Factores Críticos de Sucesso para a Implementação de uma Política de Segurança em Clínicas de Saúde

Critical Success Factors for the Implementation of a Security Policy in Health Clinics

Isabel Maria Lopes
Instituto Politécnico de Bragança
Bragança, Portugal
isalopes@ipb.pt

Pedro Oliveira
Instituto Politécnico de Bragança
Bragança, Portugal
pedrooli@ipb.pt

Resumo — **A Segurança de Sistemas de Informação (SSI) é primordial em todos e cada um dos serviços oferecidos pelas organizações. De entre as medidas de segurança, as políticas assumem na literatura um papel central. Todavia, nota-se a existência de um reduzido número de estudos empíricos sobre a implementação de políticas SSI e quais os fatores críticos de sucesso para a sua implementação. Este artigo contribui para minimizar essa falha mediante a apresentação dos resultados de um inquérito sobre a adoção de políticas de SSI em clínicas de saúde. Se bem que todas as organizações apresentem requisitos próprios ao nível da SSI, reconhece-se que o sector da saúde oferece um dos casos mais interessantes para o estudo da temática da SSI em particular e das tecnologias de informação e sistemas de informação em geral. Os resultados são discutidos á luz da literatura e identificam-se trabalhos futuros com vista a potenciar a implementação de políticas de SSI.**

Palavras Chave – Segurança da informação; implementação de políticas de segurança; políticas de segurança de sistemas de informação.

Abstract — **Information systems security (ISS) is crucial in all and each of the services provided by organizations. Among the security measures, policies assume a central role in literature. However, there is a reduced number of empirical studies about the implementation of ISS policies and which are the critical success factors for its implementation. This paper contributes to mitigate this flaw by presenting the results of a survey in the adoption of ISS policies in health clinics. While all organizations have their own ISS requirements, the health sector is recognized to offer one the most interesting cases for the thematic study of ISS in particular and information technology and information systems in general. The results are discussed in literature and future works are identified with the aim of enabling the implementation of ISS policies.**

Keywords – Information Security; implementaction of security policies; information systems security policies.

I. INTRODUÇÃO

A SSI é um aspeto crítico para a maioria das organizações. Com o advento das tecnologias de informação e a utilização massiva da Internet e dos serviços que lhe estão associados, o número de ataques a que a informação está sujeita é cada vez mais elevado e consequentemente a necessidade de proteger os sistemas de informação torna-se mais premente.

As organizações manipulam cada vez mais, grandes quantidades de informação em suportes tecnológicos, por isso são imprescindíveis controlos de segurança cada vez mais rigorosos e abrangentes. O processo tecnológico pode funcionar como um catalisador de ameaças, mas por si só não é suficiente para garantir a efetiva segurança da informação.

As organizações têm uma cultura própria ao nível da SSI que as diferencia umas das outras, contudo as organizações que operam na área da saúde merecem um olhar mais atento em questões de segurança, nomeadamente sobre os dados e informações de que são detentoras.

As clínicas de saúde assumem uma relevância própria, dado concentrarem uma exigência cada vez mais forte por parte dos seus utentes sobre os seus serviços de informação e pela diversidade e quantidade de informação confidencial que manipulam inerente às suas funções (situação clínica do doente, diagnóstico, prognóstico, tratamentos e dados pessoais). Logo, a eficácia dos seus sistemas de informação revela-se crucial. Face à informação que recebem, armazenam, processam e distribuem, a segurança dos seus sistemas de informação é imprescindível para a normal laboração e para a salvaguarda dos dados pessoais de cada utente que lhes são confiados.

Tanto ou mais importante que atingir os níveis de segurança de informação adequados a cada organização, é conseguir mantê-los. Não basta ter software e hardware que contribua para a segurança da informação, mas também uma política de segurança e uma boa gestão da segurança, de forma

a alicerçar devidamente os esforças de proteção dos ativos do sistema de informação [1].

