Este trabalho foi co-financiado pelo Fundo Social Europeu

Ministério da Educação prodep III

União Europeia
Fundo Social Europeu

Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação

António Carvalho Santos

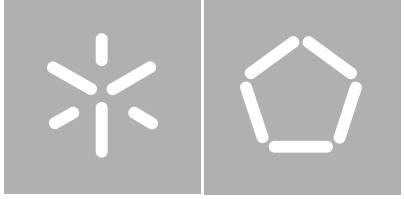
UM | 2007

Universidade do Minho
Escola de Engenharia

António Manuel Rodrigues Carvalho dos Santos

Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação

Março de 2007



Universidade do Minho
Escola de Engenharia

António Manuel Rodrigues Carvalho dos Santos

Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação

Tese de Doutoramento
Tecnologias e Sistemas de Informação
Sistemas de Computação e Comunicação

Trabalho efectuado sob a orientação de
Professor Doutor Henrique Manuel Dinis dos Santos

Março de 2007

DECLARAÇÃO

Nome: António Manuel Rodrigues Carvalho dos Santos

Endereço electrónico: ac1972@sapo.pt **Telefone:** +351 919232284

Número do Bilhete de Identidade: 9776847

Título da Tese de Doutoramento:

Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação

Orientador: Professor Doutor Henrique Manuel Dinis dos Santos

Ano de conclusão: 2007

Designação do Doutoramento: Doutoramento em Tecnologias e Sistemas de Informação

Sistemas de Computação e Comunicação

Universidade do Minho, 1 / 03 / 2007

Assinatura: _____

Ao meu filho António Miguel

Agradecimentos

Durante o desenvolvimento deste trabalho, muitas foram as sugestões de colegas e amigos. Cabe-me aqui deixar expresso o meu reconhecimento a todos aqueles que, directa ou indirectamente, contribuíram para a realização deste trabalho.

Ao Professor Doutor Henrique Manuel Dinis dos Santos, meu orientador, dirijo um agradecimento muito especial pelo apoio, orientação, colaboração, amizade e disponibilidade, não devendo ainda ficar esquecida a oportunidade que me deu de realizar este trabalho.

Ao Dr. Pedro Roldão pela sua permanente disponibilidade para ajudar ou comigo discutir uma ideia.

Ao Hospital Infante D. Pedro, nomeadamente ao Conselho de Administração e ao Serviço de Cardiologia, pelas facilidades concedidas para o desenvolvimento deste trabalho.

Ao Dr. Narciso Pinheiro e ao Enfermeiro Luís Coquim pela forma solidária e empenhada com que colaboraram.

Aos elementos que participaram nos Painéis de Delphi para a determinação do índice de risco dos documentos, Enf.ª Conceição Neves, Dr. Pedro Roldão, Enfª Céu Silvestre, Dr. César Telmo, Drª Célia Oliveira, Dª Conceição Martins, Dr. Jorge Crespo, Dr. Narciso Pinheiro, Dr. Miguel Capão Filipe, Enf. Carlos Jorge, Dr. Frederico Cerveira, Enf.ª Vera Maia, Enf.º Luís Coquim, Enf.ª Graça Costa,

Enf.ª Vera Maia, Enf.ª Clara Ribeiro, Enf.ª Graça Martins, Enf.ª Ana Cláudia, Enf.º Luís Instrumento, Enf.ª Isabel Lopes, Enfª Paula Morais, Enf.º Carlos Pascoal, Enf.ª Isabel Gonçalves, Enf.ª Fátima Almeida, Enf.º Vasco Monteiro, Enf.º Inácio Costa, Enf.º Carlos Lourenço, Enf.ª Beatriz Branco, Enf.ª Clara Monteiro, Enf.ª Catarina Fonseca, Enf.ª Paulo Mendes, Enf.ª Sandra Ferreira, por terem partilhado o seu conhecimento e experiência, contribuindo assim para os resultados deste trabalho.

À Universidade do Minho, à Escola de Engenharia e ao Departamento de Sistemas de Informação pela formação concedida.

À Escola Superior de Tecnologias da Saúde de Coimbra por ter facultado as condições necessárias para levar a bom porto este projecto.

Ao colega Rui Vasco pelo seu apoio e incentivo.

Ao Alexandre, meu irmão, ao José António, ao Nuno Raínho e à Dina Tavares pela permanente disponibilidade e amizade.

Aos meus Pais e meus aos Avós, pelos valores que me transmitiram ao longo da vida, dos quais a perseverança e a capacidade de acreditar que sou capaz, foram fundamentais para ultrapassar os obstáculos que foram surgindo ao longo do trabalho.

Finalmente à Anabela e ao António, por estarem presentes. Pela paciência, pelo incentivo, pelo apoio incondicional e pela tranquilidade que me souberam transmitir.

A todos os outros que, embora não sejam aqui referidos, contribuíram de alguma forma para que fosse possível a elaboração deste trabalho.

Um muito, muito obrigado, a todos.

Este Projecto teve o apoio da Medida 5 – Acção 5.3 – Formação avançada de Docentes do Ensino Superior, integrada no eixo 3, Sociedade de Aprendizagem da Intervenção Operacional da Educação (PRODEP III).

Segurança nos Sistemas de Informação Hospitalares: políticas, práticas e avaliação

Resumo

Orientador

Prof. Henrique Santos

Autor

António Carvalho Santos

Actualmente, a informação é genericamente considerada um recurso crítico para qualquer organização, exigindo políticas de segurança adequadas para a sua protecção. Tipicamente, a abordagem usada para o desenvolvimento dessas políticas, parte da avaliação do risco, que é feita com base no valor do recurso e na probabilidade da concretização das ameaças. Estes dois valores podem ser extremamente difíceis de determinar, especialmente quando a informação não está relacionada com objectos de valor quantificável e/ou quando o historial da ocorrência de incidentes é limitado, como é o caso da informação nas unidades de saúde. Por outro lado, algumas das abordagens existentes para a avaliação do risco consomem um elevado número de meios humanos e financeiros, originando, por vezes, limitações à aplicação do processo de gestão da segurança na organização.

Atendendo a essas limitações, o principal objectivo desta tese foi o de propor uma metodologia para a implementação de políticas de segurança em unidades de saúde. Procurou-se transformar o processo da gestão da segurança em algo que as organizações, nomeadamente unidades do tipo hospitalar, pudessem implementar e gerir de uma forma ágil e natural, sem a necessidade de recorrer a recursos extraordinários. Pretendeu-se, ainda, orientar a metodologia segundo os mais recentes desenvolvimentos ao nível do modelo de gestão dos processos desta natureza, tal como os preconizados pela recente norma ISO/IEC 27001.

Embora a metodologia proposta tenha por base alguns métodos e normas já existentes para a área da gestão da segurança da informação, apresenta soluções inovadoras para alguns dos aspectos mais críticos e que normalmente,

exigem mais recursos. Em particular, são apresentadas soluções para as fases de identificação e catalogação dos recursos (elementos informativos) a serem alvo do processo de segurança e para a determinação do índice de risco de cada recurso. Relativamente a esta última solução, é proposta a utilização da metodologia de Delphi para estimar os dois parâmetros relevantes (o valor do recurso e a probabilidade de concretização de uma ameaça) que são usados para calcular o índice do risco.

Propõe-se ainda uma nova organização para o catálogo de medidas no âmbito da política de segurança, com vista a facilitar o processo da escolha das medidas adequadas e em concordância com a filosofia de gestão da segurança subjacente à metodologia proposta. Este catálogo recolhe, naturalmente, diversos contributos já estabelecidos para outras metodologias.

Por fim, são apresentados os resultados da aplicação da metodologia numa organização hospitalar. Estes resultados demonstram a aplicabilidade da metodologia, ao mesmo tempo revelam a desejada agilidade no sentido de facilmente e naturalmente a integrar no processo de gestão da organização.

Apesar da solução proposta ter sido desenvolvida tendo por base as unidades de saúde, a generalidade dos seus princípios garante que, com algum cuidado e esforço de adaptação, esta metodologia possa ser facilmente alargada a outros tipos de organizações

Healthcare Information System Security: policies, practices e evaluations

Abstract

Advisors

Prof. Henrique Santos

Author

António Carvalho Santos

Nowadays information is recognized as a critical resource, requiring an adequate security policy. Typically the approach most often used for the development of these policies starts with a risk assessment, which is carried out on the basis of the value of the resource's value and/or the probability of threats. These two values can be extremely difficult to determine especially when the information is not related to objects whose values are quantifiable and when the history of the events is limited – which is the case with healthcare information. On the other hand, some of the existing approximations require enormous amount of human and financial resources of the organization, sometimes creating limitations for the application of a security management process in the organization.

Heeding these limitations, the main objective of this thesis was, therefore, to propose a methodology for the implementation of security policies at healthcare providers, but at the same time, try to change security management into something that organizations (in particular the hospital type) could implement and manage in a nimble and natural manner, without resorting to extra resources. Furthermore, there was the attempt to steer the methodology in accordance with the most recent developments concerning management models of processes of this nature, as extolled, for example, by the recent ISO/IEC27001 standard.

Although the proposed methodology is based on some already existing methods and standards in the field of information security management, it presents innovative solutions for some of the most critical aspects that normally require

more resources. Specifically, solutions for the identification and ranking of resources (informative elements) as the target of the security process and for the risk index determination, of each resource. Regarding the last solution, the use of the Delphi methodology is proposed to estimate the two relevant parameters (the resource value and the probability of threats) that are used to calculate the index.

To what concerns the controls to be implemented, it is also proposed an organization for the catalogue of those controls with the purpose of easing the decision making process and guaranteeing consonance with the philosophy of security management which underlies the proposed methodology. Naturally, this catalogue collects diverse contributions already established for other methodologies.

Finally, the results of the application of the methodology to a hospital organization are presented. These results demonstrate the applicability of the methodology and at the same time reveal the desired agility, in the sense of easily and naturally integrating it with the organization's main management process.

Even though the proposal was developed based on a specific healthcare provider, the generality of most of the principles implemented, guarantee that this methodology can easily be generalized to other types of organizations, with some care and effort in the its adaptation.

Índice

Índice de Figuras

Índice de Tabelas

Índice de Fórmulas e Matrizes

Fórmulas

Matrizes

Capítulo 1
Introdução

1.1 Enquadramento

Actualmente, a generalidade das organizações depende fortemente dos sistemas de informação (SI) para o desempenho da sua missão. Deles depende a continuidade e o sucesso das organizações [1]. Ora os SI foram desenhados e desenvolvidos, na maioria dos casos, sem ter em atenção muitos dos requisitos de segurança, actualmente preconizados [2]. Acresce a este facto a ausência, na maior parte das organizações, de uma cultura de segurança da informação.

Um estudo levado a cabo pela Comissão Nacional de Protecção de Dados (CNPD) a 38 hospitais portugueses revelou que não existe um cultura de segurança ou que esta é muito deficitária. Este facto é preocupante se se atender à natureza da informação com que estas organizações lidam [3] [4].

A fim de introduzir uma cultura de segurança nos SI é necessário que cada organização identifique os seus problemas relacionados com a segurança, adopte medidas de segurança adequadas e proceda à monitorização da sua eficácia [5]. Dir-se-à assim, que cada organização deve levar a cabo uma política de segurança.

Dada a diversidade das organizações, é difícil sistematizar um processo genérico de elaboração de uma política de segurança. Deste modo qualquer metodologia genérica necessita de ser adaptada à realidade de cada organização.

A avaliação dos problemas relacionados com a segurança pode fazer-se de várias formas. Uma delas baseia-se no risco que os recursos dos SI apresentam [1].

Um recurso tem tanto maior risco, quanto maior for o seu valor e a sua susceptibilidade a uma quebra de segurança. Na maioria das situações, o valor do risco não é simples de obter, obrigando a proceder a uma complexa análise de dados, o que torna o processo moroso e dispendioso.

A informação resultante da prestação de cuidados de saúde é um conjunto de recursos sensíveis do ponto de vista da segurança. O valor de cada recurso e a sua susceptibilidade a uma quebra de segurança não são conhecidos. Uma forma de os estimar é inquirir os profissionais que lidam com os recursos de forma a obter um consenso. Este consenso pode ser obtido através da técnica de Delphi, que assenta num processo iterativo com base em questionários estruturados. Apesar de criticada por alguns autores, a utilização de questionários, neste caso e devido à ausência de qualquer referencial, afigura-se como uma solução possível. Naturalmente a eficiência deste processo depende fortemente da elaboração dos questionários, nomeadamente da sua estruturação e objectividade.

Na presença dos valores referidos anteriormente é possível determinar a posição relativa de cada recurso em função do índice do risco que apresenta, percebendo assim quais os que, prioritariamente, necessitam de medidas de segurança.

Com base nesta ordenação de prioridades e com o suporte normativo e regulamentar que fornecem algumas medidas de controlo, é possível estabelecer uma política de segurança e dotar uma unidade de saúde de um documento formal de segurança.

1.2 Objectivos

O objectivo deste trabalho é propor uma metodologia para a implementação de políticas de segurança em unidades de saúde, transformando o processo de gestão da segurança em algo de fácil implementação e integrável no processo de gestão da organização. Dado as fortes restrições financeiras que a maior parte das organizações apresenta, a metodologia deve propor um processo de gestão de segurança que consuma o mínimo de recursos financeiros.

Um objectivo paralelo, é o de avaliar e comparar algumas metodologias já propostas com vista a propor eventuais alterações que possibilitem a aplicação mais efectiva da segurança da informação.

1.3 Estrutura da Dissertação

Os principais aspectos da segurança da informação que permitem contextualizar a metodologia proposta nesta dissertação são abordados no capítulo 2. Neste capítulo são definidos, entre outros, os conceitos de segurança da informação, vulnerabilidade, ameaça e política de segurança.

No capítulo 3 são detalhadas algumas das metodologias existentes e é feita uma análise crítica dessas metodologias.

Como toda a problemática da segurança deve estar balizada pelo enquadramento legal, no capítulo 4 apresenta-se a lei portuguesa de protecção da informação. Faz-se, ainda, menção ao enquadramento legal americano, pelo facto deste abordar questões específicas relacionadas com as organizações que prestam cuidados de saúde.

No capítulo 5 aborda-se a problemática da organização interna de uma unidade hospitalar e o seu fluxo de informação.

No capítulo 6 apresenta-se a metodologia proposta para a gestão do risco.

Por fim, no capítulo 7, são apresentadas as principais conclusões do trabalho e algumas perspectivas para trabalhos futuros.

Em anexo apresenta-se uma proposta de catálogo de medidas adaptado à metodologia que se propõe e apresenta-se o resultado da aplicação da metodologia numa unidade hospitalar.

Capítulo 2
Segurança da Informação

Neste capítulo são apresentados os principais conceitos relacionados com a segurança dos sistemas de informação (SI) e a sua evolução ao longo dos tempos.

São, ainda, definidos os conceitos de segurança da informação, risco, ameaça, vulnerabilidade e política de segurança.

2.1 Introdução

A visão da segurança dos SI, por parte das organizações, tem evoluído ao longo dos tempos, acompanhando de resto a própria evolução dos sistemas informáticos [6]. Cada vez mais os SI assumem um papel estratégico e relevante, tornando-se vitais para a organização. Sendo assim, é necessária e obrigatória a existência de um conjunto de mecanismos que os protejam [5] [7].

Nos dias de hoje, é importante ter a informação correcta, no momento certo. Nesta nova fase em que a organização "roda" em torno da informação - (*Information Centric Environment*) – a dependência da grande maioria dos

departamentos é total em relação ao departamento das tecnologias da informação. Devido a este novo paradigma organizacional, as questões relacionadas com a segurança deixaram de ser um problema do responsável do departamento de informática, como acontecia na década de 80, para ser um problema global de toda a organização [6] [5] [8].

Na década de 80 viveu-se uma fase que se poderia designar por "*Computer-Centric*". Nesta fase as organizações eram compostas por um conjunto de departamentos, entre eles o departamento de informática. O departamento de informática prestava apoio aos outros departamentos. A maior parte deste apoio era consubstanciado no processamento em "batch mode" de dados recolhidos em "*off-line*". Isto traduzia um certo isolamento do departamento de informática, de tal forma que possíveis falhas nos sistemas que desenvolviam e mantinham, não afectavam o funcionamento do dia a dia da instituição. Nessa época as questões de segurança tinham como principal objectivo a protecção das infra-estruturas e a operacionalidade dos sistemas. A maior parte das preocupações eram ao nível do controlo de acesso físico aos equipamentos [6].

Numa fase subsequente, com a evolução das tecnologias para as arquitecturas distribuídas, procurando flexibilizar o acesso aos recursos informáticos, o departamento de informática transforma-se num departamento de tecnologias de informação (*information technology departement*), cuja missão é manter um complexo sistema informático e de comunicações que suporta uma grande parte dos processos de negócio [5].

Devido a esta transformação, os outros departamentos organizacionais começam a ficar dependentes da operacionalidade dos sistemas geridos pelo departamento das tecnologias da informação. As tecnologias começam a ser usadas para a automatização das operações do dia a dia e, consequentemente, uma quebra de segurança não afecta só o departamento das tecnologias de informação, mas poderá afectar também os outros departamentos. Nesta fase da evolução, os mecanismos de protecção física utilizados para garantir a segurança dos sistemas deixam de alguma forma de fazer sentido, uma vez que estamos na era dos sistemas distribuídos. Rapidamente os mecanismos de controlo de acesso aos sistemas (identificação do utilizador, validação do

utilizador) e os mecanismos de codificação das comunicações, surgem como mecanismos complementares aos da protecção física [6].

O problema da segurança da informação não se limita a um conjunto de organizações que, devido à sua natureza, lidam com informação secreta ou confidencial. Este problema afecta todas as organizações, sejam elas do sector militar, financeiro, dos serviços de saúde ou de qualquer outro sector de actividade, de natureza pública ou privada [9] [10].

Actualmente a informação é vista como um recurso vital para as organizações, como já foi referido anteriormente. Do ponto de vista da necessidade de segurança deste recurso, não interessa como ele é materializado, se em suporte informático ou em suporte não informático, nem o local da organização onde ele é processado e/ou armazenado [2] [6] [11].

Já na definição dos mecanismos de segurança é necessário não só conhecer as características do suporte da informação, mas também o meio envolvente. Outro factor a ter em conta é o conjunto das vulnerabilidades a que a informação está sujeita e que é o resultado da conjugação das vulnerabilidades do suporte da informação e do meio onde é processada, acedida, armazenada e transmitida [9] [5] [7].

Do ponto de vista da segurança e de uma forma genérica, o sistema de informação de uma organização apresenta vulnerabilidades e está sujeito a ameaças internas e/ou externas à organização (Figura 2.1).

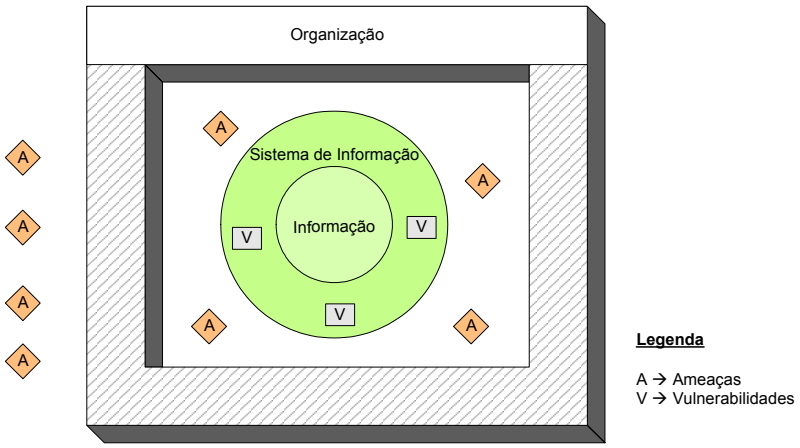


Figura 2.1 - Representação das ameaças e vulnerabilidades num SI

John D. Howard define vulnerabilidade como sendo um ponto fraco do sistema que pode ser explorado através de uma acção não autorizada/esperada, ou seja, não aprovada pelo administrador do sistema e com potencial para provocar danos à organização. No momento em que este ponto fraco seja explorado com sucesso poderá ocorrer uma, ou mais, das seguintes consequências [12]:

- Aumento não autorizado do nível do acesso de um sistema ou de um utilizador;
- Acesso e/ou disseminação de informação por alguém não autorizado para tal;
- Alteração não autorizada da informação;
- Paralisação do sistema de informação;
- Roubo de elementos integrantes do sistema.

Pfleeger apresenta uma definição idêntica para vulnerabilidade e define ameaça como sendo um conjunto de circunstâncias que permitem explorar uma ou mais vulnerabilidades. O mesmo autor propõe que as ameaças sejam classificadas em quatro classes de acordo com as consequências que podem causar [7] :

- **Intercepção** – acesso a um recurso, não estando autorizado para tal;
- **Interrupção** – provocar a negação de acesso a um recurso, quer seja provocando a sua inoperacionalidade, quer seja pelo simples impedimento do acesso;
- **Modificação** – alteração das propriedades de um recurso sem autorização para o efeito;
- **Produção** – adicionar dados ao sistema de informação, ou a um elemento que o constitui, sem ter autorização para o efeito.

Existem outros autores que propõem outras classificações para as ameaças, havendo divergência ao nível da nomenclatura de cada classe, mas preservando os mesmos conteúdos conceptuais [12] [13].

As normas ISO/IEC 17799:2005 e ISO/IEC 13335-1:2004 definem ameaça como sendo algo que potencialmente pode causar um incidente não desejado capaz de produzir um dano no sistema alvo ou na organização.

A norma ISO/IEC 17799:2005 define ainda incidente de segurança da informação como sendo um ou mais eventos que têm uma significativa probabilidade de produzirem dano.

Neste contexto é necessário que cada instituição e os seus diversos níveis organizacionais consigam enumerar as diferentes vulnerabilidades e ameaças, entender a natureza e a relevância dos riscos dos diferentes processos e sistemas, de forma a saber quais as consequências da ausência de segurança e finalmente, estudar as diversas alternativas para uma solução de protecção adequada para a organização [14] [15] [7].

O risco é a medida da potencial perda económica resultante do dano ou perda de um recurso ou investimento. Por outras palavras o risco é a medida da exposição de um determinado sistema, recurso ou entidade ao dano [16] [17].

Conjugando o que atrás foi exposto, a segurança da informação resulta da utilização de um conjunto de medidas que tendem a evitar que as vulnerabilidades dos sistemas sejam exploradas, dentro de um determinado nível de risco considerado aceitável. Essa relação pode ser visualizada através de um diagrama como o que é mostrado na figura seguinte.

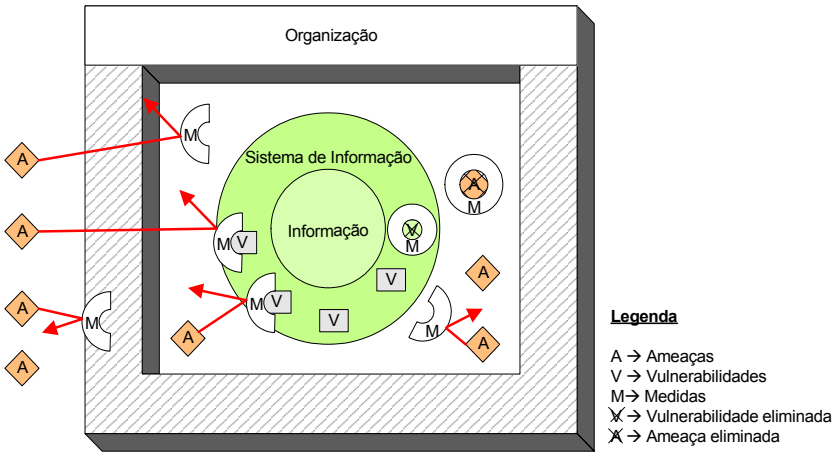


Figura 2.2 - Modelo de Segurança

Para que as medidas tenham o efeito desejado devem estar enquadradas por uma política de segurança da informação que vise garantir um nível de protecção adequado e controlado, para o que é necessário a respectiva avaliação da adequação e eficiência. Desta forma, uma política de segurança é um plano de alto nível que define as linhas orientadoras a seguir para garantir a segurança da informação. Todos os procedimentos operacionais que se venham a implementar na organização deverão estar alinhados com aquelas directrizes [11].

Por outro lado, medidas avulso e não integradas numa política global de segurança, poderão ter um efeito negativo. Um elevado número de empresas adquire produtos de protecção de perímetro da rede de comunicações (firewall, filtros de conteúdo, etc...) ou produtos de retaguarda (sistemas de descoberta de intrusão, anti-vírus, etc...) de elevado custo, sem ter avaliado as vulnerabilidades e ameaças que o sistema de informação apresenta [18] [19]. Peltier cita, no seu livro "Information Security Fundamentals", um estudo levado a cabo pelo Computer Security Institute[1] (CSI), em colaboração com o Federal Bureau of Investigation[2] (FBI), onde se conclui que a ameaça principal (65%) para a segurança da informação são os erros e omissões provocados pelos agentes que, de uma forma directa ou indirecta, usam legitimamente o sistema de informação. Por outro lado, 13% dos incidentes de segurança são provocados por empregados desonestos, enquanto que 10% têm origem em empregados desapontados. Este estudo salienta ainda que são os empregados que conhecem a melhor forma de causar danos aos sistemas de informação das organizações, uma vez que lidam diariamente com eles [20]. De facto só 8% dos incidentes estão relacionados com as falhas nos sistemas de suporte (electricidade, telecomunicações,..), ou com causas externas à organização (tempestades, inundações, fogo, atentados,...) que provocam danos nas estruturas físicas dos sistemas de informação. Finalmente os *hackers* ou *crackers*, estão presentes em cerca de 4% dos incidentes. Apesar desta

[1] http://www.gocsi.com/

[2] http://www.fbi.gov/

percentagem ser baixa, nem sempre os danos causados por este grupo de ameaça podem ser considerados insignificantes, bem pelo contrário.

Atendendo à natureza da política de segurança atrás enunciada e à forma como ela vai interferir nos SI e, consequentemente, na vida da organização, só é possível construir uma boa política se esta estiver enquadrada na vida da própria organização, com a mesma responsabilidade e naturalidade que qualquer outra actividade organizacional.

Segundo Peltier a segurança da informação, e consequentemente a política a ela associada, deve assentar nos seguintes princípios [20]:

- estar alinhada com os objectivos, ou missão, da organização;
- ser suportada por um conjunto de processos compreensíveis e integrados;
- ser avaliada periodicamente com vista à detecção de possíveis desvios e/ou para a implementação de novos mecanismos que contribuam para uma melhoria do processo;
- estar balizada pelos regulamentos, leis ou documentos afins a que a organização está sujeita;
- ter subjacente o controlo do custo/benefício da implementação de medidas. Para tal, é necessário determinar o custo da implementação das medidas e a sua pertinência. Este última parâmetro é determinado com base na análise do risco.

É universal o entendimento de que é necessária a segurança da informação e estudos nesta área recomendam a sua promoção. Porém é utópico afirmar que é possível estabelecer um nível de 100% de segurança. Este nível só seria possível com custos proibitivos [20].

Assegurar um nível óptimo de segurança para a informação não é, nem uma tarefa trivial, nem uma tarefa finalizável, mas resulta de um esforço contínuo de aperfeiçoamento sucessivo [21]. A percepção desta realidade confere à segurança da informação o estatuto de um processo de gestão, o que aliás se identifica nas normas ISO 9001, ISO 14001 e ISO/IEC 27001. As mesmas

recomendam que, para o processo de segurança seja usado o modelo *Plan – Do – Check – Act* (PDCA), em tudo semelhante ao usado nos processos de gestão. Refira-se, ainda, que as recomendações gerais da OCDE são também no sentido da aplicação deste modelo [22] [23].

Importa agora definir segurança da informação, para depois apresentar alguns modelos orientadores do processo de gestão da segurança.

2.2 Conceitos básicos da segurança da informação

A segurança da informação, tal como é definida pela norma ISO/IEC 17799[3], é o conjunto de procedimentos que visa a protecção da informação das ameaças, de forma a assegurar a continuidade da organização, a minimizar o risco e a maximizar o retorno dos investimentos e das oportunidades do negócio.

Tradicionalmente, a segurança da informação é decomposta em três dimensões: confidencialidade, integridade e disponibilidade [9] [7] [6] [24].

Pfleeger defende que é com base na correcta ponderação das três dimensões que é atingido o estado perfeito da segurança da informação. No entanto, por vezes é necessário reforçar uma das dimensões em detrimento das outras, podendo estas últimas ficar fragilizadas. Por exemplo, ao aumentar a disponibilidade (flexibilidade no acesso à informação) potencia-se a diminuição da confidencialidade e da integridade, ao expor demasiadamente a informação [7]. A reforçar este ponto de vista, Peltier afirma que a segurança da informação deve ser vista como um triângulo, em que um vértice é ocupado pela confidencialidade e os outros dois pela integridade e pela disponibilidade, respectivamente [20].

Actualmente esta divisão rígida em três dimensões é colocada em causa. Há autores, como por exemplo Paker D., que rejeitam esta abordagem simples, por acharem que não se encontra adequada às necessidades de segurança que as

[3] Igual tratamento é assumido na família de normas ISO/IEC 27000, das quais a ISO/IEC 27002 irá substituir a ISO/IEC 17799 parte 2.

organizações apresentam actualmente. Com efeito, no seu artigo “Toward a New Framework For Information Security”, 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 [24].

A necessidade de flexibilizar as dimensões da segurança também está presente na própria evolução da norma ISO/IEC 17799. Enquanto que na sua versão de 2000 só eram consideradas as três dimensões clássicas, na versão de 2005 considera-se a possibilidade de adicionar, pontualmente, outras dimensões, tais como autenticidade, responsabilidade, não repúdio e credibilidade.

A confidencialidade é definida pela norma ISO/IEC 17799 como sendo a propriedade da segurança que permite garantir que a informação é acedida exclusivamente por quem tem autorização [9]. Segundo Pfleeger a designação “acedida” deve ser entendida não só como a leitura da informação, mas também como a oportunidade de a visualizar, imprimir ou simplesmente conhecer a sua existência e/ou conteúdo [7].

A integridade é definida pela norma ISO/IEC 17799 como sendo a propriedade da segurança que preconiza os mecanismos necessários para garantir a consistência da informação ao longo do tempo, nomeadamente assegurando que as modificações da informação só são efectuadas por utilizadores autorizados e de acordo com os protocolos estabelecidos.

A disponibilidade, segundo a mesma norma, é definida como sendo a propriedade de segurança que permite garantir que a informação está acessível, a quem de direito, sempre que necessário e na forma correcta.

A norma ISO/IEC 13335-1:2004, para além das propriedades de segurança referidas nos parágrafos anteriores, acrescenta outras possíveis, definindo-as da seguinte forma [25] [8]:

- **Responsabilidade** – propriedade que assegura que uma acção é imputada a uma entidade;
- **Autenticidade** – propriedade que assegura que um recurso é verdadeiro;

- **Não repúdio** – propriedade que permite provar que uma determinada acção ou evento ocorreu efectivamente e qual o seu autor;
- **Credibilidade –** propriedade que garante a confiança sobre o conteúdo da informação.

Em função do exposto, a divisão da segurança em dimensões tem que ser adaptada ao tipo de organização, pois é com base nelas que será definida a arquitectura do processo de segurança de cada organização.

Capítulo 3
Gestão do risco

Neste capítulo apresenta-se a problemática associada à gestão do risco, bem como alguns modelos para a implementação dos processos associados à sua gestão. Nesta apresentação dos modelos inclui-se a apresentação da organização do catálogo de medidas associados a cada modelo, ou referenciados por estes. No final é feita uma análise comparativa entre os diversos modelos.

3.1 Introdução

No contexto da segurança dos sistemas de informação, a gestão do risco é o processo que permite identificar, controlar e eliminar ou minimizar possíveis eventos que possam afectar a segurança dos sistemas de informação [25] [2]. Este processo permite aos gestores estabelecer o balanço operacional e económico das medidas de protecção que a organização deve possuir, de forma a garantir que os seus objectivos sejam alcançados [20] [26]. De uma forma

genérica este processo pode ser dividido em 4 fases de aplicação sucessiva e cíclica [27] [13].

A primeira fase consiste na identificação e determinação do valor do risco associado a cada recurso.

Na segunda fase determinam-se quais as atitudes correctas a assumir, tendo em conta o valor do risco associado a cada recurso. As atitudes possíveis são [28] [20] [29]:

- **Aceitar o risco** – considerar os índices do risco como aceitáveis para a organização, não implementando quaisquer medidas;
- **Reduzir o risco** – implementar medidas de controlo adequadas com o intuito de reduzir o risco para valores aceitáveis para a organização;
- **Anular o risco** – implementar medidas com o intuito de reduzir o risco a zero. Normalmente, esta redução do risco a zero só é conseguida com base na redefinição dos procedimentos organizacionais ou em último caso, com a sua eliminação;
- **Transferir o risco** – imputar o ónus resultante do impacto de acidentes de segurança para terceiros, como por exemplo para uma seguradora.

A opção ou conjunto de opções tomadas nesta fase devem ser escolhidas em função da área de negócio da organização e no âmbito dos seus objectivos. Eloff afirma mesmo que a metodologia usada deve sofrer ligeiras modificações de forma a estar em sintonia e adaptada à organização onde vai ser aplicada [8].

No caso de se optar por reduzir o risco é necessário determinar o conjunto de medidas[4] a implementar. Avaliando o risco de cada recurso é possível decidir da necessidade de aplicação mais ou menos prioritária de medidas.

Com o intuito de ajudar à definição das medidas, existem catálogos de medidas que se podem usar como referência. Todavia, um tipo de classificação das

[4] As medidas são também designadas por “boas práticas” por alguns autores.

medidas, que normalmente não aparece nos catálogos, mas que pode ser útil para a estratégia de segurança da organização é a seguinte [9] [30] [7]:

- **Correcção** – medidas que têm como objectivo reduzir o efeito da ocorrência de um incidente de segurança;
- **Dissuasão** – medidas que visam reduzir a probabilidade de ocorrer um incidente, sem que para tal haja a eliminação da vulnerabilidade ou da ameaça;
- **Detecção** – medidas que permitem prever ou detectar a ocorrência de um incidente. No primeiro caso estas medidas poderão "disparar" medidas preventivas e, no segundo caso, medidas de correcção;
- **Diversão** – medidas que pretendem criar sistemas fictícios de forma a desviar a atenção dos agentes que podem efectuar um ataque;
- **Prevenção** – medidas que pretendem corrigir a vulnerabilidade, ou eliminar a ameaça, reduzindo assim a probabilidade, ou o impacto, da ocorrência de um incidente.

As medidas devem ser escritas de uma forma compreensiva, para que os funcionários directamente envolvidos as consigam perceber e implementar com eficiência [11].

Outro aspecto a ter em conta é que a definição das medidas não é um processo estanque, mas sim um processo que se deve adaptar à evolução da organização e ser capaz de incorporar novas medidas de uma forma dinâmica ao longo dos tempos.

Por outro lado é importante que as medidas preconizadas sejam concretizáveis, quer no aspecto monetário, quer no aspecto temporal [31].

Apesar de tudo, é necessário ter em conta que, mesmo após aplicar as medidas, existe sempre um risco residual, tal como é ilustrado na Figura 3.1 [25] [1].

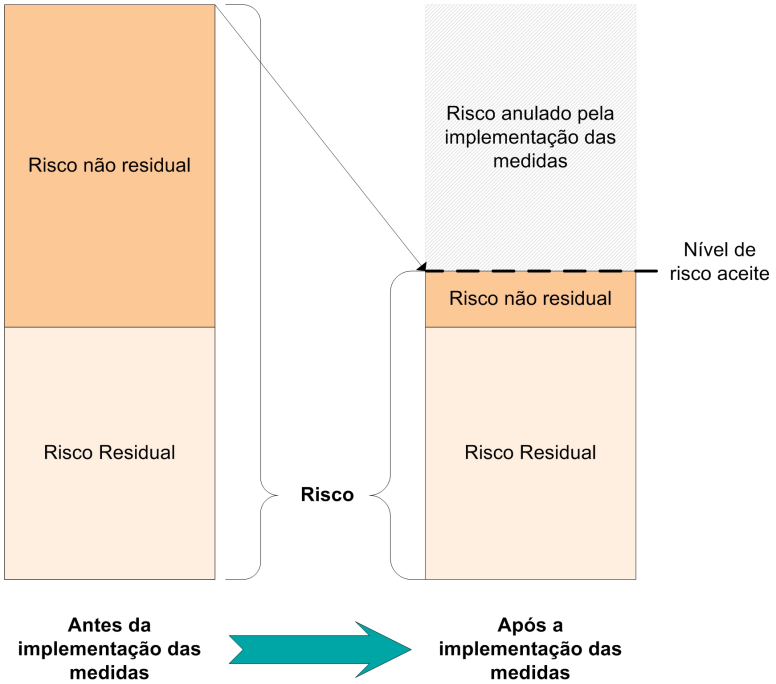


Figura 3.1 – Risco residual

A terceira fase do processo de gestão do risco consiste na implementação das medidas.

Finalmente, a quarta fase consiste em avaliar e monitorizar as medidas implementadas, terminando assim o primeiro ciclo do processo e fornecendo as bases para um novo ciclo.

Existem várias abordagens, mais ou menos elaborados, que pretendem apontar o caminho a seguir na implementação das fases descritas anteriormente. Essas abordagens, de uma forma mais ou menos rigorosa e estruturada, têm na sua génese métodos estatísticos. Para o cálculo do risco são usados os seguintes métodos [3] [8] [5] [1]:

- **Métodos quantitativos** – métodos que recorrem a ferramentas matemáticas e estatísticas para determinar o índice do risco em valor numérico;

- **Métodos qualitativos** – métodos onde o índice do risco é descrito através de adjectivos.

De seguida são apresentados três métodos estruturados para o processo de gestão do risco: o modelo ISO/IEC 13335, o modelo OCTAVE e o modelo ISRAM[5]. A escolha dos modelos OCTAVE e ISRAM prende-se com o facto de ambos terem aplicações descritas na literatura em organizações da área da saúde. Por seu lado o OCTAVE permite a certificação das instituições à luz da lei americana. O modelo ISO/IEC 13335 é de reconhecimento mundial e encontra-se na linha seguida pela *British Standards Institute* (BSI), uma das entidades que desde de algum tempo apresenta normas orientadoras para o processo de gestão do risco.

3.2 Modelo ISO/IEC 13335

A *International Organization for Standardization* (ISO) e a *International Electrotechnical Commission* (IEC) publicam, desde há muito tempo, diversas normas, em diversas áreas, incluindo a área das tecnologias de informação e comunicação, e são reconhecidas a nível mundial. Esse reconhecimento é muito importante não só para o estabelecimento de uma cultura comum, mas também por exigir convergência de compromissos face aos múltiplos interesses instituídos.

Uma das normas definidas pela ISO/IEC para o processo da gestão do risco é a ISO/IEC 13335 [32]. Segundo esta, a primeira etapa no estabelecimento de um processo de gestão do risco na organização, passa por definir quais são os objectivos de segurança. Estes devem estar em sintonia com a missão e a natureza da organização e a respectiva regulamentação legal a que a organização está obrigada. Os objectivos devem também ser definidos com base na relação de dependência da organização dos sistemas de informação. A

[5] Proposto por Karabacak e Sogukpinar.

quantificação desta relação pode estar nas respostas a uma ou mais das seguinte questões:

- Quais são os sectores da organização que dependem directamente dos sistemas de informação? Qual o seu grau de dependência e a sua importância no âmbito organizacional?
- Quais são as tarefas que não podem ser executadas sem o suporte das tecnologias da informação e comunicação?
- Que decisões críticas dependem da integridade e da disponibilidade da informação?
- Que informação deverá ser mantida confidencial?
- Quais as implicações que tem um incidente de segurança para a organização?
- Que nível do risco é aceitável para a organização?

As perguntas anteriores podem igualmente ajudar a definir a estratégia para cumprir os objectivos de segurança estabelecidos.

A norma ISO/IEC 13335 define quatro abordagens diferentes que podem ser usadas na gestão do risco, a saber: a abordagem baseada em boas práticas, a abordagem informal, a abordagem baseada na análise detalhada do risco e a abordagem heterogénea.

3.2.1 Abordagem baseada em boas práticas

De uma forma genérica, a abordagem baseada em boas práticas consiste na aplicação de medidas mais ou menos genéricas e consensuais aos sistemas existentes na organização. Estas medidas resultam de normas, documentos e directrizes cuja aplicação genérica revelou a sua utilidade. A aplicação destas medidas produz um limiar mínimo de segurança sem que para tal haja alterações apreciáveis nos processos de negócio da organização ou um elevado esforço de implementação.

3.2.2 Abordagem informal

A abordagem informal sugere que não seja usado nenhum método estruturado para a gestão do risco. Propõe que a gestão do risco seja implementada com base no conhecimento e na sensibilidade de quem está responsável por este processo.

3.2.3 Abordagem baseada na análise detalhada do risco

A abordagem baseada na análise detalhada do risco, tem como ponto central a análise do risco de cada recurso, cujo o valor é relevante para a vida da organização. A análise detalhada do risco inclui a identificação e determinação do valor de cada recurso do sistema de informação e a determinação da probabilidade da ocorrência de um ataque. Com base nestes valores é calculado o valor do risco de cada recurso e são decididas as medidas a implementar de forma a mitigar o risco.

3.2.4 Abordagem heterogénea

A abordagem heterogénea, cujo modelo de funcionamento se encontra ilustrado na Figura 3.2, propõe que, a partir dos objectivos de segurança, se dividam os sistemas da organização em sistemas críticos e não críticos.

Um sistema é classificado como crítico sempre que se verifique uma ou mais das seguintes condições:

- estar directamente relacionado com a missão (objectivo) da organização;
- ser considerado crítico por imperativo de disposições legais ou éticas;
- estar associado a um investimento elevado por parte da organização.

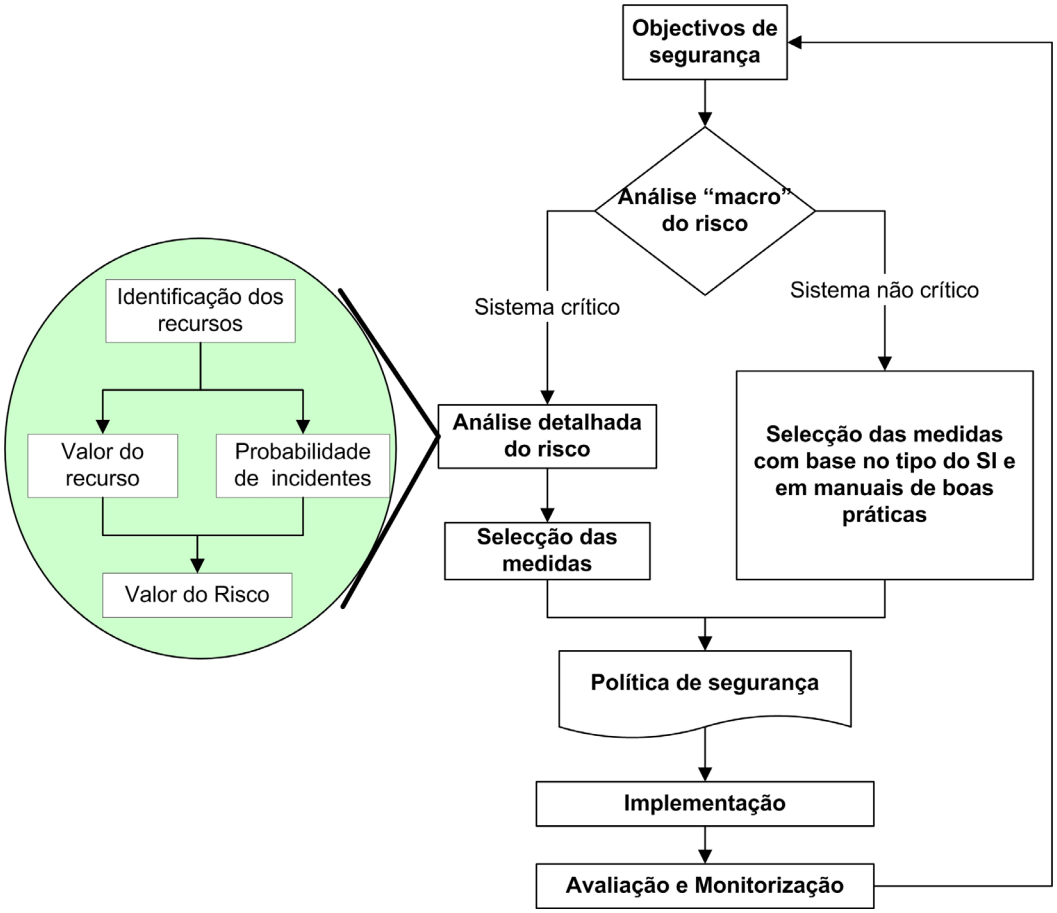


Figura 3.2 - Abordagem heterogénea

De uma forma genérica um sistema poderá ser classificado como crítico sempre que uma quebra de segurança no mesmo provoque um dano elevado à organização, quer ao nível económico ou funcional, quer ao nível da imagem.

