serviços não só para garantir o acesso físico a instalações mas também para proporcionar algum rigor no acesso. Este estudo aborda a percepção dos utilizadores em relação ao uso de tecnologias de autenticação biométrica no acesso aos serviços de saúde. Recorrendo à metodologia quantitativa, são apresentados resultados preliminares resultantes de uma sondagem por questionário. Os resultados apontam para uma tendência de aceitação deste tipo de tecnologias no acesso aos serviços de saúde. Espera-se que os resultados finais deste estudo sirvam para suportar a implementação deste tipo de tecnologias.

Palavras-chave: biometria, segurança, adopção

1. Introdução

A crescente sensação de insegurança na sociedade faz com que os investigadores na área da segurança dos Sistemas de Informação sintam necessidade de implementar meios mais seguros e fáceis de utilizar para gerir o acesso aos serviços que disponibilizam.

A sociedade está por isso, cada vez mais dependente de novas tecnologias de autenticação. O nome ou a presença da pessoa já não satisfazem os requisitos necessários de validação da identidade de um determinado indivíduo [Laux 2007].

Os investigadores na área destas tecnologias afirmam que a necessidade de segurança será ainda mais intensa, o que terá um forte impacto no uso de tecnologias biométricas tornando-as no meio mais popular de identificação e/ou autenticação [Savastano 2008].

Em 2006, foi realizado um estudo pela consultora Vanson Bourne, a pedido da LogicaCMG [LogicaCMG 2006] intitulado “European Identity Security Survey”, que pretendia aferir a predisposição dos cidadãos europeus para o uso da identidade electrónica. Nesse estudo os portugueses são, de entre os sete países europeus abrangidos pela consulta, dos mais receptivos à introdução da biometria no seu dia-a-dia.

Segundo o relatório, a maioria dos portugueses (87%) gostaria de transportar sempre consigo um bilhete de identidade com dados biométricos, com a impressão digital ou uma fotografia da íris, liderando nesta questão o conjunto dos países auscultados.

Atendendo a estes aspectos, torna-se de facto necessário que se aprofundem quais os factores que poderão influenciar a adopção deste novo conceito de identidade, partindo para um estudo mais abrangente e pormenorizado.

O lançamento do cartão do cidadão e do passaporte electrónico, também contribuem para a desmistificação das tecnologias biométricas para que no futuro sejam ainda mais preponderantes no processo de autenticação no acesso a serviços e/ou locais públicos.

Este estudo está enquadrado na 1ª fase de um projecto de doutoramento que tem como objectivo avaliar a viabilidade da utilização de tecnologias biométricas no acesso aos serviços de saúde. Os resultados desta fase pretendem exclusivamente aferir qual a percepção dos utilizadores em relação à utilização deste tipo de tecnologias. A análise dos dados recolhidos permitirá definir grupos de sujeitos dependendo do seu grau de percepção em relação à adopção voluntária deste tipo de tecnologias.

Este artigo está estruturado por forma a contextualizar a utilização das tecnologias de autenticação biométrica e o conceito de identidade digital, expondo de seguida a metodologia utilizada e os resultados obtidos com a sua aplicação. Termina com a análise crítica dos resultados e aborda o que se pretende concretizar na próxima etapa deste estudo.

2. Tecnologias de autenticação biométrica

As características biométricas têm sido utilizadas ao longo da existência do homem como o método mais usual de identificação de indivíduos. Todos os dias utilizamos a voz no diálogo, nas interações presenciais ou não presenciais para reconhecer amigos e familiares, entre outras características como o odor (uma das formas do recém-nascido identificar a mãe), sons, forma de andar, entre outras.

Se entendermos a questão das tecnologias biométricas como o método de identificação que nos vai permitir identificar (dentro de contextos adequados), quem realmente são as pessoas com

quem interagimos dentro de uma comunidade, talvez seja mais fácil o caminho para adopção deste tipo de tecnologias. No caso de pessoas conhecidas, o processo de confiança na sua identidade é criado com o tempo, mas quando não se pode usufruir desse privilégio, seria porventura necessário providenciar algo que garantisse a verdadeira identidade desse(s) indivíduo(s).

Neste campo entrariam as tecnologias de autenticação biométrica, como alternativa mais fiável (mas não infalível) no processo de identificação/verificação de indivíduos, em detrimento dos métodos tradicionais (e.g.: papéis, documentos sem verificação electrónica).

Estas tecnologias são habitualmente classificadas como físicas ou comportamentais. No caso das físicas, o foco são as características do indivíduo, tais como a retina, a íris, a impressão digital, entre outras. No segundo caso, as comportamentais, estão focalizadas nas actividades realizadas por um indivíduo, como por exemplo as assinaturas, a dinâmica de digitação (*keystrokes dynamics*), o reconhecimento de voz, entre outras. Algumas dessas actividades ocorrem de forma voluntária e outras mecanizadas através da sua repetida aplicação[Fairhurst 2003].

A Tabela 1 apresenta uma comparação entre as tecnologias biométricas mais utilizadas [Liu e Silverman 2001].