No caso das clínicas médicas em Portugal, os estudos que focam as políticas de SSI são reduzidos, surgindo, assim, como dificuldade primeira um desconhecimento generalizado sobre a realidade destas organizações no que tange à adoção e aplicação de políticas de SSI. A auscultação ao universo destas empresas era de todo impossível dado o seu número elevado, por isso, a seleção de uma amostra foi inevitável.

Atentando-se nas dificuldades encontradas procurou-se mitigar a lacuna identificada na literatura mediante a realização de um Inquérito, compreendendo um conjunto de questões sobre políticas de SSI, indagando-se diretamente junto dos serviços de 250 clínicas médicas portuguesas sobre a existência e características de tais políticas.

É neste contexto que se enquadra o presente trabalho, que estruturalmente após esta introdução, prossegue-se com a revisão da literatura sobre a importância das políticas de SSI. Em seguida, na secção 3, centraliza-se no que se entende por implementação de uma política de SSI. Na secção 4, descreve-se a metodologia de pesquisa. Os resultados do estudo são discutidos na secção 5. Por último, apresentam-se as conclusões à luz dos resultados, identificam-se as limitações deste estudo e propõem-se trabalhos futuros.

II. IMPORTÂNCIA DAS POLITICAS DE SEGURANÇA

A informação é um ativo que, como qualquer outro ativo importante para os negócios, tem um valor para a organização e consequentemente necessita se ser adequadamente protegido. A segurança da informação é definida pela norma [2] como o conjunto de procedimentos que visa a proteção da informação de diversos tipos de ameaças para garantir a continuidade dos negócios, minimizar os riscos e maximizar o retorno dos investimentos e as oportunidades de negócio.

Tradicionalmente, a segurança da informação é decomposta em três dimensões: Confidencialidade, Integridade e disponibilidade [3] [4] [5] [6].

Atualmente esta divisão rígida em três dimensões é colocada em causa. Esta abordagem é rejeitada por alguns autores por a considerarem simples, entendendo que não se enquadra adequada às necessidades de segurança que as organizações apresentam atualmente [6].

O autor Parker defende a existência de seis dimensões para a segurança da informação: as três dimensões clássicas (confidencialidade, integridade e disponibilidade), a utilidade, a autenticidade e a propriedade [6].

A norma ISSO/IEC 17799 na versão de 2000 só considera as três dimensões clássicas, na versão de 2005 considera a possibilidade de adicionar pontualmente, outras dimensões, tais como autenticidade, responsabilidade, não repúdio e credibilidade [2].

A divisão da segurança em dimensões tem que ser adaptada ao tipo de organização, pois é com base nelas que será definida a arquitetura do processo de segurança de cada organização [7].

A informação é considerada um recurso crítico para qualquer organização, com vista às organizações alcançarem um determinado nível de segurança dos seus SI, a literatura tem apontado as políticas de SSI como o meio mais adequado e indispensável para o lançamento e sustentação do programa de SSI das organizações.

A literatura sugere um elevado grau de consenso quanto à importância de uma política de SSI numa organização, sendo considerada por vários autores como a fundação do esforço de segurança. Esta constatação pode ser validada com as afirmações que seguidamente se apresentam [8]:

> "A política de segurança é para o ambiente da segurança como a lei para o sistema legal. (…) Uma política é o início da gestão da segurança." [9].
>
> "… um sistema de informação sem uma política de segurança é uma espécie de coleção deslocada de contra-medidas dirigidas a várias ameaças." [10].
>
> "Uma política de segurança eficaz é tão necessária para um bom programa de segurança de informação como uma fundação sólida para uma casa." [11].
>
> "A pedra angular de uma arquitetura de segurança de informação eficaz é uma declaração de política bem redigida." [12].
>
> "A política de segurança da informação é um dos documentos mais importantes numa organização." [13].
>
> "… a política de segurança é o alicerce em que toda a segurança se baseia." [14].
>
> "As políticas de segurança são a fundação e a linha da base da segurança da informação numa organização." [15].