Os sistemas críticos serão alvo de uma análise detalhada do risco. Esta análise consiste na identificação dos recursos, seguida da determinação do seu valor e da probabilidade de ocorrer um incidente de segurança que os afecte. Com base nestes dois valores, é possível determinar um índice do risco de cada recurso e assim estabelecer um conjunto de medidas de forma a diminuir este índice.

Aos sistemas classificados como não críticos aplicam-se medidas classificadas como boas práticas. Estas medidas são seleccionadas com base nas características técnicas e funcionais do sistema em causa.

Em muitos aspectos as normas ISO/IEC 13335 e ISO/IEC 17799 são complementares. Por exemplo, a norma ISO/IEC 13335 aponta como uma possível solução para o catálogo de medidas o catálogo que é apresentado na ISO/IEC 17799. Por estes factos, opta-se por apresentar a organização das medidas da ISO/IEC 17799 na secção referente à norma ISO/IEC 13335.

3.2.5 Catálogo de medidas ISO/IEC 13335 e 17799

Catálogo ISO/IEC 13335

A ISO/IEC 13335 apresenta um catálogo de boas práticas organizado de duas formas distintas [33].

A primeira forma do catálogo está organizada segundo duas grandes categorias de medidas: as medidas organizacionais e de segurança física e as medidas de segurança específicas das tecnologias dos sistemas de informação.

A categoria das medidas organizacionais e de segurança física encontra-se dividida nas seguintes sub-categorias:

- **Políticas e Gestão da segurança** – conjunto de medidas relacionadas com a definição do processo de gestão da segurança;
- **Verificação da conformidade** – medidas que têm como objectivo garantir a conformidade da organização, quer com a política de segurança definida, quer com as obrigações legais a que a organização está sujeita;
- **Actuação aquando a ocorrência de um incidente** – medidas que estabelecem os procedimentos a cumprir quando é detectado um incidente de segurança;

- **Boas práticas dos funcionários** – medidas que pretendem reduzir os incidentes de segurança causados por erros intencionais ou não, dos funcionários;
- **Questões operacionais** – medidas que garantem que as funcionalidades dos sistemas de informação são executadas de forma correcta e de acordo com o que está definido;
- **Plano de continuidade** – medidas que visam minimizar o impacto causado pela ocorrência de incidentes;
- **Segurança física** – medidas que pretendem garantir a integridade e a inviolabilidade física das instalações e das infra-estruturas de suporte aos sistemas de informação.

A categoria das medidas de segurança específicas das tecnologias dos sistemas de informação é dividida nas seguintes sub-categorias:

- **Identificação e autenticação** - medidas que têm como objectivo identificar o utilizador e certificar esta mesma identificação;
- **Controle de acesso lógico e auditoria** - medidas que visam limitar o acesso aos recursos só a quem de direito e ao mesmo tempo estabelecer mecanismos de registo e de auditoria dos acessos efectuados;
- **Protecção contra código malicioso** – medidas que pretendem proteger os sistemas da execução e da proliferação do código malicioso;
- **Gestão da rede** – conjunto de medidas que englobam tópicos de planificação, operação e administração da rede de dados de forma a minimizar os incidentes de segurança;
- **Cifra** – medidas que visam implementar procedimentos de codificação da informação.

A segunda forma do catálogo ISO/IEC 13335 encontra-se organizado segundo as dimensões de confidencialidade, de integridade e de disponibilidade. São ainda, apresentadas algumas considerações sobre as medidas a usar para a garantia da responsabilidade e autenticidade. Para cada uma das dimensões de segurança, as medidas estão agrupadas segundo o tipo de incidente que pode afectar a respectiva dimensão.

São considerados incidentes capazes de afectar a confidencialidade os seguintes:

- **Escutas** – a intercepção de uma comunicação entre uma entidade emissora e uma entidade receptora, sem que estas tenham conhecimento de tal acto;
- **Radiação Electromagnética** – a intercepção por terceiros das radiações electromagnéticas que os equipamentos emitem;
- **Código malicioso –** a presença, proliferação ou execução de código malicioso;
- **Usurpação de identidade –** uma entidade que se faz passar por outra de forma a ter os seus privilégios, podendo assim ter acesso a informação indevida;
- **Erro de destino** – se no momento do envio ou do reenvio, da informação houver um engano e, consequentemente a informação for enviada para um destino diferente;
- **Erros nos programas informáticos –** ocorrência de um desvio não previsto na execução de um programa informático;
- **Roubo** – apropriação ou subtracção indevida de componentes do sistema de informação, nomeadamente de componentes que contenham informação confidencial;
- **Acesso não autorizado aos sistemas de informação (computadores, dados, serviços, aplicações)** – o acesso ilegítimo não autorizado a um recurso ou a um sistema;
- **Acesso não autorizado a componentes de armazenamento -** O acesso ilegítimo a componentes de armazenamento da informação.

São considerados incidentes capazes de afectar a disponibilidade os seguintes:

- **Ataque destrutivo** – a destruição do sistema ou de parte dele;
- **Degradação do suporte da informação** – a deterioração do suporte da informação devido a factores físicos, químicos e biológicos;
- **Falha dos canais de comunicação** – inoperacionalidade ou funcionamento defeituoso dos canais de comunicação;
- **Fogo, inundações** – de um modo geral o suporte da informação e os equipamentos constituintes dos sistemas de informação são susceptíveis de serem destruídos pelo fogo ou pela água;
- **Erros de manutenção** – ausência de manutenção ou execução de procedimentos incorrectos durante o processo de manutenção dos equipamentos;
- **Código Malicioso;**
- **Usurpação de identidade**;
- **Uso inapropriado dos recursos** – a utilização anormal dos recursos de forma a provocar a paralisação dos sistema de informação;
- **Desastres naturais** – ocorrência de tempestades, inundações, furacões, etc;
- **Erros nos programas informáticos;**
- **Falha de sistemas complementares** - a falha em sistemas como o ar condicionado, a alimentação eléctrica, entre outros,;
- **Roubo** ;
- **Tráfego excessivo** – um excesso, ocasional, ou não, pode bloquear um canal de comunicação e impedir o acesso à informação;
- **Erros no processo de transmissão** – erros ocorridos no canal de comunicação que provoquem a alteração da informação no momento da sua transmissão;

- **Acesso não autorizado aos sistemas de informação (computadores, dados, serviços, aplicações)**;
- **Uso de programas não autorizados** – a execução de aplicações informáticas ou procedimentos não autorizados;
- **Acesso não autorizado a componentes de armazenamento**;
- **Erros provocados pelos utilizadores** – os erros intencionais ou não dos utilizadores.

Por fim, são considerados os seguintes incidentes capazes de afectar a integridade:

- **Degradação do suporte da informação;**
- **Erros de manutenção**;
- **Código malicioso**;
- **Usurpação de identidade**;
- **Erros nos programas informáticos**;
- **Falha de sistemas complementares**;
- **Erros no processo de transmissão**;
- **Acesso não autorizado aos sistemas de informação (computadores, dados, serviços, aplicações)**;
- **Uso de programas ou procedimentos não autorizados**;
- **Acesso não autorizado a componentes de armazenamento**;
- **Erros provocados pelos utilizadores**.

Catálogo ISO/IEC 17799

O catálogo da norma ISO/IEC 17799 para além de apresentar orientações para o processo de gestão da segurança, sugere um conjunto boas práticas organizadas da seguinte forma:

- **Segurança dos recursos humanos** – conjunto de boas práticas que pretende garantir que os funcionários da organização e as entidades externas que lhe prestam serviços, conheçam e entendam as suas responsabilidades na área da segurança, e que executem correctamente as regras estipuladas;
- **Segurança física** – conjunto de boas práticas que visa prevenir os recursos da organização do acesso físico não autorizado, do dano, da perda ou do roubo;
- **Gestão operacional e comunicação** – Conjunto de boas práticas que têm como objectivo:
  - Assegurar a correcta execução dos procedimentos estipulados;
  - Implementar e manter um nível de segurança da informação adequado nos processos que são executados por entidades externas à organização;
  - Prevenir e detectar a introdução de código malicioso nos sistemas;
  - Estabelecer rotinas de cópias de segurança;
  - Assegurar a segurança da informação quando esta circula na rede de comunicações;
  - Garantir a segurança dos serviços disponibilizados através da Internet, nomeadamente quando se tratam de serviços de comércio electrónico;
  - Estabelecer procedimentos de monitorização para detectar a execução de procedimentos não autorizados ou executados por entidades não autorizadas;
- **Controlo de acessos** – conjunto de boas práticas que pretende controlar o acesso aos recursos da organização;
- **Aquisição, desenvolvimento e manutenção dos sistemas de informação** – conjunto de boas práticas que visa garantir que a

segurança é parte integrante dos sistemas, devendo ser levada em conta no momento do seu desenvolvimento, utilização e manutenção;

- **Gestão dos incidentes de segurança da informação** – conjunto de boas práticas que pretende assegurar que, por um lado haja um processo estabelecido de registo e de comunicação de incidentes de segurança e que, por outro, a organização responda a um incidente com a acção mais correcta;
- **Continuidade do negócio** – conjunto de boas práticas que visa garantir o funcionamento da organização aquando de um incidente que afecte gravemente o sistema de informação ou em situações de catástrofes;
- **Conformidade** – conjunto de boas práticas que pretende garantir que a organização cumpra todas as leis, regulamentações, orientações a que está sujeita ao nível da segurança da informação.

3.3 Modelo OCTAVE

A metodologia OCTAVE (Operaticonal Critical Threat, Asset and Vulnerability Evaluation), encontra-se em fase emergente nos EUA. Esta metodologia, desenvolvida pela universidade Carnegie Mellon University[6], pretende operacionalizar alguns dos aspectos da gestão do risco por parte das organizações.

De acordo com a bibliografia existente, esta metodologia já foi aplicada em várias organizações. São exemplos dessas organizações, na área da saúde, o *Georgetown University Medical Center*[7] e a rede de hospitais da região de Washington DC [34] [35] [36].

[6] http://www.cert.org/octave/

[7] A metodologia OCTAVE foi aplicada no Departamento de Radiologia.

De acordo com esta metodologia e à semelhança de outras, a gestão do risco compreende um conjunto de fases que podem ser divididas em dois grupos. No primeiro grupo o objectivo é a avaliação dos riscos e a indicação das formas como se devem tratar esses riscos. O segundo grupo é composto pelas fases de implementação e monitorização das medidas.

A metodologia OCTAVE detalha como devem ser conduzidas as diferentes fases do primeiro grupo e limita-se a efectuar algumas considerações sobre as restantes fases do processo de gestão do risco.

O modelo OCTAVE propõe seis grandes tarefas (ou fases) para a gestão do risco, que são:

- **Identificar** – identificação dos recursos e das suas propriedades em termos de segurança. Nesta fase, são ainda identificadas as ameaças a que cada recurso está exposto, bem como as vulnerabilidades que a infra-estrutura tecnológica apresenta;
- **Analisar** – determinação das prioridades das acções a tomar em função do valor do risco de cada recurso;
- **Planificar** – desenvolvimento de uma estratégia de forma a reduzir o valor do risco que os diversos recursos apresentam. Nesta fase também deverá ser elaborado um plano com vista à implementação das medidas a tomar;
- **Implementar** - como o próprio nome indica, esta tarefa consiste na aplicação das medidas estipuladas;
- **Monitorizar** – consiste na actividade de acompanhamento do processo, avaliando a eficiência do plano estipulado e, em simultâneo, detectando o surgimento de novos riscos ou alterações na organização, que motivem uma nova iteração do processo de gestão do risco;
- **Controlar** – esta tarefa consiste na análise dos resultados obtidos na fase de monitorização e a consequente identificação de possíveis correcções à implementação do plano de redução do risco. Estas correcções podem variar desde pequenas alterações à política de

segurança e/ou à sua implementação, até à reavaliação do risco e à remodelação da política de segurança.

O OCTAVE designa por *avaliação do risco da segurança da informação* (referido frequentemente só por avaliação do risco) as fases de identificação, análise e uma parte da fase de planificação que diz respeito ao desenvolvimento da estratégia com vista à redução do risco (Figura 3.3). É, essencialmente para avaliação do risco que o OCATVE propõe procedimentos, directrizes e métodos, como já foi referido anteriormente.

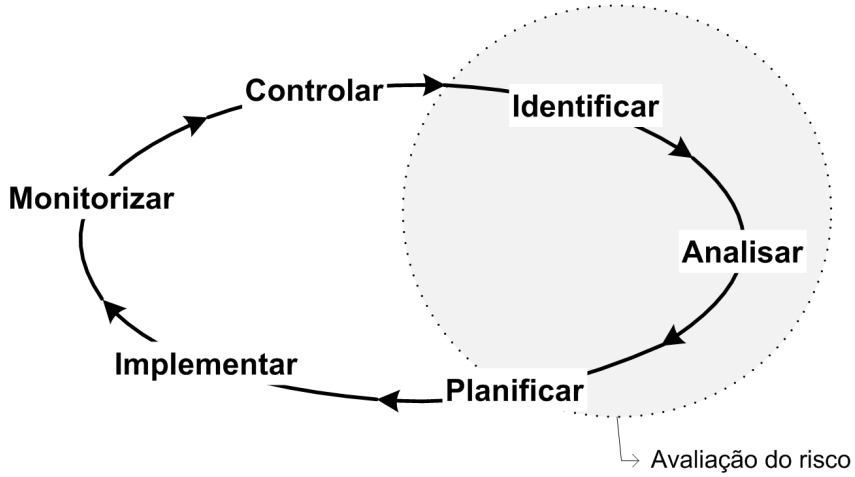


Figura 3.3 - Gestão do risco segundo o OCTAVE

O OCTAVE preconiza um processo de avaliação do risco conduzido, essencialmente, por elementos da própria organização. Para isso, defende que seja constituído um grupo interdisciplinar, designado por equipa, ou grupo, de análise. Esta equipa deverá integrar elementos da área das tecnologias da informação e das outras áreas da organização. A justificação apresentada para a inclusão de elementos ligados à área tecnológica, é que estes conhecem a infra-estrutura tecnológica, a forma de a configurar e de a manter operacional. A inclusão de outros profissionais, por outro lado, enriquece o conhecimento da

equipa, relativamente aos aspectos sociais e organizacionais, dado que estes estão mais ligados à actividade de negócio da organização.

O *Software Engineering Institute*[8] (SEI) desenvolveu um conjunto de directrizes e instrumentos de suporte à implementação da metodologia OCTAVE (OCTAVE Method Implementation Guide v2.0). No entanto a metodologia OCTAVE admite outros caminhos para a sua implementação, mas estabelece que aqueles devem obedecer a um conjunto de critérios vulgarmente designados por *Critério OCTAVE*. Esta abertura da metodologia OCTAVE permite a adaptabilidade do método às diferentes realidades organizacionais.

3.3.1 Critério Octave

O *Critério OCTAVE* aparece como o núcleo central da metodologia OCTAVE, sendo constituído por um conjunto de princípios, atributos e resultados, que qualquer metodologia deve respeitar para estar de acordo com a filosofia OCTAVE.

Assim define princípios ao nível do processo de avaliação do risco, da gestão do risco e da cultura organizacional. Os princípios que devem reger a condução do processo de avaliação do risco são os seguintes:

- **Auto–administração** - Capacidade de o método ser aplicado pela própria organização sem ter que recorrer a entidades externas. A condução de todo o processo, quer ao nível da avaliação do risco quer ao nível da tomada de decisão sobre as eventuais medidas a implementar, deve ser da responsabilidade interna da organização;
- **Adaptabilidade à evolução** - Todo o processo deve ser definido tendo em conta a rapidez com que os sistemas de informação e as tecnologias associadas, evoluem. O processo de avaliação do risco deverá conter mecanismos para prever e actuar perante essas alterações nos sistemas de informação;

[8] http://www.sei.cmu.edu/

- **Caracterização do processo** - Todo o processo de avaliação do risco, deve estar definido e documentado. Entre os parâmetros definidos devem estar o nome do responsável da condução do processo, quais os procedimentos que compõem o processo, quais as ferramentas e os instrumentos que se vão utilizar, qual o formato dos documentos que se irão produzir, nomeadamente os documentos dos resultados;
- **Processo contínuo e cíclico** – O processo da avaliação do risco, deve ser implementado de forma a promover que a gestão do risco faça parte da rotina diária da organização, e seja um processo contínuo.

Em relação ao processo de gestão do risco os princípios exigidos são os seguintes:

- **Visão evolutiva** - A equipa deve ter uma visão estratégica do futuro sobre os problemas da segurança da informação e não se limitar só aos problemas que foram identificados na avaliação do risco;
- **Centralização nos recursos críticos** – Este princípio impõe que todo o processo de gestão do risco esteja centrado nos recursos que apresentam um índice mais elevado do risco. Esta centralização faz com que o processo de gestão do risco produza resultados num curto espaço de tempo, mesmo com uma reduzida equipa de recursos humanos e com uma dotação orçamental não muito elevada;
- **Gestão integrada** - Este princípio garante que as políticas de segurança e as estratégias desenvolvidas no decurso do processo de gestão do risco, demonstrem consistência e alinhamento com a política geral da organização.

Os princípios organizacionais e culturais têm por objectivo criar um suporte organizacional ao processo de gestão da segurança, alargado a todos os actores que lidam com os recursos envolvidos na política de segurança. É de salientar

que estes princípios não são exclusivos do domínio da segurança da informação e são hoje considerados fundamentais para que a organização tenha sucesso. Os princípios organizacionais a respeitar são os seguintes:

- **Comunicação aberta** – Este princípio defende que devem ser criadas formas ágeis de comunicação e divulgação da informação, inerentes ao processo da gestão do risco. Esta comunicação é essencial quer na fase de avaliação do risco, quer nas fases seguintes. Esta política exige a definição clara e exacta dos procedimentos de comunicação entre as diversas estruturas organizacionais e pode ser dinamizada através da realização de seminários ou inquéritos (estes associados ou não a técnicas de consenso);
- **Perspectiva globalizante** – Em todo o processo deve haver uma visão global da segurança da informação. Contudo, deverá ser definida uma estratégia que, apesar de olhar para a organização como um todo, tenha uma atenção particular à segurança da informação dos sistemas directamente relacionados com a principal missão da organização;
- **A equipa** - Na organização deverá existir uma equipa multidisciplinar responsável quer pela condução, quer pela operacionalização de todo o processo. Cabe igualmente a esta equipa, a definição das estratégias a seguir bem como das metodologias a usar.

Os atributos que o *Critério Octave* impõe estão relacionados com os princípios que foram enumerados anteriormente. Os atributos são pois as propriedades resultantes de cada princípio. Por exemplo para o princípio *equipa* é imposto que a equipa seja composta por elementos da organização em causa e tenha um carácter multidisciplinar. Além disso, ao longo do processo de avaliação, esta equipa deverá ter a capacidade de implementar uma estratégia de enriquecimento dos seus conhecimentos sobre a problemática da segurança. Deverá ainda, ter a capacidade e a flexibilidade de incluir novos elementos, de forma temporária ou não, eventualmente externos à própria organização, de forma a enriquecer o conhecimento da equipa. Por fim, é imposto que haja a

participação de elementos seniores da organização na equipa de avaliação, e que se fomente o trabalho em equipa, com vista à partilha dos diversos saberes.

O Critério OCTAVE impõe que os resultados observáveis (independentemente da sua forma de registo) no decurso da avaliação do risco sejam os seguintes:

- Identificação dos recursos críticos em função do tipo e da missão da organização;
- Identificação das necessidades de segurança de cada recurso;
- Identificação, explícita, das ameaças a que cada recurso está sujeito;
- Enumeração das medidas, práticas e directrizes que se encontram implementadas aquando da avaliação e que visam garantir a segurança da informação;
- Enumeração de práticas organizacionais inadequadas no que respeita à segurança da informação e que, por si só, constituem vulnerabilidades;
- Enumeração dos equipamentos críticos envolvidos no processamento, transmissão e armazenamento da informação;
- Identificação das vulnerabilidades que a tecnologia apresenta e que originam pontos fracos e de possível exploração, nos sistemas que as integram.
- Para cada recurso crítico enumerar o impacto negativo ou as consequências para a organização, no caso deste recurso sofrer um incidente de segurança;
- Definir o risco de cada recurso crítico tendo por base a probabilidade de ocorrer um incidente e o impacto que este possa provocar;
- Plano estratégico que deverá apontar as linhas orientadoras de como a organização deverá obter um determinado nível de segurança;
- Plano com vista à redução do risco dos recursos críticos.

3.3.2 Catálogo OCTAVE

O catálogo OCTAVE divide as medidas em dois grupos: as de carácter estratégico e as de carácter operacional [13].

O grupo das medidas estratégicas engloba aquelas que têm a haver directamente com as questões de suporte à gestão da segurança, nomeadamente com os processos organizativos, de formação e de actuação que a organização deve apresentar no âmbito da segurança. Estas são divididas nos seis itens seguintes:

- **Sensibilização e treino** – conjunto de medidas que têm como objectivo a sensibilização e o treino dos elementos da organização na área da segurança da informação;
- **Estratégia da segurança** – conjunto de medidas que têm como objectivo definir uma estratégia de forma a que exista uma política de segurança e que esta esteja de acordo com os objectivos da organização;
- **Gestão da Segurança** – medidas que definem o processo de gestão da segurança;
- **Política de segurança e regulamentos** – conjunto de medidas que visa definir a organização do documento formal que representa a política de segurança. Engloba ainda medidas que estabelecem a periodicidade e o modo de revisão da política de segurança bem como a sua conformidade com o quadro legal em vigor;
- **Política de segurança nas relações com terceiros** – conjunto de medidas a considerar, com o intuito de garantir que entidades externas que prestam serviços à organização apresentem um nível de segurança aceitável;
- **Planos de contingência e de recuperação** – conjunto de medidas relacionadas com a definição, implementação e revisão dos planos de contingência e de recuperação no caso de ocorrência de incidentes.

O grupo das medidas de carácter operacional, reúne as boas práticas a ter em conta em relação ao uso dos sistemas de informação e às tecnologias usadas. Este encontra-se dividido em três itens:

- **Segurança física** – conjunto de medidas que visam garantir a segurança física dos sistemas de informação e dos seus elementos. Estas medidas estão divididas em três grupos: procedimentos e planos de segurança física, controlo de acesso físico, monitorização e auditoria da segurança física;
- **Segurança das tecnologias de informação** – conjunto de medidas que tem como objectivo impor níveis de segurança ao nível das tecnologias associadas aos sistemas. Este conjunto de medidas está dividido em sete grupos: "*gestão dos sistemas e da rede", "ferramentas de administração dos sistemas", "monitorização e auditoria da segurança", "autenticação e autorização", "gestão das vulnerabilidades", "cifra"*, e "*arquitectura de segurança"*;
- **Segurança da equipa** – conjunto de medidas orientadas para a protecção de incidentes, cuja origem são os funcionários da organização. Este conjunto de medidas divide-se em dois grupos: *"a gestão dos incidentes de segurança"* e o grupo *"práticas gerais dos funcionários"*.

3.4 Modelo ISRAM

Karabacak e Sogukpinar propuseram o ***I**nformation **S**ecurity **R**isk **A**nalysis **M**ethod* (ISRAM), que não sendo verdadeiramente um modelo de gestão do risco, pretende contribuir para este como uma solução ao nível da análise do risco [5]. Trata-se de um método descrito recentemente e proposto por uma equipa de investigadores e, talvez por isso, pouco aplicada a nível mundial. A referência neste trabalho a esta metodologia prende-se com o tipo de abordagem que ela preconiza para avaliação do risco.

O ISRAM é essencialmente um método quantitativo, embora apresente a possibilidade de o risco ser traduzido por uma expressão qualitativa. Este método apresenta uma formulação matemática para o cálculo do índice do risco, sendo esta formulação sustentada por um conjunto de questionários [37].

O método segue a linha defendida pelo modelo OCTAVE quanto à necessidade de a análise do risco ser feita com o recurso a profissionais pertencentes à instituição.

O ISRAM está dividido em sete fases de aplicação sucessiva, como é apresentado na Figura 3.4.

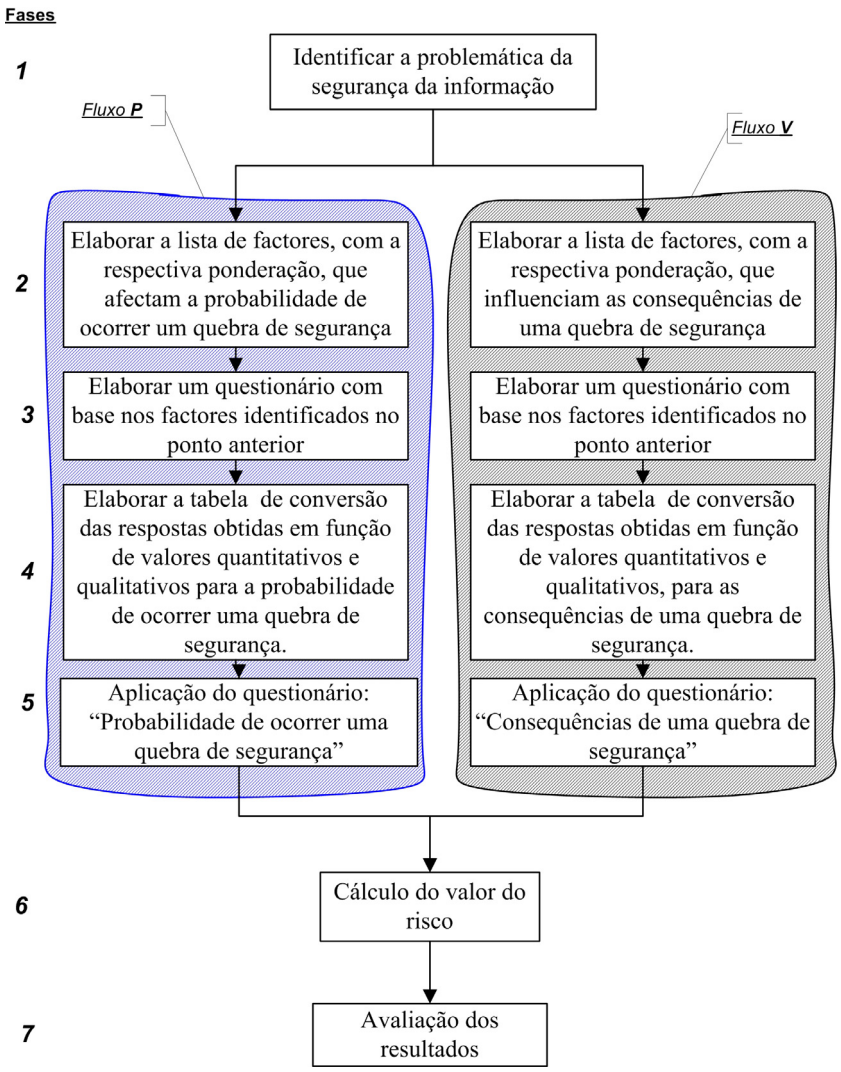


Figura 3.4 - Modelo ISRAM

A primeira fase do ISRAM tem como objectivo principal a identificação do problema de segurança que envolve a organização em estudo. Este levantamento torna-se importante não só para a condução das fases seguintes, mas também para estimular a necessária motivação que os sectores de chefia da organização devem ter em todo este processo.

Após a primeira fase, e até à sexta fase, o método preconiza dois fluxos paralelos de tarefas. Um fluxo está directamente relacionado com a determinação da probabilidade de ocorrer uma quebra de segurança e o outro com a determinação das consequências de ocorrer uma quebra de segurança. Para facilitar a sua identificação o primeiro fluxo será identificado como *fluxo P* e o segundo como *fluxo V.*

Na segunda fase do fluxo P, são listados todos os factores que podem influenciar a ocorrência de uma quebra de segurança. Para a mesma fase no fluxo V, é feito o levantamento de todos os factores que influenciam as consequências que uma quebra de segurança pode originar. Para ambos os casos, deverão ainda ser determinados os pesos relativos de cada factor. Segundo os autores do método, a necessidade de estabelecer a ponderação de cada factor é devida à possibilidade de haver uma maior influência de determinados factores em relação a outros e, naturalmente, influenciar as prioridades da aplicação de medidas.

Segundo os autores a execução da segunda fase deve ser levada a cabo, quer por peritos em segurança, quer por funcionários da organização.

Seguidamente, na terceira fase são convertidos os factores identificados na fase anterior em questões, que irão fazer parte dos respectivos questionários (um para o fluxo P e outro para o fluxo V). Nesta fase ainda é necessário estabelecer qual o formato de cada resposta.

Na quarta fase para o fluxo P é construída uma tabela que permite a conversão dos resultados do questionário no valor da probabilidade de ocorrer uma quebra de segurança. Por seu turno, no fluxo V, procede-se de igual forma, mas agora relativamente ao valor da consequência de uma quebra de segurança.

A quinta fase, consiste na aplicação dos questionários aos utilizadores.

Na sexta fase, é calculado o índice do risco.

O ISRAM usa uma fórmula simples, frequentemente utilizada por muitos autores, em que o risco é o produto da probabilidade de ocorrer uma quebra de segurança pelo valor das consequências a ela associadas (Fórmula 3.1) [27] [5].

$$Risco = \begin{bmatrix} \text{Probabilidade de ocorrer} \\ \text{uma quebra de segurança A} \end{bmatrix} \text{x} \begin{bmatrix} \text{Consequência da ocorrência} \\ \text{da quebra de segurança A} \end{bmatrix}$$

Fórmula 3.1 - Cálculo do risco

Do ponto de vista matemático as parcelas da fórmula anterior são calculadas utilizando a fórmula seguinte:

$$Risco = \left(\frac{\sum_{m} \left[T_1 \left(\sum_{i} w_i \, p_i \right) \right]}{m} \right) \left(\frac{\sum_{n} \left[T_2 \left(\sum_{j} w_j \, p_j \right) \right]}{n} \right)$$

Fórmula 3.2 - Expressão matemática do risco usada no ISRAM

onde:

i – número das questões usadas para determinar a probabilidade de ocorrer uma quebra de segurança;

j – número das questões usadas para determinar a consequência de ocorrer uma quebra de segurança;

m – número de pessoas que participaram no questionário para a determinação da probabilidade de ocorrer uma quebra de segurança;

n – número de pessoas que participaram no questionário para a determinação da consequência de ocorrer uma quebra de segurança;

w_i – peso da questão i;

w_j – peso da questão j;

p_i – valor atribuído (com base numa escala pré-definida) por quem responde ao inquérito;

p_i – valor atribuído (com base numa escala pré-definida) por quem responde ao inquérito;

T_1 – função matemática que transforma o resultado ($\sum_i w_i\, p_i$) de cada questionário, usado para avaliar a probabilidade de ocorrer uma quebra de segurança, num valor qualitativo e num valor quantitativo, segundo uma tabela;

T_2 – função matemática que transforma o resultado ($\sum_j w_j\, p_j$) de cada questionário, usado para avaliar a consequência de ocorrer uma quebra de segurança, num valor qualitativo e num valor quantitativo, segundo uma tabela;

Na sétima e última fase, é feita a análise dos resultados com o intuito de tentar apontar medidas que corrijam os problemas de segurança.

3.5 Análise dos modelos

3.5.1 Análise individual

Nesta secção procura-se fazer a análise de cada modelo apresentado, com o objectivo de identificar os pontos fortes e fracos de cada um, no contexto em questão, para melhor suportar a decisão relativamente à escolha de um deles.

Na Tabela 3.1 são apresentadas as vantagens e desvantagens relativamente à **abordagem baseada em boas práticas** [38]**.**

Vantagens	Desvantagens
• Definição num curto espaço de tempo de uma política de segurança. • Requer o envolvimento de um número limitado de recursos humanos.	• Elevada probabilidade de haver inadequação do nível de protecção dos sistemas. • Não prevê um processo de gestão contínuo, uma vez que não estabelece a necessidade de reavaliação.

Tabela 3.1 - Características da abordagem baseada em boas práticas

As vantagens desta abordagem derivam do facto das medidas a implementar terem por base a simples caracterização dos sistemas de informação. De facto a ausência de uma análise pormenorizada do risco envolve menos recursos mas pode conduzir a um nível excessivo de segurança em alguns sistemas, sem que haja justificação para o efeito. O contrário também poderá acontecer, ou seja, a definição de medidas que conduzam a um nível de segurança demasiado baixo, para outros sistemas de informação.

Relativamente à **abordagem informal** apresenta-se na tabela seguinte o resumo das suas vantagens e das desvantagens [38].

Vantagens	Desvantagens
• Definição num curto espaço de tempo de uma política de segurança. • Requer o envolvimento de um número limitado de recursos humanos.	• Elevada probabilidade de pormenores importantes serem esquecidos ou relevados para segundo plano. • Ausência de justificação objectiva para a necessidade de uma medida. • Não define quem tem a capacidade e os conhecimentos necessários para efectuar a gestão do risco.

Tabela 3.2 - Características da abordagem informal

Novamente as vantagens são justificadas por uma ausência de análise pormenorizada do risco. Trata-se de uma metodologia não estruturada, sem "*checklists*" ou instrumentos equivalentes, permitindo assim que componentes do sistema sejam esquecidos ou relevados para segundo plano. Por outro lado, permitindo a definição da política de segurança com base nos conhecimentos de uma única pessoa, compromete-se a visão global dos problemas da segurança da organização e há maior dificuldade em sensibilizar os diferentes departamentos para a implementação da política definida. Acresce a isto, a dificuldade na definição de quem tem capacidade e conhecimentos para liderar o processo.

A **abordagem baseada na análise detalhada do risco** evidencia as vantagens e desvantagens que são descritas na tabela seguinte [38].

Vantagens	Desvantagens
• Justificação objectiva para a necessidade das medidas.	• Tempo da definição da política de segurança elevado; • Necessidade de recorrer a recursos externos; • Processo oneroso.

Tabela 3.3 - Características da abordagem baseada na análise detalhada do risco

A principal vantagem que a abordagem baseada na análise detalhada do risco apresenta, deriva do facto da escolha das medidas ter por base uma análise pormenorizada do risco. De facto, consoante o valor do risco e os factores que o influenciam, assim se justifica a implementação de uma ou outra medida para proteger o recurso. Contudo, esta identificação do risco associado a cada recurso, normalmente resulta num processo que se arrasta no tempo e quase sempre consumidor de consideráveis recursos humanos e financeiros.

A última abordagem apresentada pela norma ISO/IEC 13335 é a **abordagem heterogénea**. Em resumo, propõe que os sistemas críticos sejam alvo de uma análise detalhada do risco (secção 3.2.3), enquanto que os sistemas não críticos sejam tratados por uma abordagem baseada em boas práticas (secção 3.2.1).

Com a abordagem heterogénea pretende-se de alguma forma minimizar o tempo e os recursos usados e, ao mesmo tempo, garantir um nível de segurança adequado a cada sistema de informação. Nos dias de hoje, estas vantagens são particularmente importantes dado que as organizações têm, geralmente, um número limitado de recursos financeiros e humanos. O principal perigo desta abordagem é o de classificar erroneamente um sistema como não crítico, pelo facto da classificação inicial se basear numa análise pouco pormenorizada. Contudo, dado que o processo de gestão do risco é contínuo e cíclico, um sistema onde se usou uma abordagem baseada em boas práticas pode, noutra fase, ser alvo de uma análise detalhada do risco.

Face ao exposto, das várias abordagens que a ISO/IEC 13335 propõe, a abordagem heterogénea é a que apresenta a melhor relação vantagens/desvantagens. Por este facto, a partir deste ponto do trabalho, quando se referir a metodologia proposta pela ISO/IEC 13335 para a gestão do risco, considera-se a abordagem heterogénea.

Outro modelo apresentado para a gestão do risco foi o modelo **OCTAVE** (secção 3.3). Na tabela seguinte são apresentadas as principais vantagens e desvantagens deste modelo.

Vantagens	Desvantagens
• Implementação por elementos da própria organização; • Justificação objectiva para a necessidade das medidas; • Método estruturado.	• Baseado em reuniões de trabalho; • Tempo da definição da política de segurança elevado; • Requer um número elevado de recursos humanos e financeiros.

Tabela 3.4 - Características do modelo OCTAVE

O modelo OCTAVE tem como vantagem estabelecer que o processo de gestão do risco seja conduzido por elementos da própria organização, não excluindo a participação de peritos externos. A implementação da metodologia OCTAVE exige a realização de várias reuniões de trabalho o que poderá ser uma dificuldade, dada a necessidade de conjugar os horários dos vários elementos da equipa. Além disso, este método apesar de bem estruturado, evidencia uma elevada complexidade na sua execução. Reconheça-se porém, que o modelo OCTAVE permite que a estrutura da sua aplicação seja alterada de forma a tornar-se menos complexa e mais adaptável à organização. A única condição que a nova estrutura tem que apresentar é respeitar o *Critério Octave* (secção 3.3.1).

O **ISRAM**, por seu turno, é uma proposta que detalha a forma de determinar o valor do risco, omitindo ou referindo-se de forma superficial às outras etapas de gestão do risco. À semelhança do OCTAVE é proposto que a análise do risco seja feita por elementos da própria organização**.** O ISRAM propõe que a determinação do risco se faça com base em questionários e recorre a uma fórmula específica para o cálculo do índice do risco. O recurso a questionários torna o cálculo do risco numa tarefa fácil e ágil.

No que respeita ao catálogo de medidas, a norma ISO/IEC 13335 apresenta uma solução onde se agrupam as medidas em função das dimensões de segurança. Todavia, elege as dimensões confidencialidade, integridade e disponibilidade, havendo apenas uma breve referência a outras consideradas importantes.

O catálogo OCTAVE propõe dois grandes grupos de medidas. As medidas estratégicas definem um conjunto de medidas de carácter genérico e independentes da missão de organização. As medidas operacionais (tal como a maioria dos catálogos) têm uma estreita relação com as tecnologias informáticas, o que poderá conduzir à necessidade de acrescentar novos itens aos catálogos, nomeadamente quando os sistemas de informação apresentarem um baixo nível de informatização.

3.5.2 Análise comparativa dos modelos

Para suportar, de forma mais adequada, a decisão relativamente ao modelo a adoptar, faz-se, de seguida, uma comparação global seguindo um conjunto de características consideradas mais relevantes no contexto deste trabalho. Assim os critérios usados foram os seguintes:

- **definição completa do processo de gestão do risco** – este critério reflecte se a metodologia proposta engloba todas as fases do processo de gestão do risco;
- **aplicabilidade a organizações complexas** (com elevado número de recursos) – este critério reflecte a facilidade de aplicação da

metodologia em organizações que apresentem um elevado número de sistemas de informação;

- **abordagem prioritária dos sistemas críticos** – este critério reflecte se a metodologia permite uma aplicação iterativa, abordando numa primeira fase o(s) sistema(s) onde uma quebra de segurança cause um elevado dano;
- **tempo de implementação** – este critério destina-se a avaliar qualitativamente o tempo de aplicação da metodologia ou de um ciclo, no caso em que tal se aplique. Este critério é importante, dado o ritmo acelerado com que ocorrem as mudanças nas organizações. Processos demorados correm o risco de implementar políticas de segurança obsoletas relativamente à realidade;
- **aplicação por elementos internos à organização** – este critério reflecte se a metodologia propõe ou não, que o processo de gestão do risco seja efectuado por elementos internos à organização. A participação dos funcionários neste processo é igualmente importante não só para sensibilizá-los para a problemática da segurança, mas também para os motivar a aplicar as regras para as quais contribuíram;
- **necessidade de recursos humanos e financeiros** – este critério destina-se a reflectir as necessidades de recursos financeiros e humanos. Dadas as restrições financeiras que as organizações normalmente impõem para este tipo de actividades, este é um critério preponderante para a escolha da metodologia;
- **aplicação em unidades de saúde** – este critério destina-se a reflectir se a metodologia foi ou não aplicada em unidades de saúde;
- **apresentação de um catálogo de medidas** – este critério reflecte a existência ou não, de um catálogo de medidas associado à metodologia. Reconhece-se vantagens quando há um catálogo de medidas, uma vez que ele reflecte naturalmente a filosofia subjacente à definição do próprio processo de gestão do risco;

- **universalidade** – este critério reflecte o reconhecimento alargado da metodologia. As organizações reconhecem como uma mais valia a possibilidade de, no final da aplicação de uma metodologia, obterem uma certificação com reconhecimento mundial.

Utilizando os critérios apresentados, faz-se uma avaliação (Tabela 3.5) das metodologias estudadas.

	ISO/IEC 13335	OCTAVE	ISRAM
Definição completa do processo de gestão do risco	Sim	Sim	Não
Aplicabilidade a organizações complexas*	Baixa	Baixa	Média
Abordagem prioritária dos sistemas críticos	Sim	Sim	Não
Tempo de implementação*	Alto	Alto	Baixo
Aplicação por elementos internos	--[9]	Sim	Sim
Necessidade de recursos humanos e financeiros*	Elevado	Elevado	Baixo
Referência de aplicação em unidades de saúde	Não[10]	Sim	Sim
Apresentação de um catálogo de medidas	Sim	Sim	Não
Universalidade	Sim	Não	Não

* - Critério de avaliação subjectivo (resulta da análise da metodologia).

Tabela 3.5 - Comparação dos modelos de gestão do risco

[9] A norma nada refere relativamente a este ponto, mas dada a sua complexidade é provável que haja necessidade de recorrer a consultores externos.

[10] No final da norma ISO/IEC 13335 há uma referência sobre a sua aplicabilidade no domínio das organizações de saúde, mas não existem referências bibliográficas que comprovem a sua aplicação.

Mais uma vez se pode concluir que todas as metodologias têm vantagens e desvantagens.

As metodologias OCATVE e ISO/IEC 13335 são muito parecidas em função destes critérios. No entanto a ISO/IEC 13335 tem reconhecimento mundial e permite que as entidades que a apliquem possam obter uma certificação de reconhecimento nacional e europeu.

Uma metodologia com provavelmente melhor desempenho, poderá então ser aquela que se baseia na ISO/IEC 13335, mas que incorpore algumas das vantagens dos outros métodos.

Capítulo 4
Enquadramento legal

Como foi referido nos capítulos anteriores a política de segurança de uma organização tem de respeitar as leis a que a organização está sujeita.