Características Tecnologia	Facilidade de utilização	Ocorrência de erros	Exactidão	Aceitação utilizador	Nível de segurança exigido	Estabilidade a médio longo prazo
Impressão Digital	Alta	Seca, sujidade, idade	Alta	Média	Alto	Alta
Reconhecimento da face	Média	Idade, óculos, iluminação	Alta	Média	Médio	Média
Leitura de retina	Baixa	Óculos	Muito Alta	Média	Alto	Alta
Leitura da íris	Média	Má qualidade imagem	Muito Alta	Média	Muito Alto	Alta
Reconhecimento de voz	Alta	Ruído, gripes, tempo	Alta	Alta	Médio	Média
Geometria da mão	Alta	Mão aleijada, idade	Alta	Média	Médio	Média
Assinatura	Alta	Mudança na assinatura	Alta	Muito Alta	Médio	Média

Tabela 1 - Comparação de tecnologias biométricas

Existem ainda outras biometrias, alvo de estudo que não sendo neste momento ainda opção às identificadas anteriormente, poderão no futuro, e após estudos de operacionalização serem consideradas uma alternativa, como por exemplo: ADN, odor, batimentos cardíacos, entre

outros. Alguns destes novos métodos são meios eficazes mas ainda impraticáveis (em larga escala), devido ao processo de verificação e aos requisitos associados para manipulação deste tipo de amostras [Rodrigues e Santos 2009].

Convém referir que as biometrias para serem consideradas como habilitadas para avaliação devem obedecer aos seguintes princípios[Yun 2002]; [Prabhakar et al. 2003]; [Zorkadis e Donos 2004]:

- **Universalidade** – todas as pessoas devem ter essa característica, o que na realidade pode não acontecer devido a problemas de saúde, lesões, entre outras.
- **Singularidade** – o elemento biométrico deve distinguir duas pessoas, ou seja, é tida em conta a capacidade de distinção entre duas amostras.
- **Permanência** – a capacidade da biometria se manter inalterável com o passar do tempo. Neste caso a impressão digital, a íris e o ADN são as características que se mantêm praticamente inalteráveis no tempo. No entanto estas duas últimas são mais fiáveis a longo prazo, visto que, as lesões nos dedos são comuns.
- **Mensurabilidade** – a característica biométrica deve ser quantitativamente mensurável e fácil de recolher. Neste caso a leitura da retina e a análise ADN, são consideradas invasivas (apesar de seguras), no entanto a assinatura sendo menos segura é facilmente colectável.
- **Desempenho** – a fiabilidade, a velocidade e os requisitos dos sistemas biométricos, devem ser contempladas para que sejam práticos.
- **Aceitabilidade** – representa o grau de aceitação destes sistemas por parte dos utilizadores, no sentido em que acrescentam valor e facilidade de uso.
- **Protecção** – caracteriza a robustez do sistema e avalia o nível de dificuldade em contornar o sistema utilizando por exemplo impressões digitais falsas.

3. A autenticação biométrica

Dependendo do contexto de aplicação, um sistema de autenticação utiliza os seguintes métodos: identificação e verificação [Prabhakar et al. 2003]; [Bolle et al. 2003].

O processo é muito similar e funciona sob a mesma filosofia, variando apenas no processo de comparação da amostra que se insere no sistema biométrico e a que já está armazenada na base de dados.

Os processos de associação entre um indivíduo e a sua identidade digital [Prabhakar et al. 2003];[Bolle et al. 2003]:

- **Verificação** – a biometria pode apurar com bastante fiabilidade se o João é realmente o João através da comparação da amostra armazenada na base de dados com a amostra fornecida no processo de associação. É um processo de combinação de um-para-um, “*você é quem diz ser?*”
- **Identificação** – o utilizador não precisa confirmar quem é, o sistema procura a amostra recolhida pelo sistema biométrico na base de dados. Quando for encontrada uma combinação, o utilizador é "identificado" como um utilizador registado, ou seja, o sistema encontra quem é. É um processo de combinação de um-para-muitos, “*quem é você?*”

Além destes dois processos de associação, um outro ganha espaço na literatura devido à natureza específica dos sistemas de autenticação biométrica onde é implementado, sendo no entanto muito similar ao processo de verificação [Jain et al. 2006].

- **Rastreio** – este tipo de sistemas comparam amostras no sentido de apurar se um determinado indivíduo pertence a alguma lista de identidades sobre observação (ex. criminosos). Já existem algumas aplicações destas em aeroportos e casinos.

A principal diferença entre a verificação e a identificação reside essencialmente na forma como é feita a procura e comparação das amostras no sistema. A verificação reporta-se à confirmação ou negação de uma alegada identidade de um indivíduo, enquanto a identificação refere-se ao problema de estabelecer a identidade, desconhecida à partida, de um indivíduo [Magalhães e Santos 2003].

No entanto, a identificação é um sistema mais complexo em termos de desenho e implementação, devido ao número de amostras para comparação que poderá ter uma base de dados [Jain et al. 2006].

Componentes de um sistema biométrico

Um sistema biométrico funciona de forma muito simples, reconhece um indivíduo a partir de uma característica física ou comportamental comparando-a com uma amostra armazenada na base de dados do sistema [Prabhakar et al. 2003].

Na Figura 1,2,3 e 4 podemos ver como é feito o processo de registo, verificação e identificação das amostras num sistema biométrico [Prabhakar et al. 2003]; [Jain et al. 2006].