As razões para esta elevação do grau de importância das políticas de SSI encontram-se na utilidade que estes documentos demonstram ao nível das iniciativas desenvolvidas pelas organizações para a proteção dos SI [16].

As políticas de SSI auxiliam ainda na coordenação das ações de proteção dos recursos do sistema de informação, evitando a fragmentação dos esforços e servindo de guia para o processo de seleção, desenvolvimento e implementação de controlos apropriados de SSI [17].

Outro aspeto a destacar é a política contribuir para que todos dentro da organização se comportem coerentemente de forma aceitável relativamente à segurança da informação [18].

Para além da sua formulação, implementar devidamente a política de SSI é crucial para o seu êxito. A implementação de uma política pode ser considerada como um conjunto de atividades que visam prescrever o que se encontra no documento da política.

III. IMPLEMENTAÇÃO DE POLÍTICAS DE SEGURANÇA DE SISTEMAS DE INFORMAÇÃO

A informação é um dos principais ativos das organizações atuais, pelo que é natural que os sistemas que suportam essa informação estejam cada vez mais expostos a ameaças, sejam elas de natureza intencional ou acidental. Estas ameaças podem

colocar em causa a confidencialidade, a integridade e a disponibilidade da informação e dos sistemas que a manipulam, pelo que os responsáveis das organizações devem ponderar e implementar medidas que visem prevenir, detetar e reagir face à concretização dessas ameaças.

Com o desígnio das organizações conseguirem um determinado nível de segurança dos seus SI, a literatura tem mostrado que as políticas de SSI são o recurso mais apropriado e indispensável para a projeção e sustentação da gestão da SSI das organizações.

A criação de uma política de SSI segue um ciclo de vida completo desde a sua formulação até à sua revisão, passando pela implementação. É sobre a implementação de uma política de SSI que este estudo recai. Existem seis princípios fundamentais a levar em linha de conta no processo de implementação de uma política de SSI [19]:

- A organização assegurará que a sua informação seja mantida segura e utilizada de forma apropriada;
- A organização fornecerá aos recursos humanos, orientações claras relativamente à segurança da informação;
- Todos os recursos humanos que trabalham para e em nome da organização colaborarão com a política de segurança da informação na organização;
- A organização assegurará que os seus recursos humanos conhecem todas as orientações relevantes, acerca da segurança da informação da organização;
- A organização informará os clientes como os seus registos serão mantidos seguros e a quem eles serão facultados;
- A organização obedecerá a toda a legislação nacional e à melhor orientação relativamente à segurança da informação.

Um processo de implementação de uma política de SSI [20] é apresentado na Fig. 1, 2 e 3 e inclui elementos de input, que alimentam certos processamentos de atividade que vão dar origem a um conjunto de outputs.

Input

- Documento da política de segurança
- Conhecimento acerca da cultura da organização

Figura 1. Processo de implementação de uma política de segurança (Input)

Atividades

- Fornecer instruções acerca da aplicação da política de segurança
- Fornecer aos utilizadores do Sistema de Informação formação e educação adequadas acerca da utilização da política de segurança e procedimentos
- Monitorizar e avaliar o uso de políticas de segurança
- Monitorizar e avaliar procedimentos de segurança
- Implementar parâmetros de segurança técnicos e organizacionais

Figura 2. Processo de implementação de uma política de segurança (Atividades)

Output

- Consciência da segurança
- Avaliação da implementação da utilização da política de segurança e aplicação dos procedimentos de segurança

Figura 3. Processo de implementação de uma política de segurança (Output)

Este processo tem como resultado último a implementação e consequente consciencialização dos utilizadores e dirigentes da obrigatoriedade de utilizar essa política com o máximo de rigor e seriedade.