Neste capítulo faz-se uma análise do enquadramento legal português, o qual deriva da legislação europeia. Mencionam-se ainda algumas directivas legais americanas que focam aspectos específicos da segurança em organizações que lidam com informação clínica.

4.1 Enquadramento legal português

A lei fundamental portuguesa consagra, no artigo 35, que todo o cidadão tenha acesso aos seus dados informatizados, podendo solicitar em qualquer momento a sua rectificação. Além disso o cidadão tem igualmente direito a saber qual a finalidade a que se destina a recolha de dados [39]. O mesmo artigo proíbe o tratamento de dados referentes *a "convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante*

consentimento expresso do titular, autorização prevista por lei, com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis"[11]. É igualmente, proibida a atribuição de um número único a cada cidadão e o acesso a dados pessoais por terceiros, salvo os casos previstos na Lei.

Para efeito do disposto no artigo 35º são equiparados aos dados informatizados os dados constantes em ficheiros manuais.

Em 1998 foi publicada a Lei n.º 67/98 intitulada "Lei da Protecção de Dados Pessoais" que revogou as Leis n.º 10/91- Lei da Protecção de dados pessoais face à Informática" e a Lei n.º 28/94 – Medidas de reforço da Protecção de Dados Pessoais" [40] [41] [42].

4.1.1 Lei n.º 67/98

O objecto da lei n.º 67/98 é a transposição para a ordem jurídica Portuguesa da Directiva 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

Esta lei, no seu artigo 3º, apresenta um conjunto de conceitos que são usados ao longo da sua redacção, dos quais se transcrevem os mais importantes, de forma a se compreender o espírito da Lei. Assim:

- ***"Dados Pessoais** – qualquer informação, de qualquer natureza e independentemente do respectivo suporte, incluindo som e imagem, relativa a uma pessoa singular identificada ou identificável ("titular dos dados"); é considerada identificável a pessoa que possa ser identificada directa ou indirectamente, designadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social*";

[11] N.º 3 do art. 35º da Constituição da República Portuguesa

- ***"Tratamento de dados pessoais ("tratamento")*** *– qualquer operação ou conjunto de operações sobre dados pessoais, efectuadas com ou sem meios automatizados, tais como a recolha, o registo, a organização, a conservação, a adaptação ou alteração, a recuperação, a consulta, a utilização, a comunicação por transmissão, por difusão ou por qualquer outra forma de colocação à disposição, com comparação ou interconexão, bem como o bloqueio, apagamento ou destruição";*
- ***"Responsável pelo tratamento*** *– pessoa singular ou colectiva, a autoridade pública, o serviço ou qualquer outro organismo que, individualmente ou em conjunto com outrem, determine as finalidades e os meios de tratamento dos dados pessoais, sempre que as finalidades e os meios do tratamento sejam determinados por disposições legislativas ou regulamentares, o responsável pelo tratamento deve ser indicado na lei de organização e funcionamento ou no estatuto da entidade legal ou estatutariamente competente para tratar os dados pessoais em causa";*

A Lei n.º 67/98 não se aplica exclusivamente ao tratamento de dados pessoais por sistemas automatizados, mas também a sistemas manuais de tratamento de dados.

No que diz respeito às questões da segurança a Lei n.º 67/98 apresenta uma secção (Capítulo II - Secção III – Segurança e confidencialidade do tratamento) dedicada a este assunto. Nesta secção, no ponto 1 do artigo 14º (Segurança do tratamento) é afirmado: *"O responsável pelo tratamento deve pôr em prática as medidas técnicas e organizativas adequadas para proteger os dados pessoais contra a destruição, acidental ou ilícita, a perda acidental, a alteração, a difusão ou o acesso não autorizados, nomeadamente quando o tratamento implicar a sua transmissão por rede, e contra qualquer outra forma de tratamento ilícito; estas medidas devem assegurar, atendendo aos conhecimentos técnicos disponíveis e aos custos resultantes da sua aplicação, um nível de segurança adequado em relação aos riscos que o tratamento apresenta e à natureza dos dados a proteger*".

A definição e implementação das medidas consagradas no ponto 1 do artigo 14 podem ser subcontratadas a uma terceira entidade, desde que esta ofereça um conjunto de garantias suficientes para a execução de tais tarefas. Nestes casos a entidade subcontratada deverá ser obrigada, por contrato, a cumprir as medidas de segurança que o responsável pelo tratamento de dados definir.

A Lei n.º 67/98 impõe (artigo 15º) que, quando são tratados dados pessoais referentes à saúde, à vida sexual, a dados genéticos, a convicções filosóficas ou políticas, a filiação partidária ou sindical, a fé religiosa, à vida privada e à origem racial ou étnica, sejam definidas medidas adicionais de forma a garantir o cumprimento dos seguintes pressupostos:

a) *"Impedir o acesso de pessoas não autorizadas às instalações utilizadas para o tratamento desses dados (controlo da entrada nas instalações)";*

b) *"Impedir que suportes de dados possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada (controlo dos suportes de dados)";*

c) *"Impedir a introdução não autorizada, bem como a tomada de conhecimento, a alteração ou a eliminação não autorizadas de dados pessoais inseridos (controlo da inserção)";*

d) *"Impedir que sistemas de tratamento automatizados de dados possam ser utilizados por pessoas não autorizadas através de instalações de transmissão de dados (controlo da utilização)";*

e) *"Garantir que as pessoas autorizadas só possam ter acesso aos dados abrangidos pela autorização (controlo de acesso)";*

f) *"Garantir a verificação das entidades a quem possam ser transmitidos os dados pessoais através das instalações de transmissão de dados (controlo da transmissão)";*

g) *"Garantir que possa verificar-se à posteriori, em prazo adequado à natureza do tratamento, a fixar na regulamentação aplicável a cada sector, quais os dados pessoais introduzidos quando e por quem (controlo da introdução)";*

h) *"Impedir que, na transmissão de dados pessoais, bem como no transporte do seu suporte, os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada (controlo do transporte)".*

No entanto, a Comissão Nacional de Protecção de Dados (CNPD), pode em função da natureza das entidades responsáveis pelo tratamento e o tipo das instalações onde o tratamento é efectuado, dispensar a obrigação do cumprimento de alguns dos pressupostos referidos anteriormente.

No artigo 38º da Lei n.º 67/98 são definidas as coimas a aplicar para as entidades que não cumpram[12] as obrigações estabelecidas na Lei, nomeadamente as referidas nos parágrafos anteriores. Estas coimas podem variar entre os 500€ e os 5000€, havendo no entanto situações em que podem ser agravadas até ao valor de 10000€. Além disso, os artigos 43º a 49º da Lei n.º 67/98 definem um conjunto de penas a aplicar pelo incumprimento de obrigações relativas à protecção de dados, e à prática de actos que coloquem ou que violem a segurança dos dados. Assim a moldura penal, mínima, para os crimes cometidos é a seguinte:

- "*Quem, sem a devida autorização, por qualquer modo, aceder a dados pessoais cujo acesso lhe está vedado, é punido com prisão até um ano ou multa até 120 dias"*;
- "*Quem, sem a devida autorização, apagar, destruir, danificar, suprimir ou modificar dados pessoais, tornado-os inutilizáveis ou afectando a sua capacidade de uso, é punido com prisão até dois anos ou multa até 240 dias*";
- "*Quem, obrigado a sigilo profissional, nos termos da lei, sem justa causa e sem o devido consentimento, revelar ou divulgar no todo ou*

[12] Para o efeito da aplicação das coimas é considerado não cumprimento os actos de negligência ou de tentativa.

em parte dados pessoais é punido com prisão até dois anos ou multa até 240 dias".

4.2 Enquadramento Legal Americano

Nos Estados Unidos da América, em 1996, foi publicada a lei 104-191, também conhecida como *Health Insurance Portability and Accountability Act of 1996*, ou simplesmente HIPAA [43] [44].

O HIPAA surge da necessidade de garantir a segurança da informação associada à prestação dos cuidados de saúde, da necessidade de consolidar o formato e as formas de comunicação dos dados de saúde entre as instituições, e da necessidade de normalizar alguns processos das unidades de saúde de forma a minimizar os custos [45].

Todas as entidades americanas que prestem cuidados de saúde ou que tenham acesso a dados provenientes das unidades de saúde, estão abrangidas pelo HIPAA. Ou seja, desde o simples consultório médico ao grande hospital americano, passando pelas companhias de seguros de saúde, todos têm que estar de acordo com as normas definidas no HIPAA.

No seguimento da lei HIPAA foram publicados dois documentos regulamentares, que apresentam um conjunto de boas práticas que as organizações devem implementar de forma a garantir um nível mínimo de segurança da informação. Estes documentos foram a *Security Rule* e a *Privacy Rule [46].*

De seguida descreve-se o HIPAA e os seus documentos regulamentares.

4.2.1 HIPAA

O HIPAA é composto por cinco componentes de regulamentação. Uma componente consiste na regulamentação do uso da informação clínica de cada utente, nas instituições de saúde, tendo em conta o direito de cada um à privacidade. A segunda componente de regulamentação é na área da segurança

dos registos electrónicos, no que diz respeito a questões organizacionais, técnicas e físicas dos sistemas. As outras componentes de regulamentação, que se encontram de alguma forma relacionadas, dizem respeito à definição do formato a usar para a transferência de informação clínica e administrativa entre duas entidades, ao uso de identificadores únicos para cada um dos intervenientes na prestação de cuidados de saúde e ao uso de códigos, ou designações, *standards* nos registos electrónicos que contêm as informações de saúde [47].

Ao nível estrutural o HIPAA encontra-se dividido em 5 capítulos [48].

O primeiro capítulo intitulado “Health Care Access, Portability, and Renewability”, estabelece as normas para a circulação da informação no sistema se saúde Americano, nomeadamente, quando há necessidade de transferir informações entre as unidades de prestação de cuidados de saúde e as entidades que suportam financeiramente esse cuidados.

O HIPAA apresenta um segundo capítulo intitulado “Preventing Health Care Fraud and Abuse; Administrative Simplification; Medical Liability Reform” que pretende criar boas práticas administrativas (algumas delas directamente relacionadas com as questões de segurança) associadas à prestação de cuidados de saúde.

O HIPAA contempla ainda os capítulos “Tax-Related Health Provisions”, “Application and Enforcement of Group Health Plan Requirements” e “Revenue Offsets”, que são capítulos que não estão directamente relacionados com a problemática da segurança [43] [48] [45].

Apesar de toda a regulamentação apresentada no HIPAA estar direccionada para a indústria da saúde, o HIPAA tenta igualmente, de alguma forma educar e informar os doentes sobre os direitos que eles têm sobre a confidencialidade da sua informação clínica/administrativa.

O HIPAA, defende que, no primeiro contacto do doente com a instituição de saúde, este seja informado, notificado, sobre que dados o sistema de informação vai conter a seu respeito, quem vai ter acesso, como é que ele pode aceder à informação que lhe diz respeito, quais são as medidas de segurança e, por fim, qual será o uso destes registos [49].

No respeitante à segurança, a regulamentação apresentada no HIPAA encontra-se dividida em quatro categorias. A primeira categoria diz respeito às imposições de segurança ao nível organizacional, a segunda ao nível da necessidade de definir barreiras físicas no acesso, a terceira ao nível da tecnológico e, por fim a quarta está relacionada com a comunicação e transmissão da informação [48].

O HIPAA impõe ainda que seja definido, de um modo formal, como a informação é processada e quais os mecanismos destinados a garantir a sua segurança. Em particular no que respeita ao processamento de informação sensível, o HIPAA exige que sejam estabelecidos mecanismos formais para o controlo de acessos.

Ao nível organizacional ainda é imposto que sejam definidos os procedimentos de auditoria das políticas de segurança, os procedimentos de gestão da segurança e as sanções a aplicar quando as directrizes de segurança não são cumpridas.

4.2.2 Security Rule

Enquadrada pelo HIPAA, o *Department of Health and Human Services* (DHHS) publicou, em Fevereiro de 2003, uma regulamentação intitulada "*Health Insurance Reform: Security Standards; Final Rule",* que vulgarmente é conhecida por *"Security Rule"*.

A *Security Rule* especifica um conjunto de procedimentos administrativos, organizacionais, técnicos e físicos que as unidades de saúde (ou entidades que tenham acesso a dados de saúde) devem implementar, de forma a garantir a segurança da informação que se encontra em formato digital [45] [50].

A *Security Rule* encoraja as organizações a melhorar as suas infraestruturas tecnológicas, com o objectivo de aumentar o nível de segurança da informação e, paralelamente, a eficiência da organização.

No entanto, a *Security Rule* é neutra em relação à tecnologia a usar, ou seja, indica quais são os requisitos que o sistema deve apresentar, sem que haja uma imposição de uma determinada tecnologia.

A *Security Rule* impõe que ao nível organizacional e administrativo as organizações, que estejam abrangidas pelo HIPAA, cumpram os seguintes itens:

- Definir e implementar políticas e procedimentos para prevenir, detectar, conter e corrigir situações de incidentes de segurança. Esta gestão de segurança deverá conter a análise do risco, a gestão do risco e as sanções a aplicar quando há incumprimento das regras;
- Identificar de forma inequívoca quem é o responsável pelo desenvolvimento e implementação das políticas de segurança da informação;
- Definir e implementar políticas e procedimentos de forma a assegurar que os utilizadores dos sistemas de informação tenham um nível de acesso adequado às suas funções e categorias profissionais, nomeadamente no que diz respeito ao acesso a registos electrónicos de dados clínicos protegidos;
- Definir um plano de formação no âmbito da segurança da informação, que deverá abranger todos os funcionários da instituição, sem excepção;
- Definir políticas e procedimentos que permitam caracterizar um incidente de segurança, quando ele ocorrer;
- Definir um plano de contingência, a implementar em situações de emergência, nomeadamente quando ocorrer um incêndio, um acto de vandalismo, um desastre natural, e que provoquem dano nos sistemas que contêm informação clínica sensível em formato digital. Este plano deverá conter, naturalmente, os planos de cópias de segurança e de restauro dos registos electrónicos e os planos de actualização e de teste do próprio plano de contingência;
- Definir e implementar políticas de forma a garantir que as entidades externas que necessitem de aceder a informações protegidas, apresentem uma política de segurança que garanta o mesmo nível de segurança que a organização que detém os dados.

Ao nível da segurança física a *Security Rule* impõe que as organizações cumpram os seguintes itens:

- Definir e implementar políticas e procedimentos para limitar o acesso físico aos sistemas informáticos, de forma a diminuir a possibilidade de acesso indevido à informação protegida e sensível;
- Definir e implementar políticas e procedimentos segundo as características físicas e o fim a que se destina cada componente do sistema informático;
- Definir e implementar políticas com o objectivo de garantir a segurança física dos dispositivos de armazenamento amovíveis que contenham dados que necessitem de protecção.

No capítulo das boas práticas da segurança associadas à tecnologia de suporte dos sistemas de informação, a *Security Rule* impõe que sejam cumpridos os seguintes itens:

- Definir e implementar procedimentos tecnológicos para os sistemas de informação que contenham tecnologias informáticas, de forma a existir a implementação de níveis de acesso à informação;
- Implementar procedimentos tecnológicos de forma a registar e a analisar as actividades dos sistemas de informação;
- Definir e implementar políticas e procedimentos tecnológicos de forma a garantir a protecção dos dados em formato digital, principalmente no que diz respeito à protecção contra a alteração ou a destruição indevida;
- Definir e implementar medidas de segurança de forma a garantir que, quando transmitida através de redes informáticas a informação não seja acedida por pessoas ou sistemas não autorizados.

4.2.3 Privacy Rule

Em Agosto de 2002 o DHHS, também na sequência do HIPAA publicou o "*Standards for Privacy of Individually Identifiable Health Information; Final Rule*", também conhecido simplesmente por "*Privacy Rule"* .

A regulamentação *Privacy Rule* inúmera um conjunto de boas práticas a ter em conta de forma a proteger a privacidade e a confidencialidade da informação clínica dos utentes do sistema de saúde americano [51]. A *Privacy Rule* tem, ainda, o objectivo de dotar os utentes das unidades de saúde do controlo efectivo sobre os seus dados clínicos, dando forma a uma das exigências do HIPAA. Assim, a *Privacy Rule* estipula que no primeiro contacto do utente com a unidade de saúde, este seja informado e notificado sobre os dados que o sistema de informação vai conter a seu respeito, quem lhes pode aceder e como ele próprio pode aceder a essa informação [49]. Além disso, *Privacy Rule* define os critérios para o uso de informações referentes aos utentes em estudos científicos, bem como as sanções para as situações de violação da privacidade e da quebra de confidencialidade dos dados clínicos.

A *Privacy Rule* classifica a informação em função do uso e da necessidade (ou não) de autorização para o seu processamento [52]. Desta forma, define uma categoria que diz respeito às informações que são usadas no decurso do processo de prestação ou de facturação dos cuidados de saúde. Noutra categoria engloba o uso de dados que, estando abrangidos pela necessidade de protecção, são usados em pesquisas científicas, necessitando para isso de autorização dos utentes. Por fim, define noutra categoria as informações relacionadas com a prestação de cuidados de saúde e que podem ser usadas sem a necessidade de qualquer tipo de autorização. No entanto, para que um registo se enquadre nesta categoria é necessário que não contenha qualquer informação que, por si só ou conjugada com outra, permita identificar a que utente pertence o registo. Desta forma o registo não deverá conter, entre outros, os campos com o seguinte conteúdo:

- nomes;

- referências geográficas ou administrativas que identifiquem áreas inferiores às de um estado[13], nomeadamente nome de ruas, nomes de bairros, nomes de cidades, códigos postais;
- datas relacionadas directamente com o utente, por exemplo, data de nascimento, data da admissão, data da alta, data da morte. Apenas se admite a referência ao ano;
- números de telefones;
- números de fax's;
- endereços de correio electrónico;
- números da segurança social ou similares;
- número do processo clínico;
- números identificativos dos seguros ou planos de saúde;
- matrícula de veículos;
- dados biométricos;
- imagens da face ou de partes do corpo que permita identificar o utente;
- qualquer código único que esteja atribuído ao utente.

É ainda permitido às entidades usar métodos estatísticos para substituir o conteúdo dos campos que contenham as informações atrás referidas, desde que não haja campos cujo conteúdo permita identificar um utente em concreto.

[13] Região administrativa americana.

4.3 Análise crítica

Nos EUA existe uma regulamentação específica para as organizações que lidam com informação associada à prestação dos cuidados de saúde. Não se deve extrapolar as leis de um país para o outro, no entanto a lei americana poderá servir como um documento orientador na área da segurança. O OCTAVE por exemplo, é uma metodologia desenhada para a gestão do risco e que baseia os seus princípios de segurança no HIPAA e em toda a regulamentação que lhe está associada. Por este facto, existem organizações americanas que optam pelo OCTAVE como forma de cumprirem o enquadramento legal a que estão obrigadas.

O enquadramento legal português, bem como a situação das organizações portuguesas na área da saúde é bem diferente. Repare-se no "*relatório de auditoria ao tratamento de informação de saúde nos hospitais"* produzido pela Comissão Nacional de Protecção de Dados (CNPD) [4].

Este relatório teve como base a análise de 38 hospitais portugueses. Do estudo efectuado podem retirar-se as seguintes conclusões:

- a generalidade dos hospitais apresentam uma taxa elevada (cerca de 50%) de tratamentos de dados, sem a prévia e devida notificação à CNPD;
- a generalidade dos hospitais apresentam graves lacunas no que diz respeito ao direito de informação e de acesso que cada doente tem relativamente ao seus dados;
- há incumprimento generalizado do que alei estipula para o uso dos dados dos doentes para fins de investigação científica;
- a CNPD encontrou situações em que foram instaladas aplicações informáticas de gestão da prestação de cuidados de saúde, sem o conhecimento e controlo da direcção do hospital;
- foram encontradas 54 situações em que se usava telemedicina nos hospitais estudados. Em nenhum desses casos havia notificação à CNPD. Sobre este assunto é escrito: "*... Nenhuma destas esperiências de telemedicina se encontra notificada à CNPD, facto que explica um*

desconhecimento generalizado sobre as regras de segurança adoptadas, a inexistência de quaisquer regras escritas ou cláusulas de responsabilidade decorrentes de um eventual erro de diagnóstico, bem como a adopção de procedimentos para assegurar o direito de informação dos doentes";

- outro facto observado, prende-se com a falta de garantias efectivas de que o processo clínico não possa sair do hospital, correndo-se o risco de não estar disponível quando necessário.

Pelos resultados que a auditoria da CNPD produziu, apesar de estar confinada à análise de 38 hospitais, há fortes indícios de que, na generalidade das organizações que lidam com informações provenientes da prestação de cuidados de saúde, existem graves lacunas na área da segurança da informação. 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.

Face ao resultados da auditoria, a comissão CNPD recomenda que os hospitais invistam mais em formação e sensibilização dos utilizadores, de forma a evitar a ocorrência de incidentes, assim como na explicação (escrita) dos procedimentos que definam as regras de acesso à informação e os critérios de atribuição de códigos de acesso;

Capítulo 5
A informação em unidades de saúde (hospitais)

Neste capítulo apresenta-se o resultado de uma análise relativa aos fluxos da informação nas unidades de saúde, nomeadamente nas unidades hospitalares.

Inicialmente são caracterizados os aspectos organizacionais das unidades hospitalares e a sua relação com o fluxo da informação em função da prestação de cuidados de saúde. Por fim aborda-se o problema da segurança da informação da área clínica/administrativa das unidades de saúde.

5.1 Análise da organização hospitalar

As unidades de saúde classificam-se em unidades de cuidados primários, unidades hospitalares ou em unidades de prestação de cuidados continuados, quando se considera o tipo de cuidados que prestam.

As unidades hospitalares[14] portuguesas, integradas na rede de prestação de cuidados de saúde, do ponto de vista da sua natureza jurídica podem assumir os seguintes estatutos [53] [54] [55] [56]:

- *"Estabelecimentos públicos, dotados de personalidade jurídica, autonomia administrativa e financeira, com ou sem autonomia patrimonial;*
- *Estabelecimentos públicos, dotados de personalidade jurídica, autonomia administrativa, financeira e patrimonial e natureza empresarial (EPE);*
- *Estabelecimentos privados, com ou sem fins lucrativos".*

As unidades hospitalares públicas estão sujeitas a normas legislativas mas que não definem de forma rígida a sua organização interna. O legislador define a organização interna dos hospitais ao nível dos órgãos de gestão, deixando que cada unidade hospitalar determine a sua organização funcional, impondo somente que esta conste do regulamento interno de cada unidade em causa.

A estrutura organizacional irá depender das valências clínicas que estão atribuídas ao hospital e do tipo de cuidados que presta.

De acordo com a lei, os hospitais do tipo EPE apresentam órgãos de administração (Conselho de Administração), de fiscalização (Fiscal Único), de consulta (Conselho Consultivo) e de apoio técnico (Comissão de Ética; Comissão de Humanização e Qualidade de Serviços; Comissão de Controlo da Infecção Hospitalar; Comissão de Farmácia e Terapêutica) [56] [54].

Os hospitais encontram-se organizados[15] em três grandes áreas funcionais a área de prestação de cuidados de saúde, a área de suporte à prestação de cuidados e a área de apoio à gestão e logística [57] [58] [59] [60] [61].

---

[14] *Unidade hospitalar ou hospital* é definida pelo Conselho Superior de Estatística da seguinte forma: "Estabelecimento de saúde dotado de internamento, ambulatório e meios de diagnóstico e terapêutica, com o objectivo de prestar à população assistência médica curativa e de reabilitação, competindo-lhe também colaborar na prevenção da doença, no ensino e na investigação científica."

De acordo com o Decreto Lei 188/2003 estas áreas organizacionais devem ser divididas em departamentos, serviços e/ou unidades funcionais, em função do tipo e da dimensão do hospital [56]. As unidades funcionais são agregações especializadas de recursos humanos e tecnológicos, devendo estar integradas num serviço ou departamento. O serviço é a unidade básica da organização, funcionando autonomamente ou, de forma agregada, em departamentos. O departamento é uma unidade funcional que agrega vários serviços e unidades funcionais.

A área de prestação de cuidados de saúde engloba todos os serviços que prestam directamente cuidados de saúde aos utentes do hospital.

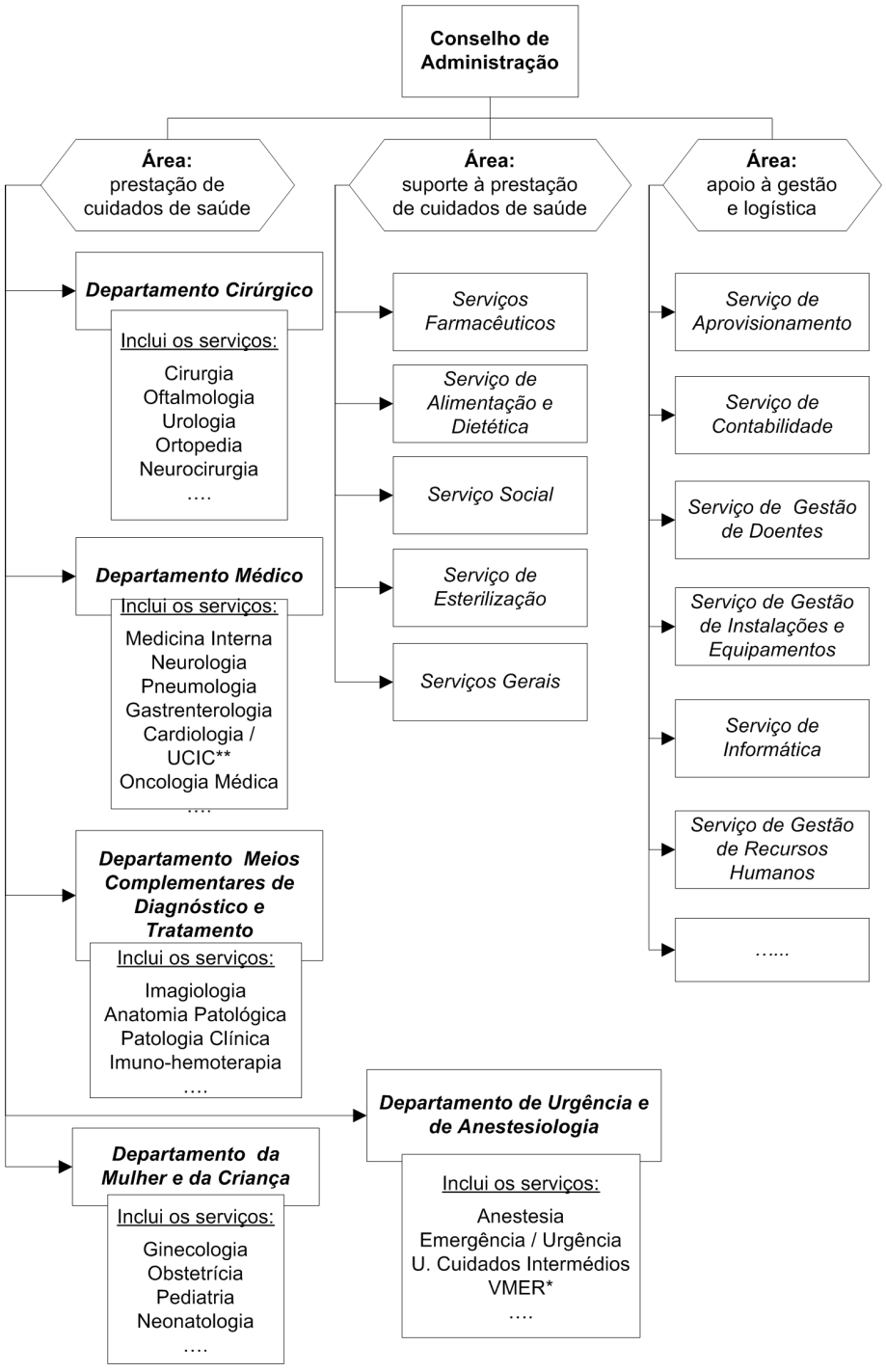
Dependendo da dimensão do hospital e das valências clínicas adstritas a cada unidade hospitalar, de uma forma geral a área de prestação de cuidados de saúde encontra-se dividida nos seguintes departamentos: *Departamento Cirúrgico; Departamento Médico; Departamento da Mulher e da Criança; Departamento de Psiquiatria e Saúde Mental; Departamento dos Meios Complementares de Diagnóstico e Tratamento e Departamento de Urgência* (em alguns hospitais este último departamento é mais abrangente e é designado por *Departamento de Anestesiologista e Cuidados Críticos*).

A área de suporte à prestação de cuidados engloba os serviços farmacêuticos, o serviço de alimentação e dietética, o serviço social, o serviço de esterilização e os serviços gerais.

São normalmente incluídos na área de apoio à gestão e logística os serviços de Aprovisionamento, Contabilidade, Informática, Gestão de Doentes, Gestão Hoteleira, Gestão de Instalações e Equipamentos, Relações Públicas, Gestão de Recursos Humanos, Apoio e Vigilância e o Gabinete Jurídico.

Na figura seguinte apresenta-se um diagrama da organização de uma unidade hospitalar.

[15] Ao analisarem-se vários hospitais, constatou-se que apresentam uma organização interna muito semelhante.



* VMER - Viatura Médica de Emergência e Reanimação
** UCIC – Unidade de Cuidados Intensivos Coronários

Figura 5.1 - Organização hospitalar

5.2 Actividade hospitalar

A missão das unidades hospitalares é, em última instância, a prestação de cuidados de saúde, de forma a restabelecer o equilíbrio físico, psíquico e social do doente.

A prestação de cuidados de saúde é uma actividade que pode ser representada com base no diagrama da Figura 5.2 [62].

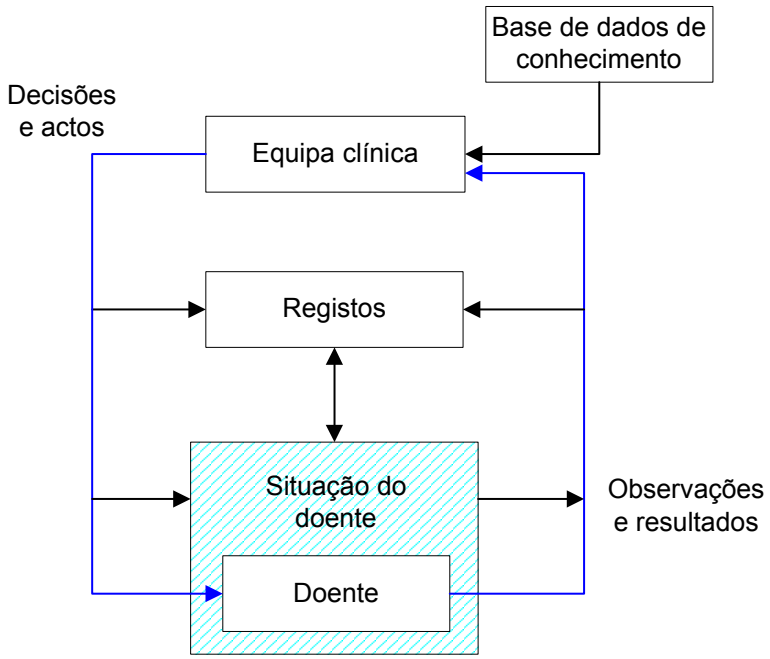


Figura 5.2 - Cuidados de saúde

Como se pode observar, a equipa dos profissionais de saúde recolhe um conjunto de dados acerca do doente e da sua situação clínica (história clínica, parâmetros vitais e dados do exame físico) que, juntamente com o conhecimento adquirido e o conhecimento dos seus pares científicos, servem para a tomada de uma decisão e/ou a prestação de um acto. A decisão ou o acto prestado têm implicações no doente e na sua situação e o ciclo é reiniciado. Nas diferentes fases deste ciclo existe a necessidade de registar informação.

Porém, a prestação dos cuidados de saúde não pode ser analisada como um processo autónomo e isolado, mas sim enquadrado no meio onde é realizado.

Existe um conjunto de outras actividades que são necessárias para garantir a concretização e eficiência da prestação dos cuidados de saúde. Apesar do centro da actividade hospitalar ser a prestação dos cuidados de saúde pelos profissionais de saúde, como já foi referido, para a sua realização são necessárias um conjunto de procedimentos administrativos (o registo, o agendamento, a solicitação de colaboração, etc...), que pertencem a um nível imediatamente envolvente, denominado nível de gestão clínica.

Em torno do nível de gestão clínica, encontra-se o nível de apoio à prestação dos cuidados de saúde que suporta a realização dos mesmos cuidados. Neste nível estão presentes actividades como a realização de exames de diagnóstico, a gestão da farmácia hospitalar, a gestão hoteleira, as comunicações e os transportes. Por fim, existe o nível da gestão hospitalar, que tem como objectivo o controlo da actividade hospitalar.

Para as unidades hospitalares uma das representações possíveis da sua actividade é apresentada na Figura 5.3 [62].

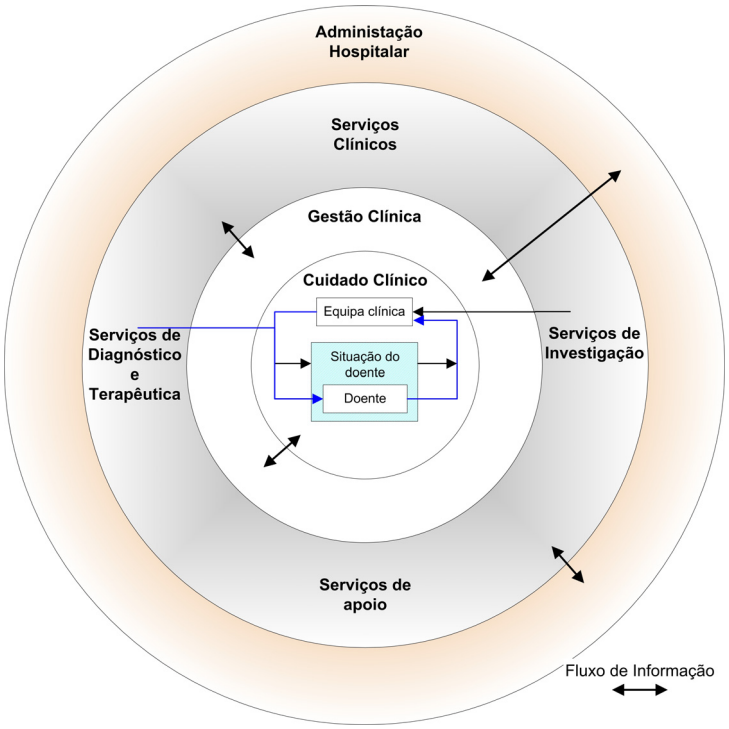


Figura 5.3 - Actividade hospitalar

Cada nível da actividade hospitalar, identificado anteriormente, tem a necessidade de gerar, aceder, processar e armazenar informação quer para as actividades que se encontram afectas a ele, quer para responder a solicitações dos outros níveis.

Tim Benson apresenta no artigo "*Why General Practitioners use computers and Hospital doctors do not – Part 2: scalability*" um diagrama (Figura 5.4) que ilustra o modo de como a informação circula nos hospitais pertencentes ao NHS[16] Britânico [63].

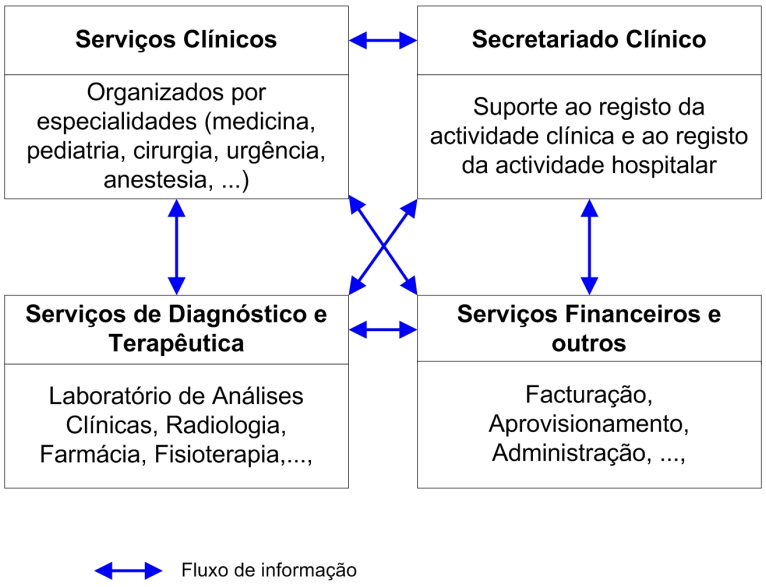


Figura 5.4 - Fluxo de informação hospitalar

Apesar do fluxo de informação dizer respeito aos hospitais Britânicos, ele pode ser extrapolado para a maioria das unidades hospitalares e, com as devidas adaptações (por exemplo a ausência de determinados serviços), à maioria das unidades de saúde.

[16] NHS – **N**ational **H**ealth **S**ervice

Face ao exposto é possível distinguir duas grandes áreas de informação nas unidades de saúde: a área administrativa/económica e a área clínica/administrativa [62] [63].

A área administrativa/económica contém a informação respeitante à organização interna da unidade de saúde, aos seus funcionários, aos seus bens e aos seus fornecedores. Esta informação não está directamente relacionada com a área de negócio da organização e poder-se-á dizer que é transversal a qualquer tipo de organização empresarial [64]. Por exemplo uma unidade hospitalar tem um conjunto de serviços (tais como o serviço de aprovisionamento, de recursos humanos, de informática), que pode existir em qualquer outro tipo de organização.

A área de informação clínica/administrativa é específica das unidades de saúde e diz respeito aos dados clínicos, laboratoriais e imagiológicos relacionados com cada doente. Para além destes dados, também fazem parte da informação clínica/administrativa, os dados referentes ao resultado dos processos administrativos associados à prestação dos cuidados de saúde [65] [66]. Do ponto de vista organizacional, esta área da informação está directamente relacionada com níveis organizacionais de prestação de cuidados saúde e de suporte à prestação de cuidados.

A informação da área clínica/administrativa é passível de ser organizada em função de vários aspectos com se descreve na secção seguinte.

5.3 Taxinomia da informação clínica/administrativa

No contexto deste trabalho e tendo como objectivo a caracterização da informação com vista à aplicação de um processo de gestão do risco, é conveniente organizar devidamente os conceitos que permitem classificar a informação clínica/administrativa de uma unidade hospitalar. Naturalmente serão seguidos alguns dos princípios definidos nas normas anteriormente descritas (gerais e específicas), associados à própria natureza da informação, tal como é compreendida no seio da organização.

A taxinomia a definir não é simples e não é, seguramente, uma solução universal, já que diferentes contextos (sociais, jurídicos e organizacionais), podem impor restrições. Além disso não há na literatura classificações sistematizados no âmbito das unidades de saúde. No entanto, um esforço semelhante será sempre necessário para a implementação de um processo de gestão da segurança da informação.

5.3.1 Definição de recurso e de documento

Define-se recurso como um conjunto de elementos informativos que são gerados aquando da prestação de cuidados de saúde a um doente. De notar que esta definição restringe o conceito mais genérico que é apresentado na ISO/IEC 13335. Porém, tem a vantagem de focar a análise nos aspectos menos tecnológicos dos SI que, neste ambiente, julgamos ser bastante mais relevante. Não obstante, será sempre possível alargar o âmbito do conceito, em ciclos de evolução posteriores. Para simplificar, neste trabalho designa-se este tipo de recurso apenas por documento.

A definição dada de documento pode englobar os elementos informativos que são assimilados pelos próprios profissionais que lidam com eles, mas estes não serão alvo do estudo. Esta decisão deve-se ao facto dessa eventual inclusão conduzir, certamente, a questões de ordem deontológica, saindo claramente do âmbito deste trabalho.

5.3.2 Proposta de organização dos documentos por tipo de episódio

É possível organizar os documentos da área clínica/administrativa referentes a cada doente com base no tipo de episódio que lhe deu origem.

Um episódio, de acordo com a definição do Conselho Superior de Estatística, é o "período que decorre desde a primeira comunicação de um problema de saúde ou doença a um prestador de cuidados, até à realização do último encontro respeitante a esse mesmo problema ou doença" [67].

De uma forma genérica, numa unidade hospitalar podem ser considerados três tipos de episódios: internamento, ambulatório e urgência.

Um episódio de internamento está relacionado com a prestação de cuidados de saúde a um indivíduo que, após ser admitido, ocupa uma cama, para diagnóstico, tratamento ou cuidados paliativos, com permanência de, pelo menos, 24 horas na unidade hospitalar [67].

Um episódio de ambulatório resulta da prestação de cuidados de saúde programados e prestados nas instalações hospitalares, a indivíduos não internados [67].

Um episódio de urgência resulta da prestação de cuidados de saúde prestados numa unidade de saúde em instalações próprias, a um indivíduo com alteração súbita ou agravamento do seu estado de saúde [67].

Esta organização dos documentos com base no tipo de episódio, reflecte, por outro lado, a divisão funcional e espacial que é usada frequentemente nos hospitais. Assim é vulgar encontrar nos hospitais a área do Ambulatório, do Internamento e da Urgência/Emergência. Assumindo que a informação associada a cada um destes episódios é suficientemente independente, este parece ser um bom modelo para promover uma avaliação mais objectiva da informação, com vista à geração de um processo de gestão do risco.

5.3.3 Proposta de organização dos documentos segundo o seu tipo

Os documentos da área clínica/administrativa podem, também, ser organizados em função de algumas propriedades comuns.

Assim há um conjunto de documentos que agrega informação clínica (registos médicos, registos de enfermagem, resultados de exames, relatórios) e que servem para reconstruir, sempre que necessário, a história do episódio a que se refere. Ao conjunto de documentos elaborados num episódio de internamento ou de urgência atribui-se o nome de *Processo de Internamento* ou *Processo de Urgência*, respectivamente. No caso da origem dos documentos ser um episódio de ambulatório, ser-lhes-á atribuído um nome em função da área de ambulatório

a que se referem: *Processo da Consulta Externa*; *Processo do Hospital de Dia* e *Processo da Cirurgia de Ambulatório*.

Outro grupo de documentos é o que serve de suporte à solicitação de exames complementares de diagnóstico, à requisição de produtos (por exemplo, a requisição de produtos hemoderivados, ou a requisição de medicamentos) e à solicitação de consultoria clínica numa área específica. Este grupo de documentos é designado, globalmente, por *Pedidos*.

Designa-se por *Documentos de Saída* o conjunto de documentos que têm como destino entidades externas à unidade hospitalar. São exemplos destes documentos a certidão de óbito, os relatórios da situação do utente com destino ao médico de família e os documentos de comunicação oficial de doenças a determinadas entidades.

É possível definir outro conjunto de documentos, designado por *Documentos Transversais*, que reúne a informação dos diferentes episódios que cada utente teve ao longo do tempo na unidade hospitalar. Um exemplo de um documento que pertence a este grupo, é o processo clínico único.

Por fim, existe um conjunto de documentos designado por *Sistemas Automáticos de Apoio Clínico*, e que engloba os documentos que estão directamente relacionados com o funcionamento desse tipo de sistemas. Estes sistemas existem habitualmente em serviços de doentes críticos, tais como unidade de cuidados intensivos, e efectuam a monitorização do doente, gerem a prestação dos cuidados de saúde (por exemplo a gestão da administração de medicação), etc ...