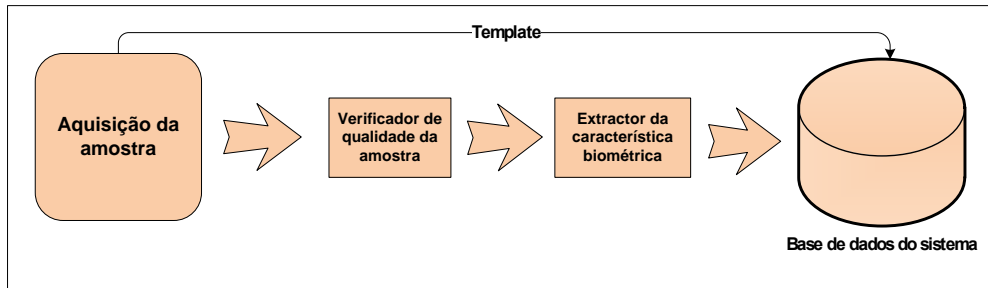


Figura 1- Registo no sistema biométrico

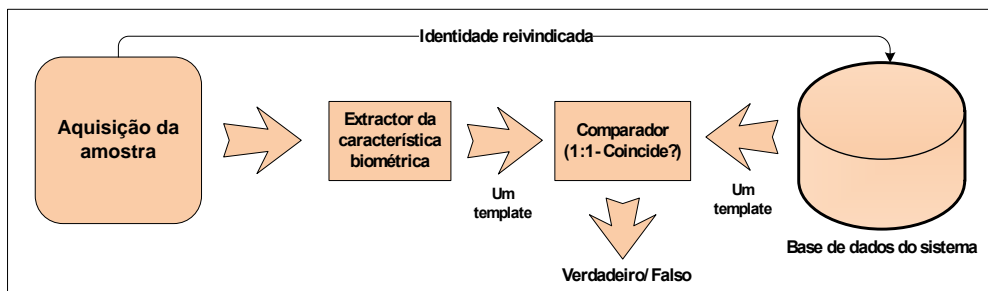


Figura 2 - Verificação

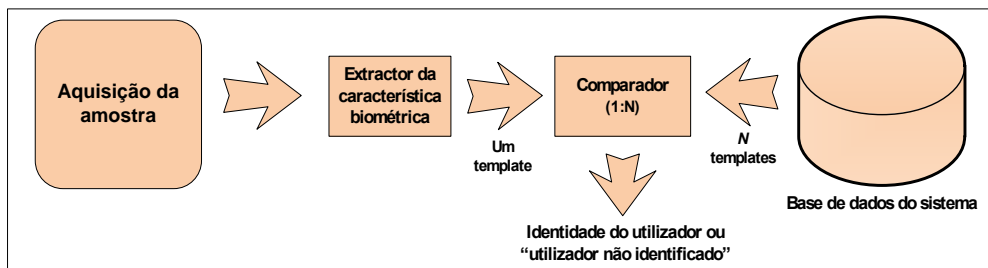


Figura 3 - Identificação

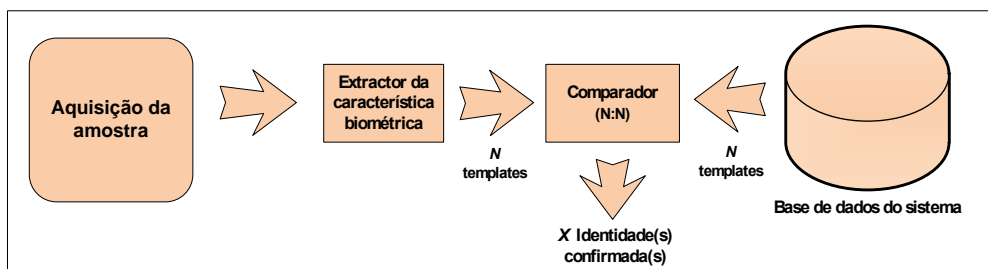


Figura 4 - Rastreio

Taxas de erro

Nos sistemas de verificação biométrica podemos ter dois tipos de erros:

- FAR (False Acceptance Rate – Taxa de Falsas Aceitações) – refere-se aos utilizadores não autorizados incorrectamente identificados como válidos.

- FRR (False Rejection Rate – Taxa de Falsas Rejeições) - representa utilizadores autorizados que são incorrectamente rejeitados.

A FAR leva à ocorrência de fraude e a FRR causa decepção nos utilizadores em relação ao uso deste tipo de sistemas. O grau de fiabilidade de um sistema biométrico será então aferido tendo em atenção o equilíbrio entre FAR e o FRR, mas infelizmente estas variáveis são mutuamente dependentes, não sendo possível minimizar ambas [Magalhães e Santos 2003].

Esse equilíbrio denomina-se CER (Crossover Error Rate – Taxa de Intersecção de Erros), tal como indicado na figura 5 [Liu e Silverman 2001].

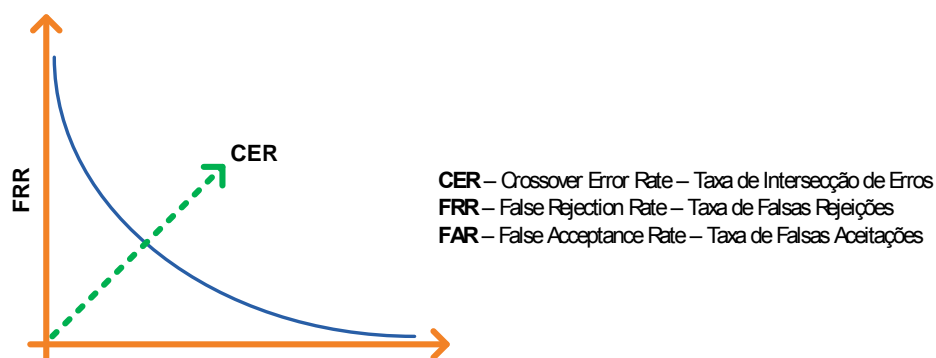


Figura 5 - CER – Crossover Error Rate – Taxa de Intersecção de Erros

Se conseguirmos encontrar esse equilíbrio, alcançando o CER mais baixo possível, mais preciso será o sistema biométrico [Liu e Silverman 2001].