IV. Metodologia de Pesquisa

Com vista a caracterizar empiricamente a adoção de políticas de SSI pelas clínicas médicas, entendeu-se apropriado aplicar a técnica de inquérito, uma vez que potencia uma resposta clara, direta e objetiva às questões apresentadas aos inquiridos. Além disso, uma vez que o universo em estudo compreende milhares de clínicas, das quais 250 foram inquiridas, julgou-se que este número inviabilizava ou desaconselhava a adoção de técnicas de investigação alternativas.

Dado o inquérito incidir sobre políticas de SSI, assumiu importância central a adoção de uma definição suscetível de transmissão e fácil compreensão por parte dos inquiridos. Assim, optou-se pela adoção da definição preconizada por de Sá-Soares [16], para quem as políticas de SSI são "documentos que orientam ou regulam as ações das pessoas ou sistemas no domínio da segurança dos sistemas de informação".

A. População

Foram efetuados 250 questionários, contudo só 201 tiveram uma resposta efetiva o que corresponde a uma taxa de resposta de 80%. Para a seleção recorreu-se a uma amostragem aleatória, com base no tipo de clínica e distribuída pelos 18 distritos de Portugal mais os arquipélagos da Madeira e dos Açores.

Dos 201 contactos efetuados, em 198 obtiveram-se as respostas por via telefónica e em 3 casos via correio eletrónico, na sequência de um contacto telefónico prévio.

Tentou-se no maior número de casos possíveis que o respondente a este inquérito fosse o responsável pela informática, caso não existisse contactou-se o responsável pela clínica.

O estudo foi realizado entre os meses de setembro e novembro de 2014.

B. Estrutura

A estrutura do Inquérito resultou da revisão de literatura sobre políticas de SSI e do enquadramento legal Português, nomeadamente a Lei n.º67/98 – Lei de proteção de dados pessoais, que revogou a Lei n.º10/91 – Lei de proteção de dados pessoais face à informática e a Lei n.º 28/94 – Medida de reforço da proteção de dados pessoais.

As questões do inquérito, de resposta individual e de natureza confidencial, foram organizadas em três grupos.

O primeiro grupo visava obter uma breve caracterização da empresa e do respondente, seguindo-se os grupos de questões atinentes à segurança da informação, as quais eram antecedidas pela questão fundamental: "A empresa adota uma cultura de segurança da informação?".

Após a pergunta principal, e caso a resposta fosse negativa, passava-se para o grupo de questões onde se questionava os inquiridos se estavam a pensar adotar algumas medidas e comportamento que possam contribuir para que a empresa ter uma política de segurança da informação, uma vez que ainda não possuíam esse documento, e caso estivessem a pensar adotar alguma medida, se a mesma já estava em processo de preparação. Se não estivessem a pensar adotar qualquer medida, eram questionados se essa opção seria por não considerarem a segurança da informação importante.

Caso a resposta à questão principal fosse positiva, passava-se aos grupos de questões em que se focava que tipo de medidas têm adotadas e que fatores pertinentes poderiam indicar no que diz respeito aos fatores que facilitam e inibem a sua adoção de uma política de SSI. Uma última questão formulada aos inquiridos relacionava-se com a existência e identificação de outros mecanismos de proteção da informação.

O inquérito foi bastante abrangente, contudo para este estudo o foco recaiu só nos fatores críticos de sucesso para a implementação de uma política de SSI.

V. RESULTADOS

A segurança da informação e da privacidade no sector da saúde é um tema de importância crescente [21]. Na generalidade das clínicas há uma permanente recolha, processamento, armazenamento e consulta de informação prevenientes de cuidados de saúde. Desta forma até pela obrigação que as organizações têm de cumprir a lei, é imperioso que cada uma implemente um processo de gestão de segurança da informação, que seguramente terá de passar pela implementação de uma política de SSI.

A existência ou não dessa política foi a questão principal do inquérito que se prendia-se com o apuramento da existência de políticas de SSI nas clínicas de saúde inquiridas.