5.3.4 Proposta de organização dos documentos por serviço ou departamento de origem

Outra possível organização dos documentos da área clínica/administrativa é aquela que se baseia no princípio de agrupar os documentos em função do serviço ou departamento que foi responsável pela sua produção, assumindo que o valor dessa informação varia em função dessa propriedade. Por exemplo, este princípio é facilmente compreendido para os documentos elaborados nos

serviços de Psiquiatria. Dada a natureza das informações que contêm é prática comum que sejam guardados separadamente dos restantes documentos.

5.4 Classes de processos da área clínica/administrativa

Para além da forma como os documentos podem ser organizados, importa também perceber como é que eles são produzidos, manipulados, utilizados e comunicados.

Os documentos da área clínica/administrativa são alvo de um conjunto de processos, ao longo do seu ciclo de vida nas unidades de saúde.

Após uma análise cuidada, é possível estabelecer um conjunto mínimo de processos genéricos a que os documentos da área clínica/administrativa estão sujeitos. Assim, é possível identificar os seguintes processos:

- **consultar** - processo que permite, a quem de direito, aceder a um determinado documento e conhecer o seu conteúdo;
- **criar -** processo que permite que uma entidade origine um documento;
- **editar -** processo que permite a uma determinada entidade alterar o conteúdo de um documento;
- **organizar -** processo que, ao ser executado, permite organizar um conjunto de documentos em suporte de papel;
- **eliminar** - processo que permite a uma entidade eliminar parte ou a totalidade de um documento;
- **comunicar -** processo que permite a transferência de documentos entre duas entidades;
- **armazenar –** processo que reúne todos os procedimentos inerentes à conservação e guarda dos documentos num determinado local.

5.5 Classes de actores

Depois da definição dos documentos existentes numa unidade hospitalar e os processos a que os documentos estão sujeitos, falta caracterizar os actores intervenientes para que seja possível estabelecer um modelo genérico.

Quanto aos actores que podem interagir directa ou indirectamente com os documentos da área clínica/administrativa, é possível estabelecer classes em função do papel que desempenham. Desta forma, identificaram-se as seguintes classes:

- **Equipa médica do serviço** – conjunto de médicos que pertencem ao serviço onde se encontra o doente e que sãos os responsáveis directos pela assistência ao doente;
- **Equipa de enfermagem do serviço** – conjunto de enfermeiros que pertencem ao serviço onde o doente se encontra, para receber os cuidados de saúde;
- **Equipa de auxiliares da acção médica** - conjunto de auxiliares de acção médica que pertencem ao serviço onde o doente se encontra, para receber os cuidados de saúde;
- **Secretariado clínico** - funcionários administrativos que pertencem ao serviço onde o doente se encontra, para receber os cuidados de saúde e que apoiam as tarefas administrativas da equipa médica e de enfermagem;
- **Médicos consultores** – médicos que não pertencem ao serviço onde o doente se encontra e cuja colaboração é solicitada para o doente;
- **Equipa de técnicos de diagnóstico e terapêutica** – conjunto de técnicos de diagnóstico e terapêutica que, apesar de pertencerem a outros serviços, colaboram na prestação dos cuidados de saúde;
- **Outros** – Conjunto de outros funcionários (estafetas, maqueiros, funcionários administrativos e de vigilância) que não pertencem às

classes definidas anteriormente, mas que indirectamente contribuem para a prestação do cuidado de saúde.

5.6 Diagrama funcional da informação num serviço hospitalar

De acordo com o que foi apresentado anteriormente é possível estabelecer um diagrama funcional, que descreva as relações entre os documentos da área clínica/administrativa, os processos e os actores.

Na Figura 5.5 apresenta-se um exemplo de um diagrama funcional, para um episódio de internamento de um serviço genérico designado por ***X***. Os documentos do episódio do internamento no serviço ***X*** estão organizados segundo o seu tipo (secção 5.3.3).

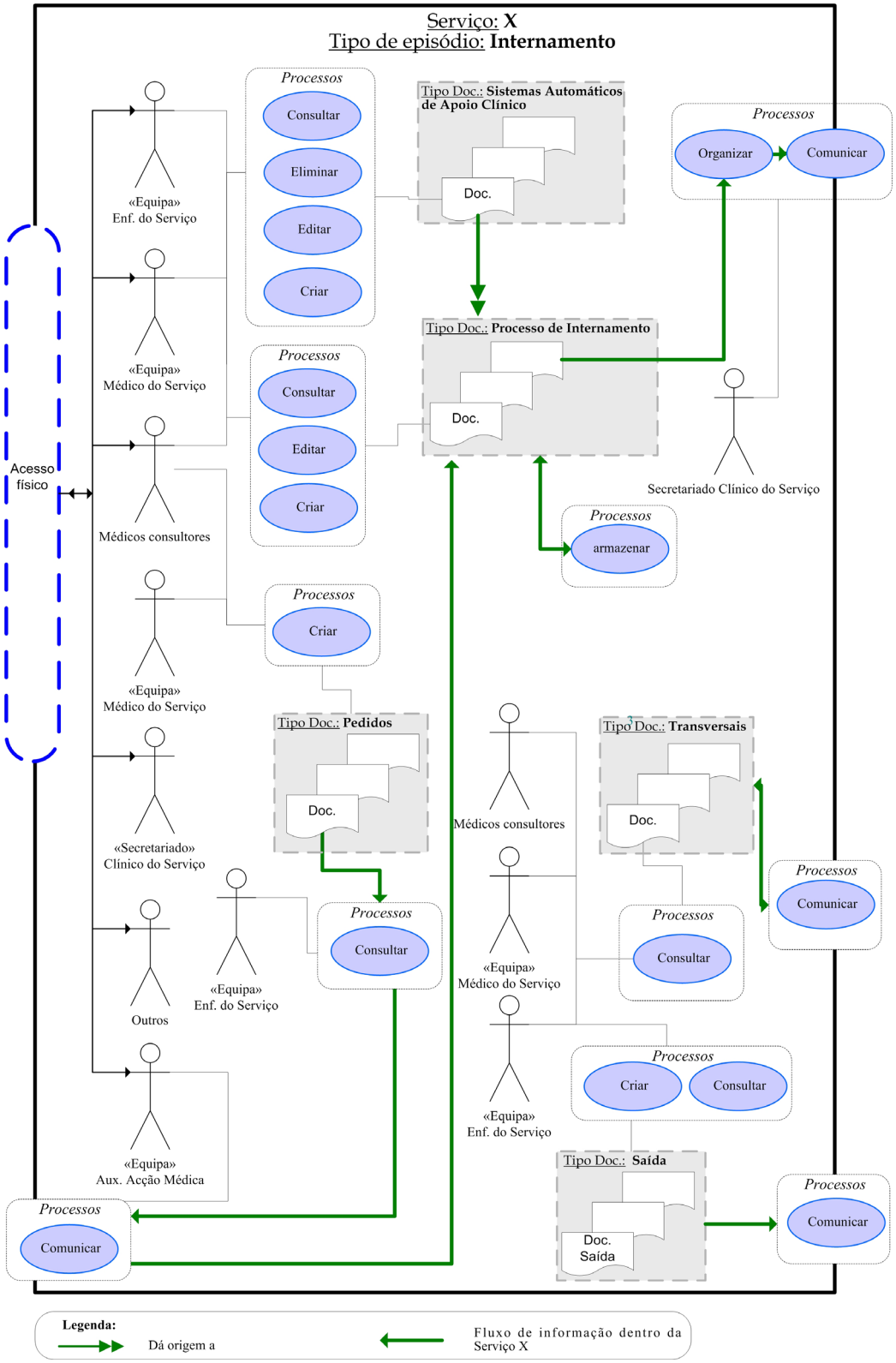


Figura 5.5 - Exemplo da organização da informação com vista à gestão do risco.

5.7 A segurança da informação na área clínica/administrativa

Do ponto de vista da segurança da informação ambas as áreas clínica/administrativa e a administrativa/económica, referidas na secção 5.2, carecem de uma política de segurança [68] [15]. No entanto, dada a natureza distinta de cada área, a atitude por parte da organização no que respeita à segurança da informação tem que ser diferente.

Se uma quebra de segurança na área administrativa/económica pode ser grave para o bom funcionamento da unidade de saúde enquanto "empresa", uma quebra de segurança na área clínica/administrativa pode ser bem mais nefasta [69] [70]. Dada a natureza da informação da área clínica/administrativa, os seus documentos têm necessidades especiais quanto às dimensões da segurança (confidencialidade, disponibilidade e integridade) definidas na secção 2.2.

O conceito de segurança da informação na área clínica/administrativa tem sofrido uma grande evolução. Desde do século 4 AC, que os médicos cumprem o Juramento de Hipócrates, onde está expressa a protecção da privacidade do doente [71]. Porém a noção de confidencialidade da informação clínica já ultrapassou a relação médico/doente, não só pelo surgimento de outros profissionais de saúde, mas também pela evolução tecnológica. Assim o compromisso da "protecção da privacidade" está consagrado na maior parte dos códigos deontológicos das carreiras dos profissionais da área da saúde e actualmente é exigido aos sistemas de informação [49].

As consequências de uma quebra da confidencialidade da informação clínica/administrativa tem muitas vezes um impacto pessoal e social elevado, por exemplo quando são divulgadas informações pessoais como hábitos sexuais, doenças sexualmente transmissíveis, doenças mentais, consumo de droga, entre outras [72] [28].

A confidencialidade da informação, todavia, não é a única componente a ter em conta em relação ao registos clínicos. Também a integridade da informação clínica/administrativa tem uma importância primordial. Uma informação não íntegra, pode conduzir, por exemplo, à aplicação de um tratamento menos adequado, cujas consequências poderão ser graves.

Por último, mas não a menos importante, a disponibilidade da informação, ou melhor dizendo a sua indisponibilidade, poderá acarretar consequências negativas para quem necessita de um determinado cuidado de saúde [28].

Muito autores consideram assim que na área clínica/administrativa se mantêm válida a decomposição da segurança nas três dimensões: confidencialidade, integridade e disponibilidade [19] [28] [73]. Para outros autores esta área tem uma natureza específica e às três dimensões clássicas, consideram que se deve juntar a dimensão autoria/responsabilidade [70] [74] [75] [15] [76]. Esta dimensão é definida como a propriedade que permite conhecer o autor e o responsável por uma determinada informação ou processo. A dimensão autoria/responsabilidade revela-se de importância vital nos dias de hoje, dada a necessidade de determinar com exactidão onde começa e acaba a responsabilidade de cada profissional de saúde interveniente nos cuidados prestados a um doente.

5.8 Síntese

Neste capítulo foi caracterizada a informação presente nas unidades de saúde bem como toda a estrutura organizacional associada a uma unidade hospitalar. Identificaram-se formas de organizar os documentos associados à área clínica/administrativa e classificaram-se os documentos segundo algumas das suas propriedades. Por fim identificaram-se os processos e os actores, bem como a sua interdependência relativamente aos documentos.

Uma vez caracterizada a informação alvo e identificados os processos e actores, na lógica da gestão do risco, estão reunidas as condições para avançar com uma proposta para gestão do risco para as unidades hospitalares, em sintonia com a análise dos modelos de gestão do risco efectuada no Capítulo 3.

Capítulo 6
Metodologia proposta para a gestão do risco

Neste capítulo propõe-se uma metodologia para a gestão do risco, tendo por objectivo a sua aplicação em unidades de saúde. Esta proposta tem em conta a especificidade das unidades de saúde descritas no capítulo anterior e as diversas soluções que existem para a gestão do risco (Capítulo 3).

É ainda apresentada uma reflexão teórica sobre as técnicas de consenso, uma vez que o uso destas técnicas é preconizado pela metodologia proposta.

6.1 Introdução

Talvez em nenhum outro tipo de organização, a importância da informação seja primordial como nas organizações que prestam cuidados de saúde.

Dada a importância da informação nas unidades de saúde e a sua especificidade, o desafio subjacente ao trabalho que aqui se apresenta foi o de criar uma metodologia para a gestão do risco. Tal como já foi referido, esta

deveria ser de fácil aplicação, de reconhecimento universal e permitir conduzir a uma ordenação dos documentos em função do índice do risco que cada um apresenta. Assim, mais importante do que saber o valor exacto do índice do risco de cada documento, é conseguir encontrar o valor relativo de cada documento. Com base nesta posição relativa, é possível estabelecer um plano de actuação, que terá em atenção, em primeira instância, os documentos que apresentam um índice do risco mais elevado [77].

Assim, de acordo com o resultado da análise efectuada no Capítulo 3, a metodologia proposta tem a sua origem na ISO/IEC 13335. Como foi referido na secção 3.5 dentro das várias abordagens que a ISO/IEC 13335 apresenta, a abordagem designada por *abordagem heterogénea* é a que tem a melhor relação vantagens/desvantagens. Contudo, essa abordagem deixa alguns aspectos da sua aplicação em aberto e outros são de difícil concretização ou necessitam que a organização mobilize um elevado número de recursos humanos e financeiros. Por este facto, a metodologia que se propõe, além de assentar os seus alicerces na ISO/IEC 13335, mais propriamente na aproximação heterogénea, vai incorporar vantagens, quer do modelo OCTAVE, quer do modelo ISRAM. Uma consequência da adopção da ISO/IEC 13335 é a abordagem da segurança em função das dimensões de segurança.

Apesar da metodologia proposta estar vocacionada para ser aplicada em organizações de saúde, em particular em unidades hospitalares, ela poderá ser facilmente adaptada a outras realidades.

De seguida são apresentadas e discutidas as diversas etapas que compõem a metodologia proposta para a gestão do risco.

6.2 Objectivos de segurança

A primeira etapa da metodologia que se apresenta, à semelhança do que é preconizado pela ISO/IEC 13335 e em geral por todas as metodologias de gestão do risco, consiste na definição dos objectivos da organização para a segurança da informação.

Em relação a esta etapa propõe-se o uso das directivas preconizadas pela ISO/IEC 13335 e referidas na secção 3.2.

Salienta-se ainda que, além de definir os objectivos de segurança, é necessário definir as fronteiras e o âmbito da gestão da segurança.

6.3 Análise "macro" do risco

Após a definição dos objectivos, a etapa seguinte consiste na *análise "macro" do risco*. Esta etapa serve para classificar os sistemas de informação em críticos e não críticos. Esta divisão permite que a abordagem nos dois grupos seja diferente, por forma a optimizar o processo de gestão do risco minimizando os recursos envolvidos e o tempo de execução.

Como foi referido na secção 5.2 os sistemas de informação de uma unidade de saúde podem ser divididos em dois grupos: os que estão associados à informação clínica/administrativa e os que estão associadas à informação administrativa/económica.

Os sistemas pertencentes ao primeiro grupo estão relacionados com a missão principal da unidade de saúde, que é a prestação de cuidados de saúde. Por outro lado, disposições legais e/ou éticas impõem que estes sistemas garantam a segurança da informação que processam e armazenam.

Os sistemas da área administrativa/económica não estão relacionados de forma directa com a missão da unidade de saúde e estão sujeitos a níveis de segurança menos exigentes decorrentes de imposições legais e éticas.

Assim, e de acordo com a definição[17] que a ISO/IEC 13335 apresenta, todos os sistema de informação da área clínica/administrativa de uma unidade de saúde são classificados como sistemas críticos, enquanto que os sistemas da área administrativa/económica são considerados como não críticos.

[17] Como foi referido na secção 3.2.4 é considerado sistema crítico todo o sistema que esteja relacionado directamente com a missão da organização ou que a lei o assim imponha.

A classificação de um sistema em não crítico na fase inicial da gestão do risco não impede que, num momento posterior, ele seja tratado como um sistema crítico, tal como é preconizado pela ISO/IEC 13335.

Na secção seguinte (Análise detalhada do risco) são descritas as etapas do processo de gestão do risco de que os sistemas críticos deverão ser alvo.

6.4 Análise detalhada do risco

6.4.1 Identificação

A primeira etapa da análise detalhada do risco consiste na identificação dos documentos. Esta tarefa, numa unidade hospitalar, mesmo de média dimensão, pode ser algo morosa devido ao elevado número de documentos existentes.

Para contornar esta adversidade é conveniente procurar definir grupos de documentos a identificar, de forma a reduzir a complexidade do processo. É contudo necessário definir as regras para a constituição dos grupos de documentos. Essas regras devem, sempre que possível, ter em conta a organização interna da unidade de saúde e a sua actividade.

Como foi referido na secção 5.3.2 os documentos podem ser divididos em três grupos (*internamento*, *ambulatório* e *urgência*) de acordo com o tipo de episódio a que se referem. Mesmo usando este critério, o número de documentos a identificar por cada grupo é muito elevado para permitir um processo de avaliação relativamente expedito.

Um outro critério que pode ser utilizado reflecte a estrutura organizacional típica de uma unidade hospitalar, como foi referido no capítulo anterior. Este critério permite agrupar os documentos de acordo com o serviço a que pertencem.

À semelhança do critério anterior, este último, por si só, origina também grupos com elevado número de documentos.

Se se interceptarem os dois critérios anteriores é possível gerar uma matriz como a que é apresentada na Tabela 6.1. Como se pode verificar, cada célula contém um número de documentos mais reduzido em relação ao número de

documentos obtidos por qualquer uma das organizações anteriores. Para além disso, as relações existentes entre os documentos existentes numa célula, permitem antever um conjunto significativo de propriedades de segurança comuns.

Documentos				
Tipos de episódio				
Internamento	***Ambulatório***	***Urgência***		
Grupo I.1	Grupo A.1	Grupo U.1	***Serviço 1***	**Serviços**
Grupo I.2	Grupo A.2	Grupo U.2	***Serviço 2***	
Grupo I.A3	Grupo A.A3	Grupo U.A3	***Unidade A / Serviço 3***	
Grupo I.B3	Grupo A.B3	Grupo U.B3	***Unidade B / Serviço 3***	
Grupo I.4	Grupo A.4	Grupo U.4	***Serviço 4***	
:	:	:	:	
:	:	:	:	
Grupo I.n	Grupo A.n	Grupo A.n	***Serviço n***	

Tabela 6.1 - Grupo de documentos

Coloca-se, agora, a questão de como identificar de forma exaustiva os documentos pertencentes a cada célula (por exemplo identificar todos os documentos que pertencem à célula *Grupo I.1*).

Esta identificação é levada a cabo com o recurso a entrevistas com o Director do Serviço e com o Enfermeiro Chefe do Serviço em causa. Cada entrevista deverá ser estruturada de forma a que os documentos sejam classificados em subgrupos, usando para tal a taxinomia apresentada na secção 5.3.3. Estes subgrupos serão designados por grandes grupos de documentos[18].

[18] Os documentos podem ser classificados segundo os seguintes grandes grupos: Processo de (internamento), Documentos de Saída, Documentos Transversais, Pedidos e Documentos dos Sistemas Automáticos de Apoio Clínico

Tomando como exemplo a célula *Grupo I.1*, a identificação dos documentos que pertencem a esta célula é realizada com o recurso a entrevistas quer com o Director do *Serviço 1*, quer com Enfermeiro Chefe do *Serviço 1*. Os documentos a identificar na célula *Grupo I.1* são os documentos que estão associados a uma situação de internamento no *Serviço 1*.

6.4.2 Agregação

A abordagem heterogénea preconizada pelo ISO/IEC 13335, apresentada na secção 3.2.4, não define nenhuma etapa intermédia entre a identificação dos documentos e a determinação do seu valor.

Apesar de na etapa de identificação se ter proposto uma solução que minimiza o número de documentos que serão alvo de análise do risco em cada grupo, o seu número ainda é demasiado elevado, tendo em vista a agilidade que se pretende para o processo de avaliação a implementar. Torna-se pois imperativo reduzir o número de documentos a avaliar, sem no entanto afectar a sua unidade, que se traduz no conjunto de propriedades comuns e que afectam a respectiva determinação do índice do risco.

A solução consiste em agregar, de acordo com as suas características, os documentos pertencentes ao mesmo grande grupo de documentos. Os pressupostos para a agregação são então o fim a que se destinam e a partilha de atributos comuns e relevantes para o cálculo do risco, por exemplo identificação, dados clínicos, etc. A lógica de agregação resume-se no seguinte enunciado: *se existem dois documentos com um número considerável de atributos comuns, então são candidatos a criar um novo documento, designado por documento genérico, que contém a reunião dos atributos dos dois documentos.*

Seguindo o princípio descrito, nas tabelas seguintes, é mostrada uma organização possível para os documentos genéricos (**DG**) do episódio de internamento, agrupados por grandes grupos (**GG**).

Documento genérico	Descrição
Registo Médico	Engloba todos os documentos inerentes aos registos efectuados pela equipa médica.
Registo de Enfermagem	Engloba todos os documentos inerentes aos registos efectuados pela equipa de enfermagem.
Resultado de Exames	Engloba todos os resultados dos exames efectuados durante o internamento.
Relatório do Sist. Monitorização	Engloba todos os documentos de saída produzidos pelo sistema de monitorização dos sinais vitais e que irão ser anexados ao histórico do episódio de internamento.
Cópia da ocorrência no S.U.	Engloba todos os documentos (cópia) referentes ao episódio de urgência que deu origem ao internamento e que integram o processo de internamento.

Tabela 6.2 - DG do GG Processo de Internamento

Documento genérico	Descrição
Sistema de Monitorização	Engloba os documentos produzidos e adquiridos em tempo real, do sistema de monitorização dos parâmetros vitais do doente.

Tabela 6.3 - DG do GG documentos dos Sistemas Automáticos de Apoio Clínico

Documento genérico	Descrição
Pedido de exames complementares de diagnóstico realizados no hospital	Engloba todos os documentos utilizados para a requisição de exames imagiológicos, de patologia clínica, de imuno-hemoterapia e de anatomia patológica.
Pedido de hemoderivados (Req\Adm)	Engloba todos os documentos utilizados para a requisição e administração de hemoderivados.
Pedido de consulta Interna	Engloba todos os documentos utilizados para o pedido de consultoria médica.
Pedido de receituário de Med. Extra-Formulário	Engloba todos os documentos utilizados para o pedido de medicamentos que não constam do formulário hospitalar.
Pedido de exames complementares de diagnóstico ao exterior	Engloba todos os documentos utilizados para a requisição de exames a entidades externas à unidade de saúde.

Tabela 6.4- DG do GG Pedidos

Documento genérico	Descrição
Documentos de óbito	Engloba todos os documentos preenchidos aquando do óbito de um doente.
Transferência/Envio do doente	Engloba todos os documentos utilizados aquando da transferência de um doente para outra unidade de cuidados de saúde.
Documentos de Alta	Engloba todos os documentos preenchidos aquando da alta do doente.
Documentos para a Comunicação Obrigatória de Doenças	Engloba todos os documentos utilizados para a comunicação obrigatória de doenças.

Tabela 6.5 - DG do GG Documentos de Saída

Documento genérico	Descrição
Registos Administrativos	Engloba todos os documentos relacionados com a parte administrativa do internamento e que irão servir, por exemplo para efeitos de facturação, de elaboração de estatísticas, de gestão de camas e de marcação de exames.
Processo único	Engloba todos os documentos dos episódios anteriores ao internamento que se referem a um doente.

Tabela 6.6 - DG do GG Documentos Transversais

6.4.3 Estimativa do valor de cada documento genérico

Voltando ao modelo adoptado para a análise detalhada do risco, a etapa que se segue, é a estimativa do valor da informação que, neste caso, será estimado para cada documento genérico.

A maior das dificuldades que esta etapa apresenta é a ausência na literatura de qualquer referencial que permita estimar o valor de cada documento genérico.

Se os documentos em causa estivessem ligados a uma área de natureza económica, uma das soluções possíveis seria usar o valor monetário que, naturalmente, lhes estava associado. Não sendo possível esta associação no tipo de documentos com que se está a trabalhar, poder-se-ía pensar em usar as coimas definidas pela lei portuguesa para os casos de se verificar uma quebra de segurança, afim de estimar o valor da informação. Todavia, na legislação portuguesa as coimas e as penas previstas são genéricas, ou seja, não existe uma diferenciação segundo o tipo de documento que foi alvo da quebra de segurança.

Nesta ausência de referências, propõe-se que a estimativa do valor de cada documento genérico seja efectuada com base no valor da percepção do impacto negativo da ocorrência de uma quebra de segurança que afecte o documento.

Atendendo à definição assumida para a segurança da informação e com vista a uma melhor clarificação do efeito de uma eventual quebra de segurança, a

estimativa do valor será efectuada em função das dimensões confidencialidade, integridade, disponibilidade e autoria/responsabilidade. Por outro lado, a análise por dimensão deriva também do modelo ISO/IEC 13335.

Mas, como estimar o valor do impacto negativo segundo cada uma das dimensões? Uma das soluções que se pode adaptar neste contexto, é a utilização de uma técnica de consenso suportada por métodos estatísticos [78].

De acordo com a literatura, existem vários métodos de consenso, como o método de Delphi, o método do grupo nominal e o método da conferência de consenso [79]. As técnicas de consenso mais adoptadas para as questões da área da saúde, quer ao nível clínico, quer ao nível da gestão, são os métodos de Delphi e o método do grupo nominal [80].

De seguida são descritos estes métodos e discute-se qual destes dois se adapta melhor ao problema em questão.

6.4.3.1 Método do grupo nominal

De uma forma resumida, o método do grupo nominal consiste na realização de duas reuniões de forma a obter o consenso sobre um determinado assunto. Para isso, na primeira etapa do método define-se o problema, seguindo-se a selecção do conjunto[19] de peritos que irão propor uma solução. A etapa seguinte consiste na realização da primeira reunião. Nesta reunião todos os peritos devem estar presentes e expor as suas ideias sobre o assunto em análise. Depois de discutidas todas as ideias/sugestões/respostas que foram dadas para cada questão colocada, procede-se a uma votação individual e secreta, com base numa escala predefinida, de forma a pontuar cada uma das ideias/sugestões/respostas em função da sua relevância [79] [80]. Após a votação é realizada a análise estatística e determinada a posição relativa de cada uma das ideias/sugestões/respostas. Esta primeira reunião termina com a apresentação dos resultados.

[19] O número de peritos varia tipicamente entre 9 e 12 elementos.

Na segunda reunião, onde se exige igualmente a presença dos peritos, é efectuada a discussão da ordenação obtida na primeira reunião e procede-se a uma nova votação de forma a obter a ordenação final.

6.4.3.2 Método de Delphi

O método de Delphi, ou o painel de Delphi[20], é um processo estruturado, que visa a obtenção de um consenso sobre um determinado assunto, com base na opinião de um grupo de peritos.

O método de Delphi foi criado na década de 50 pela firma Rand Corporation (Santa Monica, California). Numa fase inicial destinava-se ao uso militar (nomeadamente pela *Americam Armed Forces*), tendo sido permitido o uso civil na década de 60 [81].

Desde o momento em que foi possível o uso deste método em meio não militar, ele tem sido aplicado em áreas que vão desde a educação, aos cuidados de saúde, à engenharia, às ciências sociais, ao turismo e à gestão [78] [82].

Do ponto de vista conceptual o método de Delphi consiste na elaboração e aplicação de uma sequência de questionários a peritos. Cada aplicação do questionário recebe o nome de ronda. Entre cada ronda, o grupo de peritos, especialmente constituído para o efeito, tem ao seu dispor a avaliação estatística da ronda anterior. Os elementos estatísticos normalmente usados são a distribuição de frequência, a média e o desvio padrão das respostas [83] [78] [84]. Serão realizadas tantas rondas quantas as necessárias para obter um determinado grau de consenso [80] [85] [79].

No seu formato original, o processo começa com um questionário aberto (1ª ronda), com o objectivo de descobrir quais os itens relacionados com o estudo em causa. Estes itens, depois de analisados e tratados pelo investigador, irão fazer parte do segundo questionário (2ª ronda) [86] [87].

[20] Em alguma literatura o método de Delphi é designado por painel de Delphi.

Na segunda ronda e seguintes, o painel de peritos é convidado a dar a sua opinião sobre a pertinência de cada item e a sua importância relativa para a questão em causa, podendo cada elemento do painel mudar de opinião, tendo em conta a análise estatística das respostas dadas pelo grupo de peritos na ronda anterior.

Porém, com o intuito de diminuir o número de rondas do processo de Delphi existem algumas variações do método original. De uma forma genérica todas estas versões tendem a restringir o grau de liberdade de respostas na primeira ronda, com o objectivo do método convergir mais rapidamente [88] [89]. Por exemplo, com este intuito há casos de aplicação do método Delphi em que na primeira ronda são indicados os itens que a literatura refere para cada uma das questões colocadas [83] [90].

Um dos pontos cruciais de todo este processo está sem dúvida na escolha do painel de peritos. O perito deve ser alguém imparcial e a informação que ele fornece deve ser o reflexo do seu conhecimento ou da sua percepção actual sobre um determinado assunto [91]. Na maior parte das vezes tenta-se que o painel seja heterogéneo de forma a que nele, estejam reflectidas as diversas sensibilidades sobre o assunto em apreço [86] [92].

Quanto ao número de peritos, a literatura não é consensual, existindo diversas opiniões, especialmente variando com o tipo de estudo que se pretende efectuar. Existem, por exemplo, aplicações do método de Delphi que usam 10, 14, 18, 30, 305, 405 peritos [92] [89] [83] [81] [93].

As rondas pelo painel de peritos devem parar quando se atinge um determinado grau de consenso nas respostas obtidas. Na literatura estão descritos alguns critérios para a determinação desse consenso [92] [94]. Alguns estudos usam a distribuição das frequências das respostas e determinam que se está perante uma situação de consenso quando uma das respostas foi alvo de escolha de pelo menos 51%. Noutros estudos a percentagem de peritos com resposta similar deve ser superior a 75% para que se considere que exista consenso [89] [88].

Outros estudos usam medidas de dispersão, tais como a amplitude interquartil relativa[21], a média e desvio padrão, para determinar o grau ou a evolução do nível de consenso [92] [81].

Há estudos ainda, que usam o coeficiente de alpha de Croanbach [85] [95]. Este coeficiente mede a consistência interna das respostas a um questionário, a partir da qual se pode inferir o grau de consenso.

6.4.3.3 Análise comparativa

Uma das diferenças entre o método do grupo nominal e o método de Delphi é que, no primeiro são realizadas reuniões com a presença obrigatória dos diversos peritos, enquanto que, no segundo não existem momentos de reunião dos elementos que pertencem ao painel [86] [96]. Esta diferença é importante, especialmente quando os elementos do painel são em número elevado ou quando são de serviços ou organismos diferentes, o que dificulta a determinação de uma data para a realização das reuniões [89].

Numa unidade hospitalar em que é necessário que os seus serviços de assistência funcionem, na maior parte das vezes, 24 horas por dia, torna-se difícil promover uma data comum para a realização de reuniões, dada a rotação dos turnos de cada funcionário. Se juntarmos a esta dificuldade a diferença de horários entre as diversas classes profissionais, a determinação de uma data para a realização de uma reunião de um grupo alargado (e não é necessário que o grupo tenha um número muito elevado de elementos) não é impossível, mas apresenta um grau de dificuldade relevante.

O método de Delphi tem a vantagem de eliminar a influência que um ou alguns peritos podem ter nas respostas dos restantes. Esta influência pode advir do estatuto social e/ou da facilidade de argumentação que alguns peritos podem apresentar [78] [90] [97].

---

[21] $DIR = \frac{Q3 - Q1}{média} * 100$, onde Q3 e Q1 sãos respectivamente o 3º e 1º quartil.

Outra vantagem que o método de Delphi apresenta, embora esta também esteja presente de alguma forma no método do grupo nominal, é o anonimato das respostas [81] [85].

Face às vantagens apresentadas, optou-se por utilizar o método de Delphi para estimar o valor do impacto negativo da ocorrência de uma quebra de segurança que afecte um documento.

6.4.3.4 Aplicação do método de Delphi

Uma vez escolhido o método de Delphi, é necessário definir que critérios servem para a selecção dos elementos do painel de peritos, qual o formato do questionário e qual o critério de consenso a usar.

De seguida descrevem-se os aspectos considerados mais importantes, relativamente à implementação do método para a determinação do valor de um documento genérico, com base na percepção do impacto negativo da ocorrência de uma quebra de segurança nesse mesmo documento.

Constituição do painel de peritos

A equipa de peritos deverá ser multi-disciplinar de forma a que cada elemento possa contribuir com uma estimativa do valor do impacto, que será o reflexo da sua formação e da sua experiência profissional [3] [13] [5].

Encontram-se na literatura alguns critérios que foram seguidos para a constituição de grupos de peritos com objectivos afins ao deste trabalho. Alguns dos critérios usados foram os seguintes [3]:

- Incluir no grupo o responsável pela gestão dos sistemas de informação da organização;
- Incluir elementos que representem os profissionais que prestam cuidados de saúde;

- Incluir elementos do gabinete jurídico, do serviço de gestão de recursos humanos e do serviço responsável pela facturação dos cuidados de saúde;
- Incluir, ocasionalmente, funcionários que demonstram entusiasmo pelas questões da segurança da informação.

Tendo por referência os critérios anteriores e adaptando à realidade do estudo descrito neste trabalho, propõe-se que o painel de peritos seja uma equipa multi-disciplinar, constituída segundo os seguintes critérios:

- Ser preferencialmente constituída por elementos seniores que ocupem cargos de chefia ou equivalentes;
- Ser preferencialmente constituída por elementos ligados a áreas de carácter essencialmente clínicas (médicos e enfermeiros, técnicos superiores de saúde);
- Ser preferencialmente constituída por elementos que trabalhem na unidade de saúde onde é realizada a análise do risco;
- Incluir, nomeadamente, elementos do gabinete jurídico, do serviço de gestão de recursos humanos, do serviço responsável pela facturação dos cuidados de saúde e do serviço de gestão dos sistemas de informação;
- Incluir os elementos directamente relacionados com a gestão do serviço ou serviços a que pertencem os documentos em análise.

De acordo com os critérios referidos, os elementos da unidade hospitalar que devem integrar ou estar representados[22] no painel de peritos, chamado a pronunciar-se sobre o valor do impacto negativo são, pelo menos:

[22] Poderá haver necessidade de se adaptar a constituição do painel, se a estrutura organizacional for diferente.

- o Director Clínico (ou seu equivalente legal) da unidade de saúde;
- o Enfermeiro Director (ou seu equivalente legal) da unidade de saúde;
- o Director do serviço em análise;
- o Enfermeiro Chefe do serviço em análise;
- o responsável do Gabinete Jurídico da unidade de saúde;
- o responsável pelo serviço de gestão dos sistemas de informação da unidade de saúde;
- um administrador da área da gestão hospitalar.

Elaboração do Questionário

O questionário da primeira ronda será composto por um conjunto de perguntas indexadas aos documentos genéricos, identificados na secção 6.4.2. As respostas às perguntas pelos diversos elementos do painel de peritos, deverão exprimir a sua sensibilidade sobre o valor do impacto de uma quebra de segurança para cada um desses documentos.

Alinhando com a estratégia de abordar a segurança segundo as suas diferentes dimensões e com o objectivo de, posteriormente, identificar as medidas mais adequadas a cada documento, definiu-se a seguinte matriz para o conjunto de questões a elaborar para cada documento genérico:

- "Qual o impacto negativo, quando o documento "XPTO" sofre uma quebra de segurança segundo a dimensão confidencialidade?"
- "Qual o impacto negativo, quando o documento "XPTO" sofre uma quebra de segurança segundo a dimensão integridade?"
- "Qual o impacto negativo, quando o documento "XPTO" sofre uma quebra de segurança segundo a dimensão disponibilidade?"
- "Qual o impacto negativo, quando o documento "XPTO" sofre uma quebra de segurança segundo a dimensão autoria/responsabilidade?"

Definiu-se que a resposta a cada pergunta seria dada com base numa escala bipolar (escala de Likert[23]), crescente, de 7 pontos, de acordo com o que é a prática comum em estudos similares [98] [99] [100] [101] [90] [102]. Na escala usada o 1 corresponde ao impacto mais baixo enquanto que o 7 corresponderá ao impacto mais elevado.

Para além das perguntas anteriores, o questionário da primeira ronda deverá ser constituído pelas seguintes partes:

- uma breve introdução sobre a problemática da segurança da informação;
- um enquadramento dos objectivos do questionário;
- um conjunto de definições de conceitos relacionados com a problemática da segurança da informação e que são usados ao longo do questionário. Em particular, são dadas definições claras e precisas sobre o significado de cada uma das dimensões de segurança;
- uma descrição dos documentos genéricos referenciados no questionário;
- as instruções do preenchimento do questionário.

O questionário da segunda ronda e das rondas seguintes, será igual ao primeiro, com a diferença de se acrescentar a cada pergunta a seguinte informação:

- média e o desvio padrão dos valores obtidos nas respostas a cada pergunta, na ronda anterior;
- distribuição de frequências dos valores obtidos nas respostas a cada pergunta, na ronda anterior;
- a resposta dada pelo perito a que se destina o questionário, na ronda anterior.

[23] A escala de Likert é uma lista ordenada de respostas, que tipicamente tem 5 ou 7 pontos.

Critério de consenso

De acordo com a literatura referida na secção 6.4.3.2 optou-se por determinar o consenso com base no coeficiente *alpha de Cronbach*.

O valor do coeficiente a partir do qual se considera que existe consenso, está , para a maioria das aplicações, compreendido entre 0,7 e 0,8, embora possa ser maior ou menor consoante os contextos[24]. A Tabela 6.7 seguinte relaciona o coeficiente *alpha de Cronbach* e o graus de consenso[85] [98].

Alpha de Cronbach	**Consenso**
$\alpha \geq 0,9$	Excelente
$0,8 \leq \alpha < 0,9$	Bom
$0,7 \leq \alpha < 0,8$	Razoável
$0,6 \leq \alpha < 0,7$	Fraco
$\alpha < 0,6$	Inaceitável

Tabela 6.7 - Coeficiente *alpha de Cronbach* e o grau de Consenso

Como foi descrito, o questionário recomendado para esta fase da metodologia consiste em quatro grupos de perguntas, um por cada dimensão, para estimar o valor dos documentos genéricos. Assim, cada questionário pode ser dividido em quatro partes, as quais são independentes entre si. Para efeitos da obtenção do consenso, estes quatro grupos podem ser abordados separadamente.

Após a conclusão da segunda ronda é calculado o coeficiente *alpha de Cronbach* para cada grupo de perguntas/respostas que dizem respeito à mesma dimensão. Se o valor do *alpha de Cronbach* determinado para uma dimensão indicar um consenso razoável ou superior então, na ronda seguinte, o estudo dessa dimensão será excluído, elaborando-se o questionário apenas com as

[24] Por exemplo na área de decisão médica são exigidos valores na ordem dos 0,95.

questões que dizem respeito às outras dimensões em que ainda não se tenha atingido consenso. Quando todas as dimensões evidenciarem um nível de consenso razoável ou superior considera-se concluído o estudo.

6.4.3.5 Valor de um documento genérico

O valor de cada documento genérico segundo uma determinada dimensão, corresponde ao valor médio das respostas obtidas na última ronda, referentes a cada documento e à dimensão em causa. Assim para cada dimensão, é possível construir uma matriz (Matriz 6.1, Matriz 6.3, Matriz 6.3 e Matriz 6.4) onde cada posição representa o valor de um determinado documento.

Nas matrizes utiliza-se a seguinte nomenclatura:

- $V_{conf.\ doc_i}$ – valor do documento genérico **i** (doc_i) quando sofre uma quebra de segurança segundo a dimensão confidencialidade;
- $V_{int.\ doc_i}$ – valor do documento genérico **i** (doc_i) quando sofre uma quebra de segurança segundo a dimensão integridade;
- $V_{disp\ doc_i}$ – valor do documento genérico **i** (doc_i) quando sofre uma quebra de segurança segundo a dimensão disponibilidade;
- $V_{aut.\ doc_i}$ – valor do documento genérico **i** (doc_i) quando sofre uma quebra de segurança segundo a dimensão autoria/responsabilidade.

$$\text{Valor}_{\text{Conf.}} = \begin{bmatrix} V_{\text{Conf}}\,\text{doc}_1 \\ V_{\text{Conf}}\,\text{doc}_2 \\ \vdots \\ \vdots \\ V_{\text{Conf}}\,\text{doc}_n \end{bmatrix}$$

Matriz 6.1 - Valor dos documentos em função da confidencialidade

$$\text{Valor}_{\text{Int.}} = \begin{bmatrix} V_{\text{Int.}}\text{doc}_1 \\ V_{\text{Int.}}\text{doc}_2 \\ : \\ : \\ V_{\text{Int.}}\text{doc}_n \end{bmatrix}$$

Matriz 6.2 - Valor dos documentos em função da integridade

$$\text{Valor}_{\text{Disp.}} = \begin{bmatrix} V_{\text{Disp.}}\text{doc}_1 \\ V_{\text{Disp.}}\text{doc}_2 \\ : \\ : \\ V_{\text{Disp.}}\text{doc}_n \end{bmatrix}$$

Matriz 6.3 - Valor do documento em função da disponibilidade

$$\text{Valor}_{\text{Aut.}} = \begin{bmatrix} V_{\text{Aut.}}\text{doc}_1 \\ V_{\text{Aut.}}\text{doc}_2 \\ : \\ : \\ V_{\text{Aut.}}\text{doc}_n \end{bmatrix}$$

Matriz 6.4 - Valor dos documentos em função da autoria/responsabilidade

6.4.4 Determinação da probabilidade da concretização de uma ameaça

Paralelamente à estimativa do valor de cada documento genérico e de acordo com o modelo escolhido para a análise detalhada do risco (secção 6.1), é necessário estimar a probabilidade da concretização das ameaças a que um documento genérico está sujeito.

As ameaças a um documento derivam das ameaças associadas aos diversos processos a que o documento está sujeito durante a sua existência. No capítulo anterior (secções 5.3, 5.4, 5.5 e 5.6) foi apresentada uma descrição dos documentos da área clínica/administrativa de um serviço hospitalar, bem como dos processos que são alvo e dos autores que neles intervêm.

Considerando os documentos genéricos identificados é possível elaborar uma tabela que os relacione com os processos de que podem ser alvo (Tabela 6.8). Com o recurso a entrevistas, nomeadamente com o Director e o Enfermeiro Chefe do serviço em análise, é possível identificar os processos genéricos (PG) relacionados com os documentos genéricos.

Doc. Genéricos	**Processos Genéricos**			
	PG_1	**PG_2**	**.....**	**PG_m**
doc_1	X			
.....				
doc_n	X	X		X

Tabela 6.8 - Correspondência entre os processos e os documentos genéricos

O passo seguinte consiste na identificação das ameaças associadas a cada processo, por forma a poder determinar a probabilidade de concretização de cada uma delas.

São consideradas neste trabalho as seguintes classes de ameaças:

- **Remoção física** – remoção ou extravio de parte ou da totalidade do conteúdo de um documento, de forma intencional ou não;
- **Destruição física** – destruição do suporte físico da informação, de forma intencional ou não, ou a prática de actos que tornam a informação ilegível;

- **Alteração** – alteração de parte ou da totalidade do conteúdo de um documento de forma não protocolada;
- **Intercepção** – acesso ilegítimo a um documento, de forma intencional ou não;
- **Falsa identificação do autor** – omissão ou usurpação da identidade do autor da informação, de forma intencional ou não.

Esta classificação baseia-se nas classes de ameaças enumeradas na secção 2.1, embora a designação das classes esteja adaptada por forma a ter uma linguagem mais próxima das unidades de saúde. Adicionou-se ainda, uma nova classe de ameaças (*falsa identificação do autor*), cuja a importância é relevante nos sistemas da área clínica/administrativa.

A etapa final deste processo consiste na determinação da probabilidade da concretização da ameaça propriamente dita. Assim, para cada documento genérico, pretende-se estimar a probabilidade da concretização de uma ameaça, associada à execução de um processo genérico.