4. Vulnerabilidades, riscos e desafios

Este tipo de tecnologias torna a vida mais difícil aos impostores e controlam de certa forma o utilizador pondo em prática o não-repúdio. Além disso, todos os utilizadores gozam dos mesmos privilégios de autenticação, logo não existem elos mais fracos, normalmente os alvos preferenciais dos engenheiros sociais [Prabhakar et al. 2003].

No entanto, algumas características biométricas não são secretas [Prabhakar et al. 2003], é possível que alguém tenha acesso de uma forma simples, como por exemplo: no correio de voz, num copo, ou mesmo uma fotografia perdida com resolução suficiente para manipular uma amostra de íris [Watson 2007].

Também Alterman [Alterman 2003] reforça esta preocupação, referindo que ao disponibilizarmos as nossas características para registo numa base de dados, estamos sujeitos a que, após um acesso fraudulento não consigamos recuperar imediatamente a nossa identidade.

Mas, forjar características biométricas também não é assim tão fácil, requer experiência, dinheiro, tempo e privilégios de acesso aos sistemas [Jain et al. 2006].

Segundo o relatório europeu realizado em 2005 [JRC 2005], os erros e abusos de identidade serão menos frequentes com a utilização de tecnologias biométricas.

Mas quando acontecerem serão potencialmente mais perigosos e com repercussões sociais bem mais graves, devido à dificuldade em recuperar a identidade. E se estivermos a falar de implementações em larga escala, o roubo de identidade poderá ser uma ameaça bem mais real [Alterman 2003];[Delaitre 2006].

Tem crescido as preocupações no sentido de identificar as vulnerabilidades dos sistemas de autenticação biométrica com a finalidade de criar contra medidas que possam ser accionadas para prevenir o roubo de identidade.

Na tabela 2 podemos observar o resultado de um estudo que pretendia otimizar as metodologias e ferramentas de análise de risco adicionando a análise de risco de sistemas biométricos como componente de um sistema de informação [Dimitriadis e Polemi 2004].

Vulnerabilidades	Factor de risco %				Contra medidas
	Impressão digital	Íris	Face	Voz	
Spoofing – mimicry - artefacts	11	10	12	14	i, ii, iii
Ataques servidores – templates falsos	16				iv, v
Canais de comunicação entre componentes do sistema biométrico	11				vi
Utilização do mesmo template em duas ou mais aplicações com diferentes níveis de segurança	9				vii
Alterações de componentes (ataques ao extractor de características)	11				iv, vi
Procedimentos de registo de amostras, administração, e uso de sistemas deficitário ou mal definidos	19				iv
Flutuações ou perdas de corrente e ruídos na captura da biometria (alterações de temperatura, ruído, alterações de iluminação, etc.)	4	4	4	6	iv
Captura do consumo de corrente e do tempo de processamento	4				viii
Características residuais que ficam no leitor biométrico	7	0	0	0	iii, ix
Amostras similares – características similares	2	2	6	6	ix, x
Ataques força bruta (o impostor tenta enviar continuamente dados de amostra até coincidir na comparação)	4				xi

Contra medidas	
i. Detecção de sinais de vida associada à amostra	vii. Algoritmos codificação biométricos, com funções <i>hash</i>
ii. Arquitecturas multi-biométricas	viii. Geradores de ruído, chips de baixo consumo e desenho específico de software
iii. Autenticação interactiva	ix. Avaliação das tecnologias
iv. Políticas bem definidas de acordo com os padrões	x. Revisões de calibração dos leitores.
v. Armazenamento das amostras num meio seguro	xi. Bloqueios de conta a partir de n tentativas falhadas
vi. Integração do sistema num módulo de segurança de hardware	

Tabela 2 - Esquema sobre análise de risco em sistemas biométricos

Constata-se que existem aspectos preponderantes na concepção e implementação de sistemas biométricos. O objectivo também passa por garantir que não se cometem os mesmos erros que se têm cometido com os tradicionais meios de autenticação.

É necessário ter em atenção: o registo dos utilizadores, a gestão do processo, as regras de implementação (robustas e bem definidas) e o recurso a padrões internacionais no sentido de garantir escalabilidade e interoperabilidade dos sistemas [Dimitriadis e Polemi 2004].

Além disso os administradores dos sistemas biométricos devem obedecer aos princípios legais e morais inerentes à função que desempenham, atendendo à informação que manipulam. É importante que os aspectos legais sejam garantidos [Zorkadis e Donos 2004], para que os utilizadores não se sintam desiludidos com os sistemas e percam a confiança.

5. Identidade Digital

O conceito de identidade não é novo, acompanha-nos desde há milhares de anos, sendo o nome, o atributo mais utilizado na identificação de pessoas. Mas com o decorrer do tempo o nome deixou de ser tão relevante e então outros atributos têm vindo a ser utilizados no sentido de podermos inequivocamente identificar alguém, como se verifica no caso do bilhete de identidade, cartão do cidadão e do passaporte.

Estes documentos são utilizados tanto para identificação (“*este sou eu*”), como para autenticação de identidade (“*o meu governo diz que sou mesmo eu*”) [Camp 2004].

O passaporte tradicional para todos os efeitos já tem biometrias incorporadas (e.g.: foto, assinatura). De qualquer forma os passaportes electrónicos, emitidos desde 2006 na Comunidade Europeia, já incorporam o registo de impressões digitais, com interface previsto para o sistema AFIS. Com as alterações introduzidas na nova geração, desde 29 Junho de 2009,

passa a incorporar uma estrutura emissora de certificados digitais, incumbida à Multicert [INCM 2009].