Uma dificuldade inicial com que se debateu na condução do inquérito relacionou-se com a falta de um entendimento claro e universal por parte dos respondentes para o conceito de política de SSI. Foi com alguma dificuldade que diversos respondentes associaram esse conceito ao conjunto de regras que estabelecem o regime de utilização dos SI da clínica.

Como se pode observar na Fig. 4, das 201 clínicas de saúde 49 dispõem de política e 152 não adotaram qualquer política.

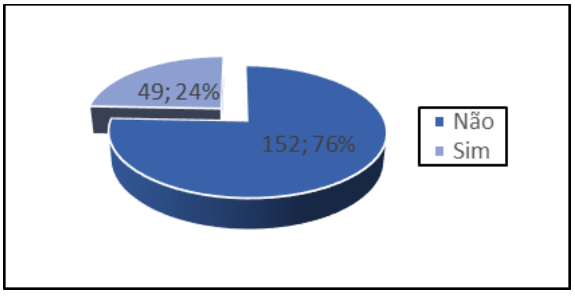

Figura 4. Adoção de políticas de SSI

Apesar do grande número de clínicas de saúde que não possuem uma política de SSI, muitas foram aquelas que em resposta ao inquérito afirmaram ponderar a formulação de uma política de SSI, estando já algumas em processo de formulação.

Face a esta resposta, foram inquiridos sobre se entendem a SSI como uma preocupação. A resposta foi invariavelmente afirmativa, ou seja, os respondentes, apesar de não estarem a pensar formular uma política, consideram a SSI como uma preocupação, justificada pelo valor que reconhecem à informação. Numa tentativa de se encontrar uma explicação para esta incongruência foram avançadas explicações pelos inquiridos que se fundam na utilização de diversas tecnologias de SSI, que as clínicas são pequenas e com poucos funcionários, o que, na ótica dos respondentes, dispensa a existência de uma política de SSI sob a forma de um documento escrito.

Quanto ao tipo de clínicas de saúde, o inquérito foi dirigido a clínicas médicas e de diagnóstico (consultas de especialidade e exames médicos), clínicas ortopédicas, clínicas médicas dentárias, clínicas de enfermagem, clínicas de fisioterapia e clínicas de oftalmologia. O número de clínicas inquiridas por tipo de clínica estão vertidos na Fig. 5, que se segue.

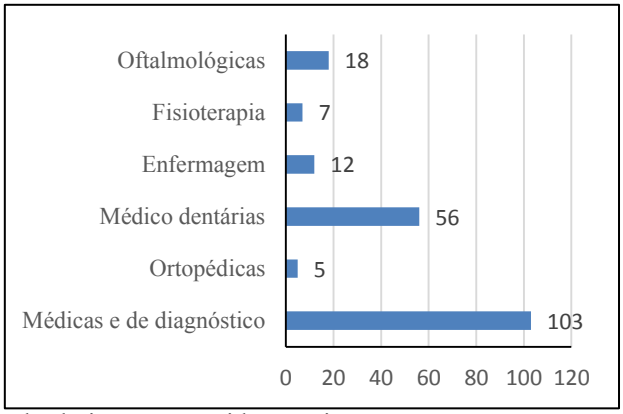

Figura 5. Tipo de clínicas de saúde

Das 49 clínicas que dispõem de uma política de SSI, verifica-se que 51% são clínicas médicas e de diagnóstico, seguindo-se as clínicas de enfermagem com 31%. A distribuição das políticas de SSI por tipo de clínica de saúde pode ser observada na Fig. 6.

Tipo de Clínica	Nº de Políticas
Médicas e de diagnóstico	25
Enfermagem	15
Médicas dentárias	6
Oftalmológicas	2
Ortopédicas	1
Fisioterapia	0

Figura 6. Adoção de uma política de SSI / Tipo de clínica

A questão principal do inquérito para este estudo prendia-se com o apuramento dos fatores críticos de sucesso para a implementação de uma política de SSI. A recolha destes elementos recaiu mais nas 49 clínicas médicas que

responderam afirmativamente à existência de uma política de SSI.