Mais uma vez não há registos sobre as ocorrências de ataques que permitam inferir o valor da probabilidade que se pretende calcular. Assim, o valor da probabilidade será estimado com base na opinião de um conjunto de peritos, à semelhança do que se descreve na literatura. À probabilidade determinada desta forma é-lhe atribuída a designação de probabilidade subjectiva [7] [103] [93] [104].

A probabilidade subjectiva tem dois problemas associados. O primeiro é a possibilidade de o seu valor poder variar ao longo do tempo, sem que para isso tenha havido alteração da constituição do painel de peritos. O outro problema reside no facto do valor da probabilidade estar intrinsecamente associado à constituição do painel, ou seja, dois painéis diferentes podem indicar valores de probabilidade diferentes [105] [96] [106].

Uma das técnicas associadas à determinação da probabilidade subjectiva é o método de Delphi, já utilizado anteriormente, sendo este o processo

seleccionado neste trabalho para estimar o valor da probabilidade da concretização das ameaças [96] [7].

6.4.4.1 Aplicação do método de Delphi

A implementação deste segundo painel de Delphi, será em tudo semelhante ao primeiro, havendo no entanto as necessárias adaptações ao nível da constituição do painel de peritos e do questionário.

Constituição do painel de peritos

A equipa de peritos deverá ser constituída por elementos que pertencem ao serviço clínico em análise, uma vez que se pretende que a resposta dos peritos seja baseada na sua experiência acumulada.

Como foi referido na secção 5.5 as classes de actores que interagem com a informação clínica/administrativa são essencialmente a classe médica e a de enfermagem. Os enfermeiros são provavelmente quem tem melhor percepção da realidade para estimar a probabilidade pretendida, dada a natureza das suas funções, as suas responsabilidades e a obrigatoriedade de estarem presentes 24 horas por dia no serviço. Deste modo o painel de peritos deve ser constituído maioritariamente por enfermeiros, embora possa incluir outras classes de actores que estejam afectas ao serviço em análise.

Elaboração do Questionário

O questionário a usar na primeira ronda será dividido em duas partes. A primeira parte contém os seguintes itens:

- uma breve introdução sobre a problemática da segurança da informação;
- um conjunto de definições de conceitos relacionados com a problemática da segurança da informação e que são usados ao longo

do questionário, nomeadamente os conceitos referentes às diferentes classes de ameaças e aos diferentes processos genéricos;

- uma descrição dos documentos genéricos referidos no questionário;
- as instruções de preenchimento do questionário.

A segunda parte do questionário é composta por um conjunto de questões destinadas a obter o valor da probabilidade da concretização de uma ameaça, sempre que um documento genérico seja sujeito a um processo genérico.

O modelo típico da pergunta que se propõe é o seguinte:

> *Quando o documento XPTO é sujeito ao processo genérico XZY, qual a probabilidade de a ameaça genérica "ABC" se concretizar ?*

Este modelo pode ser adaptado em função do documento, do processo ou da ameaça, de forma a tornar a pergunta mais clara para o perito. Por exemplo, quando se pretende determinar a probabilidade da ameaça de *alteração* quando o documento XPTO é alvo do processo de comunicação entre a entidade serviço e a entidade arquivo clínico, a pergunta poderá ter o seguinte formato:

> *Quando o documento XPTO é enviado para o arquivo clínico, qual é a probabilidade de poder haver alteração, de parte ou da totalidade, do seu conteúdo?*

A probabilidade de um evento é representada como um número real entre 0 e 1, ou no caso de se representar em percentagem, de 0 a 100. Deste modo, propõe-se para as respostas uma escala bipolar de 10 pontos. Para ajudar os peritos a quantificar a probabilidade da concretização de uma ameaça, poderá oferecer-se a correlação de cada valor da escala bipolar com um intervalo de percentagens, como se mostra na Tabela 6.9.

Item da escala	Intervalo de percentagens (%)
1	[0, 10]
2	]10, 20]
3	]20, 30]
4	]30, 40]
5	]40, 50]
6	]50, 60]
7	]60, 70]
8	]70, 80]
9	]80, 90]
10	]90, 100]

Tabela 6.9 - Escala das respostas das probabilidades

O questionário da segunda ronda e das seguintes, será em tudo igual ao da primeira ronda, acrescentando para além da resposta dada pelo perito, a média, o desvio padrão e a distribuição de frequência das respostas da ronda anterior, para cada pergunta.

Critério de consenso

Tal como na estimativa do valor de cada documento, o coeficiente *alpha de Cronbach* será também aqui usado para determinar o grau de consenso em cada ronda e, assim, usar-se-á a Tabela 6.7 para determinar uma expressão qualitativa do consenso.

Após a conclusão da 2ª ronda e até que o coeficiente *alpha de Cronbach* indique um consenso razoável ou superior, serão aplicadas tantas rondas quantas as necessárias.

6.4.4.2 Probabilidade da concretização das ameaças por dimensão de segurança

Como toda a metodologia proposta está alicerçada nas quatro dimensões da segurança, é conveniente que os valores das probabilidades sejam indexados às mesmas dimensões.

Não é difícil verificar, após uma análise cuidada das definições usadas, que uma determinada classe de ameaças afecta uma ou mais dimensões da segurança. Por exemplo, a *destruição física* afecta sobretudo as dimensões integridade e disponibilidade, enquanto que a *intercepção* afecta essencialmente a confidencialidade. A Tabela 6.10 estabelece as dimensões que são predominantemente afectadas quando se concretiza cada classe de ameaças.

Ameaça	Dimensão afectada			
	***Conf*[25].**	***Int.*[26]**	***Disp.*[27]**	***Aut.*[28]**
Remoção física (A_1)	X		X	
Intercepção (A_2)	X			
Alteração (A_3)		X		
Destruição física (A_4)		X	X	
Falsa identificação do autor (A_5)				X

Tabela 6.10 - Correspondência entre as classes de ameaças e as dimensões da segurança

[25] Conf. - Confidencialidade

[26] Int. - Integridade

[27] Disp. - Disponibilidade

[28] Aut. – Autoria/Responsabilidade

Conjugando a tabela anterior com a Tabela 6.8 e com a média das respostas do painel de peritos, é possível, para cada uma das dimensões da segurança construir a Tabela 6.11, Tabela 6.12, Tabela 6.13, Tabela 6.14, respectivamente, e onde:

- **PG_k** representa o processo genérico k, com k= 1, 2, ..., m;
- **doc_i** representa o documento genérico i, com i= 1,2, ..., n;
- **A_p** representa a classe de ameaças, onde p $\in \{1,2,3,4,5\}$
- **$P_{i,\,(PG_k\ A_p)}$** representa a probabilidade da concretização da ameaça **A_p** quando o documento genérico d**oc_i** é alvo do processo **PG_k**. Esta probabilidade é calculada com base na média das respostas obtidas na ronda onde foi atingido o consenso entre o painel de peritos. Quando um determinado documento não é alvo de um determinado processo, a probabilidade da concretização das ameaças associadas ao processo em causa é, naturalmente, zero ($P_{i,(PG_kA_p)}$=0).

	PG_1		..	PG_k		...	PG_m	
	Remoção física (A_1)	*Intercepção (A_2)*		*Remoção física (A_1)*	*Intercepção (A_2)*		*Remoção física (A_1)*	*Intercepção (A_2)*
doc_1	$P_{1,(PG_1\ A_1)}$	$P_{1,(PG_1\ A_2)}$	…	$P_{1,(PG_k\ A_1)}$	$P_{1,(PG_k\ A_2)}$	…	$P_{1,(PG_m\ A_1)}$	$P_{1,(PG_m\ A_2)}$
doc_2	$P_{2,(PG_1\ A_1)}$	$P_{2,(PG_1\ A_2)}$	…	$P_{2,(PG_k\ A_1)}$	$P_{2,(PG_k\ A_2)}$	…	$P_{2,(PG_m\ A_1)}$	$P_{2,(PG_m\ A_2)}$
:	:	:		:	:		:	:
doc_i	$P_{i,(PG_1\ A_1)}$	$P_{i,(PG_1\ A_2)}$	…	$P_{i,(PG_k\ A_1)}$	$P_{i,(PG_k\ A_2)}$	…	$P_{i,(PG_m\ A_1)}$	$P_{i,(PG_m\ A_2)}$
:	:	:		:	:		:	:
doc_n	$P_{n,(PG_1\ A_1)}$	$P_{n,(PG_1\ A_2)}$	…	$P_{n,(PG_k\ A_1)}$	$P_{n,(PG_k\ A_2)}$	…	$P_{n,(PG_m\ A_1)}$	$P_{n,(PG_m\ A_2)}$

Tabela 6.11 - Probabilidades da concretização das ameaças em função da dimensão confidencialidade

	PG_1		..	PG_k		...	PG_m	
	Alteração (A_3)	*Destruição física (A_4)*		*Alteração (A_3)*	*Destruição física (A_4)*		*Alteração (A_3)*	*Destruição física (A_4)*
doc_1	$\mathbf{P}_{1,(PG_1 A_3)}$	$\mathbf{P}_{1,(PG_1 A_4)}$	…	$\mathbf{P}_{1,(PG_k A_3)}$	$\mathbf{P}_{1,(PG_k A_4)}$	…	$\mathbf{P}_{1,(PG_m A_3)}$	$\mathbf{P}_{1,(PG_m A_4)}$
doc_2	$\mathbf{P}_{2,(PG_1 A_3)}$	$\mathbf{P}_{2,(PG_1 A_4)}$	…	$\mathbf{P}_{2,(PG_k A_3)}$	$\mathbf{P}_{2,(PG_k A_4)}$	…	$\mathbf{P}_{2,(PG_m A_3)}$	$\mathbf{P}_{2,(PG_m A_4)}$
:	:	:		:	:		:	:
doc_i	$\mathbf{P}_{i,(PG_1 A_3)}$	$\mathbf{P}_{i,(PG_1 A_4)}$	…	$\mathbf{P}_{i,(PG_k A_3)}$	$\mathbf{P}_{i,(PG_k A_4)}$	…	$\mathbf{P}_{i,(PG_m A_3)}$	$\mathbf{P}_{i,(PG_m A_4)}$
:	:	:		:	:		:	:
doc_n	$\mathbf{P}_{n,(PG_1 A_3)}$	$\mathbf{P}_{n,(PG_1 A_4)}$	…	$\mathbf{P}_{n,(PG_k A_3)}$	$\mathbf{P}_{n,(PG_k A_4)}$	…	$\mathbf{P}_{n,(PG_m A_3)}$	$\mathbf{P}_{n,(PG_m A_4)}$

Tabela 6.12 - Probabilidades da concretização das ameaças em função da dimensão integridade

	PG_1		..	PG_k		...	PG_m	
	Remoção física (A_1)	*Destruição física (A_4)*		*Remoção física (A_1)*	*Destruição física (A_4)*		*Remoção física (A_1)*	*Destruição física (A_4)*
doc_1	$\mathbf{P}_{1,(PG_1 A_1)}$	$\mathbf{P}_{1,(PG_1 A_4)}$	…	$\mathbf{P}_{1,(PG_k A_1)}$	$\mathbf{P}_{1,(PG_k A_4)}$	…	$\mathbf{P}_{1,(PG_m A_1)}$	$\mathbf{P}_{1,(PG_m A_4)}$
doc_2	$\mathbf{P}_{2,(PG_1 A_1)}$	$\mathbf{P}_{2,(PG_1 A_4)}$	…	$\mathbf{P}_{2,(PG_k A_1)}$	$\mathbf{P}_{2,(PG_k A_4)}$	…	$\mathbf{P}_{2,(PG_m A_1)}$	$\mathbf{P}_{2,(PG_m A_4)}$
:	:	:		:	:		:	:
doc_i	$\mathbf{P}_{i,(PG_1 A_1)}$	$\mathbf{P}_{i,(PG_1 A_4)}$	…	$\mathbf{P}_{i,(PG_k A_1)}$	$\mathbf{P}_{i,(PG_k A_4)}$	…	$\mathbf{P}_{i,(PG_m A_1)}$	$\mathbf{P}_{i,(PG_m A_4)}$
:	:	:		:	:		:	:
doc_n	$\mathbf{P}_{n,(PG_1 A_1)}$	$\mathbf{P}_{n,(PG_1 A_4)}$	…	$\mathbf{P}_{n,(PG_k A_1)}$	$\mathbf{P}_{n,(PG_k A_4)}$	…	$\mathbf{P}_{n,(PG_m A_1)}$	$\mathbf{P}_{n,(PG_m A_4)}$

Tabela 6.13 - Probabilidades da concretização das ameaças em função da dimensão disponibilidade

	PG_1		PG_k		PG_m
	Falsa identificação do autor (A_5)	…	*Falsa identificação do autor (A_5)*	…	*Falsa identificação do autor (A_5)*
Doc_1	$\mathbf{P_{1,(PG_1\,A_5)}}$	…	$\mathbf{P_{1,(PG_k\,A_5)}}$	…	$\mathbf{P_{1,(PG_m\,A_5)}}$
Doc_2	$\mathbf{P_{2,(PG_1\,A_5)}}$	…	$\mathbf{P_{2,(PG_k\,A_5)}}$	…	$\mathbf{P_{2,(PG_m\,A_5)}}$
:	:		:		:
doc_i	$\mathbf{P_{i,(PG_1\,A_5)}}$	…	$\mathbf{P_{i,(PG_k\,A_5)}}$	…	$\mathbf{P_{i,(PG_m\,A_5)}}$
:	:		:		:
doc_n	$\mathbf{P_{n,(PG_1\,A_5)}}$	…	$\mathbf{P_{n,(PG_k\,A_5)}}$	…	$\mathbf{P_{n,(PG_m\,A_5)}}$

Tabela 6.14 - Probabilidades da concretização das ameaças em função da dimensão autoria/responsabilidade

Com base nas tabelas anteriores, é possível para cada dimensão de segurança representar uma matriz de probabilidades.

$$P_{Ameaça_{Confidencialidade}} = \begin{bmatrix} P_{1,(PG_{1A_1})} & P_{1,(PG_{1A_2})} & \cdots & P_{1,(PG_{mA_1})} & P_{1,(PG_{mA2})} \\ P_{2,(PG_{1A_1})} & P_{2,(PG_{1A2})} & \cdots & P_{2,(PG_{mA_1})} & P_{2,(PG_{mA2})} \\ : & : & & : & : \\ : & : & & : & : \\ P_{n,(PG_{1A_1})} & P_{n,(PG_{1A2})} & \cdots & P_{n,(PG_{mA_1})} & P_{n,(PG_{mA2})} \end{bmatrix}$$

Matriz 6.5 - Probabilidade da concretização de uma ameaça que afecta a confidencialidade

$$P_{Ameaça_{Integridade}} = \begin{bmatrix} P_{1,(PG_{1A_3})} & P_{1,(PG_{1A_4})} & \cdots & P_{1,(PG_{mA_3})} & P_{1,(PG_{mA4})} \\ P_{2,(PG_{1A_3})} & P_{2,(PG_{1A4})} & \cdots & P_{2,(PG_{mA3})} & P_{2,(PG_{mA4})} \\ : & : & & : & : \\ : & : & & : & : \\ P_{n,(PG_{1A_3})} & P_{n,(PG_{1A4})} & \cdots & P_{n,(PG_{mA_3})} & P_{n,(PG_{mA4})} \end{bmatrix}$$

Matriz 6.6 - Probabilidade da concretização de uma ameaça que afecta a integridade

$$P_{Ameaça_{Disponibildade}} = \begin{bmatrix} P_{1,(PG_{1A_1})} & P_{1,(PG_{1A_4})} & \cdots & P_{1,(PG_{mA_1})} & P_{1,(PG_{mA4})} \\ P_{2,(PG_{1A_1})} & P_{2,(PG_{1A4})} & \cdots & P_{2,(PG_{mA1})} & P_{2,(PG_{mA4})} \\ \vdots & \vdots & & \vdots & \vdots \\ \vdots & \vdots & & \vdots & \vdots \\ P_{n,(PG_{1A_1})} & P_{n,(PG_{1A4})} & \cdots & P_{n,(PG_{mA_1})} & P_{n,(PG_{mA4})} \end{bmatrix}$$

Matriz 6.7 - Probabilidade da concretização de uma ameaça que afecta a disponibilidade

$$P_{Ameaça_{Autoria/\text{Re}sponsabilidade}} = \begin{bmatrix} P_{1,(PG_{1A_5})} & \cdots & P_{1,(PG_{mA5})} \\ P_{2,(PG_{1A_5})} & \cdots & P_{2,(PG_{mA5})} \\ \vdots & & \vdots \\ \vdots & & \vdots \\ P_{n,(PG_{1A_5})} & \cdots & P_{n,(PG_{mA5})} \end{bmatrix}$$

Matriz 6.8 - Probabilidade da concretização de uma ameaça que afecta a autoria/disponibilidade

6.4.5 Valor do risco

Uma vez estimado o valor de cada documento genérico e as probabilidades da concretização das ameaças, cabe agora calcular o índice do risco de cada documento genérico. Para cada documento genérico são calculados quatro índices do risco, um por cada dimensão de segurança. Cada índice é calculado pelo produto entre o valor do documento genérico e o valor da probabilidade máxima da concretização das ameaças que o afectam, segundo a respectiva dimensão.

Com base nas matrizes da probabilidade da concretização das ameaças (Matriz 6.5, Matriz 6.6, Matriz 6.7 e Matriz 6.8), podem-se construir quatro matrizes (n x n), em que cada valor da diagonal principal é igual ao valor máximo da respectiva linha da matriz da probabilidade, tomando os restantes elementos da

matriz o valor de zero. As matrizes resultantes são a Matriz 6.9, a Matriz 6.10, a Matriz 6.11 e a Matriz 6.12, onde *Max (y)* é uma função matemática que determina o maior valor absoluto de uma série de valores;

$$P_{Max_{Conf}} = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}$$

onde :

$$a_{11} = \text{Max}\left(\text{Valores da linha } 1 \text{ da matriz } P_{\text{Ameaça Confidenci alidade}}\right)$$
$$a_{22} = \text{Max}\left(\text{Valores da linha } 2 \text{ da matriz } P_{\text{Ameaça Confidenci alidade}}\right)$$
$$\vdots \qquad\qquad \vdots$$
$$a_{nn} = \text{Max}\left(\text{Valores da linha } n \text{ da matriz } P_{\text{Ameaça Confidenci alidade}}\right)$$

Matriz 6.9 - Probabilidade máxima da concretização das ameaças para a confidencialidade

$$P_{Max_{Int.}} = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & a_{nn} \end{bmatrix}$$

onde :

$$a_{11} = \text{Max}\left(\text{Valores da linha } 1 \text{ da matriz } P_{\text{Ameaça Integridad e}}\right)$$
$$a_{22} = \text{Max}\left(\text{Valores da linha } 2 \text{ da matriz } P_{\text{Ameaça Integridad e}}\right)$$
$$\vdots \qquad\qquad \vdots$$
$$a_{nn} = \text{Max}\left(\text{Valores da linha } n \text{ da matriz } P_{\text{Ameaça Integridad e}}\right)$$

Matriz 6.10 - Probabilidade máxima da concretização das ameaças para a integridade

$$P_{Max_{Disp..}} = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ : & : & & : \\ 0 & 0 & \dots & a_{n\,n} \end{bmatrix}$$

onde :

$$a_{11} = \text{Max}\left(\text{Valores da linha } 1 \text{ da matriz } P_{\text{Ameaça}_{\text{Disponibilidade}}}\right)$$
$$a_{22} = \text{Max}\left(\text{Valores da linha } 2 \text{ da matriz } P_{\text{Ameaça}_{\text{Disponibilidade}}}\right)$$
$$\vdots \qquad\qquad\qquad\qquad \vdots$$
$$a_{nn} = \text{Max}\left(\text{Valores da linha } n \text{ da matriz } P_{\text{Ameaça}_{\text{Disponibilidade}}}\right)$$

Matriz 6.11 - Probabilidade máxima da concretização das ameaças para a disponibilidade

$$P_{Max_{Aut.}} = \begin{bmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \dots & 0 \\ : & : & & : \\ 0 & 0 & \dots & a_{n\,n} \end{bmatrix}$$

onde :

$$a_{11} = \text{Max}\left(\text{Valores da linha } 1 \text{ da matriz } P_{\text{Ameaça}_{\text{Autoria/Responsabilidade}}}\right)$$
$$a_{22} = \text{Max}\left(\text{Valores da linha } 2 \text{ da matriz } P_{\text{Ameaça}_{\text{Autoria/Responsabilidade}}}\right)$$
$$\vdots \qquad\qquad\qquad\qquad \vdots$$
$$a_{nn} = \text{Max}\left(\text{Valores da linha } n \text{ da matriz } P_{\text{Ameaça}_{\text{Autoria/Responsabilidade}}}\right)$$

Matriz 6.12 - Probabilidade máxima da concretização das ameaças para a autoria/responsabilidade

Portanto, o índice do risco segundo a dimensão confidencialidade é uma matriz (nx1), designada por **$Risco_{conf.}$** em o elemento genérico **$risco_{conf.}$**[i] representa o valor do risco para o documento genérico **doc_i**. A matriz **$Risco_{conf.}$** É calculada pelo produto entre a matriz **$P_{max_{conf.}}$** e a matriz **$Valor_{conf.}$**. Efectua-se um cálculo

semelhante para as outras dimensões, conforme se ilustra nas fórmulas seguintes.

$$\text{Risco}_{\text{Conf.}} = \begin{bmatrix} \text{Risco}_{\text{Conf doc}_1} \\ \text{Risco}_{\text{Conf.doc}_2} \\ : \\ : \\ \text{Risco}_{\text{Conf doc}_n} \end{bmatrix} = \text{P}_{\text{Max}_{\text{Conf.}}} \text{x} \ \ \text{Valor}_{\text{Conf.}}$$

Fórmula 6.1 - Risco dos documentos segundo a dimensão confidencialidade

$$\text{Risco}_{\text{Int.}} = \begin{bmatrix} \text{Risco}_{\text{Int.doc}_1} \\ \text{Risco}_{\text{Int.doc}_2} \\ : \\ : \\ \text{Risco}_{\text{Int.doc}_n} \end{bmatrix} = \text{P}_{\text{Max}_{\text{Int.}}} \text{x} \ \ \text{Valor}_{\text{Int.}}$$

Fórmula 6.2 - Risco dos documentos segundo a dimensão integridade

$$\text{Risco}_{\text{Disp.}} = \begin{bmatrix} \text{Risco}_{\text{Disp.doc}_1} \\ \text{Risco}_{\text{Disp.doc}_2} \\ : \\ : \\ \text{Risco}_{\text{Disp.doc}_n} \end{bmatrix} = \text{P}_{\text{Max}_{\text{Disp.}}} \text{x} \ \ \text{Valor}_{\text{Disp.}}$$

Fórmula 6.3 - Risco dos documentos segundo a dimensão disponibilidade

$$\text{Risco}_{\text{Aut.}} = \begin{bmatrix} \text{Risco}_{\text{Aut.doc}_1} \\ \text{Risco}_{\text{Aut.doc}_2} \\ : \\ : \\ \text{Risco}_{\text{Aut.doc}_n} \end{bmatrix} = \text{P}_{\text{Max}_{\text{Aut.}}} \text{ x } \text{Valor}_{\text{Aut.}}$$

Fórmula 6.4 - Risco dos documentos segundo a autoria/responsabilidade

Calculados os índices do risco para cada documento, é possível, para cada dimensão, estabelecer uma ordenação dos documentos em função do respectivo risco. Esta ordenação irá permitir estabelecer as prioridades de actuação e ajudar na escolha das medidas que se devem aplicar.

6.5 Organização do catálogo de medidas e selecção das medidas

Convém agora definir a metodologia para a escolha das medidas a implementar.

Como foi apresentado no Capítulo 3, o modelo OCTAVE é o que apresenta o catálogo de medidas melhor estruturado. Porém, ao invés da norma ISO/IEC 13335, as medidas não estão organizadas segundo as dimensões de segurança. Assim, parece conveniente propor uma nova organização para as medidas que se adapte à metodologia proposta para a gestão do risco[29].

Posto isto, propõe-se, à semelhança do modelo OCTAVE, que o catálogo de medidas esteja dividido em duas partes: uma que inclua as medidas estratégicas e outra as medidas operacionais.

[29] Ver anexo A

6.5.1 Medidas Estratégicas

Excluindo as medidas estratégicas destinadas à própria definição do processo de gestão do risco, as restantes medidas que fazem parte deste grupo no OCTAVE (secção 3.3.2), são incluídas no catálogo proposto. Desta forma o catálogo deve conter os seguintes grupos de medidas:

- Sensibilização e treino;
- Política de segurança e regulamentos;
- Política de segurança nas relações com terceiros;
- Planos de contingência e de recuperação.

6.5.2 Medidas Operacionais

Como foi referido na secção 3.3.2 as medidas operacionais são o conjunto de boas práticas, relativas à segurança da informação e que devem ser aplicadas aos sistemas de informação.

Neste trabalho propõe-se, que este grupo de medidas seja subdividido em dois grupos, um de medidas designadas por *genéricas* e outro por *específicas*.

Consideram-se medidas genéricas todas as medidas operacionais que, dada a sua natureza sejam consideradas de aplicação quase obrigatória para um determinado tipo de sistemas. Estas medidas devem ser agrupadas conforme se destinam a sistemas que usam tecnologias informáticas ou não.

Por sua vez, toda a medida que não seja classificada como genérica é classificada como específica. A necessidade de utilização de uma medida específica tem por base uma análise detalhada do risco. Propõe-se então que as medidas específicas sejam organizadas segundo a dimensão de segurança que visam reforçar, à semelhança do que é proposto na norma ISO\IEC 13335.

6.5.3 Modelo proposto

Com base nas secções anteriores representa-se na Figura 6.1 o catálogo de medidas proposto. Note-se que, no sentido de agilizar o processo de escolha de

medidas, é conveniente como é referido na secção 3.1, classificar as medidas segundo o fim a que se destinam. Deste modo em cada subgrupo de medidas estruturais e operacionais as medidas devem ser classificadas como de correcção, de dissuasão, de detecção, de diversão e de prevenção.

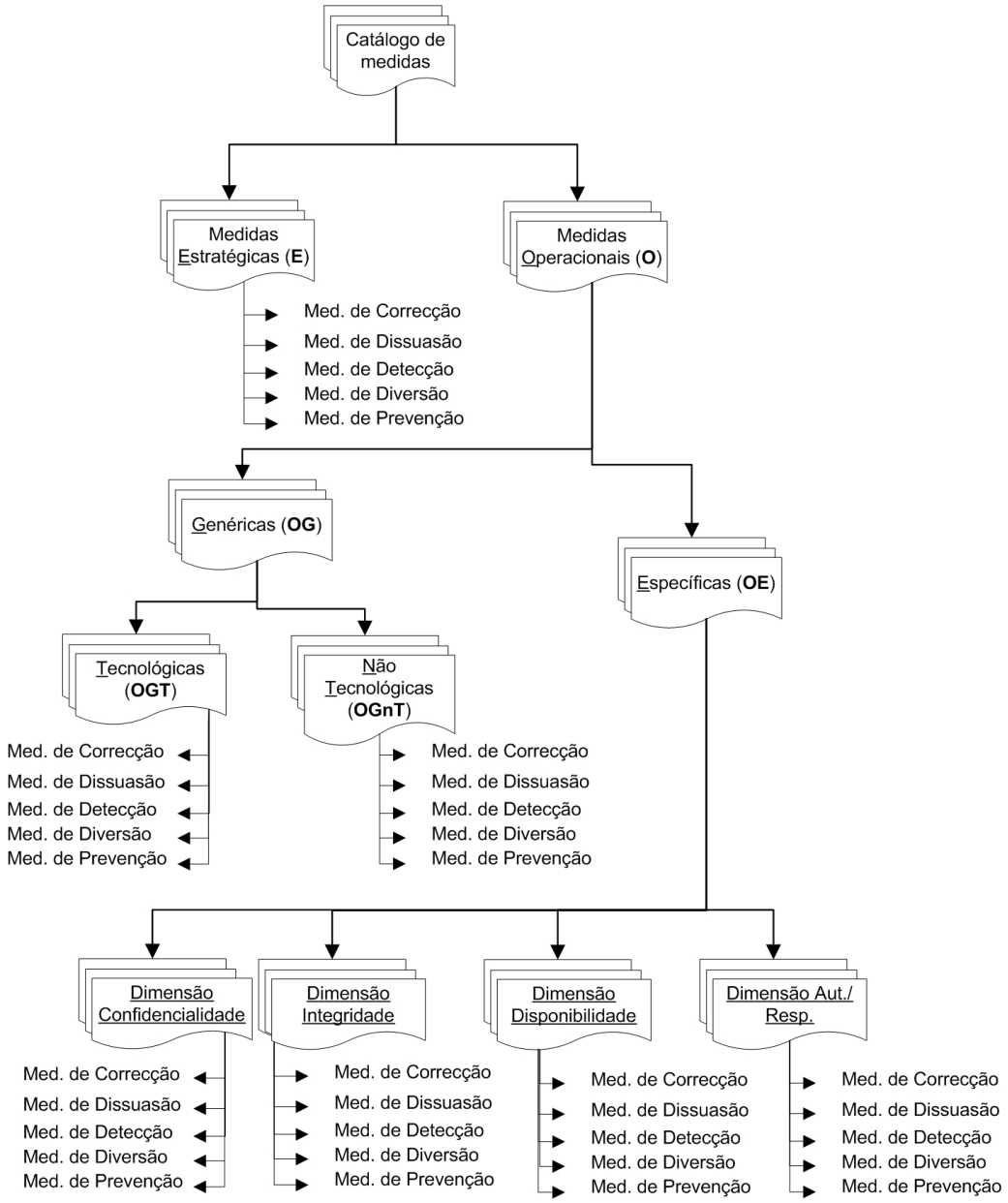


Figura 6.1 - Proposta de organização do catálogo

6.5.4 Selecção das medidas para os sistemas críticos

A selecção das medidas para os sistemas críticos é sustentada pela justificação proveniente da análise detalhada do risco. Ao gestor da organização cabe analisar o índice do risco de cada documento e o custo da implementação das medidas possíveis, para impedir os ataques.

A metodologia fornece ainda a possibilidade do gestor saber qual, ou quais são os processos genéricos de que cada documento é alvo e portanto, perceber onde uma ameaça tem mais probabilidade de se concretizar (Tabela 6.11, Tabela 6.12, Tabela 6.13 e Tabela 6.14).

Alguns modelos de gestão do risco baseiam a selecção das medidas em função da sua eficiência e das vulnerabilidades que se pretendem corrigir nos sistemas. Os catálogos de medidas que apresentam, são pois orientados segundo aquelas duas vertentes. Porém, a metodologia que sugerem para a gestão do risco é diferente daquela que se propõe neste trabalho [107].

No catálogo proposto a classificação das medidas segundo o fim a que se destinam (correcção, dissuasão, detecção, diversão e prevenção) tem como objectivo suportar para cada documento a decisão de optar por uma medida em detrimento da outra. Por exemplo, se um documento possui um elevado risco resultante de uma vulnerabilidade intrínseca, as medidas a aplicar são sobretudo de carácter preventivo. Já se o risco advém de um agente externo identificado, poderá ser mais útil a aplicação de medidas de carácter dissuasivo.

A metodologia proposta assume que a escolha da medida com maior relação custo/benefício é deixada ao critério do decisor, identificando-se, desde já, neste contexto uma linha de investigação para trabalhos futuros.

Não obstante os critérios usados, a selecção das medidas deverá ser efectuada documento a documento, partindo do documento que apresente um índice do risco mais elevado.

6.5.5 Selecção das medidas para os sistemas não críticos

De acordo com o que é preconizado pela ISO\IEC 13335, as medidas para os sistemas não críticos são seleccionadas em função do tipo de sistema e na presente proposta, tendo por base as medidas genéricas propostas no catálogo.

Obviamente, caberá ao gestor, e à semelhança da selecção das medidas para os sistemas críticos, ponderar a relação custo/benefício de cada medida.

6.6 Documento da política de segurança, implementação e avaliação

Após a fase da selecção das medidas, o modelo ISO/IEC 13335 preconiza as fases da escrita formal da política, da sua implementação e da sua avaliação e acompanhamento, sendo designadas por documento da política de segurança, por implementação e por avaliação, respectivamente. Para estas fases, o trabalho presente não sugere nenhuma nova metodologia, propondo-se o que é descrito na ISO/IEC 13335. No entanto, no futuro estas fases deverão ser alvo de uma análise profunda na perspectiva da sua optimização.

6.7 Esquema da metodologia proposta

Com base nas secções anteriores, importa agora redesenhar o diagrama do modelo da abordagem heterogénea proposta pela ISO/IEC 13335 (Figura 3.2 - página 22) de forma a esquematizar a metodologia proposta. As principais alterações prendem-se, essencialmente, com as fases do processo de gestão do risco relacionadas com os sistemas críticos e realçadas no esquema.

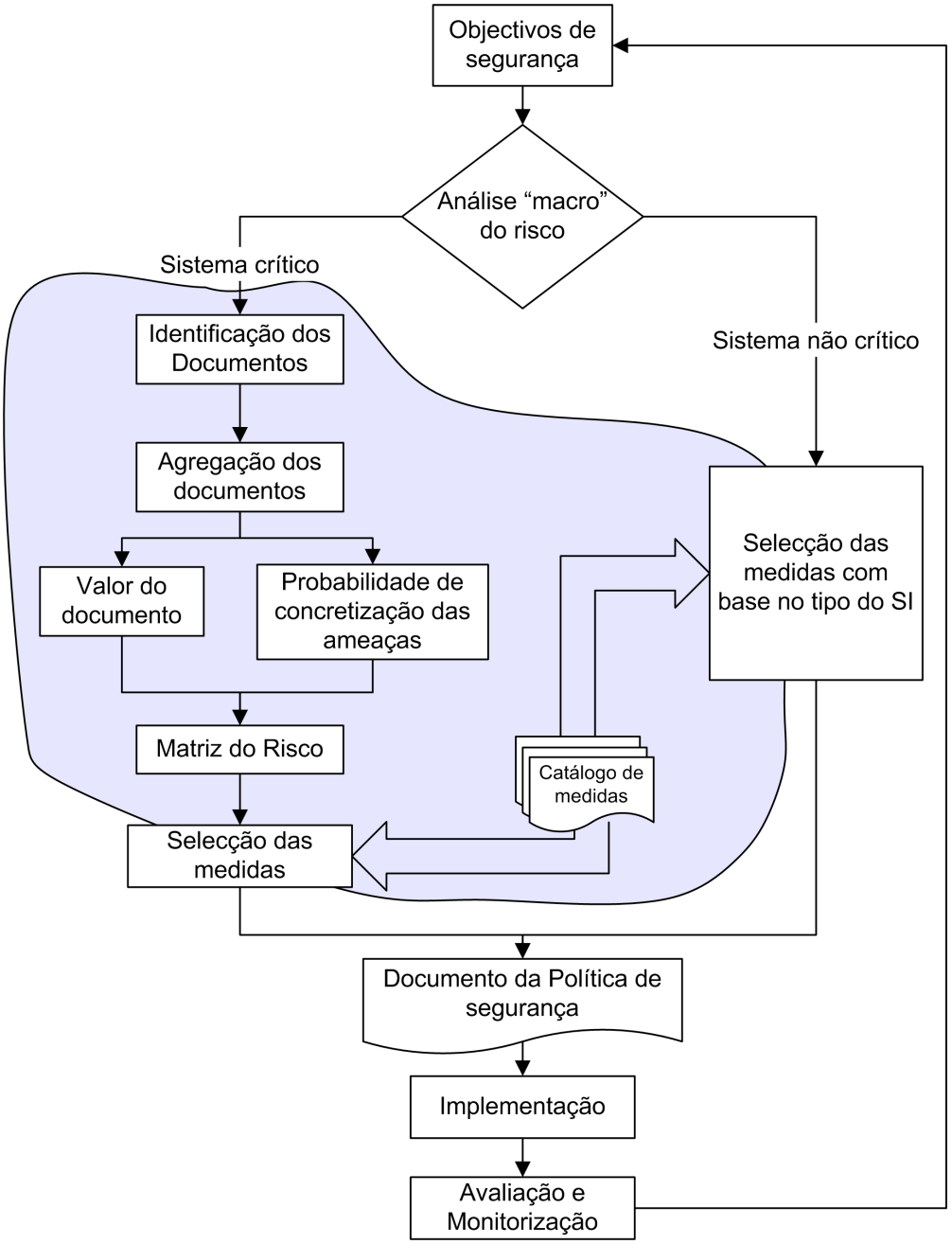


Figura 6.2 - Metodologia proposta

6.8 Análise da aplicabilidade da metodologia

Nas unidades hospitalares, verifica-se uma grande carência de sensibilização das administrações para a necessidade de implementação de um processo de gestão da segurança. Além disso, as administrações têm outras a prioridades de gestão. Assim, a aplicação da metodologia proposta neste trabalho encontrou vários entraves. Estes resultaram do facto de este trabalho não ter surgido de uma necessidade objectiva que a organização tivesse identificado, ficando desde de logo dificultadas as fases relacionadas com sua implementação. Com os condicionalismos referidos, procurou-se testar a aplicabilidade das fases de identificação, de agregação e de determinação do índice de risco dos documentos numa unidade hospitalar específica. Realce-se que a metodologia proposta apresenta novas soluções, sobretudo ao nível destas fases, e que estas fases normalmente contribuem para a dificuldade de aplicação do processo de gestão do risco.

A metodologia foi aplicada na Unidade de Cuidados Intensivos Coronários (UCIC) do Hospital Infante D. Pedro (HIP), tal como descrito no anexo **B**.

Procedeu-se em primeiro lugar à identificação e classificação dos sistemas de informação da UCIC em sistemas críticos ou não críticos (fase “Análise macro do risco” Figura 6.2). Assim, e de acordo com os critérios que a metodologia advoga todos os sistemas foram considerados críticos. Após esta classificação, procedeu-se à identificação e agregação dos documentos.

Foram identificados e caracterizados 40 documentos que se agregaram em 17 documentos genéricos.

Para estimar o valor de cada documento, foi elaborado um questionário, que se transcreve no Anexo C. Como é proposto, este questionário foi administrado a um painel de peritos segundo a técnica de Delphi. O painel de peritos era constituído por 13 elementos e ao fim da segunda ronda foi atingido o consenso ao nível das respostas, uma vez que os valores do alpha de Cronbach variaram entre 0,86 (para a dimensão confidencialidade) e 0,97 (para a dimensão autoria/responsabilidade) (AnexoB/Tabela B11).

Os valores dos documentos determinados para as várias dimensões de segurança, encontram-se dentro dos intervalos esperados. Assim os

documentos que contêm a súmula da informação, como por exemplo o processo único do doente, apresentam, em média, valores mais elevados para as dimensões confidencialidade, integridade e disponibilidade. No extremo oposto, o grupo de documentos que serve para solicitar um pedido (de uma consulta, de um exame, etc.) apresentam, em média o valor mais baixo para essas mesmas dimensões. Os documentos que saem da instituição para a comunicação de informação a outras autoridades (tais como documentos de óbito, documento para a comunicação obrigatória de doenças, etc.) apresentam, em média, o valor mais elevado na dimensão autoria/responsabilidade (AnexoB/Tabela B13).

Um processo semelhante foi aplicado na fase do cálculo da probabilidade de concretização das ameaças, seguindo as orientações da metodologia. Neste caso, o painel de peritos foi constituído por 20 elementos, todos eles pertencente às UCIC. Como no caso anterior, foi atingido o consenso após a aplicação da 2º ronda do questionário[30]. Os valores obtidos para o alpha de Cronbach variaram entre 0,86 e 0,99, conforme é apresentado na Tabela B14. Nas tabelas B15, B16, B17, B18, B19 e B20 encontram-se descritos os valores das probabilidades da concretização das ameaças por processos e documentos.

Com base nos valores determinados anteriormente e aplicando as fórmulas descritas na metodologia para o cálculo do risco (Fórmula 6.1, Fórmula 6.2, Fórmula 6.3, Fórmula 6.4) obtiveram-se as respectivas matrizes do risco e que são apresentadas no fim do anexo B (Tabela B21, Tabela B22, Tabela B23 e Tabela B24). Com bases nos valores do risco ordenaram-se os documentos. Ficaram assim, reunidas as condições para o responsável pela gestão do risco ou a equipa de gestão da organização, decidir as medidas a implementar, face à estratégia da organização quanto ao problema da segurança.

[30] O questionário encontra-se transcrito no Anexo D.

Capítulo 7
Conclusão

7.1 Síntese do trabalho realizado

No início desta tese foi sublinhado que qualquer organização necessita de uma política de segurança independentemente da sua área de negócio. Esta necessidade é ainda mais premente para as organizações que prestam cuidados de saúde ou que lidam com a informação resultante dos mesmos.

Durante a consulta e análise da literatura ficou claro que qualquer política de segurança, só pode ser coerente e eficaz quando assentar num processo de gestão do risco. Só desta forma as medidas preconizadas para estabelecer o nível de segurança pretendido estão devidamente fundamentadas e adaptadas à realidade da organização.

É também objecto de unânime referência que uma organização que envolva os seus recursos humanos no processo de gestão do risco, beneficia por estar a sensibilizar e a educar os próprios utilizadores dos sistemas. De facto, em qualquer metodologia, é salientada a necessidade de formação e educação dos funcionários na área da segurança.

Este trabalho tinha como objectivo definir uma metodologia que, tendo por base alguns métodos e normas já existentes para a área da gestão da segurança, apresentasse soluções inovadoras e capacidade de ser facilmente aplicada em unidades de saúde.

A metodologia proposta, cuja "coluna vertebral" é a abordagem heterogénea da norma ISO/IEC 13335, incorporou alguns procedimentos e especificou outros, procurando facilitar a sua implementação em organizações complexas, reduzindo o tempo e os recursos humanos e financeiros necessários, e permitindo uma possível certificação futura.

Contribuem para a facilidade de implementação a técnica de agregação de documentos e o método de Delphi, nas várias fases da análise detalhada do risco. O uso destas técnicas permite de alguma forma a redução dos custos, uma vez que a própria organização passa a ter capacidade para lidar com o processo de gestão do risco, não tendo necessidade de recorrer a entidades externas. Além disso, ao envolver os recursos humanos da própria organização, principalmente os elementos de chefia, o processo de gestão do risco cria, por si só, uma vertente formadora e sensibilizadora para a problemática da segurança.

Uma das mais valia que a metodologia apresenta é, sem dúvida, a solução para o cálculo do índice do risco para os documentos de uma unidade de saúde, em especial do tipo hospitalar. Esta inovação, prende-se sobretudo em obter de uma forma expedita, os valores com os quais é possível calcular o índice do risco.

Apesar da haver uma estreita relação entre a metodologia proposta e as unidades hospitalares, isto não impede que ela seja aplicada em organizações de outras áreas. Para tal, poderá necessitar de algumas adaptações face à estrutura organizacional e funcional da organização em causa.

O uso da metodologia proposta também garante o cumprimento, por parte das organizações portuguesas, do estipulado pela Lei nº67/98, nomeadamente no que diz respeito aos artigos 14º (segurança do tratamento da informação) e 15º (medidas especiais de segurança).

Um dos pontos críticos da metodologia proposta é a constituição dos painéis de peritos, usados para a estimativa do valor de cada documento e para a estimativa da probabilidade da concretização das ameaças. De facto, é provável

que constituições diferentes dos painéis originem valores diferentes. Porém, uma vez cumpridos os requisitos para a sua constituição e dado que não se pretendem valores exactos do risco, mas determinar o posicionamento relativo dos documentos em função do risco que apresentam, este problema é minimizado. Com certeza que este pressuposto será alvo de estudo em trabalhos futuros.