Ao falarmos de identidade digital, apenas estamos a relatar que a consulta e validação são feitas recorrendo a tecnologias específicas, e que os atributos estão armazenados de acordo com as necessidades e condições de acesso específicas [Rodrigues e Santos 2009].

Importa referir que este conceito de identidade deve conter informação relevante, que descreva de forma inequívoca uma pessoa ou entidade, mas que ao mesmo tempo contenha informação das relações com outras entidades [Windley 2005].

Será proeminente no entanto referir, que uma identidade digital não é sinónimo de identidade pessoal, mas uma limitada perspectiva de uma determinada pessoa. Neste contexto, até é possível que além do cidadão comum, também possam existir registos de pessoas fictícias e inclusive falecidos, sem a garantia sequer da sua presença, verificação visual, ou mesmo a existência de um corpo físico [Wayman 2008].

O impacto deste tipo de soluções deve ser analisado, porque em termos de interação social, quer queiramos quer não, o facto de um indivíduo possuir várias identidades também lhe permite interagir em contextos diferentes, e explorar cenários de vivências alternativos [Wayman 2008].

Para todos os efeitos, o conceito de identidade digital será independentemente do processo, ou tecnologia utilizada para a verificação, uma realidade em pleno processo evolutivo. Proporciona uma solução mais completa de segurança e diminui os custos e riscos de roubo de identidade através do recurso a tecnologias de autenticação biométrica.

6. Metodologia de estudo

A metodologia de investigação utilizada nesta fase foi uma sondagem com recurso à técnica de questionários para a recolha de dados. Esta metodologia de investigação é amplamente utilizada em áreas que envolvam opiniões de pessoas, nomeadamente na área de investigação das ciências sociais [Trochim e Donnelly 2007].

A população alvo deste questionário foi obtida através de amostra estratificada aleatória. Este tipo de amostragem permite dividir em subgrupos homogéneos por sexo e idade, sendo a amostra final aleatória simples dos elementos pertencentes a cada um dos subgrupos homogéneos [Trochim e Donnelly 2007]. Permite ainda a representatividade de todos os grupos existentes na população de estudo relativa aos utilizadores de serviços de saúde.

O questionário foi elaborado a partir do modelo Technology Acceptance Model ou TAM, adaptado da Theory of Reasoned Action ou TRA [Fishbein e Ajzen 1975], desenvolvida por Fishbein e Ajzen.

Proposto inicialmente por Davis em 1986 [Davis 1986], o TAM é considerado uma das teorias mais influentes na área de investigação em sistemas de informação no que concerne à adopção de tecnologias de Informação [Lee et al. 2003].

Ao longo dos anos têm sofrido diversas transformações, tendo recebido contributos de diversos investigadores na área. Sendo considerada mesmo umas das teorias mais poderosas desta área de investigação [Davis et al. 1989]; [Taylor e Todd 1995]; [Venkatesh e Davis 2000].

Esta teoria já foi aplicada em diferentes áreas, em diversas tecnologias, nos mais distintos ambientes, com todo o tipo de sujeitos, o que perspectiva de facto uma teoria com alguma robustez [Lee et al. 2003].

De acordo com a revisão bibliográfica efectuada, esta teoria adequa-se a esta fase do estudo dada a sua comprovada robustez e flexibilidade em estudos relacionados com a adopção de tecnologias.

O instrumento de recolha de dados foi elaborado, com recurso aos constructos do TAM 3 [Venkatesh e Bala 2008], adaptado de acordo com a revisão bibliográfica efectuada e em processos de adopção deste tipo de tecnologias [James et al. 2006]; [Jones et al. 2007]. O TAM 3 permitirá desenvolver uma rede nomológica abrangente dos factores decisórios do nível individual de adopção e utilização da tecnologia [Venkatesh e Bala 2008].

A população teórica alvo deste estudo são os utilizadores de serviços de saúde. Para o efeito seleccionou-se como população de estudo os utentes do CHNE – Centro Hospitalar do Nordeste, que assegura este tipo de serviços no distrito de Bragança. Os questionários foram distribuídos aleatoriamente por meios rurais e urbanos por forma a permitir uma amostra abrangente da população.

Como referido anteriormente a escolha da amostra aleatória estratificada foi dividida em subgrupos homogéneos por sexo e idade. Foram definidos três grupos etários: dos 18 aos 25 anos, 26 aos 50 anos e dos 51 aos 60 anos. O primeiro grupo etário caracteriza essencialmente alunos em formação universitária e em processo de integração na vida activa, tendencialmente muito dependente de novas tecnologias. O segundo grupo dos 26 aos 50 anos representa os utilizadores moderados de tecnologias, tendencialmente profissionais activos e que representam o grupo de indivíduos que nos próximos anos terá papel mais preponderante na adopção de tecnologias. O grupo dos 51 aos 60 anos representa uma faixa etária com um misto

de profissionais com diferentes tipos de formação académica. Neste grupo encontram-se indivíduos com moderada utilização de tecnologias e indivíduos com pouca ou nenhuma. Também encontramos quadros superiores devido à progressão natural na carreira e indivíduos em profissões menos remuneradas e reconhecidas socialmente.

A população de estudo obtida a partir da base de dados do CHNE para o grupo dos 18 aos 60 anos corresponde a 83577 utentes, distribuídos de acordo com a tabela 3.

Homens				Mulheres			
18-25	26-50	51-60	Total	18-25	26-50	51-60	Total
6692	23224	9339	39255	7391	26718	10213	44322

Tabela 3 – Distribuição de grupos etários por sexo

Procedeu-se à divisão proporcional da amostra para obter as quotas para cada um dos escalões etários e sexo, para posteriormente definir quantos questionários seriam atribuídos a cada grupo.