O sucesso de uma política depende muito da adoção e cumprimento da política por parte dos utilizadores. É importante delinear responsabilidades individuais, por exemplo, através da clarificação de quem tem acesso a determinada parte do sistema.

Os funcionários da clínica, assim como o pessoal subcontratado ou colaboradores externos, adquirem por sua vez, o dever de segredo, ou seja, a responsabilidade de não divulgar nenhum tipo de informação que tenham obtido na execução do seu trabalho na clínica.

Para tal, deverão conhecer, assumir e cumprir a política, normas e procedimentos de segurança vigentes, estando obrigados a manter o segredo profissional e a confidencialidade dos dados utilizados no seu trabalho e devendo comunicar, com carácter de urgência e segundo os procedimentos estabelecidos, as possíveis incidências ou problemas de segurança que se detetem.

Outro aspeto que é considerado um fator crítico de sucesso para uma boa implementação é a definição de penalizações para os utilizadores que não cumprem o estipulado pela política.

O apoio dos gestores das organizações na elaboração e implementação das políticas é também um fator crítico preponderante para o sucesso de uma política de SSI. Só com o envolvimento de todos os colaboradores e principalmente com o envolvimento dos gestores e chefias, se atinge uma boa elaboração e implementação da política.

A revisão periódica das políticas de SSI é também crucial. De pouco servirá uma política se a mesma não estiver atualizada. As organizações cada vez são mais dinâmicas e como consequência as alterações de funcionamento e de estrutura acontecem a um ritmo elevado, pelo que é necessário adaptar a política a essas novas realidades.

O intervalo de tempo utilizado para a revisão de uma política de segurança, varia muito de empresa para empresa, contudo uma certeza é conhecida, a revisão deverá ser feita sempre que foram identificados factos novos, não previstos na versão atual que possam ter impacto na segurança da clínica.

A comunicação e disseminação da política por todos aqueles que a devem conhecer e observar têm sido também apontadas como fundamental para o sucesso das políticas. Facilmente se aceitará que todos os utilizadores têm de ter conhecimento da política de segurança. Embora a forma de dar conhecimento possa variar (circular interna, disponibilização da política na Intranet da organização ou outros mecanismos), é necessário garantir que todos tiveram conhecimento do conteúdo da política.

Há quem defenda que o processo de segurança começa logo no recrutamento, uma vez que os utilizadores do sistema de informação de uma clínica médica trabalham tão proximamente com informações clínicas e pessoais dos seus utentes. As clínicas deviam aliar a política de SSI ao contrato de trabalho dos funcionários ou colaboradores.

A integração das políticas com os objetivos, processos e cultura da organização é fundamental para o sucesso da implementação da política. Uma política de SSI tem que ser um veículo construtor e de proteção e nunca um mecanismo que impeça o bom desenvolvimento do trabalho da organização. Para tal, antes de se formular uma política, é necessário ter em linha de conta os objetivos da empresa bem como os seus processos e cultura organizacional.

A exequibilidade das políticas (em termos de implementação e observância) constitui outro fator essencial. De pouco ou nada servirá ter uma política de SSI se a sua exequibilidade se revela impossível.

É necessário consciencializar os envolvidos de que a tecnologia não é o único elemento a considerar, sem a existência de uma política de SSI, métodos de resposta a incidentes ou planos de continuidade do negócio, as tecnologias não serão eficazes na proteção da informação na organização.

Outro aspeto a ter em conta diz respeito à sensibilização dos utilizadores e dirigentes em relação às problemáticas da segurança, uma vez que o fator humano é apontado como o responsável por grande parte dos incidentes de segurança. A sua sensibilização é fundamental para se conseguir que a política de SSI organizacional produza o efeito desejado [1].

A política de SSI deve incluir um conjunto de diretrizes, normas e procedimentos que devem ser seguidos e que visam consciencializar e orientar os utilizadores para o uso seguro das tecnologias, com informação sobre como gerir, guardar e proteger um dos seus principais ativos que é a informação.