A metodologia proposta também apresenta uma nova organização do catálogo das medidas, que se adapta aos seus princípios e possibilita uma melhor relação das medidas em função do fim a que se destinam.

A metodologia foi aplicada, com os condicionalismos descritos na secção 6.8, na UCIC do Hospital Infante D. Pedro. Desta aplicação resultou o cálculo do índice do risco de cada documento em função de cada dimensão de segurança. Com base nestes valores foi possível estabelecer uma ordenação dos recursos em função do seu grau de exposição ao dano. Obteve-se um elevado grau de consenso (alpha de Cronbach $\geq$ 0,8), quanto ao valor de cada documento e ao valor da probabilidade de concretização das ameaças. Apesar do hospital não ter uma política de gestão da segurança, foi receptivo a participar neste trabalho. Por parte dos profissionais que participaram nos painéis de peritos e os responsáveis pela UCIC notou-se uma elevada participação. Este facto leva a crer que a metodologia em causa é dinamizadora e motivadora, para uma área que normalmente é descorada nas organizações.

7.2 Análise da metodologia proposta

Na secção 3.5 foram definidos alguns critérios de avaliação das metodologias descritas, com base nos quais foi elaborado a Tabela 3.5. Cabe agora submeter a metodologia proposta à mesma avaliação (Tabela 7.1).

	Metodologia Proposta	ISO/IEC 13335 (abordagem heterogénea)	OCTAVE	ISRAM
Definição completa do processo de gestão do risco	Sim	Sim	Sim	Não
Aplicabilidade a organizações complexas*	Média	Baixa	Baixa	Média
Abordagem prioritária dos sistemas críticos	Sim	Sim	Sim	Não
Tempo de implementação*	Médio	Alto	Alto	Baixo
Aplicação por elementos internos	Sim	--[31]	Sim	Sim
Necessidade de recursos humanos e financeiros*	Médio	Elevado	Elevado	Baixo
Referência de aplicação em unidades de saúde	"anexo B"	Não	Sim	Sim
Apresentação de um catálogo de medidas	Sim	Sim	Não	Não
Universalidade	Sim	Sim	Não	Não

* - Critério de avaliação subjectivo (resulta da análise da metodologia).

Tabela 7.1 - Comparação da metodologia proposta

[31] A norma nada refere relativamente a este ponto, mas dada a sua complexidade é provável que haja necessidade de recorrer a consultores externos.

As vantagens que a metodologia proposta apresenta de *"Definição completa do processo de gestão do risco"* de *"Abordagem prioritária dos sistemas críticos"* e de *"Universalidade"* são consequência da metodologia derivar da ISO/IEC 13335.

As alterações e algumas inovações apresentadas na metodologia proposta e referidas na secção anterior, permitiram melhorar em alguns aspectos a abordagem heterogénea proposta pela norma ISO/IEC 13335. Destacam-se a maior facilidade de implementação, a menor necessidade de recursos humanos e financeiros e, também, capacidade de responder às necessidades das unidades de saúde.

A metodologia proposta pode ainda ser analisada à luz dos princípios (secção 3.3.1) que o OCTAVE impõe para qualquer método que pretenda estar de acordo com a sua filosofia para a gestão do risco. Nas tabelas seguintes (Tabela 7.2, Tabela 7.3 e Tabela 7.4) apresenta-se a avaliação da metodologia no que diz respeito ao cumprimento ou não dos princípios OCTAVE.

Princípios OCTAVE **(quanto à avaliação do risco)**	Descrição do princípio	Metodologia proposta
Auto–administração	Capacidade de o método ser aplicado pela própria organização sem ter que recorrer a entidades externas.	Cumpre
Adaptabilidade à evolução	A avaliação do risco deverá conter mecanismos para prever e actuar perante alterações nos SI.	Cumpre
Caracterização do processo	Todo o processo de avaliação do risco, deve estar definido.	Cumpre
Processo contínuo e cíclico	A avaliação do risco, deve ser implementada de forma a promover que a gestão do risco faça parte da rotina diária da organização e seja um processo contínuo.	Cumpre

Tabela 7.2 - Verificação dos princípios OCTAVE na metodologia proposta - I

Princípios OCTAVE **(quanto ao processo de gestão do risco)**	Descrição do princípio	Metodologia proposta
Visão evolutiva	A equipa deve ter a capacidade de ter uma visão estratégica do futuro sobre os problemas da segurança da informação.	(ver texto)
Centralização nos recursos críticos	Todo o processo de gestão do risco deve estar centrado nos recursos que apresentam um índice mais elevado do risco.	Cumpre
Gestão integrada	As políticas de segurança devem demonstrar consistência e alinhamento com a política geral da organização.	Cumpre

Tabela 7.3 - Verificação dos princípios OCTAVE na metodologia proposta - II

Princípios OCTAVE **(quanto à cultura organizacional)**	Descrição do Princípio	Metodologia proposta
Comunicação aberta	Devem ser criadas formas ágeis de comunicação e divulgação da informação, inerente ao processo da gestão do risco.	Não cumpre (ver texto)
Perspectiva globalizante	Em todo o processo deve haver uma visão global da segurança da informação.	Cumpre
A equipa	Na organização deverá existir uma equipa multidisciplinar responsável quer pela condução, quer pela operacionalização de todo o processo.	Não cumpre (ver texto)

Tabela 7.4 - Verificação dos princípios OCTAVE na metodologia proposta – III

Da análise das tabelas anteriores é possível verificar que a metodologia proposta cumpre, em grande medida, os princípios impostos para que uma metodologia esteja de acordo com o OCTAVE.

A metodologia proposta nada define de quem é o responsável máximo pela processo de gestão do risco. Ela limita-se a definir, para algumas das fases do processo os elementos que deveram dar o seu contributo.

No que diz respeito à necessidade da equipa responsável pelo processo de gestão do risco ter uma visão estratégica do futuro sobre os problemas da segurança da informação na organização, ela não se encontra explicitamente evidenciada na metodologia proposta. Todavia, ao propor-se que o processo de gestão do risco seja cíclico, contínuo e em avaliação constante, os problemas associados com a incerteza da evolução do índice do risco são reduzidos. Assim há a garantia que a política da segurança esteja, em cada momento, alinhada com a realidade da organização e do meio que a envolve.

Relativamente ao princípio da *comunicação aberta* que impõe que haja mecanismos expeditos para a comunicação e divulgação da informação referente ao processo de gestão do risco, a metodologia proposta é omissa. Dentro desta área, a metodologia proposta limita-se a usar algumas técnicas (entrevistas estruturadas, método de Delphi) que resolvem e agilizam alguns processos de comunicação entre alguns intervenientes no processo de gestão do risco.

7.3 Trabalhos futuros

No decorrer da elaboração deste trabalho foi possível identificar algumas linhas orientadoras para possíveis trabalhos a desenvolver. Nesta sequência indicam-se alguns pontos de partida para trabalhos futuros:

1. Como determinar a relação custo/benefício de uma medida? Uma vez determinado o risco dos documentos, será possível criar um sistema de apoio à escolha das medidas? Será este sistema passível de automatização?

De facto será pertinente desenvolver um sistema de suporte à selecção das medidas a aplicar a cada documento, consoante o seu índice de risco. Provavelmente alguns dos parâmetros a ter em conta serão, para além do valor do risco, a eficácia e o custo da implementação das diferentes medidas. Além disso, será necessário perceber se haverá outros parâmetros em causa e qual a interacção dos diferentes parâmetros entre si. Uma vez consolidada a identificação e caracterização dos parâmetros essenciais, será necessário construir um indicador ou uma função, que permita classificar cada medida segundo o problema de segurança que se pretende resolver.

2. Na prestação de cuidados de saúde há uma permanente recolha, sistematização, armazenamento e consulta de informação. Por certo um dos trabalhos a desenvolver será identificar e classificar as vulnerabilidades específicas das organizações que prestam aquele tipo de cuidados.

3. A metodologia proposta assumiu que as fases da avaliação e monitorização deveriam seguir o que era preconizado na ISO/IEC 13335. Estas fases são de extrema importância não só para manter adequado o nível de segurança dos recursos existentes, como também para permitir a adaptação às novas realidades da organização e do meio que a envolve.

   As questões que se colocam são se é possível tornar estas fases em processos de aplicação mais ágil, que envolvam menos recursos humanos e tempo consumido e como se pode adaptar o processo de avaliação e monitorização às unidade de saúde.

4. Um dos maiores entraves à implementação de uma qualquer política de segurança, nomeadamente em Portugal, é a falta de sensibilização das administrações para as questões de segurança. Uma tarefa que está por fazer é estudar a forma de sensibilizar eficazmente as administrações. Para além de uma metodologia ágil e consumidora de poucos recursos, haverá outros factores capazes de influenciar as administrações na adopção de uma metodologia de gestão da segurança?

5. Organizações semelhantes têm problemas de segurança comuns. Comparar índices do risco para documentos semelhantes em organizações diferentes, será um trabalho futuro difícil mas importante. O maior desafio será contudo, estabelecer indicadores capazes de permitir a comparação de diferentes metodologias e estratégias de implementação em organizações distintas. Avaliar-se-iam diferentes políticas de segurança de forma objectiva e por outro lado, fomentava-se uma cultura global de segurança.

Capítulo 8
Referências

[1] M. Gerber and R. von Solms, "Management of risk in the information age," *Computers & Security*, vol. 24, pp. 16-30, 2005.

[2] ISO/IEC-17799, "17799 - Information technology - Security techniques - Code of pratice for information security management," 2005.

[3] J. C. Dennis, *Privacy & Confidentiality of Health Information*: An AHA Press/Jossey-Bass Publication, 2000.

[4] A. Guerra, "Relatório de auditoria ao tratamento de Informação de saúde nos hospitais," Comissão Nacional de Protecção de Dados 2004.

[5] B. Karabacak and I. Sogukpinar, "ISRAM: information security risk analysis method," *Computers & Security*, vol. 24, pp. 147159, 2005.

[6] M. Gerber and R. von Solms, "From Risk Analysis to Security Requirements," *Computers & Security*, vol. 20, pp. 577-584, 2001.

[7] C. P. Pfleeger and S. L. Pfleeger, *Security in Computing*, 3nd ed ed: Prentice Hall PTR, 2002.

[8] J. H. P. Eloff and M. M. Eloff, "Information security architecture," *Computer Fraud & Security*, vol. 2005, pp. 10-16, 2005.

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

[10] A. Carneiro, *Auditoria de Sistemas de Informação*: FCA, 2004.

[11] S. Barman, *Writing Information Security Policies*, 1º ed ed: Sams, 2001.

[12] J. D. Howard and P. Meunier, "Using a "common language" for computer security incident information," in *Computer Security Handbook*, S. Bosworth and M. E. Kabay, Eds., 4º ed: John Wiley & Sons, INC, 2002.

[13] C. Alberts and A. Dorofee, *Managing Information Security Risks: the OCTAVE approach*, 2º ed: Pearson Educations, Inc, 2004.

[14] A. Carneiro, *Introdução à Segurança dos Sistemas de Informação*: FCA - Editora de Informática, 2002.

[15] B. Barber, K. Louwerse, and J. Davey, "White Paper on Health Care Information Security," vol. 2003: Implementing Secure Healthcare Telematics Applications in Europe, 1997.

[16] T. Petrocelli, *Data Protection and Information Lifecycle Management*: Prentice Hall PTR, 2005.

[17] A. Miguel, *Gestão do Risco e da Qualidade no Desenvolvimento de Software*: FCA, 2002.

[18] D. Forte, "Information Security Assessment: Procedures and Methodology: When investing in technology isn't enough," *Computer Fraud & Security*, vol. 2000, pp. 9-12, 2000.

[19] B. H. Waldo, "Managing Data Security: Developing a Plan to Protect Patient Data," *Nursing Economic$*, vol. 17, pp. 49-52, 1999.

[20] T. R. Peltier, J. Peltier, and J. Blackley, *Information security fundamentals*: Auerbach Publications - A CRC Press Company, 2005.

[21] D. Trcek, "Security policy conceptual modeling and formalization for networked information systems," *Computer Communications*, vol. 23, pp. 1716-1723, 2000.

[22] H. D. Santos, "ISO/IEC 27001 – A norma das normas em Segurança da Informação," *Publicação da Associação Portuguesa para a Qualidade*, vol. 1, pp. 11-19, 2006.

[23] R. Kazman and D. N. Port, "Risk Management for IT Security," in *Handbook of Information Security - Threats, Vulnerabilities, Prevention, Detection, and Management*, vol. 3, J. Wiley, Ed., 2006.

[24] D. B. 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.

[25] ISO/IEC-13335(1), "Information technology - Security techniques - Management of information and communications technology security," in *Part 1: - Concepts and models for information and communications technology security management*, 2004.

[26] R. J. Anderson, *Security Engineering: A Guide to Building Dependable Distributed system*: Wiley Computer Publishing, 2001.

[27] R. V. Jacobson, "Risk Assessment and Risk Management," in *Computer Security Handbook*, S. Bosworth and M. E. Kabay, Eds., 4º ed: John Wiley & Sons, INC, 2002.

[28] E. Cavalli, A. Mattasoglio, F. Pinciroli, and P. Spaggiari, "Information security concepts and practices: the case of a provincial multi-specialty hospital," *International Journal of Medical Informatics*, vol. 73, pp. 297-303, 2004.

[29] M. Cremonini and P. Samarati, "Contingency Planning Management," in *Handbook of Information Security - Threats, Vulnerabilities, Prevention, Detection, and Management*, vol. 3, J. Wiley, Ed., 2006.

[30] H. D. Santos, "O Combate Electrónico - Ataques e Defesas sobre a Rede," presented at A Evolução Tecnológica na Protecção da Informação em Sistemas Distribuídos, Instituto de Defesa Nacional, Lisboa, 2002.

[31] J. Sherwood, A. Clark, and D. Lynas, *Enterprise Security Architecture: A Business - Drivem Approach*: CMP Books, 2005.

[32] ISO/IEC-13335, "Information technology - Security techniques - Management of information and communications technology security," 2004.

[33] ISO/IEC-13335(4), "Information technology - Security techniques - Management of information and communications technology security," in *Part 4: -Selection of safeguards*, 2000.

[34] J. Collmann, A. Alaoui, D. Nguyen, and D. Lindisch, "Safe teleradiology: Information assurance as project planning methodology," *Journal of the American Medical Informatics Association*, vol. 12, pp. 84-89, 2005.

[35] J. Collmann, "Assessing information security risk in dual-use health information systems," *International Congress Series*, vol. 1281, pp. 296-301, 2005.

[36] J. Coleman, "Assessing information security risk in healthcare organizations of different scale," *International Congress Series*, vol. 1268, pp. 125-130, 2004.

[37] B. Karabacak and I. Sogukpinar, "A quantitative method for ISO 17799 gap analysis," *Computers & Security*, vol. 25, pp. 413-419, 2006.

[38] ISO/IEC, "13335 - Information technology - Security techniques - Management of information and communications technology security," 2004.

[39] A. d. República, "Constituição da República Portuguesa," http://www.parlamento.pt/const_leg/crp_port/constpt2005.pdf, Ed., 2005.

[40] "Lei n.º 67/98," in *Lei da Protecção de Dados Pessoais (transpõe para a ordem jurídica portuguesa a Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados)*, 1998, pp. D.R. n.º 247, Série I-A de 26 de Novembro.

[41] "Lei n.º 10/91," in *Lei da Protecção de Dados Pessoais face à Informática*, 1991, pp. D.R. n.º 98, Série I-A de 29 de Abril.

[42] "Lei n.º 28/94," in *Aprova medidas de reforço da protecção de dados pessoais*, 1994, pp. D.R. n.º 199, Série I-A de 29 de Agosto.

[43] "Public Law 104-191 - Health Insurance Portability and Accountability," in *http://aspe.hhs.gov/admnsimp/pl104191.htm*, 1996.

[44] J. Tan, *E-Health Care Information Systems: An Introduction for Students and Professionals*: Jossey-Bass/ Wiley, 2005.

[45] K. Beaver and R. Herold, *The Pratical Guide to HIPAA privacy and security compliance*: Auerbach, 2004.

[46] D. Krager and C. Krager, *HIPAA for Medical Office Personnel*: Thomson - Delmar Learning, 2005.

[47] R. Wood, J. Van Moore, Arl, and M. J. Kelley, "The Headache That Has HIPAA Written All Over It!," *Journal of the American College of Radiology*, vol. 2, pp. 708-711, 2005.

[48] D. A. Tribble, "The Health Insurance Portability and Accountability Act: Security and Privacy Requirements," *Am J Health-Syst Pharm*, vol. 58(9), pp. 763-770, 2001.

[49] G. J. Annas, "HIPAA - Regulations - A New Era of Medical-Record Privacy ?," *New England Journal of Medicine*, vol. 348(15), pp. 1486 - 1490, 2003.

[50] "45 CFR Parts 160, 162 anda 164 Health Insurance Reform: Security Standars; Final Rule," in *Department of Health anda Human Services*. http://www.cms.hhs.gov/SecurityStandard/Downloads/securityfinalrule.pdf: (acedido em 17/7/2006), 2006.

[51] United States Department of Healt and Human Services, "Protecting Personal Health Information in Research: Understanding the HIPAA Privacy Rule," NIH Publication number 03-5388, 2004.

[52] D. S. Friedman, "HIPAA and Research: How Have the First Two Years Gone?," *American Journal of Ophthalmology*, vol. 141, pp. 543, 2006.

[53] "Lei n.º 27/2002," in *Aprova o novo regimento jurídico da gestão hospitalar e procede à primeira alteração à Lei nº 48/90 de 24 de Agosto*, 2002, pp. DR - I Série/A, nº 258 de 8 de Novembro de 2002.

[54] "Decreto-Lei nº. 233/2005," 2005, pp. DR - I Série/A, nº 249 de 29 de Dezembro de 2005.

[55] "Decreto-Lei nº. 93/2005," 2005, pp. DR - Série I-A, n.º 191 de 20 de Agosto de 2003.

[56] "Decreto-Lei nº. 188/2003," 2003.

[57] "Informação Institucional," in *Hospital Infante D. Pedro - Aveiro*. http:\\www.hip.pt\hospital5.htm: (acedido em 17/7/2006), 2004.

[58] "Organograma do Hospital de São Marcos - Braga," in *Hospital de São Marcos - Braga*. http://www.hsmbraga.min-saude.pt: (acedido em 17/7/2006), 2005.

[59] "Estrutura hierárquica e funcional do hospital," in *Hospital de São Sebastião, EPE*. http://www.hospitalfeira.min-saude.pt: (acedido em 17/7/2006), 2006.

[60] "Organograma do HDFF, EPE," in *Hospital Distrital da Figueira da Foz, EPE*. http://www.hdfigueira.min-saude.pt: (acedido em 12/10/2006), 2006.

[61] "Organograma do Hospital de Santarém," in *Hospital Distrital de Santarém, EPE*. http://www.hds.min-saude.pt: (acedido em 17/7/2006), 2006.

[62] K. Simpson and M. Gordon, "The anatomy of a clinical information system," *BMJ*, vol. 316, pp. 1655-1658, 1998.

[63] Tim Benson, "Why general practitioners use computers and hospital doctors do not - Part 2: scalability," *BMJ*, vol. 325, pp. 1090-3, 2002.

[64] M. A. Green and M. J. Bowie, *Essentials of Health Information Management: Principles and Practices*: Thomson Delmar Learning, 2005.

[65] F. M. Behlen and S. B. Johnson, "Multicenter Patiente Records Research: Security Policies and Tools," *Journal American Medical Informatics Association*, vol. 6, pp. 435-443, 1999.

[66] T. C. Rindfleisch, "Confidentiality, Information Technology, and Health Care," School of Medicine, Standford University, 1997.

[67] "Conceitos Estatísticos," in *Instituto Nacional de Estatística*. http://conceitos.ine.pt/pesquisa2.asp: (acedido em 17/7/2006), 2006.

[68] K. Wilber, "HIPAA Security Requirements," *Healthplan*, vol. 44(1), pp. 28 - 31, 2003.

[69] N. M. Martel, "Medical Records Security," in *Handbook of Information Security - Threats, Vulnerabilities, Prevention, Detection, and Management*, vol. 3, J. Wiley, Ed., 2006.

[70] P. J. Brusil and D. Harley, "Medical Records Security," in *Computer Security Handbook*, S. Bosworth and M. E. Kabay, Eds., 4º ed: John Wiley & Sons, INC, 2002.

[71] C. Laske, "Legal Liability for telemedicine and healthcare networking," vol. 2003: ISHTAR, 1998.

[72] G. Pangalos, "Confidentiality in Healthcare in Greece," EHTO Enterprise, 1998.

[73] L. Ravera, I. Colombo, M. Tedeschi, and A. Ravera, "Security and privacy at the private multispecialty hospital Istituto Clinico Humanitas: strategy and reality," *International Journal of Medical Informatics*, vol. 73, pp. 321-324, 2004.

[74] The Royal College of Radiologists, *Clinical Radiology and Electronic Records*: Board of Faculty of Clinical Radiology & Royal College of Radiologists, London, 2002.

[75] P. White, "Privacy and security issues in teleradiology," *Seminars in Ultrasound, CT, and MRI*, vol. 25, pp. 391-395, 2004.

[76] B. Baum-Waidner and B. Blobel, "Requirements for a Secure Healthcare System Architecture," vol. 2003: ISHTAR, 1998.

[77] T. R. Peltier, *Information Security Risk Analysis*: CRC Press LLC, 2001.

[78] S. J. van Zolingen and C. A. Klaassen, "Selection processes in a Delphi study about key qualifications in Senior Secondary Vocational Education," *Technological Forecasting and Social Change*, vol. 70, pp. 317-340, 2003.

[79] C. P. Andres, "Deben estar las técnicas de consenso incluidas entre las técnicas de investigación cualitativa," *Rev. Esp. Salud Publica*, vol. 74, 2000.

[80] J. Jones and D. Hunter, "Qualitative Research: Consensus methods for medical and health services research," *BMJ*, vol. 311, pp. 376-380, 1995.

[81] J. Landeta, "Current validity of the Delphi method in social sciences," *Technological Forecasting and Social Change*, vol. 73, pp. 467-482, 2006.

[82] A. J. Angus, I. D. Hodge, S. McNally, and M. A. Sutton, "The setting of standards for agricultural nitrogen emissions: a case study of the Delphi technique," *Journal of Environmental Management*, vol. 69, pp. 323-337, 2003.

[83] S. M. Campbell, J. A. Cantrill, and D. Roberts, "Prescribing indicators for UK general practice: Delphi consultation study," *BMJ*, vol. 321, pp. 425-428, 2000.

[84] L. Santos and L. Amaral, "Estudos Delphi com Q-Sort sobre a web : a sua utilização em sistemas de informação," presented at 5º Conferência da Associação Portuguesa de Sistemas de Informação, Lisboa, 2004.

[85] B. Graham, G. Regehr, and J. G. Wright, "Delphi as a method to establish consensus for diagnostic criteria," *Journal of Clinical Epidemiology*, vol. 56, pp. 1150-1156, 2003.

[86] S. Keeney, F. Hasson, and H. P. McKenna, "A critical review of the Delphi technique as a research methodology for nursing," *International Journal of Nursing Studies*, vol. 38, pp. 195-200, 2001.

[87] L. D. Santos, "Factores determinantes do sucesso de serviços de informação online em sistemas de gestão de ciência e tecnologia," in *Tese de Doutoramento*: Universidade do Minho, 2004.

[88] A. Alahlafi and S. Burge, "What should undergraduate medical students know about psoriasis? Involving patients in curriculum development: modified Delphi technique," *BMJ*, vol. 330, pp. 633-636, 2005.

[89] J. Stewart, C. O'Halloran, P. Harrigan, J. A. Spencer, J. R. Barton, and S. J. Singleton, "Identifying appropriate tasks for the preregistration year: modified Delphi technique," *BMJ*, vol. 319, pp. 224-229, 1999.

[90] A. M. Deshpande, R. N. Shiffman, and P. M. Nadkarni, "Metadata-driven Delphi rating on the Internet," *Computer Methods and Programs in Biomedicine*, vol. 77, pp. 49-56, 2005.

[91] C. M. Goodman, "The Delphi technique: a critique," *Journal of Clinical Nursing*, vol. 12, pp. 729-734, 1987.

[92] M. K. Rayens and E. J. Hahn, "Building Consensus Using the Policy Delphi Method," *Policy Polit Nurs Pract*, vol. 1, pp. 308-315, 2000.

[93] L. L. Gustafson, S. K. Ellis, and C. A. Bartlett, "Using expert opinion to identify risk factors important to infectious salmon-anemia (ISA) outbreaks on salmon farms in Maine, USA and New Brunswick, Canada," *Preventive Veterinary Medicine*, vol. 70, pp. 17-28, 2005.

[94] G. Elwyn, A. O'Connor, D. Stacey, R. Volk, A. Edwards, A. Coulter, R. Thomson, A. Barratt, M. Barry, S. Bernstein, P. Butow, A. Clarke, V. Entwistle, D. Feldman-Stewart, M. Holmes-Rovner, H. Llewellyn-Thomas, N. Moumjid, A. G. Mulley, C. Ruland, K. Sepucha, A. Sykes, T. Whelan, and on behalf of the International Patient Decision Aids Standards (IPDAS) Collaboration, "Developing a quality criteria framework for patient decision aids: online international Delphi consensus process," *BMJ*, pp. bmj.38926.629329.AE, 2006.

[95] S. G. J. Rodel, R. H. Geelkerken, J. A. v. Herwaarden, E. E. Kunst, J. C. v. d. Berg, J. v. d. Palen, J. A. W. Teijink, and F. L. Moll, "Consistency in endovascular aneurysm repair suitability assessment requires group decision audit," *Journal of Vascular Surgery*, vol. 43, pp. 671-676, 2006.

[96] R. Giribone and B. Valette, "Principles of failure probability assessment (PoF)," *International Journal of Pressure Vessels and Piping 29th MPA Seminar in the series Safety and Reliability of Pressure Components - Stuttgart, October 9th and 10th, 2003*, vol. 81, pp. 797-806, 2004.

[97] R. O'Loughlin and A. Kelly, "Equity in resource allocation in the Irish health service: A policy Delphi study," *Health Policy*, vol. 67, pp. 271-280, 2004.

[98] M. M. Hill and A. Hill, *Investigação por questionário*: Edições Sílabo, 2002.

[99] J. P. Thomas and N. Siupsinskiene, "Frozen versus fresh reconstituted botox for laryngeal dystonia," *Otolaryngology - Head and Neck Surgery*, vol. 135, pp. 204-208, 2006.

[100] J. M. Foster, L. Aucott, R. H. W. van der Werf, M. J. van der Meijden, G. Schraa, D. S. Postma, and T. van der Molen, "Higher patient perceived side effects related to higher daily doses of inhaled corticosteroids in the community: A cross-sectional analysis," *Respiratory Medicine*, vol. 100, pp. 1318-1336, 2006.

[101] N. D. Ferguson, A. M. Davis, A. S. Slutsky, and T. E. Stewart, "Development of a clinical definition for acute respiratory distress syndrome using the Delphi technique," *Journal of Critical Care*, vol. 20, pp. 147-154, 2005.

[102] C. Moldrup and J. M. Morgall, "Risks of Future Drugs: A Danish Expert Delphi," *Technological Forecasting and Social Change*, vol. 67, pp. 273-289, 2001.

[103] J. W. Beckstead, "Reporting peer wrongdoing in the healthcare profession: the role of incompetence and substance abuse information," *International Journal of Nursing Studies*, vol. 42, pp. 325-331, 2005.

[104] V. J. Easton and J. H. McColl, "Statistics Glossary v1.1," in *acedido em 7-6-2006*, www.stats.gla.ac.uk/steps/glossary/probability.html, Ed.: STEPS, 2006.

[105] F. A. Dahl, "Representing human uncertainty by subjective likelihood estimates," *International Journal of Approximate Reasoning*, vol. 39, pp. 85-95, 2005.

[106] N. O. Siu and D. L. Kelly, "Bayesian parameter estimation in probabilistic risk assessment," *Reliability Engineering & System Safety*, vol. 62, pp. 89-116, 1998.

[107] P. S. Anton, R. H. Anderson, R. Mesic, and M. Scheiern, *The Vulnerability Assessment and Mitigation Methodology*: RAND - National Defense Research Institute, 2003.

Anexo A

Catálogo de medidas

A. Catálogo de medidas

Apresenta-se neste anexo um catálogo de medidas segundo a organização proposta na secção 6.5.

À frente de cada medida é colocada, entre parênteses rectos, a sua classificação de acordo com as definições apresentadas no Capítulo 3. Em alguns casos uma medida pertence a dois ou mais grupos e noutros não é possível aplicar as regras de classificação.

O catálogo apresentado, não é, nem nunca será um catálogo fechado e acabado. À medida que a metodologia vai sendo aplicada em diversas organizações com certeza que serão acrescentadas novas entradas ao catálogo.

A.1. Medidas Estratégicas

A.1.1. Política de sensibilização e treino (E1)

1. Todos os funcionários devem perceber as regras de segurança a que estão sujeitos, bem como as responsabilidades que lhes são inerentes **[dissuasão]**;
2. O plano de formação deverá permitir dotar a organização de peritos nas diversas tecnologias usadas pela organização, de forma a que as tecnologias sejam usadas de modo seguro **[prevenção]**;
3. Deverão ser efectuadas, de forma regular, acções de formação na área da segurança da informação para todos os funcionários da organização. Estas acções deverão ser adaptadas em função dos funcionários e da área da organização onde exercem a sua actividade **[prevenção]**;
4. Deverá ser estabelecido um plano de divulgação das medidas adoptadas. A divulgação das medidas deverá ser feita de forma regular e apresentada com carácter pedagógico. Por exemplo, o recurso ao correio electrónico personalizado ou a utilização das mensagens nos protectores de écran podem ser dois meios a ter em conta na divulgação **[dissuasão] e [prevenção]**.

A.1.2. Política de segurança nas relações com terceiros (E2)

1. A organização deverá garantir que o acesso à informação por parte da entidade externa se encontra dentro do enquadramento legal;
2. Quando entidades externas tiverem acesso ao sistema de informação ou a elementos que o constituem, a organização deve monitorizar e documentar detalhadamente cada acesso, bem como todas as comunicações de dados de e para a entidade externa **[detecção]**;
3. Às entidades externas a organização deve, dentro do limite legal, exigir um nível de segurança, pelo menos, equivalente ao existente na organização para o tipo de informação a que tenham acesso.

A.1.3. Planos de contingência (E3)

1. Deverão ser elaborados planos de contingência para os sistemas de informação de forma a estabelecer o seu funcionamento em situações de emergência, nomeadamente decorrentes da eventualidade de um incidente de segurança **[correcção]**;
2. Deverão ser elaborados planos de recuperação dos sistemas de informação caso a ocorrência de um incidente de segurança comprometa parcialmente ou na totalidade, o seu funcionamento **[correcção]**;
3. Os planos de recuperação e de contingência deverão ser testados e revistos de forma periódica, ou sempre que haja alterações nos sistemas de informação **[correcção]**;

A.1.4. Política de segurança e regulamentos (E4)

1. Definição do intervalo de tempo máximo admissível entre duas revisões sucessivas das políticas de segurança. Esta definição não deverá colocar em causa o princípio cíclico do processo de segurança;

2. Estabelecer um plano de auditorias de forma a detectar desvios no cumprimento na política de segurança adoptada **[detecção]**;
3. A política de segurança deve estar documentada e constar de um documento formal, o qual deverá conter pelos mesmos os seguintes itens:
    - Enquadramento legal;
    - Objectivos;
    - Modelo gestão do risco;
    - Medidas adoptadas. Havendo para cada uma das medidas os seguintes itens:
        - Descrição da medida;
        - Finalidade da medida;
        - Destinatários (responsáveis pela implementação e pela execução da medida);
        - Data da criação da medida;
        - Data da última revisão da medida;
        - Procedimentos de implementação;
        - Penalidades para o não cumprimento do estabelecido na medida;
        - Condições excepcionais que obriguem a rever ou suspender a medida ou a aplicar uma medida alternativa.

A.2. Medidas Operacionais (O)

Apesar de se usar a taxinomia seguida na metodologia OCTAVE (medidas operacionais), optou-se por usar as medidas indicadas pelo catálogo ISO/IEC 13335, uma vez que, este organiza as medidas em função das dimensões (confidencialidade, integridade e disponibilidade). Contudo há algumas

medidas[32] cujo objectivo é comum na ISO/IEC 17799 e na ISO/IEC 13335. Nestes casos optou-se pelas medidas preconizadas pela ISO/IEC 17799, que são mais detalhadas, mantendo no entanto a mesma indexação às dimensões presente na ISO\IEC 13335.

A.2.1. Genéricas (OG)

Medidas genéricas não tecnológicas (OGnT)

1. Cada funcionário da organização têm a obrigação de comunicar qualquer tipo de incidente de segurança que tenha conhecimento a quem de direito. Para uma melhor eficiência, a organização deve definir um protocolo a usar para a identificação e a comunicação dos incidentes. Poderão existir sistemas que identifiquem e relatem de forma automática os incidentes de segurança **[detecção]**;
2. Os funcionários da organização devem registar qualquer vulnerabilidade que detectem e comunicá-la a quem de direito no mais curto espaço de tempo **[detecção]**;
3. Todos os funcionários da organização devem estar sujeitos a cláusulas contratuais que estipulem a obrigatoriedade do cumprimento da política de segurança instituída **[dissuasão]**;
4. Todos os registos decorrentes da execução dos diversos procedimentos, devem ser analisados, periodicamente, de forma a detectar a execução de procedimentos não autorizados ou executados por entidades não autorizadas **[detecção]**;

[32] Por exemplo, as medidas relacionadas com a prevenção, detecção e correcção do código malicioso.

5. Todos os funcionários da organização devem conhecer as consequências do não cumprimento da política de segurança **[dissuasão]**;
6. Na organização deve estar implementada uma política de inventário **[dissuasão]**;
7. Deverá ser efectuada a manutenção periódica dos recursos existentes na organização de acordo com um determinado protocolo **[prevenção]**;
8. Deverá haver um registo de todas as intervenções efectuadas em cada recurso, com a indicação, no mínimo, da data e do responsável pela operação, bem como uma breve descrição da intervenção efectuada **[dissuasão]**;
9. Deverão ser asseguradas as condições ambientais de temperatura e humidade recomendadas para cada recurso **[prevenção]**;
10. Todas as operações efectuadas de gestão dos sistemas de informação devem ser executadas de forma a minimizar os erros técnicos que possam ocorrer na sua execução **[prevenção]**;
11. Todos os funcionários que lidam com os sistemas de informação devem ser treinados e formados de forma a minimizar a ocorrência de erros de utilização **[prevenção]**;

Medidas genéricas associados à tecnologia (OGT)

1. Verificação periódica dos suportes físicos da informação, de forma a detectar deteriorações que coloquem em causa a disponibilidade da informação **[detecção]** ;
2. Estabelecer uma política formal de protecção dos riscos associados há proliferação e execução de código malicioso, nomeadamente no que se refere à instalação e actualização de sistemas de detecção e correcção **[detecção], [prevenção] e [correcção]**;

3. Estabelecer procedimentos de forma a recolher a informação disponível sobre o código malicioso, por exemplo com o recurso a mails-list, "certs" **[prevenção]**;
4. Os funcionários devem registar qualquer mau funcionamento das aplicações informáticas e comunicá-las a quem de direito no mais curto espaço de tempo **[detecção]**;
5. Os recursos devem estar protegidos contra falhas de energia, por exemplo com o recurso a unidades interruptas de energia **[prevenção]**;
6. Proibição da instalação de qualquer tipo de programa informático, ou alteração dos instalados, sem a prévia autorização do responsável pela segurança da organização **[prevenção] e [dissuasão]**;
7. A rede de telecomunicações (voz e dados) deve ser planeada de forma a evitar a ocorrência de congestionamento de tráfego **[prevenção]**.

A.2.2. Específicas (OE)

Por uma questão de organização apresentam-se inicialmente as medidas que, segundo a ISO/IEC 13335, afectam todas as dimensões. Posteriormente mencionam-se as medidas que se destinam a cada uma das dimensões.

Medidas que afectam todas as dimensões

Ref	Medida	Dimensão			
		C	*I*	*D*	*A/R*[33]
1	Usar mecanismos de identificação e autenticação dos utilizadores com base em algo que o utilizador conhece (tipicamente pwd) **[prevenção]**.	X	X	X	X
2	Usar mecanismos de identificação e autenticação dos utilizadores com base em algo que o utilizador possui (um cartão, ...) **[prevenção]**.	X	X	X	X
3	Usar mecanismos de identificação e autenticação dos utilizadores com base em características intrínsecas ao utilizador (biometria,...) **[prevenção]**.	X	X	X	X
4	Usar mecanismos de identificação e autenticação dos utilizadores que combinem algo que o utilizador conhece, com algo que possui ou com alguma característica biométrica do utilizador **[prevenção]**.	X	X	X	X
5	Combinação de mecanismos de controlo de acessos lógicos com os mecanismos de identificação e autenticação de forma a prevenir o acesso não autorizado **[prevenção]** .	X	X	X	X
6	Os dispositivos de armazenamento amovíveis devem ser alvo de medidas que dificultem acesso não autorizado **[prevenção]**.	X	X	X	X

Tabela A.1 - Medidas que afectam todas as dimensões

[33] A dimensão autoria/responsabilidade não é considerada na ISO/IEC 13335, no entanto as medidas foram avaliadas quanto a esta dimensão.

Medidas que afectam a confidencialidade

1. As divisões, as paredes e os edifícios devem ser construídos de forma a dificultar ou a impedir a ocorrência de qualquer tipo de escutas (incluindo a intercepção electromagnética) **[prevenção]**.
2. As redes de energia eléctrica e de telecomunicações (voz e dados) associadas aos sistemas de informação, devem ser protegidas de intercepções, sobrecargas ou danos acidentais, ou intencionais **[prevenção]**;
3. Estabelecer regras rígidas de quem, onde e de que forma a informação sensível pode ser "comunicada" **[dissuasão]**;
4. Instalar equipamentos que emitam um baixo nível de radiação electromagnética **[prevenção];**
5. Estabelecer o isolamento físico e/ou lógico da rede informática de suporte aos sistemas críticos **[prevenção]**;
6. Estabelecer regras de cifra da informação **[prevenção]**;
7. Estabelecer regras de utilização da assinatura digital **[prevenção]**;
8. Controlo físico da saída dos recursos dos locais de onde se encontram **[prevenção]**;
9. Codificar a informação quando ela se encontra armazenada **[prevenção]**.

Medidas que afectam a Integridade

1. Estabelecer medidas de verificação da integridade da informação quando se encontra armazenada **[detecção]**;
2. Estabelecer protocolos de comunicação que permitam detectar erros na transmissão dos dados (por exemplo a implementação de mecanismos de checksums, ...) **[detecção]**;
3. Estabelecer regras de cifra da informação **[prevenção]**;
4. Estabelecer regras de utilização da assinatura digital **[prevenção]**;

5. Codificar a informação quando ela se encontra armazenada **[prevenção]**;
6. Estabelecer uma política de cópias de segurança da informação **[correcção]**;

Medidas que afectam a Disponibilidade

1. Dotar os sistemas de redundância **[prevenção]**;
2. Todos os edifícios ou locais que contenham os sistemas de informação (ou partes destes) e cuja a informação com que lidam é sensível, devem ter, dentro do possível, um sistema de protecção de incêndios, inundações e desastres naturais **[prevenção]**;
3. Definição de um plano de continuidade para quando a organização é afectada por um incêndio, uma inundação ou um desastre natural **[correcção]**;
4. Implementar sistemas que permitam detectar o uso abusivo de um determinado recurso ou sistema **[detecção]**;
5. Controlo físico da saída dos recursos dos locais de onde se encontram **[prevenção]**;
6. Estabelecer uma política de cópias de segurança da informação **[correcção]**.

Medidas que afectam a Autoria/Responsabilidade

1. Estabelecer regras de cifra da informação **[prevenção]**;
2. Estabelecer regras de utilização da assinatura digital **[prevenção]**;

Anexo B

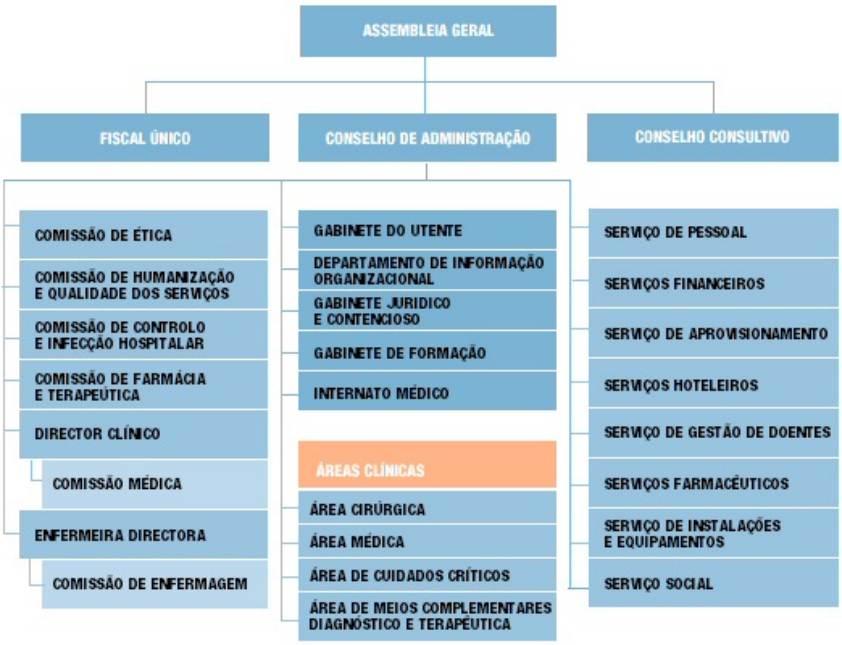
Aplicação da metodologia proposta

B. Aplicação da metodologia proposta

B.1. Caracterização do hospital

Algumas etapas da metodologia proposta foram testadas no Hospital Infante D. Pedro (HIP). Este hospital é do tipo distrital, tem cerca de 400 camas e o seu regime jurídico é EPE.

Na figura é apresentada a organização interna do hospital.



Fonte: http://www.hip.pt/hospital5.htm

Figura B1 – Organiograma do HIP

O estudo referido foi feito na unidade de Cuidados Intensivos Coronários (UCIC).

B.2. Caracterização da unidade de cuidados intensivos coronários

A UCIC está integrada no serviço de Cardiologia do HIP, o qual pertence ao Departamento Médico (designada por área médica no organiograma anterior).

A UCIC tem uma lotação de 5 camas para doentes críticos. Quanto aos recursos humanos, o quadro de o Serviço de Cardiologia[34] em Novembro de 2006, era constituído por 25 enfermeiros, 8 médicos, 9 auxiliares de acção médica e dois funcionários administrativos. À UCIC estão adstritos diariamente elementos do Serviço de Cardiologia, havendo permanência de pelo menos dois enfermeiros, um médico e um auxiliar de acção médica.

Apesar de se tratar de uma unidade os fluxos de informação não estão simplificados. Genericamente, os fluxos são comuns aos dos outros serviços de internamento. Além disso como se trata de uma unidade de doentes críticos a segurança da informação é ainda mais relevante.

B.3. Aplicação de metodologia proposta

B.3.1. Definição dos objectivos

O objectivo do trabalho realizado na UCIC era o de observar aplicabilidade das fases de análise detalhada do risco, nomeadamente a determinação dos índices do risco.