A amostra foi calculada para um intervalo de confiança de 95%, com um erro de amostragem de 4%.

O resultado do cálculo da amostra aponta para a utilização de 596 sujeitos no estudo. Após o cálculo proporcional de cada um dos grupos etários por sexo, obtemos a distribuição de sujeitos tal como indica a tabela 4.

Homens				Mulheres			
18-25	26-50	51-60	Total	18-25	26-50	51-60	Total
48	167	65	280	54	191	71	316

Tabela 4 - Distribuição de sujeitos por grupos etários e por sexo

7. Resultados Preliminares

Os resultados obtidos como referido anteriormente, apenas servem para aferir a percepção dos utilizadores em relação à utilização de tecnologias de autenticação biométrica, não sendo possível apenas a partir desta sondagem aferir a viabilidade na adopção deste tipo de tecnologias.

Para tal, o estudo terá uma segunda fase com o recurso a instrumentos que permitirão uma análise interpretativa em relação às expectativas, comportamentos e experiências directas, mediada através da intervenção e observação [LaRose e Eastin 2004].

Análise exploratória de dados

Numa primeira análise, constata-se que o género não é um factor relevante no que respeita à adopção deste tipo de tecnologias. Se repararmos na tabela 5, 328 dos inquiridos manifestaram conhecimento deste tipo de tecnologias e inclusive 62 afirmam que utilizam no local de

trabalho, restando 205 indivíduos que correspondem a 34,5% dos inquiridos, que afirmam que a partida a informação que possuem sobre este tema é insuficiente. A biometria no universo dos inquiridos que utilizam este tipo de tecnologias no local de trabalho é a impressão digital.

Conhecimento	Idade		Sexo?		Total
			Masculino	Feminino	
Insuficiente	Qual a sua idade?	18-25	24	23	47
		26-50	46	58	104
		51-60	28	26	54
	Total		98	107	205
Estou informado	Qual a sua idade?	18-25	24	28	52
		26-50	96	111	207
		51-60	32	37	69
	Total		152	176	328
Uso no local de trabalho	Qual a sua idade?	18-25	0	2	2
		26-50	25	22	47
		51-60	5	8	13
	Total		30	32	62

Tabela 5 - Percepção das tecnologias de autenticação biométrica por sexo e grupos etários

Percepção de utilidade

Em relação a este item um dos constructos do TAM, o resultado do conjunto de questões que pretendiam aferir qual a percepção de utilidade que os inquiridos tinham em relação à utilização deste tipo de tecnologias, constata-se que grande parte têm a percepção da utilidade deste tipo de tecnologias num eventual processo de autenticação perante um serviço de saúde. Da análise, constatamos que apenas 15.4% dos inquiridos não têm opinião sobre este item, e os valores de discordância têm pouco significado no contexto. Seria importante aferir nesta situação, que informação adicional seria necessária para que os inquiridos sem opinião pudessem exprimir a sua apreciação. A tabela 6 ilustra os resultados obtidos a partir dos itens utilizados para aferir a percepção de utilidade.

	Frequência	%
Discordo Totalmente	2	,3
Discordo	8	1,3
Nem Concordo nem Discordo	92	15,4
Concordo	330	55,4
Concordo Totalmente	164	27,5

Tabela 6 - Tabela de frequências para a percepção de utilidade

Percepção de facilidade de uso

Apesar de no constructo anterior (tabela 6) se verificar que a percepção de utilidade deste tipo de tecnologias é vista como uma mais-valia, o número de inquiridos sem opinião relativamente

à facilidade de uso aumentou (tabela 7). Este fenómeno está relacionado com a pouca experiência na utilização deste tipo de tecnologias. Exceptuando os indivíduos que utilizam em contexto de trabalho que representam 10,4 %, os restantes apenas conseguem relacionar a utilização deste tipo de tecnologias ao registo de impressões digitais para emissão do cartão do cidadão, ou então através da observação, nomeadamente através da televisão ou mesmo em organismos públicos onde os funcionários utilizam sistemas de autenticação biométrica para registar a entrada e saída do respectivo serviço. Uma das ilações que podemos retirar dos dados apresentados na tabela 7 aponta para a necessidade de experienciar a tecnologia para poder formar uma opinião relativamente à facilidade de uso.

	Frequência	%
Discordo Totalmente	3	,5
Discordo	21	3,5
Nem Concordo nem Discordo	141	23,7
Concordo	283	47,5
Concordo Totalmente	148	24,8

Tabela 7 - Tabela de frequências para a percepção de facilidade de uso

Intenção comportamental para o uso

Os dois constructos anteriores condicionam a intenção comportamental de uso no sentido de aferir a atitude positiva ou negativa em relação à adopção voluntária deste tipo de tecnologias por parte de um indivíduo. A tabela 8 ilustra um cenário de adopção coerente, mas mais uma vez é importante referir que o número de inquiridos sem opinião formada em relação à intenção de uso levanta um conjunto de questões que deverão ser exploradas no sentido de poder interpretar que argumentos poderão levar em particular este grupo de indivíduos a mudar a sua atitude em relação à utilização deste tipo de tecnologias. As razões associadas à indecisão de 21,1% dos inquiridos poderá estar relacionada com falta de informação, falta de experimentação da tecnologia, receio na utilização de tecnologias inovadoras, entre outras razões que não serão facilmente identificáveis a não ser que seja elaborado um estudo de natureza interpretativa no sentido de apurar o que poderá levar à adopção voluntária. Sendo essa a preocupação deste estudo numa próxima fase.