Como é de se esperar em todo o processo que envolve mudanças há resistência natural das pessoas, e no caso da segurança da informação especificamente há um detalhe a "desinformação sobre o tema". As pessoas não "entendem facilmente", pelo menos no início, o real motivo e a necessidade de tantos controles, processos e evidencias, e não é raro, observarmos algumas reações, dentre as mais diversas possíveis, no momento de colocar em prática alguma ação orientada a promover a segurança.

O Apoio dos gestores é fundamental para que a política de segurança da informação seja efetiva, sem a presença deste apoio, iniciar qualquer ação neste sentido é algo no mínimo "temerário".

Os gestores ou responsáveis das clínicas, devem ter a responsabilidade de promover e apoiar o estabelecimento de medidas de segurança que garantam a integridade, disponibilidade e confidencialidade dos ativos informáticos, com o propósito de evitar a sua possível alteração, destruição, roubo, cópia, falsificação e outras ameaças existentes, sejam estas acidentais ou não.

A política de segurança só deve ser posta em prática após os utilizadores terem conhecimento do seu conteúdo, após terem formação e assinarem uma declaração de compromisso.

Para além disso, fornecer treinamentos regulares em segurança da informação aos colaboradores além de fundamental é o que de facto garantirá o sucesso da aplicação das diretrizes contidas na política de segurança da informação.

Uma forma eficaz e relativamente fácil de sensibilizar os empregados para as questões da segurança da informação, é fornecer políticas que sejam compreensíveis para todos os funcionários de uma organização e sejam de fácil acesso a qualquer momento [22].

A política de SSI deve ser aplicável a todos os sistemas de informação da clínica independentemente da tecnologia que suporta.

A política tem de envolver todo o tipo de informação criada ou utilizada pela clínica, independentemente do seu formato ou meio de armazenamento, uma vez que as clínicas processam muita informação em formato não digital.

De tudo o que foi referido é importante enfatizar que a nova realidade que vivemos em termos das novas tecnologias de informação e comunicação exige uma maior atenção no âmbito da SSI. A institucionalização de políticas de SSI tem de ser uma realidade nas organizações, independentemente da sua dimensão e da área em que operam.

VI. CONCLUSÕES

Por forma a alcançarem sucesso nas suas ações de proteção dos seus SI, as organizações necessitam de adotar medidas de diferentes naturezas, ou seja, não basta aplicar medidas técnicas de SSI, mas também e cada vez mais medidas de índole organizacional e social, pois só assim será possível o bem-estar organizacional e a manutenção da integridade das organizações [23].

Com a massificação das tecnologias, o direito à privacidade é suscetível das maiores ameaças. As clínicas de saúde, de forma a garantir a confidencialidade e integridade dos dados clínicos e pessoais dos seus utentes, têm de adotar políticas de segurança que salvaguardem os seus sistemas de informação.

Para além da implementação de uma política de SSI, recomenda-se que as clínicas de saúde em particular e o unidades de saúde em geral, invistam mais em formação e sensibilização dos utilizadores do sistema de informação, de forma a evitar a ocorrência de incidentes. Qualquer organização necessita de uma política de SSI independentemente da sua área de negócio, contudo esta necessidade é ainda mais premente para as organizações que prestam cuidados de saúde ou que lidam com a informação resultante dos mesmos.

Uma das limitações deste trabalho de investigação prende-se com a delimitação do estudo às clínicas de saúde e á amostra estudada. Embora se creia que se tenham gerado dados suficientes para os propósitos deste trabalho, facilmente se aceitará que um maior número e abrangência poderia resultar num conjunto de dados mais rico e mais sustentado.

De entre os trabalhos futuros a realizar, realça-se um dos fatores críticos de sucesso identificado neste trabalho para a implementação de uma política de SSI, que é a sensibilidade da Administração paras as questões da segurança, facto que nem sempre se verifica. Seria interessante estudar a forma de sensibilizar eficazmente as Administrações, identificando os fatores críticos de sucesso capazes de influenciar as Administrações na adoção de uma metodologia de gestão da SSI.