B.3.2. Análise do risco macro

Dado a sua natureza, todos os sistemas de informação existentes na UCIC, são da área clínica/administrativa, pelo que de acordo com a metodologia são classificados como críticos. Esta classificação obriga a que todos sejam alvo de uma análise detalhada do risco.

[34] Refere-se os dados referentes ao Serviço de Cardiologia, onde está integrada a UCIC, uma vez que esta não tem quadro de pessoal próprio.

B.3.3. Identificação dos documentos

Como a metodologia proposta recomenda, fez-se o levantamento dos documentos existentes na unidade através de entrevistas com o Enfermeiro Chefe da Cardiologia e o Director do Serviço de Cardiologia.

Nas reuniões com cada um dos responsáveis citados, foi possível identificar os seguintes documentos[35] em cada grande grupo de documentos:

- Grande grupo de documentos: Processo de Internamento

Ref.	Designação
1	"Registo de Internamento"
2	"hip- diário clínico"
3	"hda-374 folha terapêutica"
4	"hip-092 Registo de análises"
5	“hip-162 História clínica de enfermagem”
6	“hip-091 Folha operatória”
7	“hip-160 Registo do diário clínico de enfermagem”
8	“hip-302 Folha terapêutica enfermagem”
9	“hip-303A Internamento”
10	“hip-585 Perfil glicémico”
11	“hda-513 Balanço hidroelectrolítico”
12	“Resultado de Exames: Imagiológicos; Laboratoriais; e outros
13	“Relatório do Sistema de Monitorização”
14	“Fotocópia do documento do "hip-339-A Ocorrência do S.U”

Tabela B1 – Doc. do processo de internamento

[35] Cada documento foi designado com a referência atribuída pelo hospital.

- Grande grupo de documentos: Sistemas Automáticos de Apoio Clínico

Ref.	Designação
15	“Sistema de monitorização dos doentes”

Tabela B2 – Doc. sistemas automáticos de apoio clínico

- Grande grupo de documentos: Pedidos

Ref.	Designação
16	"hip-535 Requisição de Exames Imagiológicos";
17	"hda-558 - Pedido de análises de Imuno-Hematologia";
18	"hip-559 - Pedido de Transfusão";
19	"hda 419 - Pedido de análises de Anatomia Patológica";
20	"hip-068 Pedido de Ecocardiograma/Electrocardiograma";
21	"hip-433 Pedido de análises Urgentes";
22	"hip-413 Pedido de análises de Hematologia e Coagulação";
23	hip-547 Pedido de análises de Química Clínica";
24	"hip-547/A Pedido de análises de Endocrinologia/Imunologia";
25	hip-580/A Pedido de análises de Microbiologia";
26	"INCM-1804 Medicamentos Hemoderivados";
27	"hip-130 Pedido de Consulta Interna";
28	"hip-658 Justificação de medicamentos extra-formulário";
29	“hip 114 Requisição de exames ao exterior";
30	"Exames requisitados de cardiologia";
31	"Relatório do Serviço de Cardiologia";
32	"hpa - VS Mod 151 a-R*";
33	"Protocolo de pedido de cateterismo cardíaco - SMIC";

Tabela B3 – Doc. dos pedidos

- Grande grupo de documentos: Saída

Ref.	Designação
34	“INCM-1725 Certificado de óbito”;
35	“hip – 049 – Boletim de Informação Clínica e/ou Circunstancial”
36	"hip-183 Transferência/Envio do doente";
37	"Nota de Alta";
38	"Verbete - GDH";

Tabela B4 – Doc. de saída

- Grande grupo de documentos: Transversais

Ref.	Designação
39	“Sonho” (Sistema Gestão de Doentes Hospitalares) – informação referentes ao episódio de internamento;
40	“Processo único”

Tabela B5 – Doc. transversais

Para além da identificação dos documentos, procedeu-se à sua caracterização quanto aos atributos que os constituem. Esta caracterização servirá de base para a agregação dos documentos identificados em documentos genéricos.

B.3.4. Agregação dos documentos

Nesta fase procedeu-se à agregação de documentos semelhantes quanto aos atributos de segurança e quanto ao tipo de informação que contêm. Assim os documentos identificados no secção anterior deram origem aos seguintes documentos genéricos, agrupados por grande grupos:

- Grande grupo de documentos: Processo de Internamento

  1. **"Registo médico"** - documento genérico que agrega todos os registos efectuados pela equipa médica que acompanhou o doente no internamento. Os documentos reais que lhe deram origem foram:
     - "Registo de Internamento",
     - "hip- diário clínico";
     - "hda-374 folha terapêutica";
     - "hip-092 Registo de análises";

  2. **"Registo de enfermagem"** - documento genérico que agrega todos os registos efectuados pela equipa de enfermagem que acompanhou o doente no internamento. Os documentos reais que lhe deram origem foram:
     - "hip-162 História clínica de enfermagem";
     - "hip-091 Folha operatória";
     - "hip-160 Registo do diário clínico de enfermagem";
     - "hip-302 Folha terapêutica enfermagem";
     - "hip-303A Internamento";
     - "hip-585 Perfil glicémico";
     - "hda-513 Balanço hidroelectrolítico";

3. **“Resultado de Exames”** - documento genérico que engloba todos os resultados dos exames que foram efectuados ao doente, aquando do internamento;

4. **“Relatório do Sist. Monitorização”** - documento genérico que agrega toda a informação que pode ser impressa a partir do sistema de monitorização em tempo real;

5. **“Fotocópia da ocorrência no S.U.”** - documento genérico que agrega toda a informação relativa ao episódio de Urgência que motivou o internamento. O documento real que lhe deu origem foi o "hip-339-A Ocorrência do S.U.";

- Grande grupo de documentos: Sistemas Automáticos de Apoio Clínico

6. **“Sistema de Monitorização”** - documento genérico que agrega toda a informação existente no sistema de monitorização em tempo real do doente;

- Grande grupo de documentos: Pedidos

7. “**Pedido de exames Imagiológicos\Patologia Clínica/Imuno-Hemoterapia/Anatomia Patológica”** - documento genérico que agrega todos os pedidos de exames complementares de diagnósticos solicitados ao longo do período de internamento. Os documentos reais que lhe deram origem foram:
    - "hip-535 Requisição de Exames Imagiológicos";
    - "hda-558 Pedido de análises de Imuno-Hematologia";
    - "hip-559 Pedido de Transfusão";
    - "hda 419 Pedido de análises de Anatomia Patológica",
    - "hip-068 Pedido de Ecocardiograma/ Electrocardiograma";

- "hip-433 Pedido de análises Urgentes";
- "hip-413 Pedido de análises de Hematologia e Coagulação";
- hip-547 Pedido de análises de Química Clínica";
- "hip-547/A Pedido de análises de Endocrinologia/ Imunologia";
- hip-580/A Pedido de análises de Microbiologia";

8. **"Hemoderivados (Req\Adm)"** - documento genérico que permite o registo da requisição, distribuição e administração de hemoderivados. O documento real que lhe deu origem foi o "INCM-1804 Medicamentos Hemoderivados";

9. **"Pedido de consulta Interna"** - documento genérico que permite efectuar o pedido de colaboração (consulta interna) de outra especialidade. O documento real que lhe deu origem foi o "hip-130 Pedido de Consulta Interna";

10. **"Pedido de receituário de Med. Extra-Formulário"** - documento genérico permite solicitar medicamentos que não constam no formulário hospitalar. O documento real que lhe deu origem foi o "hip-658 Justificação de receituário de medicamentos extra-formulário";

11. **"Pedido de Exames ao Exterior"** - documento genérico que utilizado para efectuar um pedido de exames, análises ou actos médicos realizados por entidades externas ao hospital. Os documentos reais que lhe deram origem foram:
    - "hip 114 Requisição de exames ao exterior";
    - "Exames requisitados de cardiologia";

- "Relatório do Serviço de Cardiologia";
- "hpa - VS Mod 151 a-R*";
- "Protocolo de pedido de cateterismo cardíaco - SMIC";

- Grupo de documentos: Saída

12. "**Documento de óbito"** - documento genérico que engloba todos os documentos gerados aquando o óbito. Os documento reais que lhe deram origem foram:
    - "INCM-1725 Certificado de óbito";
    - "hip – 049 – Boletim de Informação Clínica e/ou Circunstancial";

13. **"Transferência/Envio do doente"** - documento genérico que acompanha o doente, quanto este é transferido ou enviado para outra unidade de saúde. O documento real que lhe deu origem foi o "hip-183 Transferência/Envio do doente";

14. **"Documento de Alta"** - documento que engloba todos os documentos gerados aquando a alta do doente. Os documentos reais que lhe deram origem foram:
    - "Nota de alta"
    - "Verbete - GDH";

- Grande grupo de documentos: Transversais

15. **"Informação administrativa"** - documento genérico que pretende representar toda a informação de carácter administrativo associada a cada episódio de internamento;

16. **"Processo único"**- documento genérico que agrega o histórico dos episódios de internamento, de consulta, de urgência, de hospital de dia, bem como os exames complementares de diagnóstico;

- Grande grupo de documentos: Saída[36]

17. **"Documento para a Comunicação Obrigatória de Doenças"** – documento genérico que agrega os documentos utilizados para a declaração obrigatória de doenças a entidades externas, nomeadamente, às autoridades de Saúde Pública. O documento real que lhe deu origem foi o modelo 1536 da INCM.

De seguida são apresentados os atributos de cada documento genérico referido anteriormente, de acordo com os documentos que lhe deram origem.

[36] O documento 17 só foi identificado após a primeira ronda do painel de Delphi. Para se manter a coerência da numeração atribuída na 1º ronda aos documentos, atribuí-se o n.º 17 a este documento, embora ele pertença ao grande grupo de documentos "Saída".

Grupo de documentos: Processo de Internamento

Documento Genérico	Lista de atributos
Registo Médico	"Data(s)", "Diagnóstico(s)", "Diário clínico", "História clínica", "ID[37] do doente", "ID do(s) médico(s)", "Terapêutica"
Registo de Enfermagem	"Data(s)", "Diário de enfermagem", "História clínica de enfermagem", "ID do doente", "ID do(s) enfermeiro(s)", "Registos relacionados com a prestação de cuidados de enfermagem"
Resultado de Exames	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do Serviço", "Resultado(s)"
Fotocópia da ocorrência no S.U.	"Data(s)", "Descrição das observações médicas", "Descrição do motivo da vinda", "Descrição/destino do espólio", "Diagnóstico(s)", "Exames pedidos", "ID da proveniência do doente", "ID do acompanhamento", "ID do destino do doente", "ID do doente", "ID do(s) interveniente(s)", "Notas de enfermagem", "Registo de medicação", "Registo dos procedimentos/actos médicos efectuados ", "Registos dos parâmetros metabólicos/vitais e das drenagens", "Triagem de prioridades"
Relatório do Sist. Monitorização	"Data(s)", "Frequência cardíaca", "ID do doente", "Traçado de ECG"

Tabela B6 – Atributos dos Doc. do processo de internamento

[37] ID - Identificação

Grupo de documentos: Pedidos

Documento Genérico	Lista de atributos
Pedido de exames Imagiológicos/ Patologia Clínica/ Imuno-Hemoterapia/ Anatomia Patológica	"Data(s)", "Diagnóstico(s)", "Exames/análises Pedidos", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Material enviado *"
Hemoderivados (Req\Adm)	"Data(s)", "Dose/frequência/duração", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Produto requisitado", "Registo de administração", "Registo de distribuição"
Pedido de consulta Interna	"Data realização da consulta *", "Data(s)", "Designação da consulta pretendida", "ID do doente", "ID do médico que efectuou a consulta", "ID do médico requisitante", "ID do receptor do pedido *"
Pedido de receituário de Med. Extra-Formulário	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Medicamento"
Pedido de Exames ao Exterior	"Data(s)", "Diagnóstico(s)", "Exames/análises/actos médicos pedidos", "ID do doente", "ID do hospital", "ID do médico requisitante", "ID do serviço requisitante", "Inf. da pré-facturação*", "Inf. de autorização*", "Informação/justificação clínica"

Tabela B7 – Atributos dos Doc. Pedidos

Grupo de documentos: Sistemas Automáticos de Apoio Clínico

Documento Genérico	Lista de atributos
Sistema de Monitorização	"Data(s)", "Valores limite/alarmes", "Diagnóstico(s)", "ID do doente", "Sinais vitais", "Traçado de ECG"

Tabela B8 – Atributos dos Doc. dos sist. automáticos de apoio clínico

Grupo de documentos: Saída

Documento Genérico	Lista de atributos
Documento de óbito	"Causa da morte", "Data do óbito", "ID do doente", "ID do local onde ocorreu o óbito", "ID do médico que certifica", "Indicação, especial, para inumação/cremação", "Nº do certificado "', “Informação Clínica”, “Informação Circunstancial”
Transferência/ Envio do doente	"Cuidados prestados", "Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) interveniente(s)", "Informação/justificação clínica"
Documento de Alta	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) médico(s)", "Orientações Propostas", "Resumo do Internamento"
Documento para a Comunicação Obrigatória de Doenças	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) médico(s)", “Informação Clínica”

Tabela B9 – Atributos dos Doc. saída

Grupo de documentos: Transversais

Documento Genérico	Lista de atributos
Informação Administrativa	"Data(s)", "Diagnóstico(s)", "GDH", "ID do destino do doente", "Registo dos MCDT realizados", "ID do doente", "ID do Internamento", "ID do(s) médico(s)", "Procedimentos/Acto(s) médico(s) realizados"
Processo único	"ID do doente", "Súmula dos atributos existentes no processo de internamento, no processo de consulta, no processo de hospital de dia e nos resultados dos exames"

Tabela B10 – Atributos dos Doc. transversais

Após a identificação dos documentos genéricos é possível apresentar o seguinte diagrama para a o UCIC (Figura B2).

Uma vez identificados e agregados os documentos em documentos genéricos a fase seguinte consiste na estimativa do valor de cada documento genérico.

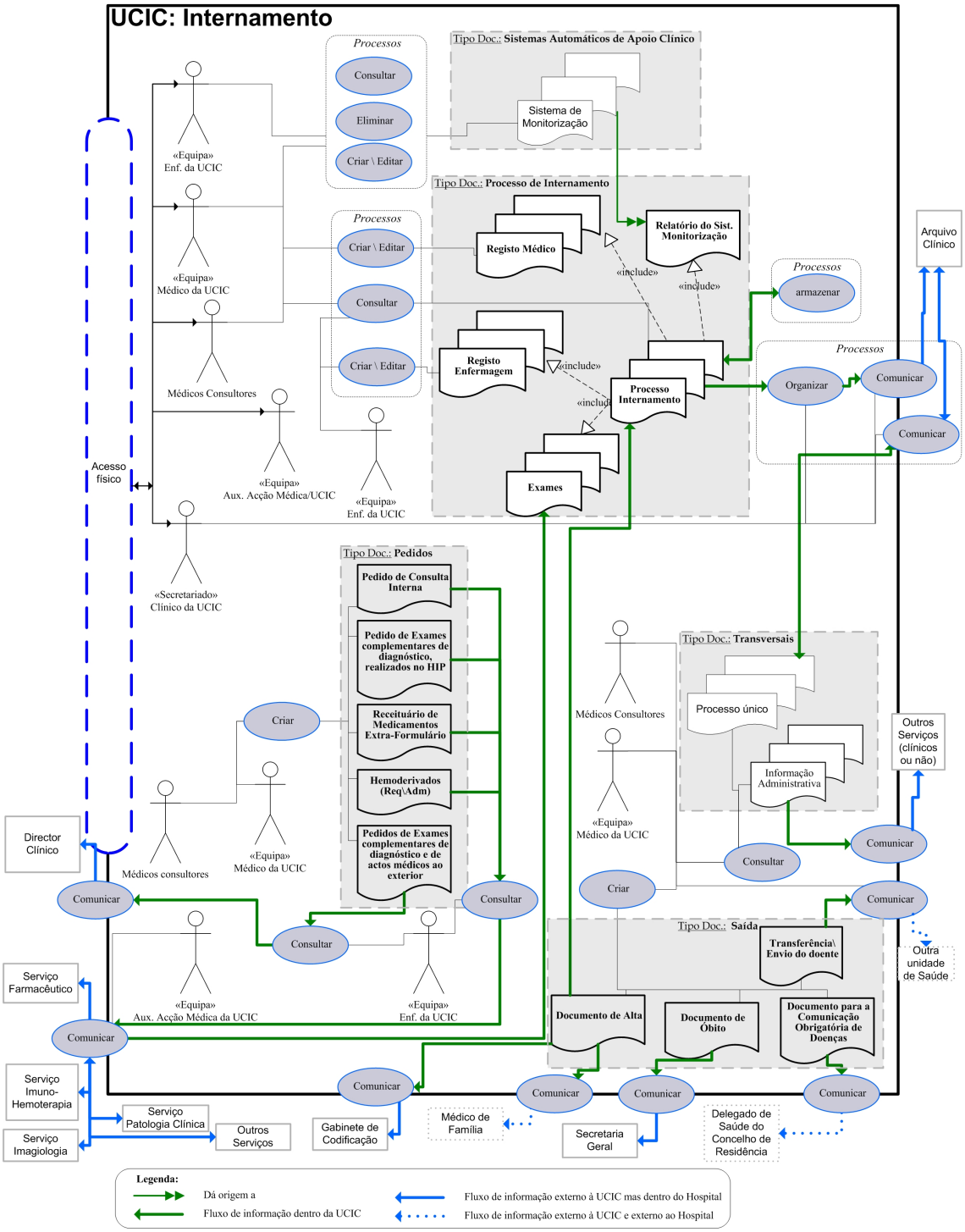


Figura B2 – Fluxo de informação da UCIC

B.3.5. Determinação do valor dos documentos

Seguindo-se a metodologia proposta, de seguida apresenta-se o painel de peritos, o questionário usado e os respectivos resultados.

Caracterização do painel I de Delphi

O painel de peritos foi assim constituído:

- Enfermeira Conceição Neves, Enfermeira Directora do HIP, com o grau académico de mestre e docente na Escola Superior de Saúde de Aveiro;
- Enfermeira Céu Silvestre, licenciada e com pós graduação em Sistemas de Informação, funcionária do HIP com a categoria de especialista;
- Técnico Superior de Informática César Telmo, responsável pelo Serviço de Informática do HIP, com o grau académico de mestre, licenciado em medicina e docente na Escola Superior de Saúde de Aveiro;
- Médica infecciologista Célia Oliveira , licenciada em medicina, funcionária do HIP responsável pela unidade de infecciologia;
- Administrador Hospitalar Pedro Roldão, licenciado em sociologia e pós graduação em administração hospitalar, ex-administrador do Serviço de Informática, Arquivo Clínico e Gestão de Doentes do HIP, actualmente Vogal Executivo dos Hospitais da Universidade de Coimbra;
- Advogada Conceição Martins, licenciada em direito, responsável pelo gabinete jurídico e contencioso do HIP;
- Médico de Medicina Interna Jorge Crespo, licenciado em medicina, director do serviço de Medicina Interna do HIP;

- Médico Cardiologista Narciso Pinheiro, licenciado em medicina, director do serviço de Cardiologia[38] do HIP;
- Enfermeiro Luís Coquim, Enfermeiro Chefe do Serviço de Cardiologia do HIP;
- Médico de Medicina Interna Miguel Capão Filipe, licenciado em medicina, Director Clínico do HIP;
- Enfermeiro Carlos Jorge, grau académico de mestre, enfermeiro especialista no Serviço de Urgência do HIP, docente na Escola Superior de Saúde de Aveiro;
- Médico de Patologia Clínica Frederico Cerveira, licenciado em medicina, director do serviço de Patologia Clínica do HIP;
- Enfermeira Vera Maia, licenciada, enfermeira especialista da UCIC do HIP.

Questionário I

Com base nos documentos genéricos, referidos na secção anterior e nas instruções que a metodologia proposta sugere, criou-se um questionário a submeter ao painel de peritos.

No anexo C apresenta-se o questionário usado nas rondas do painel de Delphi, diferindo de ronda para ronda apenas os elementos estatísticos que se reportam aos resultados da ronda anterior.

Resultados / Valor

Como é determinado na metodologia proposta, ao fim da segunda ronda calculou-se o coeficiente *alpha de Cronbach* em função das dimensões de segurança, tendo-se obtido os seguintes valores:

[38] E por inerência Director da UCIC.

	Dimensão			
	Conf.	Int.	Disp.	Aut.\Resp.
alpha de Cronbach	0,864	0,975	0,923	0,967

Tabela B11 – Coeficientes *alpha de Cronbach*

Com base nos valores indicados na tabela anterior e nos critérios referidos na metodologia para a classificação do grau de consenso, o consenso obtido para as diferentes dimensões é o seguinte:

	Dimensão			
	Conf.	Int.	Disp.	Aut.\Resp.
Consenso	Bom	Excelente	Excelente	Excelente

Tabela B12 – Consenso por dimensão

Na segunda ronda foi portanto, atingido o grau de consenso razoável[39] pelo que foi suspensa a aplicação do questionário.

A média obtida na segunda ronda e o respectivo desvio padrão são apresentados, em função das diferentes dimensões, na tabela seguinte.

[39] Isto é, alpha de Cronbach >= 0,7, ou em termo qualitativos um consenso razoável ou superior.

	Dimensão							
	Conf.		Int.		Disp.		Aut.\Resp.	
Doc.	V*	σ+	V*	σ+	V*	σ+	V*	σ+
1	6,85	0,38	6,38	1,39	5,77	1,42	5,62	1,56
2	6,23	0,83	5,77	1,48	5,46	1,33	5,38	1,76
3	6,62	0,96	6,08	1,71	5,46	1,76	5,23	1,79
4	5,69	1,49	5,69	1,80	6,31	0,75	4,77	1,74
5	5,31	1,32	5,54	1,85	6,15	0,99	4,85	1,46
6	7,00	0,00	6,46	1,39	6,46	0,66	6,15	0,55
7	5,23	1,83	4,92	1,85	5,23	1,48	4,85	1,82
8	6,00	1,00	5,69	1,75	5,85	1,34	6,00	1,73
9	4,62	1,56	5,15	1,72	5,00	1,83	4,54	1,56
10	5,23	1,36	5,31	1,32	5,38	1,56	5,46	1,45
11	5,77	1,42	5,69	1,55	5,77	1,74	5,92	1,61
12	6,69	0,48	6,23	1,36	5,77	1,42	6,08	1,38
13	6,77	0,44	6,31	1,38	6,46	0,66	6,08	1,12
14	6,85	0,38	6,46	1,13	6,38	1,39	6,23	1,54
15	6,92	0,28	6,54	1,13	6,31	1,65	5,92	1,75
16	7,00	0,00	6,77	0,83	6,38	1,66	6,23	1,64
17	7,00	0,00	6,31	0,95	5,69	1,18	6,31	0,75

Tabela B13 – Valores dos documentos

* Média do valor

+ Desvio padrão

B.3.6. Determinação da probabilidade da concretização das ameaças

Apresenta-se de seguida a aplicação da metodologia proposta no que diz respeito à estimativa da probabilidade da concretização das ameaças.

Painel de Delphi

Como se pretendia que o painel indica-se a probabilidade da concretização das ameaças, escolheu-se a equipa de enfermagem da UCIC para fazer parte do painel. Estes profissionais são os que passam mais tempo na unidade e, por isso e pela sua actividade têm uma visão mais crítica dos diferentes processos.

O número de enfermeiros da equipa da UCIC é de 20 elementos.

Questionário II

Com base nos pressupostos da metodologia, elaborou-se um questionário para avaliar a probabilidade de concretização de cada ameaça. Este questionário é apresentado no anexo D.

Resultados / Probabilidade de concretização de uma ameaça

Relativamente ao valor do *alpha de Cronbach* das respostas da segunda ronda foi de 0,998. Os valores deste índice para cada classe de processos foram os seguintes:

	Processo				
	Criar / Editar	Consultar	Comunicar	Armazenar	Organizar
alpha de Cronbach	0,992	0,993	0,993	0,992	0,866

Tabela B14 – Coeficientes *alpha de Cronbach*

Mais uma vez o consenso foi atingido na 2ª ronda de questionários.

De seguida, para classe de processos, apresentam-se os valores médios da probabilidade de concretização das ameaças relativamente a cada documento.

Ref. Doc.	Remoção física	destruição física	alteração	intercepção	falsa identificação do autor
1	3,35	3,05	3,6	4,4	3,65
2	3,3	3	3,65	4,2	2,95
7	2,3	2,05	2	3,1	2,65
8	2,15	1,85	1,95	3	2,3
9	2,75	2,05	2,15	3,2	2,5
10	2,35	2,15	2,05	2,9	2,45
11	2,4	2,2	2,1	3,55	2,3
12	2,1	2,1	1,9	3	2
13	2,4	2,15	1,9	3,3	2,1
14	2,25	2,05	1,95	3,3	2,25
17	2,25	1,95	1,8	2,6	2

Tabela B15 – Processo: Criar \ Editar

Ref. Doc.	remoção física	destruição física	alteração	intercepção
1	2,8	2,35	3,05	4,45
2	2,8	2,2	2,95	4,15
3	2,85	2,45	2,45	4,3
5	2,8	2,35	2,35	3,9
6	2,75	2,45	2,35	4,2
7	2,7	2,45	2,3	3,55
8	2,45	2,3	2,15	3,2
9	2,4	2,4	2,15	3,4
10	2,4	2,3	2,1	3,15
11	2,4	2,4	2,05	3,5
12	2,15	2,25	1,95	3,15
13	2,35	2,35	2,05	3,25
14	2,3	2,45	2	3,45
16	2,8	2,55	2,9	4,3
17	2,3	2,4	2,2	3,05

Tabela B16 – Processo: Consultar

Ref. Doc.	remoção física	destruição física	alteração	intercepção
1	2,85	2,3	2,3	4,05
2	2,85	2,3	2,3	4,05
3	2,85	2,3	2,3	4,05
5	2,85	2,3	2,3	4,05
6	2,85	2,3	2,3	4,05

Tabela B17 – Processo: Organizar

Ref. Doc.	remoção física	destruição física	alteração	intercepção
1	5	4,75	2,5	3,75
2	5	4,75	2,5	3,75
3	5	4,75	2,5	3,75
5	5	4,75	2,5	3,75
6	5	4,75	2,5	3,75
7	3,35	2,9	2,1	3,7
8	3,2	2,85	1,95	3,5
9	3,3	3	2,1	3,6
10	3,15	2,85	1,95	3,3
11	3,25	2,9	2,05	3,45
12	3,15	2,7	1,95	3,3
13	3,2	2,95	2,1	3,45
14	3,3	2,8	1,95	3,4
16	3,45	3,3	2,45	4
17	2,95	2,65	1,95	3,3

Tabela B18 – Processo: Comunicação

Quando as ameaças são concretizadas por actores internos à UCIC

Ref. Doc.	remoção física	destruição física	alteração	intercepção
1	3,55	2,6	2,85	3,65
2	3,55	2,6	2,7	3,75
3	3,5	2,55	2,15	3,6
5	3,2	2,3	2,1	3,35
6	3,2	2,4	2,2	3,35
16	3,1	2,45	2,7	3,95

Tabela B19 – Processo: Armazenamento 1

Quando as ameaças são concretizadas por actores externos à UCIC

Ref. Doc.	remoção física	destruição física	alteração	intercepção
1	1,75	1,75	1,8	1,65
2	1,75	1,75	1,8	1,6
3	1,8	1,7	1,75	1,6
5	1,65	1,65	1,6	1,5
6	1,75	1,8	1,7	1,65
16	1,9	1,85	1,9	2,05

Tabela B20 – Processo: Armazenamento 2

B.4. Matriz do risco

Com base nos valores apresentados nas secções anteriores e na fórmula apresentada pela metodologia para o cálculo do índice do risco, apresentam-se, em função de cada dimensão de segurança, o índice do risco de cada documento. É ainda apresentada a posição relativa de cada documento segundo o seu índice de risco.

Ref. Doc.	Doc. Genérico	Índice do Risco	% do Risco[40]	Posição Relativa
1	Registo médico	34,25	49%	2º
2	Registo enfermagem	31,15	45%	4º
3	Resultado de Exames	33,10	47%	3º
5	Relatório do Sist. Monitorização	26,55	38%	6º
6	Fotocópia da ocorrência no S.U.	35,00	50%	1º
7	Pedido de exames Imagiológicos\Patologia Clínica/Imuno-Hemoterapia/Anatomia Patológica	19,35	28%	13º
8	Hemoderivados (Req\Adm)	21,00	30%	11º
9	Pedido de consulta Interna	16,63	24%	15º
10	Pedido de receituário de Med. Extra-Formulário	17,26	25%	14º
11	Pedido de Exames ao Exterior	20,20	29%	12º
12	Documento de óbito	22,08	32%	10º
13	Transferência/Envio do doente	23,36	33%	8º
14	Documento de Alta	23,63	34%	7º
16	Processo único	30,10	43%	5º
17	Documento para a Comunicação Obrigatória de Doenças	23,10	33%	9º

Tabela B21 – Índice do risco segundo a confidencialidade

[40] % Risco = Índice do risco / Valor máximo * 100, onde valor máximo = 70

Ref. Doc.	Doc. Genérico	Índice do Risco	% do Risco[41]	Posição Relativa
1	Registo médico	30,31	43%	2º
2	Registo enfermagem	27,41	39%	4º
3	Resultado de Exames	28,88	41%	3º
5	Relatório do Sist. Monitorização	26,32	38%	5º
6	Fotocópia da ocorrência no S.U.	30,69	44%	1º
7	Pedido de exames Imagiológicos\Patologia Clínica/Imuno-Hemoterapia/Anatomia Patológica	14,27	20%	15º
8	Hemoderivados (Req\Adm)	16,22	23%	12º
9	Pedido de consulta Interna	15,45	22%	13º
10	Pedido de receituário de Med. Extra-Formulário	15,13	22%	14º
11	Pedido de Exames ao Exterior	16,50	24%	11º
12	Documento de óbito	16,82	24%	9º
13	Transferência/Envio do doente	18,61	27%	7º
14	Documento de Alta	18,09	26%	8º
16	Processo único	22,34	32%	6º
17	Documento para a Comunicação Obrigatória de Doenças	16,72	24%	10º

Tabela B22 - Índice do risco segundo a integridade

[41] % Risco = Índice do risco / Valor máximo * 100, onde valor máximo = 70

Ref. Doc.	Doc. Genérico	Índice do Risco	% do Risco[42]	Posição Relativa
1	Registo médico	28,85	41%	3º
2	Registo enfermagem	27,30	39%	4º
3	Resultado de Exames	27,30	39%	4º
5	Relatório do Sist. Monitorização	30,75	44%	2º
6	Fotocópia da ocorrência no S.U.	32,30	46%	1º
7	Pedido de exames Imagiológicos\Patologia Clínica/Imuno-Hemoterapia/Anatomia Patológica	17,52	25%	12º
8	Hemoderivados (Req\Adm)	18,72	28%	10º
9	Pedido de consulta Interna	16,50	24%	15º
10	Pedido de receituário de Med. Extra-Formulário	16,95	24%	13º
11	Pedido de Exames ao Exterior	18,75	28%	9º
12	Documento de óbito	18,18	26%	11º
13	Transferência/Envio do doente	20,67	30%	8º
14	Documento de Alta	21,05	30%	7º
16	Processo único	22,01	31%	6º
17	Documento para a Comunicação Obrigatória de Doenças	16,79	24%	14º

Tabela B23 – Índice do risco segundo a disponibilidade

[42] % Risco = Índice do risco / Valor máximo * 100, onde valor máximo = 70

Ref. Doc.	Doc. Genérico	Índice do Risco	% do Risco[43]	Posição Relativa
1	Registo médico	20,51	29%	1º
2	Registo enfermagem	15,87	23%	2º
7	Pedido de exames Imagiológicos\Patologia Clínica/Imuno-Hemoterapia/Anatomia Patológica	12,85	18%	7º
8	Hemoderivados (Req\Adm)	13,80	20%	4º
9	Pedido de consulta Interna	11,35	16%	11º
10	Pedido de receituário de Med. Extra-Formulário	13,38	19%	6º
11	Pedido de Exames ao Exterior	13,62	19%	5º
12	Documento de óbito	12,16	17%	10º
13	Transferência/Envio do doente	12,77	18%	8º
14	Documento de Alta	14,02	20%	3º
17	Documento para a Comunicação Obrigatória de Doenças	12,62	18%	9º

Tabela B24 – Índice do risco segundo a autoria/responsabilidade

[43] % Risco = Índice do risco / Valor máximo * 100, onde valor máximo = 70

Anexo C
Questionário usado para determinar o valor de cada documento

Identificação: _____

Questionário para a determinação do impacto

Ronda ___

Universidade do Minho

Escola de Engenharia

Departamento de Sistemas de Informação

1. Introdução

Este questionário, surge na sequência do trabalho que tem sido desenvolvido por António Manuel Rodrigues Carvalho Santos, no âmbito da elaboração da tese de Doutoramento, intitulada "Segurança nos sistemas de informação Hospitalares: Políticas, Práticas e Avaliação", na Escola de Engenharia da Universidade do Minho, sob a orientação científica do Professor Doutor Henrique Manuel Dinis dos Santos.

Um dos objectivos do trabalho é conceber uma política de segurança da informação, adequada aos processos clínicos/administrativos, ao nível das unidades hospitalares portuguesas. Uma das fases do desenvolvimento dessa política consiste na determinação do valor dos documentos. Optou-se pela avaliação das consequências (impacto) negativas quando um documento sofre uma quebra de segurança.

Para cada documento, pretende-se determinar o impacto de uma quebra em cada uma das seguintes dimensões:

- Confidencialidade;
- Integridade;
- Disponibilidade;
- Responsabilidade/Autoria.

O impacto será obtido com base numa técnica de consenso (painel de Delphi). A técnica de Delphi, foi criada pela firma Rand Corporation (década de 50) e é um processo estruturado, que visa a obtenção de consenso sobre um determinado assunto com base na opinião de um grupo de peritos. Esta técnica consiste na elaboração de uma sequência de questionários, correspondendo cada questionário a uma ronda. Entre cada ronda o grupo de peritos tem ao seu dispor a avaliação estatística da ronda anterior. Serão realizadas tantas rondas, quantas as necessárias até obter um grau de consenso razoável.

O questionário é anónimo e confidencial, havendo a garantia do investigador que efectuará todos os esforços para garantir estes dois pressupostos.

O presente questionário constitui a 2ª ronda do painel de Delphi. Nesta ronda é solicitado aos elementos do painel que se prenunciem-se sobre as mesmas questões[44] da 1ª ronda, tendo, agora, ao seu dispor alguns parâmetros estatísticos (média, desvio padrão e análise de frequência) das respostas obtidas na ronda anterior.

[44] Com à excepção de algumas pequenas alterações, que são identificadas mais à frente.

2. Definições

- *Confidencialidade*:- garantia que a informação só é acedida por utilizadores autorizados
    - *Quebra de confidencialidade*:- existe quebra de confidencialidade, quando um utilizador ou sistema tem acesso a determinada informação, não estando autorizado para tal. (Exemplo: *O resultado de um exame é tornado público, sem a autorização do doente*.)
- *Integridade*:– garantia que a informação não foi alterada pela adição, modificação ou eliminação, a não ser por utilizadores autorizados e de acordo com os protocolos estabelecidos.
    - *Quebra de integridade*:- existe quebra de integridade, quando a informação constante num determinado documento é corrompida. (Exemplo: *O desaparecimento do processo de internamento de uma determinada folha, que fazia parte do diário clínico*).
- *Disponibilidade*:– garantia que a informação está acessível sempre que necessária.
    - *Quebra de disponibilidade*:- existe quebra de disponibilidade, quando um utilizador ou sistema não consegue ter acesso à informação que consta no sistema de informação. (Exemplo: *Um médico necessita de ter acesso ao processo clínico, e este não se encontra localizável*).
- *Responsabilidade/autoria*:- Garantia que se conhece a cada momento o autor de quem gerou/modificou a informação.
    - *Quebra de responsabilidade/autoria*:- Existe quebra de responsabilidade/autoria quando não é possível determinar de forma inquestionável quem foi o autor de determinada informação. (Exemplo: *Uma requisição sem a identificação inequívoca do seu autor*).
- *Atributos*:- Característica/propriedade específica de um documento.

- Exemplo: O documento “Pedido de Rx” tem, entre outros, os atributos “ID do doente”(contém a informação que identifica o doente), “ID do médico requisitante” (contém todas as informações que identificam quem efectua o pedido de Rx).

- *Impacto negativo*:- dano organizacional que a quebra de segurança de um documento pode provocar.

3. Documentos em análise

Irão ser analisados os documentos gerados durante o internamento de um doente na Unidade de Cuidados Intensivos Coronários (UCIC) do hospital em estudo.

Os documentos reais foram agregados, de acordo com as suas características, dando origem a documentos genéricos. Obtiveram-se assim os seguintes documentos genéricos:

1. **"Registo médico"** - documento genérico que agrega todos os registos efectuados pela equipa médica que acompanhou o doente no internamento. Os documentos reais que lhe deram origem foram: "Registo de Internamento", "hip- diário clínico", "hda-374 folha terapêutica", "hip-092 Registo de análises".
2. **"Registo de enfermagem"** - documento genérico que agrega todos os registos efectuados pela equipa de enfermagem que acompanhou o doente no internamento. Os documentos reais que lhe deram origem foram: "hip-162 História clínica de enfermagem", "hip-091 Folha operatória", "hip-160 Registo do diário clínico de enfermagem", "hip-302 Folha terapêutica enfermagem", "hip-303A Internamento", "hip-585 Perfil glicémico", "hda-513 balanço hidroelectrolitico".
3. **"Resultado de Exames"** - documento genérico que engloba todos os resultados dos exames que foram efectuados ao doente, aquando do internamento.
4. **"Sistema de Monitorização"** - documento genérico que agrega toda a informação existente no sistema de monitorização em tempo real do doente.
5. **"Relatório do Sist. Monitorização"** - documento genérico que agrega toda a informação que pode ser impressa a partir do sistema de monitorização em tempo real.
6. **"Fotocópia da ocorrência no S.U."** - documento genérico que agrega toda a informação relativa ao episódio de Urgência que

motivou o internamento. O documento real que lhe deu origem foi o "hip-339-A Ocorrência do S.U.".

7. **“Pedido de exames Imagiológicos\Patologia Clínica/Imuno-Hemoterapia/Anatomia Patológica”** - documento genérico que agrega todos os pedidos de exames complementares de diagnósticos solicitados ao longo do período de internamento. Os documentos reais que lhe deram origem foram: "hip-535 Requisição de Exames Imagiológicos", "hda-558 - Pedido de análises de Imuno-Hematologia", "hip-559 - Pedido de Transfusão", "hda 419 - Pedido de análises de Anatomia Patológica", "hip-068 Pedido de Ecocardiograma/Electrocardiograma", "hip-433 Pedido de análises Urgentes", "hip-413 Pedido de análises de Hematologia e Coagulação"; hip-547 Pedido de análises de Química Clínica", "hip-547/A Pedido de análises de Endocrinologia/Imunologia", hip-580/A Pedido de análises de Microbiologia".
8. **“Hemoderivados (Req\Adm)”** - documento genérico que permite o registo da requisição, distribuição e administração de hemoderivados. O documento real que lhe deu origem foi o "INCM-1804 Medicamentos Hemoderivados".
9. **“Pedido de consulta Interna”** - documento genérico que permite efectuar o pedido de colaboração (consulta interna) de outra especialidade. O documento real que lhe deu origem foi o "hip-130 Pedido de Consulta Interna".
10. **“Pedido de receituário de Med. Extra-Formulário”** - documento genérico permite solicitar medicamentos que não constam no formulário hospitalar. O documento real que lhe deu origem foi o "hip-658 Justificação de receituário de medicamentos extra-formulário".
11. **“Pedido de Exames ao Exterior”** - documento genérico que utilizado para efectuar um pedido de exames, análises ou actos médicos realizados por entidades externas ao hospital. Os documentos reais que lhe deram origem foram: "hip 114 Requisição de exames ao exterior", "exames requisitados de cardiologia", " Relatório serviço de

Cardiologia", "hpa - VS Mod 151 a-R*", "Protocolo de pedido de cateterismo cardíaco - SMIC"**.**

12. **"Documento de óbito"**[45] - documento genérico que engloba todos os documentos gerados aquando o óbito. Os documento reais que lhe deram origem foram: "INCM-1725 Certificado de óbito", "hip – 049 – Boletim de Informação Clínica e/ou Circunstancial".
13. **"Transferência/Envio do doente"** - documento genérico que acompanha o doente, quanto este é transferido ou enviado para outra unidade de saúde. O documento real que lhe deu origem foi o "hip-183 Transferência/Envio do doente".
14. **"Documento de Alta"**[46] - documento que engloba todos os documentos gerados aquando a alta do doente. Os documentos reais que lhe deram origem foram: "nota de alta" e o "verbete - GDH".
15. **"Informação Administrativa"** - documento genérico que pretende representar toda a informação administrativa associada a um episódio.
16. **"Processo único"**- documento genérico que agrega o histórico dos episódios de internamento, de consulta, de urgência, de exames e do hospital de dia".
17. **"Documento para a Comunicação Obrigatória de Doenças**" – documento genérico que agrega os documentos utilizados para a declaração obrigatória de doenças a entidades externas, nomeadamente, às autoridades de Saúde Pública. O documento real que lhe deu origem foi o modelo 1536 da INCM.

Os documentos genéricos foram agrupados em grandes grupos, de acordo com o tipo e a natureza a que se destina cada um deles, conforme a tabela II.

[45] A designação anterior era "Certificado de óbito"

[46] A designação anterior era "Nota de Alta".

Grande grupo de documentos: Processo de Internamento

Documento Genérico	Lista Atributos
Registo Médico	"Data(s)", "Diagnóstico(s)", "Diário clínico", "História clínica", "ID do doente", "ID do(s) médico(s)", "Terapêutica"
Registo de Enfermagem	"Data(s)", "Diário de enfermagem", "História clínica de enfermagem", "ID do doente", "ID do(s) enfermeiro(s)", "Registos relacionados com a prestação de cuidados de enfermagem"
Resultado de Exames	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do Serviço", "Resultado(s)"
Fotocópia da ocorrência no S.U.	"Data(s)", "Descrição das observações médicas", "Descrição do motivo da vinda", "Descrição/destino do espólio", "Diagnóstico(s)", "Exames pedidos", "ID da proveniência do doente", "ID do acompanhamento", "ID do destino do doente", "ID do doente", "ID do(s) interveniente(s)", "Notas de enfermagem", "Registo de medicação", "Registo dos procedimentos/actos médicos efectuados ", "Registos dos parâmetros metabólicos/vitais e das drenagens", "Triagem de prioridades"
Relatório do Sist. Monitorização	"Data(s)", "Frequência cardíaca", "ID do doente", "Traçado de ECG"

Grande grupo de documentos: Sistemas Automáticos de Apoio Clínico

Documento Genérico	Lista Atributos
Sistema de Monitorização	"Data(s)", "Valores limite/alarmes", "Diagnóstico(s)", "ID do doente", "Sinais vitais", "Traçado de ECG"

Grande grupo de documentos: Pedidos

Documento Genérico	Lista Atributos
Pedido de exames Imagiológicos/ Patologia Clínica/ Imuno-Hemoterapia/ Anatomia Patológica	"Data(s)", "Diagnóstico(s)", "Exames/análises Pedidos", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Material enviado *"
Hemoderivados (Req\Adm)	"Data(s)", "Dose/frequência/duração", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Produto requisitado", "Registo de administração", "Registo de distribuição"
Pedido de consulta Interna	"Data realização da consulta *", "Data(s)", "Designação da consulta pretendida", "ID do doente", "ID do médico que efectuou a consulta", "ID do médico requisitante", "ID do receptor do pedido *"
Pedido de receituário de Med. Extra-Formulário	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Medicamento"
Pedido de Exames ao Exterior	"Data(s)", "Diagnóstico(s)", "Exames/análises/actos médicos pedidos", "ID do doente", "ID do hospital", "ID do médico requisitante", "ID do serviço requisitante", "Inf. da pré-facturação*", "Inf. de autorização*", "Informação/justificação clínica"

Grande grupo de documentos: Saída

Documento Genérico	Lista Atributos
Documento de óbito	"Causa da morte", "Data do óbito", "ID do doente", "ID do local onde ocorreu o óbito", "ID do médico que certifica", "Indicação, especial, para inumação/cremação", "Nº do certificado "', “Informação Clínica”, “Informação Circunstancial”
Transferência/ Envio do doente	"Cuidados prestados", "Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) interveniente(s)", "Informação/justificação clínica"
Documento de Alta	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) médico(s)", "Orientações Propostas", "Resumo do Internamento"
Documento para a Comunicação Obrigatória de Doenças	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) médico(s)", “Informação Clínica”

Grande grupo de documentos: Transversais

Documento Genérico	Lista Atributos
Informação administrativa	"Data(s)", "Diagnóstico(s)", "GDH", "ID do destino do doente", "Registo dos MCDT realizados", "ID do doente", "ID do Internamento", "ID do(s) médico(s)", "Procedimentos/Acto(s) médico(s) realizados"
Processo único	"ID do doente", "Sumula dos atributos existentes no processo de internamento, no processo de consulta, no processo de hospital de dia e nos resultados dos exames"

4. Questionário

4.1. Instruções

Cada questão apresentada, deve ser respondida tendo em conta cada uma das dimensões (confidencialidade, integridade, disponibilidade, responsabilidade/autoria) da segurança da informação. A resposta deve ser feita segundo uma escala bipolar, crescente, de 7 pontos. Os extremos encontram-se localizados no início e no fim da escala.