	Frequência	%
Discordo Totalmente	1	,2
Discordo	11	1,8
Nem Concordo nem Discordo	126	21,1
Concordo	373	62,6
Concordo Totalmente	85	14,3

Tabela 8 - Intenção comportamental para o uso

Fiabilidade e garantia de segurança acrescida

Este item faz parte de um conjunto de questões que foram colocadas no sentido de perceber qual a perspectiva dos inquiridos em relação às tecnologias de autenticação biométrica no que concerne à fiabilidade e à garantia de segurança acrescida perante o acesso aos serviços de saúde. Constatou-se que grande parte vê neste tipo de tecnologias um meio que garante que o processo de autenticação perante um serviço de saúde é mais fiável e seguro, percebendo que, por exemplo, a falsificação de documentos e a troca de identidade é mais difícil (tabela 9). Assim como a limitação de alguns erros que ocorrem nos serviços (e.g.: prescrições e ministração de medicação erradas). Apesar de ser observável na tabela 9, a tendência de concordância em relação a este item, o número de 16.3% de inquiridos sem opinião representam um grupo de utilizadores que poderá carecer de informação complementar sobre este tipo de tecnologias.

	Frequência	%
Discordo Totalmente	2	,3
Discordo	14	2,3
Nem Concordo nem Discordo	97	16,3
Concordo	313	52,5
Concordo Totalmente	170	28,5

Tabela 9 - Fiabilidade e garantia de segurança acrescida

Privacidade e segurança

As questões relacionadas com a privacidade e a segurança são preponderantes no que concerne à manipulação de dados privilegiados e na área da saúde é um tema bastante sensível. Do grupo de questões relacionado com este item, 85.7% (tabela 9) dos inquiridos concorda que os dados associados à sua identidade devem ser adequados, relevantes e nunca excedentes em relação ao objectivo pelo qual foram recolhidos e processados, que o armazenamento dos dados biométricos deve ser feito de forma a poder ser controlado pelo utilizador e devem ser definidos padrões que contribuam para aumentar a segurança, mantendo a privacidade dos utentes como uma garantia. É evidente a preocupação com as questões relacionadas com este item, dando uma clara imagem de receio em relação ao processo de implementação deste tipo de tecnologias.

	Frequência	%
Discordo Totalmente	0	0
Discordo	5	,8
Nem Concordo nem Discordo	80	13,4
Concordo	353	59,2
Concordo Totalmente	158	26,5

Tabela 10 - Privacidade e segurança

Vantagens na implementação deste tipo de tecnologias nos serviços de saúde

Como constatamos através da tabela 11, 81% dos inquiridos consideram a implementação deste tipo de tecnologias como uma mais-valia nos serviços de saúde. Na linha dos itens anteriores este tipo de sistemas proporcionaria um acesso mais fiável e seguro, mais simples e de fácil utilização. Se compararmos as tabelas 8, 9, 10 e 11, constatamos que os inquiridos perspectivam a utilização deste tipo de sistemas como vantajosa como meio de identificação num determinado serviço de saúde. Neste item grande parte dos inquiridos também consideraram que seria mais confortável utilizar este tipo de sistemas do que transportar diversos documentos para atestar a nossa identidade perante um determinado serviço. Considerando inclusive que este meio de autenticação satisfaria da mesma forma os utilizadores e os próprios serviços de saúde.

	Frequência	%
Discordo Totalmente	1	,2
Discordo	13	2,2
Nem Concordo nem Discordo	99	16,6
Concordo	353	59,2
Concordo Totalmente	130	21,8

Tabela 11 - Vantagens na implementação deste tipo de sistemas na saúde

8. Conclusões e trabalho futuro

Os dados apontam claramente para a abertura dos inquiridos em relação à adopção destas tecnologias. Segundo estes, existem vantagens inerentes à utilização deste tipo de tecnologias nos serviços de saúde. A maioria demonstra predisposição para a adopção, vê no processo vantagens e reforça expectativas no sentido da voluntariedade na adopção deste tipo de sistemas. Porém constatamos também que alguns inquiridos se manifestaram relutantes no que concerne a emitir uma opinião sobre os itens apresentados e avaliados nos diversos constructos. Presume-se que os cenários de utilização ilustrados aquando da distribuição do questionário possam ter sido insuficientes, bem como a falta de experimentação da tecnologia.

Importa numa segunda fase deste estudo analisar que argumentos e estratégias poderão influenciar o processo de adopção. Não podemos deixar de aferir o que poderá ser determinante no processo de decisão por parte dos inquiridos sem opinião nos diversos itens. Algumas das estratégias na segunda fase do estudo, passarão por, avaliar em ambiente de laboratório os conhecimentos dos utilizadores em contexto de utilização da tecnologia, explorando cenários de optimização do processo de adopção voluntária. Serão analisados comportamentos e factores motivacionais baseados na teoria Social Cognitive Theory [Compeau et al. 1999]; [Compeau e Higgins 1995]

Espera-se uma leitura abrangente desta problemática associada à adoção deste tipo de tecnologias, que providencie um modelo que possa otimizar o processo de aceitação, e sem que ponha em causa os princípios éticos, salvaguardando a privacidade e a dignidade humana.