REFERÊNCIAS BIBLIOGRÁFICAS

[1] I. Lopes, Adopção de Políticas de Segurança de Sistemas de Informação na Administração Pública Local em Portugal, Tese de Doutoramento, Universidade do Minho, Guimarães, 2012.

[2] ISO/IEC 17799, International Standard ISO/IEC 17799:2000 Code of Practice for Information Security Management, International Organization for Standardization/International Electrotechnical Commission, 2012.

[3] C. Pfleeger and S. Pfleeger, Security in Computing, 3 nd ed ed: Prentice Hall PR, 2012.

[4] A. Calder and S. Walkins, IT Governance: a manager's guide to date security and bs 7799/iso17799, 2nd ed ed: London and Sterling, VA, 2003.

[5] M. Gerber and R. von Salms, "From Risk Analysis to Security Requirements", Computer & Security, vol. 24, pp. 147-159, 2005

[6] D. Parker, "Toward a New Framework for Information Security", in Computer Security Handbook, S. Bosworth and M. E. Kabay, Eds., 4º ed: John Wiley & Sons, INC, 2002.

[7] A. C. Santos, Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação, Tese de Doutoramento, Universidade do Minho, 2007.

[8] I. M. Lopes, and F. de Sá-Soares, "Information Systems Security Policies: A Survey in Portuguese Public Administration", proceedings of the IADIS International Conference Information System, Porto (Portugal), pp. 61-69, 2010.

[9] H. N. Higgins, "Corporate system security: towards an integrated management approach", Information Management & Computer Security, vol. 7, no. 5, pp. 217–222, 1999.

[10] B. Schneier, "Secrets and Lies: Digital Security in a Networked World", John Wiley & Sons, New York, 2000.

[11] C. M King, Security Architecture: Design, Deployment, and Operations, Osborne/McGraw-Hill, Berkeley, 2001.

[12] T. R. Peltier, "Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management", Auerbach Publications, Boca Raton, 2002.

[13] K. Höne, and J. Eloff, "Information security policy — what do international information security standards say?", Computers & Security, vol. 21, no. 5, pp. 402–409, 2002.

[14] B. Shorten, "Information Security Policies from the Ground Up", in H. F. Tipton e M. Krause (Eds.), Information Security Management Handbook (Fifth ed.), Auerbach, Boca Raton, pp. 917–924, 2004.

[15] C. Kee, "Security Policy Roadmap – Process for Creating Security Policies", SANS Institute, 2001.

[16] F. de Sá-Soares, Interpretação da Segurança de Sistemas de Informação Segundo a Teoria da Acção, Tese de Doutoramento em Tecnologias e Sistemas de Informação, Universidade do Minho, Guimarães, 2005.

[17] S. Barman, "Writing Information Security Policies", New Riders, Indianapolis, 2001.

[18] D. Lee, "Developing Effective Information Systems Security Policies", SANS Institute, 2001.

[19] N.Gaunt, "Installing an appropriate information security policy", International Journal of Medical Informatics, vol. 49, no. 1. pp. 131-134, 1998.

[20] M. Karyda, E. Kiountouzis, and S. Kokolakis, "Information systems security policies: a contextual perspective", Computers & Security, vol. 24, no 3, pp. 246-260, 2005.

[21] A. Appari, and M. Johnson, "Information Security and Privacy in Healthcare: Current State of Research, Published by Ham Ham Bogdan, 2013.

[22] F. Haeussinger, and J. Kranz, "Understanding the Antecedents of Information Security Awareness – An Emperical Study", Proceedings of the 19th Americas Conference on Information Systems, 2013.

[23] G. Dhillon, and J. Backhouse, “Information System Security Management in the New Millennium”. Communications of ACM, 43 (7), 125-128, 2000.