Por favor, para cada dimensão, coloque apenas uma cruz no quadrado que melhor expressa a sua opinião.

Para anular uma resposta coloque um círculo à volta da cruz (⊗) e coloque uma cruz no novo valor do impacto (ver no exemplo seguinte a resposta para a dimensão disponibilidade)

Por favor não escreva o seu nome no questionário. As suas respostas serão tratadas de forma confidencial.

Exemplo:

Qual o impacto negativo, quando o documento "XPTO" sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade									*7*	*6.8*	*0.4*
		F.						*2*	*11*			
	Integridade									*2*	*6.3*	*1.5*
		F.		*1*			*2*	*1*	*9*			
	Disponibilidade									*4*	*5.7*	*1.6*
		F		*1*		*2*	*4*		*6*			
	Responsabilidade/ Autoria									*5*	*5.8*	*1.7*
		F.	*2*				*3*	*3*	*5*			

Neste exemplo é apresentado ao inquirido, alguns dados estatísticos das respostas obtidas na ronda anterior. Por uma questão de melhor identificação estes dados são apresentados com um fundo do tipo . Os dados estatísticos são:

- A média do valor das respostas (designada na tabela por “Média”)
- O desvio padrão (designada na tabela por Dev. P)
- A frequência estatística de cada valor, i.e. o nº de inquiridos que escolheram determinada opção (designada por “F”).

Para além dos parâmetros estatísticos, é apresentada ainda qual foi a sua opção na ronda anterior.

4.2. Determinação do impacto

Secção A. Documentos pertencentes ao Grande Grupo – <u>Processo de Internamento</u>

4.2.1. Considere o documento "Registo Médico" (pertencente ao Grande Grupo "Processo de Internamento") que apresenta os atributos "Data(s)", "Diagnóstico(s)", "Diário clínico", "História clínica", "ID do doente", "ID do(s) médico(s)", "Terapêutica".

Qual o impacto negativo, quando o documento "Registo Médico" sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.2. Considere o documento "Registo de Enfermagem" (pertencente ao Grande Grupo "Processo de Internamento") que apresenta os atributos "Data(s)", "Diário de enfermagem", "História clínica de enfermagem", "ID do doente", "ID do(s) enfermeiro(s)", "Registos relacionados com a prestação de cuidados de enfermagem".

Qual o impacto negativo, quando o documento "Registo de Enfermagem" sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.3. Considere o documento "Resultado de Exames" (pertencente ao Grande Grupo "Processo de Internamento") que apresenta os atributos "Data(s)", "Diagnóstico(s)", "ID do doente", "ID do Serviço", "Resultado(s)".

Qual o impacto negativo, quando o documento “Resultado de Exames” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.4. Considere o documento "Sistema de Monitorização" (pertencente ao Grande Grupo "Sistemas Automáticos de Apoio Clínico") que apresenta os atributos "Data(s)", "Valores limite/alarmes", "Diagnóstico(s)", "ID do doente", "Sinais vitais", "Traçado de ECG".

Qual o impacto negativo, quando o documento “Sistema de Monitorização” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.5. Considere o documento "Relatório do Sist. Monitorização" (pertencente ao Grande Grupo "Processo de Internamento") que apresenta os atributos Data(s)", "Frequência cardíaca", "ID do doente", "Traçado de ECG".

Qual o impacto negativo, quando o documento "Relatório do Sist. Monitorização" sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.6. Considere o documento "Fotocópia da ocorrência no S.U." (pertencente ao Grande Grupo "Processo de Internamento") que apresenta os atributos "Data(s)", "Descrição das observações médicas", "Descrição do motivo da vinda", "Descrição/destino do espólio", "Diagnóstico(s)", "Exames pedidos", "ID da proveniência do doente", "ID do acompanhamento", "ID do destino do doente", "ID do doente", "ID do(s) interveniente(s)", "Notas de enfermagem", "Registo de medicação", "Registo dos procedimentos/actos médicos efectuados ", "Registos dos parâmetros metabólicos/vitais e das drenagens", "Triagem de prioridades".

Qual o impacto negativo, quando o documento "Fotocópia da ocorrência no S.U." sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

Secção B. Documentos pertencentes ao Grande Grupo – <u>Pedidos</u>

4.2.7. Considere o documento "Pedido de exames Imagiológicos/Patologia Clínica/Imuno-Hemoterapia/Anatomia Patológica" (pertencente ao Grande Grupo "Pedidos") que apresenta os atributos "Data(s)", "Diagnóstico(s)", "Exames/análises Pedidos", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Material enviado *".

Qual o impacto negativo, quando o documento “Pedido de exames Imagiológicos/Patologia Clínica/Imuno-Hemoterapia/Anatomia Patológica” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.8. Considere o documento "Hemoderivados (Req\Adm)" (pertencente ao Grande Grupo "Pedidos") que apresenta os atributos "Data(s)", "Dose/frequência/duração", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Produto requisitado", "Registo de administração", "Registo de distribuição".

Qual o impacto negativo, quando o documento “Hemoderivados (Req\Adm)” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.9. Considere o documento "Pedido de consulta Interna" (pertencente ao Grande Grupo "Pedidos") que apresenta os atributos "Data realização da consulta *", "Data(s)", "Designação da consulta pretendida", "ID do doente", "ID do médico que efectuou a consulta", "ID do médico requisitante", "ID do receptor do pedido *".

Qual o impacto negativo, quando o documento “Pedido de consulta Interna” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.10. Considere o documento "Pedido de receituário de Med. Extra-Formulário" (pertencente ao Grande Grupo "Pedidos") que apresenta os atributos "Data(s)", "Diagnóstico(s)", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Medicamento".

Qual o impacto negativo, quando o documento “Pedido de receituário de Med. Extra Formulário” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.11. Considere o documento "Pedido de Exames ao Exterior" (pertencente ao Grande Grupo "Pedidos") que apresenta os atributos "Data(s)", "Diagnóstico(s)", "Exames/análises/actos médicos pedidos", "ID do doente", "ID do hospital", "ID do médico requisitante", "ID do serviço requisitante", "Inf. da pré-facturação*", "Inf. de autorização*", "Informação/justificação clínica".

Qual o impacto negativo, quando o documento “Pedido Exames ao Exterior” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

Secção C. Documentos pertencentes ao Grande Grupo – "Saída"

4.2.12. Considere o documento "Documento de óbito" (pertencente ao Grande Grupo "Saída") que apresenta os atributos "Causa da morte", "Data do óbito", "ID do doente", "ID do local onde ocorreu o óbito", "ID do médico que certifica", "Indicação, especial, para inumação/cremação", "Nº do certificado ", "Informação Clínica", "Informação Circunstancial".

Qual o impacto negativo, quando o documento "Documento de óbito" sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.13. Considere o documento "Transferência/Envio do doente" (pertencente ao Grande Grupo "Saída") que apresenta os atributos "Cuidados prestados", "Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) interveniente(s)", "Informação/justificação clínica".

Qual o impacto negativo, quando o documento “Transferência/Envio do doente” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.14. Considere o documento "Documento de Alta" (pertencente ao Grande Grupo "Saída") que apresenta os atributos "Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) médico(s)", "Orientações Propostas", "Resumo do Internamento".

Qual o impacto negativo, quando o documento “Documento de Alta” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.15. Considere o documento "Documento para a Comunicação Obrigatória de Doenças" (pertencente ao Grande Grupo "Saída") que apresenta os atributos "Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) médico(s)", “Informação Clínica”.

Qual o impacto negativo, quando o documento “Documento para a Comunicação Obrigatória de Doenças” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							1ª ronda		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

Secção D. Documentos pertencentes ao Grande Grupo – <u>“Transversais”</u>

4.2.16. Considere o documento "Informação Administrativa" (pertencente ao Grande Grupo "Transversais") que apresenta os atributos "Data(s)", "Diagnóstico(s)", "GDH", "ID do destino do doente", "ID do doente", "ID do Internamento", "ID do(s) médico(s)", "Procedimentos/Acto(s) médico(s) realizados".

Qual o impacto negativo, quando o documento “Informação Administrativa” sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							1ª ronda		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

4.2.17. Considere o documento "Processo único" (pertencente ao Grande Grupo "Transversais") que apresenta a sumula dos atributos existentes no processo de internamento, no processo de consulta, no processo de hospital de dia e nos resultados dos exames.

Qual o impacto negativo, quando o documento "Processo único" sofre uma quebra de segurança segundo as seguintes dimensões?

			Impacto							**1ª ronda**		
			1 (Baixo)	2	3	4	5	6	7 (Alto)	A sua opção	Média	Desv. P
Dimensões	Confidencialidade											
		F										
	Integridade											
		F										
	Disponibilidade											
		F										
	Responsabilidade/ Autoria											
		F										

OBS:

FIM

Anexo D

Questionário usado para determinar a probabilidade da concretização de uma ameaça

Identificação: _____.

Nº de Ordem: _____

Questionário para a determinação da probabilidade de uma vulnerabilidade ser explorada

2ª Ronda

Dpt. de Sistemas de Informação

Escola de Engenharia

Universidade do Minho

Dpt. das Ciências Exactas, Biológicas e Engenharias

Escola Superior de Tecnologias da Saúde de Coimbra

Instituto Politécnico de Coimbra

1. Introdução

Este questionário, surge na sequência do trabalho que tem sido desenvolvido por António Manuel Rodrigues Carvalho Santos, no âmbito da elaboração da tese de Doutoramento, intitulada "Segurança nos Sistemas de Informação Hospitalares: Políticas, Práticas e Avaliação", na Escola de Engenharia da Universidade do Minho, sob a orientação científica do Professor Doutor Henrique Santos.

Um dos objectivos do trabalho é conceber uma política de segurança da informação, adequada às unidades hospitalares portuguesas. Uma das fases do trabalho, consiste na determinação da probabilidade de uma vulnerabilidade ser explorada. Para a determinação da probabilidade vai-se usar a técnica de Delphi.

A técnica de Delphi, foi criada pela firma Rand Corporation e é um processo estruturado, que visa a obtenção de consenso sobre um determinado assunto com base na opinião de um grupo de peritos. Esta técnica consiste na elaboração de uma sequência de questionários, correspondendo cada questionário a uma ronda. Entre cada ronda o grupo de peritos tem ao seu dispor a avaliação estatística da ronda anterior. Serão realizadas tantas rondas, quantas as necessárias até obter um grau de consenso razoável.

O questionário é **confidencial**, havendo a garantia do investigador que efectuará todos os esforços para garantir este pressuposto.

2. Definições

Em seguida, listam-se as definições de um conjunto de acções que podem ser executadas sobre um determinado documento e que podem comprometer a sua segurança (numa das suas componentes: confidencialidade, integridade, disponibilidade, autoria/responsabilidade).

- **Remoção física**

  Remoção ou extravio de parte ou da totalidade do conteúdo de um documento, de forma intencional ou não.

- **Destruição física**

  Destruição do suporte físico da informação, de forma intencional ou não, ou a prática de actos que tornam a informação ilegível.

- **Alteração**

  Alteração de parte ou da totalidade do conteúdo de um documento de forma não protocolada.

- **Intercepção**

  Acesso ilegítimo a um documento, de forma intencional ou não.

- **Falsa identificação do autor**

  Omissão ou usurpação da identidade do autor da informação, de forma intencional ou não.

3. Documentos em análise

Irão ser analisados os documentos gerados durante o internamento de um doente na Unidade de Cuidados Intensivos Coronários (UCIC) do hospital em estudo.

Os documentos reais foram agregados, de acordo com as suas características, dando origem a documentos genéricos. Os documentos genéricos apresentam as mesmas características físicas dos documentos reais que lhe deram origem, i.e apresentam o mesmo tipo de suporte (papel, digital, etc ...).

Obtiveram-se assim os seguintes documentos genéricos:

1. **"Registo médico"**: - documento genérico que agrega todos os registos efectuados pela equipa médica que acompanhou o doente no internamento. Os documentos reais que lhe deram origem foram: "Registo de Internamento", "hip- diário clínico", "hda-374 folha terapêutica", "hip-092 Registo de análises";
2. **"Registo de enfermagem"**: - documento genérico que agrega todos os registos efectuados pela equipa de enfermagem que acompanhou o doente no internamento. Os documentos reais que lhe deram origem foram: "hip-162 História clínica de enfermagem", "hip-091 Folha operatória", "hip-160 Registo do diário clínico de enfermagem", "hip-302 Folha terapêutica enfermagem", "hip-303A Internamento", "hip-585 Perfil glicémico", "hda-513 balanço hidroelectrolitico";
3. **"Resultado de Exames"**: - documento genérico que engloba todos os resultados dos exames que foram efectuados ao doente, aquando do internamento;
4. **----------**
5. **"Relatório do Sist. Monitorização"**: - documento genérico que agrega toda a informação que pode ser impressa a partir do sistema de monitorização em tempo real;
6. **"Fotocópia da ocorrência no S.U."**: - documento genérico que agrega toda a informação relativa ao episódio de Urgência que motivou o

internamento. O documento real que lhe deu origem foi o "hip-339-A Ocorrência do S.U.";

7. **“Pedido de exames complementares de diagnóstico (MCDT), realizados no hospital”**: - documento genérico que agrega todos os pedidos de exames complementares de diagnósticos solicitados ao longo do período de internamento. Os documentos reais que lhe deram origem foram: "hip-535 Requisição de Exames Imagiológicos", "hda-558 - Pedido de análises de Imuno-Hematologia", "hip-559 - Pedido de Transfusão", "hda 419 - Pedido de análises de Anatomia Patológica", "hip-068 Pedido de Ecocardiograma/Electrocardiograma", "hip-433 Pedido de análises Urgentes", "hip-413 Pedido de análises de Hematologia e Coagulação"; hip-547 Pedido de análises de Química Clínica", "hip-547/A Pedido de análises de Endocrinologia/Imunologia", hip-580/A Pedido de análises de Microbiologia";
8. **“Hemoderivados (Req\Adm)”**: - documento genérico que permite o registo da requisição, distribuição e administração de hemoderivados. O documento real que lhe deu origem foi o "INCM-1804 Med. Hemod";
9. **“Pedido de consulta Interna”**: - documento genérico que permite efectuar o pedido de colaboração de outra especialidade. O documento real que lhe deu origem foi o "hip-130 Pedido de Consulta Interna";
10. **“Pedido de receituário de Med. Extra-Formulário”**: - documento genérico permite solicitar medicamentos que não constam no formulário hospitalar. O documento real que lhe deu origem foi o "hip-658 Justificação de receituário de medicamentos extra-formulário";
11. **“Pedido de Exames ao Exterior”**: - documento genérico que utilizado para efectuar um pedido de exames, análises ou actos médicos realizados por entidades externas ao hospital. Os documentos reais que lhe deram origem foram: "hip 114 Requisição de exames ao exterior", "exames requisitados de cardiologia", " Relatório serviço de Cardiologia", "hpa - VS Mod 151 a-R*", "Protocolo de pedido de cateterismo cardíaco - SMIC";

12. **“Documento de óbito”**: - documento genérico que engloba todos os documentos gerados aquando o óbito. Os documento reais que lhe deram origem foram: “INCM-1725 Certificado de óbito”, “hip – 049 – Boletim de Informação Clínica e/ou Circunstancial”;
13. **“Documento de Transferência/Envio do doente”**: - documento genérico que acompanha o doente, quanto este é transferido ou enviado para outra unidade de saúde. O documento real que lhe deu origem foi o "hip-183 Transferência/Envio do doente";
14. **“Documento de Alta”**: - documento que engloba todos os documentos gerados aquando a alta do doente. Os documentos reais que lhe deram origem foram: "nota de alta" e o "verbete - GDH";
15. ----------
16. **“Processo único”**:- documento genérico que agrega o histórico dos episódios de internamento, de consulta, de urgência, de exames e do hospital de dia";
17. **“Documento para a Comunicação Obrigatória de Doenças**” – documento genérico que agrega os documentos utilizados para a declaração obrigatória de doenças a entidades externas, nomeadamente, às autoridades de Saúde Pública. O documento real que lhe deu origem foi o modelo 1536 da INCM;

Os documentos genéricos foram agrupados em grandes grupos, de acordo com o tipo e a natureza a que se destina cada um deles, conforme as tabelas seguintes.

Grande grupo de documentos: Processo de Internamento

Documento Genérico	Lista Atributos
Registo Médico	"Data(s)", "Diagnóstico(s)", "Diário clínico", "História clínica", "ID do doente", "ID do(s) médico(s)", "Terapêutica"
Registo de Enfermagem	"Data(s)", "Diário de enfermagem", "História clínica de enfermagem", "ID do doente", "ID do(s) enfermeiro(s)", "Registos relacionados com a prestação de cuidados de enfermagem"
Resultado de Exames	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do Serviço", "Resultado(s)"
Relatório do Sist. Monitorização	"Data(s)", "Frequência cardíaca", "ID do doente", "Traçado de ECG"
Fotocópia da ocorrência no S.U.	"Data(s)", "Descrição das observações médicas", "Descrição do motivo da vinda", "Descrição/destino do espólio", "Diagnóstico(s)", "Exames pedidos", "ID da proveniência do doente", "ID do acompanhamento", "ID do destino do doente", "ID do doente", "ID do(s) interveniente(s)", "Notas de enfermagem", "Registo de medicação", "Registo dos procedimentos/actos médicos efectuados ", "Registos dos parâmetros metabólicos/vitais e das drenagens", "Triagem de prioridades"

Grande grupo de documentos: Pedidos

Documento Genérico	Lista Atributos
Pedido de MCDT, realizados no hospital	"Data(s)", "Diagnóstico(s)", "Exames/análises Pedidos", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Material enviado *"
Pedido de Hemoderivados	"Data(s)", "Dose/frequência/duração", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Produto requisitado", "Registo de administração", "Registo de distribuição"
Pedido de consulta Interna	"Data realização da consulta *", "Data(s)", "Designação da consulta pretendida", "ID do doente", "ID do médico que efectuou a consulta", "ID do médico requisitante", "ID do receptor do pedido *"
Pedido de receituário de Med. Extra-Formulário	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do médico requisitante", "ID do serviço requisitante", "Informação/justificação clínica", "Medicamento"
Pedido de Exames ao Exterior	"Data(s)", "Diagnóstico(s)", "Exames/análises/actos médicos pedidos", "ID do doente", "ID do hospital", "ID do médico requisitante", "ID do serviço requisitante", "Inf. da pré-facturação*", "Informação/justificação clínica"

Grande grupo de documentos: Saída

Documento Genérico	Lista Atributos
Documento de óbito	"Causa da morte", "Data do óbito", "ID do doente", "ID do local onde ocorreu o óbito", "ID do médico", "Indicação, especial, para inumação/cremação", "Nº do certificado "', "Informação Clínica", "Informação Circunstancial"
Doc. Transferência /Envio do doente	"Cuidados prestados", "Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) interveniente(s)", "Informação/justificação clínica"
Documento de Alta	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) médico(s)", "Orientações Propostas", "Resumo do Internamento"
Doc. Comunicação Obrigatória de Doenças	"Data(s)", "Diagnóstico(s)", "ID do doente", "ID do(s) médico(s)", "Informação Clínica"'

Grande grupo de documentos: Transversais

Documento Genérico	Lista Atributos
Processo único	"ID do doente", "Sumula dos atributos existentes no processo de internamento, no processo de consulta, no processo de hospital de dia e nos resultados dos exames"

4. Questionário

Instruções

Cada questão apresentada deve ser respondida tendo em conta um documento e a probabilidade da concretização de uma ameaça associada à sua manipulação. Deve ser, ainda, considerado:

- O normal funcionamento da UCIC;
- Que todos os documentos se encontram no espaço físico da UCIC, pelo facto de estarem associados ao internamento de um doente;
- A resposta deve ser feita segundo uma escala, crescente, de 10 pontos, onde:

Nº	Probabilidade associada
1	[0%, 10%]
2	]10%, 20%]
3	]20%, 30%]
4	]30%, 40%]
5	]40%, 50%]

Nº	Probabilidade associada
6	]50%, 60%]
7	]60%, 70%]
8	]70%, 80%]
9	]80%, 90%]
10	]90%, 100%]

- Para cada documento, coloque uma cruz no quadrado que melhor expressa a sua opinião;
- Para anular uma resposta coloque um círculo à volta da cruz (⊗) e coloque uma cruz no novo valor da probabilidade (ver exemplo);

Exemplo: P 1.X.X – Quando os documentos seguintes são consultados, qual é a probabilidade de poder haver **destruição física**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
XPTO			⊗				X					*1*	*5*	*1.2--*
	Freq.	*1*	*3*	*--*	*4-*	*--*	*--*	*--*	*4*	*--*	*3*			

Neste exemplo, o inquirido considerou que:

- para o documento XPTO a probabilidade é 6
- São ainda apresentados os seguintes dados relativos à 1ª ronda:
  - a média do valor das respostas (designada na tabela por "Média");
  - o desvio padrão (designada na tabela por Dev. P);
  - a frequência estatística de cada valor, i.e. o nº de inquiridos que escolheram determinada opção (designada por "Freq");
- qual foi a sua opção na 1ª ronda foi 1.

4.1. Questionário

4.1.1. Documentos pertencentes ao Processo de Internamento

Processo “Criar/Editar” (associado ao grupo “Processo de Internamento”)

Num episódio de internamento, a tarefa “Criar/Editar”, agrupa o conjunto de acções que a equipa médica e/ou de enfermagem realizam sobre um determinado documento, com o objectivo de registar informações inerentes ao desempenho da sua função.

Quando os documentos seguintes são criados/editados com novos registos, qual é a probabilidade de poder haver **remoção física**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a11_1) Registo Médico														
	Freq.													
(a11_2) Registo Enfermagem														
	Freq.													

Quando os documentos seguintes são criados/editados, qual é a probabilidade de poder haver **destruição física**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a12_1) Registo Médico														
	Freq.													
(a12_2) Registo Enfermagem														
	Freq.													

Quando os documentos seguintes são criados/editados, qual é a probabilidade de poder haver **alteração**, de parte ou da totalidade, do informação já registada?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a13_1) Registo Médico														
	Freq.													
(a13_2) Registo Enfermagem														
	Freq.													

Quando os documentos seguintes são criados/editados, qual é a probabilidade de poder haver **intercepção**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a14_1) Registo Médico														
	Freq.													
(a14_2) Registo Enfermagem														
	Freq.													

Quando os documentos seguintes são criados/editados, qual é a probabilidade de poder haver **falsa identificação (por omissão ou por usurpação)** de quem efectua o registo da informação?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a15_1) Registo Médico														
	Freq.													
(a15_2) Registo Enfermagem														
	Freq.													

Processo "Consultar" (associado ao grupo "Processo de Internamento")

Num episódio de internamento a tarefa "Consultar", agrupa o conjunto de acções que a equipa médica e/ou de enfermagem realizam sobre um determinado documento, com o objectivo de obter a informação necessária para o desempenho da sua função.

Quando os documentos seguintes são consultados, qual é a probabilidade de poder haver **remoção física**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a21_1) Registo Médico														
	Freq.													
(a21_2) Registo Enfermagem														
	Freq.													
(a21_3) Resultado de exames														
	Freq.													
(a21_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a21_5) Relatório Sist Monitorização														
	Freq.													

Quando os documentos seguintes são consultados, qual é a probabilidade de poder haver **destruição física**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a22_1) Registo Médico														
	Freq.													
(a22_2) Registo Enfermagem														
	Freq.													
(a22_3) Resultado de exames														
	Freq.													
(a22_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a22_5) Relatório Sist Monitorização														
	Freq.													

Quando os documentos seguintes são consultados, qual é a probabilidade de poder haver **alteração**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a23_1) Registo Médico														
	Freq.													
(a23_2) Registo Enfermagem														
	Freq.													
(a23_3) Resultado de exames														
	Freq.													
(a23_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a23_5) Relatório Sist Monitorização														
	Freq.													

Quando os documentos seguintes são consultados, qual é a probabilidade de poder haver **intercepção**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a24_1) Registo Médico														
	Freq.													
(a24_2) Registo Enfermagem														
	Freq.													
(a24_3) Resultado de exames														
	Freq.													
(a24_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a24_5) Relatório Sist Monitorização														
	Freq.													

Processo “Comunicação” (associado ao grupo “Processo de Internamento”)

A tarefa “Comunicação”, agrupa o conjunto de acções que o secretariado clínico realiza de forma a enviar os documentos, inerentes a um episódio de internamento, para o Arquivo Clínico.

Quando o documento seguinte é enviado para o arquivo clínico, qual é a probabilidade de poder haver **remoção física**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a31_A) Processo de Internamento														
	Freq.													

Quando o documento seguinte é enviado para o arquivo clínico, qual é a probabilidade de poder haver **destruição física**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a31_A) Processo de Internamento														
	Freq.													

Quando o documento seguinte é enviado para o arquivo clínico, qual é a probabilidade de poder haver **alteração**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a31_A) Processo de Internamento														
	Freq.													

Quando o documento seguinte é <u>enviado para o arquivo clínico</u>, qual é a probabilidade de poder haver **intercepção**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a31_A) Processo de Internamento														
	Freq.													

Armazenamento

O armazenamento é o local e a forma onde os documentos são guardados, <u>no espaço físico da UCIC, enquanto o doente se encontra internado.</u>

Qual é a probabilidade, <u>de um elemento da equipa da UCIC (médico, enfermeiro, auxiliar, administrativo, ...)</u> poder **remover fisicamente**, a parte ou à totalidade, dos seguintes documentos, quando estes se encontram no local de armazenamento?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a41_1) Registo Médico														
	Freq.													
(a41_2) Registo Enfermagem														
	Freq.													
(a41_3) Resultado de exames														
	Freq.													
(a41_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a41_5) Relatório Sist Monitorização														
	Freq.													

Qual é a probabilidade, de um elemento da equipa da UCIC (médico, enfermeiro, auxiliar, administrativo, ...) poder **destruir fisicamente**, a parte ou à totalidade, dos seguintes documentos, quando estes se encontram no local de armazenamento?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a42_1) Registo Médico														
	Freq													
(a42_2) Registo Enfermagem														
	Freq													
(a42_3) Resultado de exames														
	Freq													
(a42_6) Fotocópia ocorrência no S.U.														
	Freq													
(a42_5) Relatório Sist Monitorização														
	Freq													

Qual é a probabilidade, de um elemento da equipa da UCIC (médico, enfermeiro, auxiliar, administrativo, ...) poder **alterar**, parte ou à totalidade, da informação já introduzida nos seguintes documentos, quando estes se encontram no local de armazenamento?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a43_1) Registo Médico														
	Freq.													
(a43_2) Registo Enfermagem														
	Freq.													
(a43_3) Resultado de exames														
	Freq.													
(a43_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a43_5) Relatório Sist Monitorização														
	Freq.													

Qual é a probabilidade, de um elemento da equipa da UCIC (médico, enfermeiro, auxiliar, administrativo, ...) poder **interceptar** parte ou à totalidade, da informação já introduzida nos seguintes documentos, quando estes se encontram no local de armazenamento?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a44_1) Registo Médico														
	Freq.													
(a44_2) Registo Enfermagem														
	Freq.													
(a44_3) Resultado de exames														
	Freq.													
(a44_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a44_5) Relatório Sist Monitorização														
	Freq.													

Qual é a probabilidade, de um elemento **externo** à equipa da UCIC poder **remover fisicamente**, a parte ou à totalidade, dos seguintes documentos, quando estes se encontram no local de armazenamento?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a45_1) Registo Médico														
	Freq.													
(a45_2) Registo Enfermagem														
	Freq.													
(a45_3) Resultado de exames														
	Freq.													
(a45_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a45_5) Relatório Sist Monitorização														
	Freq.													

Qual é a probabilidade, de um elemento **externo** à equipa da UCIC poder **destruir fisicamente**' a parte ou à totalidade, dos seguintes documentos, quando estes se encontram no local de armazenamento?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a46_1) Registo Médico														
	Freq.													
(a46_2) Registo Enfermagem														
	Freq.													
(a46_3) Resultado de exames														
	Freq.													
(a46_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a46_5) Relatório Sist Monitorização														
	Freq.													

Qual é a probabilidade, de um elemento **externo** à equipa da UCIC poder **alterar**' parte ou à totalidade, da informação já introduzida nos seguintes documentos, quando estes se encontram no local de armazenamento?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a47_1) Registo Médico														
	Freq.													
(a47_2) Registo Enfermagem														
	Freq.													
(a47_3) Resultado de exames														
	Freq.													
(a47_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a47_5) Relatório Sist Monitorização														
	Freq.													

Qual é a probabilidade, de um elemento **externo** à equipa da UCIC poder **interceptar** parte ou à totalidade, da informação já introduzida nos seguintes documentos, quando estes se encontram no local de armazenamento?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a48_1) Registo Médico														
	Freq.													
(a48_2) Registo Enfermagem														
	Freq.													
(a48_3) Resultado de exames														
	Freq.													
(a48_6) Fotocópia ocorrência no S.U.														
	Freq.													
(a48_5) Relatório Sist Monitorização														
	Freq.													

Processo "Organizar" (associado ao grupo "Processo de Internamento")

Num episódio de internamento, a tarefa "Organizar", agrupa o conjunto de acções que o secretariado clínico realiza de forma a organizar fisicamente um determinado documento.

Quando o documento seguinte é organizado, qual é a probabilidade de poder haver **remoção física**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										**Resultados da 1ª ronda**		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a51_A) Processo de Internamento														
	Freq.													

Quando o documento seguinte é organizado, qual é a probabilidade de poder haver **destruição física**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a52_A) Processo de Internamento														
	Freq.													

Quando o documento seguinte é organizado, qual é a probabilidade de poder haver **alteração**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a53_A) Processo de Internamento														
	Freq.													

Quando o documento seguinte é organizado, qual é a probabilidade de poder haver **intercepção**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(a54_A) Processo de Internamento														
	Freq.													

4.1.2. Documentos pertencentes ao Sistemas Automáticos de Apoio Clínico

Não existem perguntas para este grupo

4.1.3. Documentos pertencentes ao Grande Grupo C - Pedidos e Grande Grupo D – Saída

C1 / D.1 - Processo "Criar/Editar" (associado aos grupos "Pedidos" e "Saída")

Num episódio de internamento, a tarefa "Criar/Editar" agrupa o conjunto de acções que a equipa médica e/ou de enfermagem realizam sobre um determinado documento, com o objectivo de aí registar informação pertinente.

C.1.1 / D.1.1 - Quando os documentos seguinte são criados/editados, qual é a probabilidade de poder haver **remoção física**, de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c11_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c11_8) Pedido de Hemoderivados														
		Freq.													
	(c11_9) Pedido de consulta Interna														
		Freq.													
	(c11_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c11_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d11_12)* Documento de óbito														
		Freq.													
	(d11_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d11_14) Documento de Alta														
		Freq.													
	(d11_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.1.2/ D.1.2 - Quando os documentos seguinte são criados/editados, qual é a probabilidade de poder haver **destruição física**, de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c12_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c12_8) Pedido de Hemoderivados														
		Freq.													
	(c12_9) Pedido de consulta Interna														
		Freq.													
	(c12_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c12_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d12_12)* Documento de óbito														
		Freq.													
	(d12_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d12_14) Documento de Alta														
		Freq.													
	(d12_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.1.3 / D.1.3 - Quando os documentos seguinte são criados/editados, qual é a probabilidade de poder haver **alteração**, de parte ou da totalidade, da informação já registada?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c13_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c13_8) Pedido de Hemoderivados														
		Freq.													
	(c13_9) Pedido de consulta Interna														
		Freq.													
	(c13_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c13_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d13_12)* Documento de óbito														
		Freq.													
	(d13_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d13_14) Documento de Alta														
		Freq.													
	(d13_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.1.4 / D.1.4 - Quando os documentos seguinte são criados/editados, qual é a probabilidade de poder haver **intercepção** de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c14_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c14_8) Pedido de Hemoderivados														
		Freq.													
	(c14_9) Pedido de consulta Interna														
		Freq.													
	(c14_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c14_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d14_12)* Documento de óbito														
		Freq.													
	(d14_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d14_14) Documento de Alta														
		Freq.													
	(d14_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.1.5 / D.1.5 - Quando os documentos seguintes são criados/editados, qual é a probabilidade de poder haver **falsa identificação (por omissão ou por usurpação)** do autor?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c15_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c15_8) Pedido de Hemoderivados														
		Freq.													
	(c15_9) Pedido de consulta Interna														
		Freq.													
	(c15_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c15_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d15_12)* Documento de óbito														
		Freq.													
	(d15_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d15_14) Documento de Alta														
		Freq.													
	(d15_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.2/ D.2 - Processo "Consultar" (associado aos grupos "Pedidos" e "Saída")

Num episódio de internamento a tarefa "Consultar", agrupa o conjunto de acções que a equipa médica e/ou de enfermagem realizam sobre um determinado documento, com o objectivo de obter a informação necessária para o desempenho da sua função.

C.2.1/ D.2.1 - Quando os documentos seguintes são consultados, qual é a probabilidade de poder haver **remoção física** de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c21_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c21_8) Pedido de Hemoderivados														
		Freq.													
	(c21_9) Pedido de consulta Interna														
		Freq.													
	(c21_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c21_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d21_12)* Documento de óbito														
		Freq.													
	(d21_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d21_14) Documento de Alta														
		Freq.													
	(d21_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.2.2/ D.2.2 - Qual é a probabilidade, de quando os documentos seguintes são consultados, poder haver **destruição física** de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c22_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c22_8) Pedido de Hemoderivados														
		Freq.													
	(c22_9) Pedido de consulta Interna														
		Freq.													
	(c22_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c22_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d22_12)* Documento de óbito														
		Freq.													
	(d22_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d22_14) Documento de Alta														
		Freq.													
	(d22_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.2.3/ D.2.3 - Quando os documentos seguintes são consultados, qual é a probabilidade de poder haver **alteração** de parte ou da totalidade, do seu conteúdo?

GG	Documentos		Probabilidade										Resultados da 1ª ronda		
			1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c23_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c23_8) Pedido de Hemoderivados														
		Freq.													
	(c23_9) Pedido de consulta Interna														
		Freq.													
	(c23_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c23_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d23_12)* Documento de óbito														
		Freq.													
	(d23_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d23_14) Documento de Alta														
		Freq.													
	(d23_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.2.4 / D.2.4 - Quando os documentos seguintes são consultados, qual é a probabilidade de poder haver **intercepção** de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c24_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c24_8) Pedido de Hemoderivados														
		Freq.													
	(c24_9) Pedido de consulta Interna														
		Freq.													
	(c24_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c24_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d24_12)* Documento de óbito														
		Freq.													
	(d24_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d24_14) Documento de Alta														
		Freq.													
	(d24_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

Processo "Comunicação" (associado aos grupos "Pedidos" e "Saída")

A tarefa "Comunicação" agrupa o conjunto de acções realizas de forma a enviar cada documento para o respectivo destino.

C.3.1 / D.3.1 - Quando os documentos seguintes são enviados para o, respectivo, destino, qual é a probabilidade de poder haver **remoção física** de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c31_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c31_8) Pedido de Hemoderivados														
		Freq.													
	(c31_9) Pedido de consulta Interna														
		Freq.													
	(c31_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c31_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d31_12)* Documento de óbito														
		Freq.													
	(d31_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d31_14) Documento de Alta														
		Freq.													
	(d31_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.3.2 / D.3.2 - Quando os documentos seguintes são <u>enviados</u> para o, respectivo, destino, qual é a probabilidade de poder haver **destruição física** de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c32_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c32_8) Pedido de Hemoderivados														
		Freq.													
	(c32_9) Pedido de consulta Interna														
		Freq.													
	(c32_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c32_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d32_12)* Documento de óbito														
		Freq.													
	(d32_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d32_14) Documento de Alta														
		Freq.													
	(d32_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.3.3/ D.3.3 - Quando os documentos seguintes são enviados para o, respectivo, destino, qual é a probabilidade de poder haver **alteração** de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
GG	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c33_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c33_8) Pedido de Hemoderivados														
		Freq.													
	(c33_9) Pedido de consulta Interna														
		Freq.													
	(c33_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c33_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d33_12)* Documento de óbito														
		Freq.													
	(d33_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d33_14) Documento de Alta														
		Freq.													
	(d33_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

C.3.4 / D.3.4 - Quando os documentos seguintes são <u>enviados</u> para o, respectivo, destino, poder haver **intercepção** de parte ou da totalidade, do seu conteúdo?

			Probabilidade										**Resultados da 1ª ronda**		
G G	**Documentos**		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
Pedidos	*(c34_7)* Pedido de MCDT realizados no hospital														
		Freq.													
	(c34_8) Pedido de Hemoderivados														
		Freq.													
	(c34_9) Pedido de consulta Interna														
		Freq.													
	(c34_10) Pedido de receituário de Med. Extra-Formulário														
		Freq.													
	(c34_11) Pedido de Exames ao Exterior														
		Freq.													
Saída	*(d34_12)* Documento de óbito														
		Freq.													
	(d34_13) Documento de Transferência/Envio do doente														
		Freq.													
	(d34_14) Documento de Alta														
		Freq.													
	(d34_17) Doc. para a Comunicação Obrigatória de Doenças														
		Freq.													

4.1.4. Documentos Transversais

Processo "Consultar" (associado ao grupo "Transversais")

Num episódio de internamento a tarefa "Consultar", agrupa o conjunto de acções que a equipa médica e/ou de enfermagem realizam sobre um determinado documento, com o objectivo de obter a informação necessária para o desempenho da sua função.

Quando o documento seguinte é consultado, qual é a probabilidade de poder haver **remoção física** de parte ou da totalidade, do seu conteúdo?

		Probabilidade										Resultados da 1ª ronda		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e11_16) Processo único														
	Freq.													

Quando o documento seguinte é consultado, qual é a probabilidade de poder haver **destruição física,** de parte ou da totalidade, do seu conteúdo?

		Probabilidade										Resultados da 1ª ronda		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e12_16) Processo único														
	Freq.													

Quando os documento seguinte é consultado, qual é a probabilidade de poder haver **alteração**, de parte ou da totalidade, do seu conteúdo?

		Probabilidade										Resultados da 1ª ronda		
Documentos		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e13_16) Processo único														
	Freq.													

Quando o documento seguinte é <u>consultado</u>, qual é a probabilidade de poder haver **intercepção**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e14_16) Processo único														
	Freq.													

<u>Processo "Comunicação" (associado ao grupo "Transversais")</u>

A tarefa "Comunicação" agrupa o conjunto de acções que a o secretariado clínico realiza de forma a transferir do Arquivo Clínico para a UCIC e vice-versa, o "Processo único" do doente, durante um episódio de internamento.

Quando o documento seguinte é <u>enviado para o arquivo clínico,</u> qual é a probabilidade de poder haver **remoção física**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e21_16) Processo único														
	Freq.													

Quando o documento seguinte é <u>enviado para o arquivo clínico</u>, qual é a probabilidade de poder haver **destruição física**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e22_16) Processo único														
	Freq.													

Quando o documento seguinte é enviado para o arquivo clínico, qual é a probabilidade de poder haver **alteração**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e23_16) Processo único														
	Freq.													

Quando o documento seguinte é enviado para o arquivo clínico, qual é a probabilidade de poder haver **intercepção**, de parte ou da totalidade, do seu conteúdo?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e24_16) Processo único														
	Freq.													

Armazenamento

O armazenamento é o local e a forma onde os documentos são guardados, no espaço físico da UCIC, enquanto o doente se encontra internado.

Qual é a probabilidade, de um elemento da equipa da UCIC (médico, enfermeiro, auxiliar, administrativo, ...) poder **remover fisicamente**' a parte ou à totalidade, dos seguintes documentos, quando estes se encontram no local de armazenamento?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e31_16) Processo único														
	Freq.													

Qual é a probabilidade, de um elemento da equipa da UCIC (médico, enfermeiro, auxiliar, administrativo, ...) poder **destruir fisicamente**, a parte ou à totalidade, dos seguintes documentos, quando estes se encontram no local de armazenamento?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e32_16) Processo único														
	Freq.													

Qual é a probabilidade, de um elemento da equipa da UCIC (médico, enfermeiro, auxiliar, administrativo, ...) poder **alterar**, parte ou à totalidade, da informação já introduzida nos seguintes documentos, quando estes se encontram no local de armazenamento?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e33_16) Processo único														
	Freq.													

Qual é a probabilidade, de um elemento da equipa da UCIC (médico, enfermeiro, auxiliar, administrativo, ...) poder **interceptar**, parte ou à totalidade, da informação já introduzida nos seguintes documentos, quando estes se encontram no local de armazenamento?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e34_16) Processo único														
	Freq.													

Qual é a probabilidade, de um elemento **externo** à equipa da UCIC poder **remover fisicamente**' a parte ou à totalidade, dos seguintes documentos, quando estes se encontram no local de armazenamento?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e35_16) Processo único														
	Freq.													

Qual é a probabilidade, de um elemento **externo** à equipa da UCIC poder **destruir fisicamente**' a parte ou à totalidade, dos seguintes documentos, quando estes se encontram no local de armazenamento?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e36_16) Processo único														
	Freq.													

Qual é a probabilidade, de um elemento **externo** à equipa da UCIC poder **alterar**' parte ou à totalidade, da informação já introduzida nos seguintes documentos, quando estes se encontram no local de armazenamento?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e37_16) Processo único														
	Freq.													

Qual é a probabilidade, de um elemento **externo** à equipa da UCIC poder **interceptar**' parte ou à totalidade, da informação já introduzida nos seguintes documentos, quando estes se encontram no local de armazenamento?

Documentos		Probabilidade										Resultados da 1ª ronda		
		1	2	3	4	5	6	7	8	9	10	A sua opção	Média	Desv. P
(e38_16) Processo único														
	Freq.													

OBS:

FIM do Questionário