9. Referências

- Alterman, A. "A piece of yourself": Ethical issues in biometric identification," *Ethics and Information Technology* (5:3) 2003, pp 139-150.
- Bolle, R., Connell, J., Pankanti, S., Ratha, N., and Senior, A. *Guide to Biometrics* SpringerVerlag New york, 2003.
- Camp, J. L. "Digital identity," *Technology and Society Magazine, IEEE* (23:3) 2004, pp 34-41.
- Compeau, D., Higgins, C. A., and Huff, S. "Social Cognitive Theory and Individual Reactions to Computing Technology: A Longitudinal Study," *MIS Quarterly* (23:2) 1999, pp 145-158.
- Compeau, D. R., and Higgins, C. A. "Application of Social Cognitive Theory to Training for Computer Skills," *Information Systems Research* (6:2) 1995, pp 118-143.
- Davis, F. D. "A technology acceptance model for empirically testing new end-user information systems : theory and results," in: *Sloan School of Management*, Sloan School of Management, MIT, 1986.
- Davis, F. D., Bagozzi, R. P., and Warshaw, P. R. "User Acceptance of Computer Technology: A Comparison of Two Theoretical Models," *Management Science* (35:8) 1989, pp 982-1003.
- Delaitre, S. "Risk management approach on identity theft in biometric systems context," Availability, Reliability and Security, 2006. ARES 2006. The First International Conference on, 2006, p. 4 pp.
- Dimitriadis, C. K., and Polemi, D. "Risk Analysis of Biometric Systems " 2nd International Workshop on Security In Information Systems, INSTICC Press, Porto, Portugal, 2004, pp. 23-32.
- Fairhurst, M. C. "Document identity, authentication and ownership: the future of biometric verification," Document Analysis and Recognition, 2003. Proceedings. Seventh International Conference on, 2003, pp. 1108-1116.
- Fishbein, M., and Ajzen, I. *Belief, attitude, intention, and behavior : an introduction to theory and research* Addison-Wesley Pub. Co., Reading, Mass., 1975.
- INCM "A Imprensa Nacional-Casa da Moeda e a nova geração do Passaporte Electrónico Europeu com suporte no protocolo EAC," IMPRENSA NACIONAL – CASA DA MOEDA, S. A., 2009.
- Jain, A. K., Ross, A., and Pankanti, S. "Biometrics: a tool for information security," *Information Forensics and Security, IEEE Transactions on* (1:2) 2006, pp 125-143.
- James, T., Pirim, T., Boswell, K., Reithel, B., and Barkhi, R. "Determining the Intention to Use Biometric Devices: An Application and Extension of the Technology Acceptance Model," *Journal of Organizational & End User Computing* (18:3) 2006, pp 1-24.
- Jones, L. A., Antón, A. I., and Earp, J. B. "Towards understanding user perceptions of authentication technologies," in: *Proceedings of the 2007 ACM workshop on Privacy in electronic society*, ACM, Alexandria, Virginia, USA, 2007, pp. 91-98.

- JRC "Biometrics at the Frontiers: Assessing the Impact on Society," EUR 21585 EN, EU Joint Research Centre, Brussels EC.
- LaRose, R., and Eastin, M. S. "A Social Cognitive Theory of Internet Uses and Gratifications: Toward a New Model of Media Attendance," *Journal of Broadcasting & Electronic Media* (48:3) 2004, pp 358-377.
- Laux, D. D. "A study of biometric authentication adoption in the credit union industry," Iowa State University, 2007, p. 62.
- Lee, Y., Kozar, K. A., and Larsen, K. R. T. "The Technology Acceptance Model: Past, Present, and Future," *Communications of AIS* (2003:12) 2003, pp 752-780.
- Liu, S., and Silverman, M. "A practical guide to biometric security technology," *IT Professional* (3:1) 2001, pp 27-32.
- LogicaCMG "E-Identity: European attitudes towards biometrics," 2006.
- Magalhães, P. S., and Santos, H. D. "Biometria e Autenticação," 4ª Conferência da Associação Portuguesa de Sistemas de Informação, Associação Portuguesa de Sistemas de Informação, Porto, 2003.
- Prabhakar, S., Pankanti, S., and Jain, A. K. "Biometric recognition: security and privacy concerns," *Security & Privacy, IEEE* (1:2) 2003, pp 33-42.
- Rodrigues, P., and Santos, H. D. "Estudo da resistência à aplicação de tecnologias biométricas," 9ª Conferência da Associação Portuguesa de Sistemas de Informação, Associação Portuguesa de Sistemas de Informação Viseu, Portugal, 2009.
- Savastano, M. "Biometrics: Modelling the Body," Computer Modeling and Simulation, 2008. UKSIM 2008. Tenth International Conference on, 2008, pp. 14-17.
- Taylor, S., and Todd, P. A. "Understanding Information Technology Usage: A Test of Competing Models," *Information Systems Research* (6:2) 1995, pp 144-176.
- Trochim, W., and Donnely, J. P. *The Research Methods Knowledge Base*, (3rd ed.) Thomson Publishing, Mason, OH., 2007.
- Venkatesh, V., and Bala, H. "Technology Acceptance Model 3 and a Research Agenda on Interventions," *Decision Sciences* (39:2) 2008, pp 273-315.
- Venkatesh, V., and Davis, F. D. "A Theoretical Extension of the Technology Acceptance Model: Four Longitudinal Field Studies," *Management Science* (46:2) 2000, p 186.
- Watson, A. "Biometrics: easy to steal, hard to regain identity," Nature Publishing Group, 2007, pp. 535-535.
- Wayman, J. L. "Biometrics in Identity Management Systems," *Security & Privacy, IEEE* (6:2) 2008, pp 30-37.
- Windley, P. J. *Digital Identity* O'Reilly Media, 2005.
- Yun, Y. "The '123' of Biometric Technology," *Synthesis Journal*) 2002, pp 83-96.
- Zorkadis, V., and Donos, P. "On biometrics-based authentication and identification from a privacy-protection perspective: Deriving privacy-enhancing requirements," *Information Management & Computer Security* (12:1) 2004, pp 125-137.